UNIDAD ADMINISTRATIVA ESPECIAL
DIRECCIÓN DE IMPUESTOS Y ADUANAS NACIONALES
UAE-DIAN

MODELO DE REQUISITOS PARA LA GESTIÓN DE DOCUMENTOS ELECTRÓNICOS

COORDINACIÓN DE DOCUMENTACIÓN

Febrero de 2025

Historia de Revisiones

Versión	Fecha	Descripción del Cambio
1	25/11/2013	Versión Inicial
2	11/12/2013	Versión Segunda
3	21/12/2013	Versión Final
4	28/02/2014	Versión Final Ajustada
5	21/04/2014	Versión Final Corregida
6	14/05/2014	Versión Final Cambiada
7	02/10/2024	Actualización de acuerdo con los requerimientos del SGDEA
8	18/02/2025	Actualización de acuerdo con el ajuste de requerimientos del SGDEA

Contenido

Listado de Gráficos

INTRODUCCIÓN

En el marco de la Modernización de la DIAN y de acuerdo con las necesidades de la Entidad, se hace relevante contar con herramientas que garanticen la gestión, uso y almacenamiento eficiente de la información y la documentación con el fin de garantizar su integridad, autenticidad y disponibilidad a lo largo del tiempo, acorde con las exigencias de la normatividad vigente dictada por el Archivo General de la Nación y el Ministerio de Tecnologías de la Información y las Comunicaciones, así como, las políticas institucionales.

El presente documento establece el modelo de requerimientos funcionales y no funcionales que deben cumplir los documentos electrónicos de archivo como resultado del ejercicio de análisis de la mencionada normatividad y especial, la revisión de la Guía del Archivo General de la Nación - AGN denominada “Implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo”, en adelante SGDEA, en el que se establece a modo general, la necesidad de estructurar una estrategia de integración de sistemas de gestión que facilite la aplicabilidad y control de cada una de las etapas de la gestión de documentos (creación, mantenimiento, difusión y administración).

Esta propuesta de requerimientos funcionales y no funcionales son los que debería cumplir el Sistema de Gestión de Documentos Electrónicos de Archivo de la UAE-DIAN.

1. GENERALIDADES

El Modelo de Requisitos para la Gestión de Documentos Electrónicos es un esquema teórico que se integra a la gestión documental de la UAE-DIAN y sirve de base para la administración de los documentos que produce la Entidad, mediante la estructura orgánico funcional que soporta la producción documental, integralmente relacionadas para contribuir con los objetivos de eficacia administrativa.

El Modelo es una representación abstracta del Sistema de Gestión Documental de la Entidad, enfocada en la administración integral de documentos electrónicos y físicos, que pretende ayudar a entender, explicar y mejorar la manera en que la UAE-DIAN controla la documentación que produce como reflejo del cumplimiento de sus actividades. Si bien se enfoca en los requisitos del soporte electrónico, no desagrega y, por el contrario, recomienda la integración de los materiales físicos y digitales, coexistiendo en las agrupaciones documentales formalmente constituidas en la Entidad.

1.1. DEFINICIONES

Archivo electrónico: Conjunto de documentos electrónicos producidos y tratados archivísticamente, siguiendo la estructura-orgánico funcional del productor, acumulados en un proceso natural por una persona o institución pública o privada, en el transcurso de su gestión.[1]

Autenticidad: Característica técnica que permite identificar al autor de un mensaje de datos, el cual es conservado en condiciones que permitan garantizar su integridad, para preservar la seguridad de la información que busca asegurar su validez en tiempo, forma y distribución. Así mismo, garantiza el origen de la información, validando el emisor para evitar suplantación de identidades. Que pueda demostrarse que el documento es lo que afirma ser, que ha sido creado o enviado por la persona que afirma haberlo creado o enviado, y que ha sido creado o enviado en el momento que se afirma. [2]

Cuadro de Clasificación Documental (CCD): Esquema que refleja la jerarquización dada a la documentación producida por una institución y en el que se registran las secciones y subsecciones y las series y subseries documentales. [3]

Disponibilidad: Que se puede localizar, recuperar, presentar, interpretar y leer. Su presentación debe mostrar la actividad que lo produjo. El contexto de los documentos debe ser suficientemente claro y contener la información necesaria para la comprensión de las operaciones que los crearon y usaron. Debe ser posible identificar un documento en el contexto amplio de las actividades y las funciones de la organización. Se deben mantener los vínculos existentes entre los documentos que reflejan una secuencia de actividades. Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. [4]

Disposición final de documentos: Decisión resultante de la valoración hecha en cualquier etapa del ciclo vital de los documentos, registrada en las tablas de retención y/o Tablas de Valoración Documental, con miras a su conservación total, eliminación o selección. [5]

Documento electrónico de archivo: Registro de información generada, producida o recibida o comunicada por medios electrónicos, que permanece almacenada electrónicamente durante todo su ciclo de vida, producida, por una persona o entidad en razón a sus actividades o funciones, que tiene valor administrativo, fiscal, legal, o valor científico, histórico, técnico o cultural y que debe ser tratada conforme a los principios y procesos archivísticos. [6]

---

[1] Archivo General de la Nación (2024). Acuerdo 001. Anexo 1. “Definiciones”. p.99.
[2] Ibid., p.106.
[3] Ibid., p.104.
[4] Ibid., p.106.
[5] Ibid., p.106.
[6] Ibid., p.106.

Eliminación documental: Actividad resultante de la disposición final señalada en las Tablas de Retención o de Valoración Documental para aquellos documentos que han perdido sus valores primarios. [7]

Esquema de metadatos para la gestión de documentos: Instrumento que facilita la interoperabilidad y ayuda a asegurar el mantenimiento de los documentos a largo plazo, cuyo objetivo es mostrar de manera lógica las relaciones entre los diferentes componentes del conjunto de metadatos, a través de reglas para el uso y gestión específicamente relacionadas con la semántica, la sintaxis y la obligatoriedad de los valores. [8]

Estampa 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. [9]

Evento: es un suceso en el sistema que se origina en la ejecución de una función y se asocia a una entidad del sistema. Para cada evento como mínimo se debe guardar la siguiente información: Función, fecha/hora de realización, usuario que lo realizo, descripción del evento.

Expediente: Conjunto de documentos producidos y recibidos durante el desarrollo de un mismo trámite o procedimiento, acumulados por una persona, dependencia o unidad administrativa, vinculados y relacionados entre sí y que se conservan manteniendo la integridad y orden en que fueron tramitados, desde su inicio hasta su resolución definitiva. [10]

Expediente electrónico: Conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan. El expediente electrónico deberá garantizar condiciones de autenticidad, integridad y disponibilidad. [11]

Expediente híbrido: Conjunto conformado por documentos en soportes físicos y formatos electrónicos simultáneamente que, a pesar de estar separados por ser conservados en sus formatos nativos (soportes originales), forman una sola unidad documental en razón al trámite

[7] Ibid., p.107.
[8] Ibid., p.108.
[9] Ministerio de Tecnologías de la Información y las Comunicaciones. Numeral (2018). G.INF.07 Guía para la gestión de documentos y expedientes electrónicos. p. 18.
[10] Archivo General de la Nación (2024). Acuerdo 001. Anexo 1. “Definiciones”. p.108.
[11] Ibid., p.108.

o actuación que tratan, manteniendo un vínculo archivístico, apoyado por el uso de herramientas tecnológicas. [12]

Expediente virtual: Conjunto de documentos relacionados con un mismo trámite o procedimiento administrativo, conservados en diferentes sistemas electrónicos o de información, que se pueden visualizar simulando un expediente electrónico, pero no puede ser gestionado archivísticamente, hasta que no sean unificados mediante procedimiento tecnológicos seguros. [13]

Fiabilidad: Condición técnica de un sistema de información de garantizar la integridad de los datos. Su contenido representa exactamente lo que se quiso decir en él. Es una representación completa y precisa de lo que da testimonio y se puede recurrir a él para demostrarlo. Los documentos de archivo deben ser creados en el momento o poco después en que tiene lugar la operación o actividad que reflejan, por individuos que dispongan de un conocimiento directo de los hechos o automáticamente por los instrumentos que se usen habitualmente para realizar las operaciones. [14]

Firma digital: Corresponde a un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación. Esta firma se puede verificar utilizando la clave pública correspondiente al firmante. Si la firma digital se verifica correctamente y el documento no ha sido modificado desde su firma, se puede confiar en la autenticidad e integridad del documento. [15]

Firma electrónica: Corresponde a métodos tales como códigos, contraseñas, datos biométricos o claves criptográficas privadas, que permiten identificar a una persona en relación con un mensaje, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, teniendo en cuenta todas las circunstancias del caso, así como cualquier acuerdo pertinente. [16]

Gestión Documental: Conjunto de actividades administrativas y técnicas, tendientes a la planificación, manejo y organización de la documentación producida y recibida por las entidades, desde su origen hasta su destino final con el objeto de facilitar su utilización y conservación. [17]

---

[12] Ibid., p.109.
[13] Ibid., p.109.
[14] Ibid., p.109.
[15] Ibid., p.109.
[16] Ibid., p.110.
[17] Ibid., p.111.

Historial de eventos: son los eventos que se guardan con relación a las funciones que ejecuta una entidad del sistema.

Huella/Hash de un Documento: Código que identifica de forma unívoca un documento. Mediante la función de validar huella, se puede comprobar que el hash publicado y el del fichero son el mismo, lo que permite asegurar que el fichero no ha sido modificado desde su publicación.

Índice electrónico: Documento electrónico generado por el Sistema de Gestión de Documentos Electrónicos de Archivo – SGDEA para cada expediente electrónico, con la capacidad de alimentación y actualización automática. Constituye un objeto digital donde se establecen e identifican los documentos electrónicos que componen el expediente, ordenados de manera cronológica y según la disposición de los documentos, así como otros datos con el fin de preservar la integridad y permitir la recuperación. Se ha determinado que "el foliado de los expedientes electrónicos se llevará a cabo mediante un índice electrónico, firmado digitalmente por la autoridad, órgano o entidad actuante, según proceda. Este índice garantizará la integridad del expediente electrónico y permitirá su recuperación cuando se requiera. [18]

Integridad: Característica técnica de seguridad de la información con la cual se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento asociados a la misma. Condición que garantiza que la información consignada en un mensaje de datos ha permanecido completa e inalterada. [19]

Integridad de los expedientes: Los expedientes deben ser conformados respetando los principios archivísticos, con la totalidad de los documentos que lo integran. [20]

Interdependencia de los metadatos: En el esquema de metadatos para la gestión de documentos pueden existir conjuntos de metadatos relacionados que, por razones de integridad, necesitan ser gestionados como un conjunto, por ejemplo, describir en un documento un evento específico, necesita de metadatos como fecha, actividad, agente, entre otros. Los conjuntos de metadatos identificados requieren de la definición de una secuencia lógica, creando una interdependencia entre dichos metadatos, la cual ayuda a soportar la integridad de estos. [21]

Interoperabilidad: Capacidad de las organizaciones para intercambiar información y conocimiento en el marco de sus procesos de negocio para interactuar hacia objetivos mutuamente beneficiosos, con el propósito de facilitar la entrega de servicios en línea a ciudadanos, empresas y a otras entidades, mediante el

[18] Ibid., p.111.
[19] Ibid., p.112.
[20] Ibid., p.112.
[21] Ibid., p.112.

intercambio de datos entre sus sistemas. [22]

Las entidades públicas deben 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 (computadoras, medios de comunicación, redes, software y otros componentes de tecnología de la información) de interactuar e intercambiar datos de acuerdo con un método definido, con el fin de obtener los resultados esperados[23]

Lista de control de acceso: corresponde a la lista de usuarios (roles y grupos) que pueden acceder a las entidades del sistema de información SGDEA.

Metadatos contextuales: información que describe una entidad del sistema con relación a los eventos en los que participa y las funciones realizadas. Nota: los metadatos contextuales deben ser definidos por cada área a partir de su esquema de metadatos.

Metadatos para la Gestión de Documentos: información estructurada o semi-estructurada que permite la creación, gestión y uso de los documentos a lo largo del tiempo. [24]

Migración: Proceso de mover los registros de una configuración de hardware o software a otra sin cambiar el formato. / Acción de trasladar documentos de archivo de un sistema a otro, manteniendo la autenticidad, la integridad, la fiabilidad y la disponibilidad de estos. [25]

PQRS: Sistema de Peticiones, Quejas, Reclamos y Sugerencias

Preservación a Largo Plazo: conjunto de acciones y estándares aplicados a los documentos durante su gestión para garantizar su preservación en el tiempo, independientemente de su medio y forma de registro o almacenamiento. [26]

Requisito/Requerimiento funcional: define una función del sistema de software o sus componentes. Una función es descrita como un conjunto de entradas, comportamientos y salidas. [27]

---

[22] Ministerio de Tecnologías de la Información y las Comunicaciones (2019). Marco de Interoperabilidad para el Gobierno en línea, Versión 2. p. 9.
[23] Decreto 1080 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura”
[24] Archivo General de la Nación (2017). Guía Implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo-SGDEA. p.73.
[25] Ibid., p.73.
[26] Ibid., p.74.
[27] Ibid., p.74.

Requisito/Requerimiento no funcional: es, en la ingeniería de sistemas y la ingeniería de software, un requisito que especifica criterios que pueden usarse para juzgar la operación de un sistema en lugar de sus comportamientos específicos. [28]

Retención documental: Plazo que los documentos deben permanecer en el archivo de gestión o en el archivo central, tal como se consigna en la tabla de retención documental. [29]

Serie documental: Documentos organizados de acuerdo con un sistema de archivo o conservados formando una unidad como resultado de la acumulación del mismo proceso archivístico, o de la misma actividad; que tienen una forma particular, o como consecuencia de cualquier actividad derivada de su producción, recepción o utilización. [30]

Servicio: Corresponde a un subconjunto de funcionalidades orientadas a gestionar las entidades del sistema con respecto a los requisitos funcionales establecidos.

SGDEA: Sistema de información que integra todos los documentos identificados como documentos electrónicos de archivo, además de centralizar todas las actividades inherentes a la gestión documental, asegurando su autenticidad, integridad, inalterabilidad, fiabilidad, disponibilidad, conservación, preservación a largo plazo, seguridad y almacenamiento, entre otros criterios de referencia para su implementación y seguimiento.[31]

Subserie documental: Conjunto de unidades documentales que forman parte de una serie, identificadas de forma separada de ésta por su contenido y sus características específicas. [32]

Usuario: Entidad del sistema que representa una persona o sistema, al cual se le asigna un rol y/o grupo de usuario para otorgar permisos de acceso y asignación de funciones.

TRD: Tablas de retención documental. Listado de series y subseries, con sus correspondientes tipos documentales, a las cuales se asigna el tiempo de permanencia en cada etapa del ciclo vital de los documentos, así como una disposición final. [33]

Transferencia Documental: Proceso técnico, administrativo y legal mediante el cual se entrega a los archivos centrales (transferencia primaria) o a los archivos históricos (transferencia secundaria), los documentos que de conformidad con las Tablas de Retención Documental y valoración, han cumplido su tiempo de retención en la etapa de archivo de gestión o de archivo central respectivamente; implica un cambio en el responsable de la tenencia y administración de

[28] Ibid., p.74.
[29] Archivo General de la Nación (2024). Acuerdo 001. Anexo 1. “Definiciones”. p.117.
[30] Ibid., p.118.
[31] Ibid., p.118.
[32] Ibid., p.119.
[33] Ibid., p.119.

los documentos de archivo que supone obligaciones del receptor de la transferencia, quien asume la responsabilidad integral sobre los documentos transferidos. [34]

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 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 las entidades deberán 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.[35]

Trazabilidad: creación, incorporación y conservación de información sobre el movimiento y el uso de documentos de archivo. [36]

Unidad documental: Unidad archivística constituida por documentos del mismo tipo formando unidades simples o por documentos de diferentes tipos formando una unidad documental compleja (expediente). [37]

Ventanilla única: Es el sitio, sede o canal, donde se realiza la totalidad de la actuación administrativa, presencial o virtual, para la recepción de documentos, solicitudes y atender requerimientos de los ciudadanos, usuarios o grupos de valor. [38]

Vinculo Archivístico: Los documentos resultantes de un mismo trámite deben mantener el vínculo entre sí, mediante la implementación de sistemas de clasificación, sistemas descriptivos y metadatos de contexto, estructura y contenido, de forma que se facilite su gestión como conjunto. [39]

[34] Ibid., p.120.
[35] Ministerio de Tecnologías de la Información y las Comunicaciones. Numeral (2018). G.INF.07 Guía para la gestión de documentos y expedientes electrónicos. p. 126.
[36] Archivo General de la Nación (2017). Guía Implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo-SGDEA. p.75.
[37] Archivo General de la Nación (2024). Acuerdo 001. Anexo 1. “Definiciones”. p.120.
[38] Ibid., p.121.
[39] Ibid., p.122.

1.2. MARCO NORMATIVO

Para la construcción del Modelo se tuvieron en cuenta normatividad relevante según se relaciona:

- Ley 594 de 2000: “Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones”.
- Ley 962 de 2005: “Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos”.
- Ley 1437 de 2011: “Por medio de la cual se expide el código contencioso administrativo, en su capítulo IV establece la utilización de medios electrónicos en el procedimiento administrativo”.
- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”
- 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”.
- Circular 002 de 2012 AGN: Establece lineamientos en materia de adquisición de herramientas tecnológicas de gestión documental.
- Circular 05 de septiembre de 2012: Se establecen recomendaciones para llevar a cabo procesos de digitalización y comunicaciones oficiales electrónicas.
- Decreto 1080 de 2015: “Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura”.
- 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”.

La metodología aplicada para la definición del Modelo sigue los principios marcados por las siguientes especificaciones técnicas:

- ISO 15489. Diseño de Sistemas de Gestión de Documentos físicos y electrónicos.
- ISO 14721. Diseño de sistemas de gestión de documentos electrónicos de conservación a largo plazo.
- Moreq. Modelo de requisitos para la gestión de documentos electrónicos de Archivo.
- Normas de descripción Archivísticas ISAD (G) e ISAAR (CPF).
- ISO 19005. Formato de documento de archivo para preservación a largo plazo.
- ISO 27000. Seguridad de la Información.
- ISO 30300. Sistemas de Gestión para los Documentos

Adicionalmente, se consultaron las Guías Técnicas elaboradas por el Archivo General de la Nación y el Ministerio de Tecnologías de la Información y las Comunicaciones:

- Guía de Implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo realizada por el Archivo General de la Nación (AGN)
- Guía Pautas para la Utilización de la Digitalización realizada por el Archivo General de la Nación (AGN).
- Guía Técnica Gestión de Documentos y Expedientes Electrónicos elaborada por el Ministerio de Tecnologías de la Información y las Comunicaciones y el Archivo General de la Nación.

1.3. ÁMBITO DE APLICACIÓN Y ALCANCE DEL MODELO

El Modelo incide en el control sistemático de la documentación, desde su producción hasta la disposición final, a través de ciclo de vida documental, con aplicación de principios, postulados técnicos, ejercicios de mejores prácticas y normas que regulan la actividad de la UAE-DIAN.

El Modelo puede ser aplicado como alcance de gestión para la totalidad de los materiales documentales que conforman el acervo archivístico de la UAE-DIAN, y que se instrumentan a través de técnicas procedimentales de gestión documental descritas a lo largo de los contenidos de información presentes en el documento.

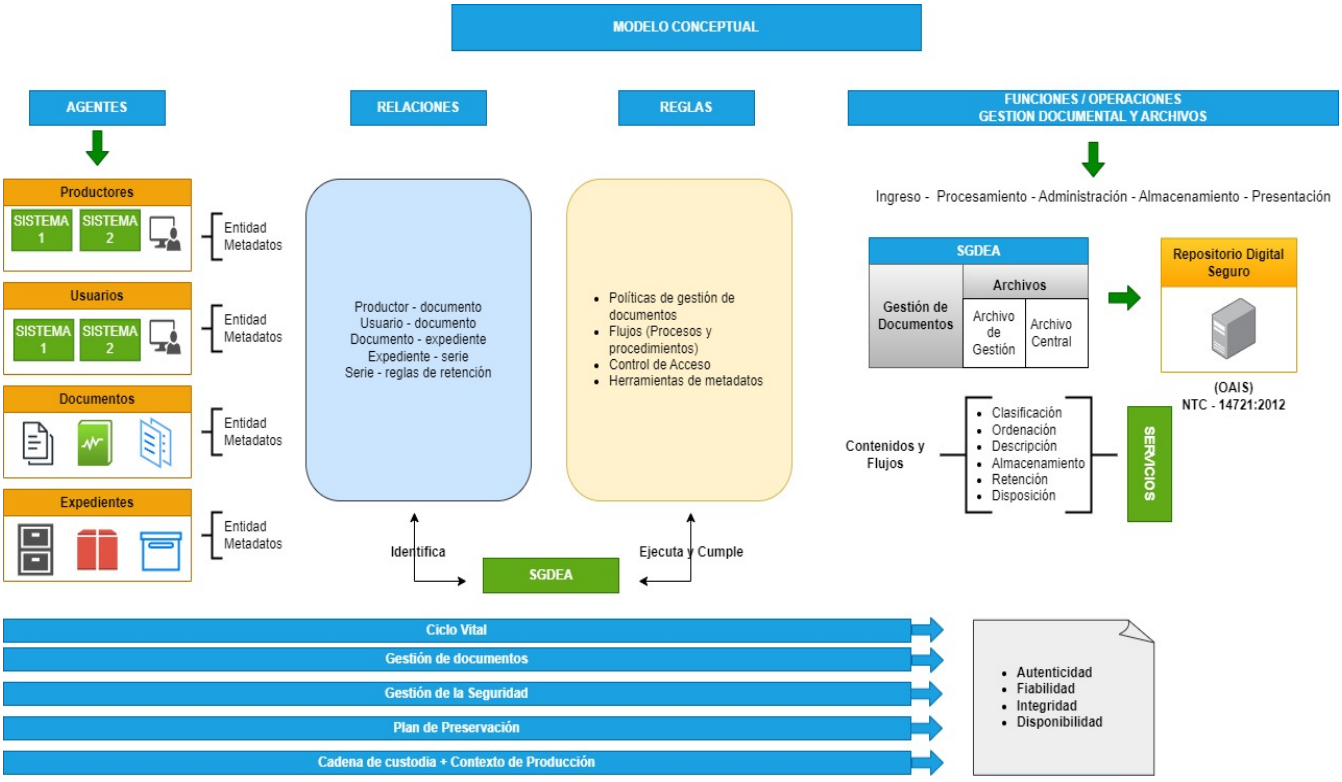
El Modelo fija su atención en la documentación que se produce en ejercicio de facultades competentes (funciones) y en cuya naturaleza de conformación los documentos han "nacido digitales" o han sido digitalizados como parte del desarrollo de las actividades. El Modelo se limita de forma explícita a los documentos formales de la UAE-DIAN, sujetos a normas y ordenamiento jurídico, conjugando la coexistencia y administración de documentos físicos y electrónicos de las mismas características.

El Modelo NO recomienda ni establece criterios de software o hardware específicos.

1.3.1. Modelo Conceptual

Para la implementación de SGDEA es fundamental tener claridad del proceso de gestión documental institucional: como se producen los documentos, cuales, en que formatos, sus flujos, quienes son los usuarios, si estos son internos y/o externos, tiempos de retención, etapas de archivo, entre otros, aspectos que se describen en los diferentes instrumentos archivísticos; con esta información consolidada se pueden empezar a denominar o identificar estos elementos y concebir un *modelo conceptual* como el que se presenta a continuación, donde se pueden identificar, por ejemplo: un *Usuario* dentro de un sistema informático, un *Agente*, el cual es una entidad descrita a partir de *Metadatos*, como un lenguaje entendible para un sistema de información, igualmente, las *Reglas* predeterminadas para que entre agentes haya una *Relación* técnica como por ejemplo las políticas de acceso y consulta y en el sistema informático se denominan *Eventos*.

A continuación, se presenta el modelo conceptual definido para la UAE-DIAN



Gráfica 1. Modelo Conceptual de un SGDEA
Fuente: Elaboración Propia

2. MODELO DE REQUISITOS PARA LA GESTIÓN DE DOCUMENTOS ELECTRÓNICOS

Un Modelo es un marco de referencia para la administración de una Entidad o sistema. Un Modelo de Requisitos para la Gestión de Documentos Electrónicos es visualizado como el esquema teórico que define las características de comportamiento y funcionalidad de los documentos en la DIAN, con el fin de lograr su administración integral desde la producción hasta la disposición final, con control de actividades y registro de responsabilidades a través del ciclo de vida documental.

La finalidad del Modelo de Requisitos para la Gestión de Documentos Electrónicos se enfoca en el cumplimiento de las siguientes acciones:

- Controlar la producción;
- Administrar la creación de documentos;
- Definir los canales de comunicación;
- Distribuir y tramitar los documentos;
- Conformar agrupaciones documentales por trámites corporativos;
- Organizar los documentos de acuerdo con procedimientos preestablecidos,
- Aplicar reglas de archivo para valoración, retención y disposición final, y
- Preservar por el tiempo requerido

2.1. ELEMENTOS CONSTITUTIVOS DEL MODELO

2.1.1. Funciones

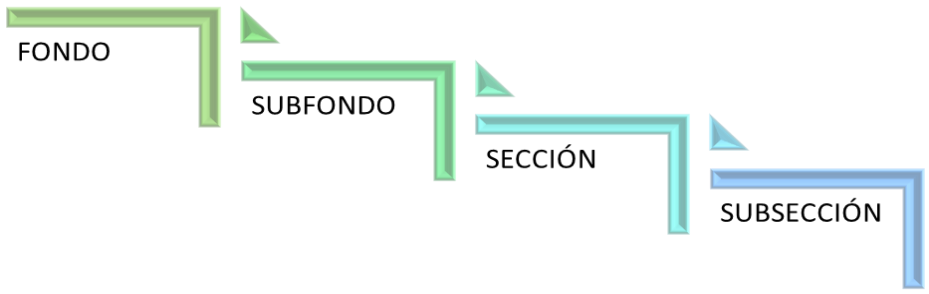
Son el conjunto de actividades que cumple la Entidad como misión corporativa y constituyen el propósito de existencia de la DIAN. Jerárquicamente presenta subdivisiones relacionadas y asociadas orgánicamente para desarrollar los objetos y competencias de la Entidad. Las Funciones representan el mayor de los niveles o "clases" para ser representados en el Modelo de Requisitos para la Gestión de Documentos Electrónicos.

2.1.2. Procesos Corporativos

Son los mecanismos de procedimiento y actividad secuencial que utiliza la DIAN, para cumplir y desarrollar las Funciones que le corresponden. Las agrupaciones existentes en el esquema procedimental (Misionales, Estratégicos, Apoyo y Control), definen en el Modelo la forma y constitución de los expedientes y volúmenes documentales.

2.1.3. Estructura Orgánica

Es la representación gráfica o narrativa de las áreas y dependencias establecidas en la DIAN, para el desarrollo de sus funciones, asignando competencias en cada uno de los niveles correspondientes. La estructura orgánica será representada en lenguaje archivístico, con los niveles correspondientes, bajo la siguiente jerarquía:



- **Fondo:** corresponde al nombre de la entidad 'Unidad Administrativa Especial Dirección de Impuestos y Aduanas Nacionales'.
- **Subfondo:** corresponde al nombre de la dirección seccional o nivel central, en la cual se están produciendo las unidades documentales.
- **Sección:** corresponde a la dependencia superior jerárquica.
- **Subsección:** corresponde a la dependencia que produce la unidad documental.

2.1.4. Agrupaciones Documentales

Conjuntos homogéneos de información documental de un mismo proceso o procedimiento, en responsabilidad de un nivel de la Estructura Orgánica. Las Agrupaciones documentales, en concordancia con legislación nacional y la tradición archivística, serán denominadas Series o Subseries Documentales.

2.1.5. Unidades Documentales Complejas

Se denominan también Expedientes y reflejan la reunión ordenada y sistemática de un conjunto de documentos que se agrupan por "caso", trámite, actuación o procedimiento y con subordinación a una Serie o Subserie. El expediente evidencia el trámite documental que ha surtido un caso particular, desarrollado de acuerdo con las reglas del procedimiento definido, que se ejecuta para cumplir una función determinada, por el área competente. Como unidad archivística integral, el Expediente goza de identificación unívoca y trámites y flujos particulares, en relación directa con el proceso/procedimiento que lo comanda. En el entorno electrónico los expedientes deben soportar la integración o representación de documentos en diversos soportes y controlar el ingreso de las agrupaciones simples (tipos documentales) de conformidad con reglas y requisitos pre configurados. Los expedientes electrónicos almacenan un alto porcentaje de tipos documentales electrónicos, pero deben estar habilitados para representar los contenidos físicos o análogos que requieran ser integrados a la Unidad Documental Compuesta. Los Expedientes están constituidos de manera exclusiva por "Documentos de Archivo".

2.1.6. Unidad Documental Simple

La Unidad Documental Simple es un conjunto de documentos de iguales características, producidos de manera periódica y secuencial numérica o cronológica. Ejemplo: actas, decretos, resoluciones, circulares, acuerdos. Unidad archivística constituida por documentos del mismo tipo[40].

2.1.7. De Documento a Documento de Archivo

Mientras "Documento" se define como la *información registrada, cualquiera que sea su forma o el medio utilizado*[41], el "Documento de Archivo" es *Registro de información producida o recibida por una persona o entidad pública o privada en razón a sus actividades o funciones, que tiene valor administrativo, fiscal, legal, científico, histórico, técnico o cultural y debe ser objeto de conservación en el tiempo, con fines de consulta posterior*[42]. Los documentos que nacen internamente en la UAE-DIAN deben ser considerados primero como "Documento" y solo hasta

[40] Ibid., p.120.
[41] Ibid., p.106.
[42] Ibid., p.106.

cumplir un protocolo o trámite, podrán eventualmente llegar a convertirse en “Documentos de Archivo”.

Un “Documento de Archivo” se caracteriza, entonces, porque en él se pueden evidenciar el contenido (información del mensaje), el contexto (información sobre la competencia funcional en virtud de la cual se ha producido), la estructura (forma en que se registra el documento) y la presentación (que, ligada al contenido y a la estructura, permite la interpretación o legibilidad del documento).

El Modelo de Requisitos para la Gestión de Documentos Electrónicos se diseña y estructura con la vinculación tanto de “documentos”, como de “documentos de archivo”, y establece que solo sobre estos últimos (las evidencias o Récords) aplicarán las reglas documentales de integración al expediente y consecuente valoración y disposición final.

2.1.8. Características Del Documento Electrónico de Archivo

Todos los servicios informáticos creados a partir de la Modernización Tecnológica deben garantizar las características del Documento Electrónico de Archivo, incluyendo los metadatos relacionados en la Tablas 2, adaptada de la Guía Técnica G.INF.07 Guía para la gestión de documentos y expedientes electrónicos:

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.

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.

Integridad
Entendida como la cualidad de un documento 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.

Disponibilidad

Entendida en un documento electrónico, 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.

Características del documento	Descripción	Mecanismos de Protección y Seguridad	Metadatos mínimos que deben contemplares para tener evidencia de dicha característica
Autenticidad	Que puede demostrar, que es lo que afirma ser, que ha sido creado o enviado por la persona que afirma haberlo creado o enviado, y que ha sido creado o enviado en el tiempo que se ha afirmado.	Utilizar los mecanismos de firma digital/electrónica, protección y seguridad autorizados por la Entidad.	• Codigo_proceso • Nombre_proceso • Codigo_procedimiento • Nombre_procedimiento • Codigo_subfondo • Nombre_subfondo • Codigo_seccion • Nombre_seccion • Codigo_subseccion • Nombre_subseccion • Codigo_serie • Nombre_serie • Codigo_suberie • Nombre_subserie • Numero_expediente •Id_unico_unidad_documental (expediente) • Titulo_exp • Fecha_apertura • Fecha_cierre • Palabras_clave_expediente • Estado • Id_unico_documento • Nombre_documento • Tipología_documental • Asunto_y/o_descripcion • Fecha_creación • Fecha_transmisión • Valor_Huella • Funcion_Resumen • Numero_paginas • Numero_folios • Formato • Tamaño • Nombre_proyector • Cargo_proyector • Nombre_revisor • Cargo_revisor • Nombre_firmante

Características del documento	Descripción	Mecanismos de Protección y Seguridad	Metadatos mínimos que deben contemplares para tener evidencia de dicha característica
			• Cargo_firmante • Otros_colaboradores • Nombre_Destinatario • Clasificación_Acceso (Nivel de Acceso) • Palabras_clave_documento Para Actos Administrativos: • Tipo De Correspondes (E Entrada O Salida) • Notifica/Comunica/Public/Tramte • Régimen • Clase De Acto • Si Interpone Recurso (S/N) • Nombre Del Recurso • Tiempo Para Interponer Recurso • Ante Qué Dependencia Se Interpone • Normatividad Del Recurso • Origen • Tipos Notificación
Fiabilidad	Que refleja de manera exacta y completa la ejecución de actividades u operaciones.	• Procedimientos Internos • Definición de Roles y Permisos. • Estampa de tiempo.	• Nombre_proyector • Cargo_proyector • Nombre_revisor • Cargo_revisor • Nombre_firmante • Cargo_firmante • Palabras_clave_documento
Integridad	Que se encuentra completo y sin alteraciones.	Utilizar los mecanismos de firma digital/electrónica, protección y seguridad autorizados por la Entidad.	• Valor Huella • Función Resumen
Usabilidad (Disponibilidad)	Que se puede localizar, recuperar, presentar e interpretar.	Técnicas y Estrategias de Preservación Digital	• Codigo_proceso • Nombre_proceso • Codigo_procedimiento • Nombre_procedimiento • Codigo_subfondo • Nombre_subfondo • Codigo_seccion • Nombre_seccion • Codigo_subseccion • Nombre_subseccion • Codigo_serie • Nombre_serie • Codigo_suberie

Características del documento	Descripción	Mecanismos de Protección y Seguridad	Metadatos mínimos que deben contemplares para tener evidencia de dicha característica
			• Nombre_subserie • Numero_expediente • Id_unico_unidad_documental (expediente) • Titulo_exp • Fecha_apertura • Fecha_cierre • Palabras_clave_expediente • Estado

Tabla 1. Características de los Documentos Electrónicos de Archivo, Mecanismos de Seguridad y Protección y Metadatos Mínimos.
Fuente: Adaptada de la Guía Técnica Guía para la Gestión de Documentos y Expedientes Electrónicos.

2.1.9. Concepto de Borrador

Es un documento que en su estado de elaboración no ha llegado a convertirse aún en "documento" o "documento de Archivo". Es considerado dentro del Modelo, precisamente por ser el "potencial" Documento de Archivo.

2.1.10. Concepto de Versión

La versión es un récord o "Documento de Archivo" y a diferencia del "Borrador", se registra como una evidencia documental de la actividad desarrollada. Tiene como característica fundamental el soporte de instancias u ocurrencias, en donde el mismo "Documento de Archivo", presenta variaciones oficial y formalmente aceptadas en la Entidad, como reflejo de la evolución del documento.

2.1.11. Fases del Ciclo Vital del Documento

Para cada fase del ciclo vital del documento: captura, gestión, almacenamiento y entrega o distribución, se menciona una serie de capacidades o funcionalidades que debe tener el sistema:

- **Captura:** se reduce a ingresar contenido en el sistema, es decir, este componente abarca la producción, creación, ingreso, captura o recepción de documentos en formato papel (u otros soportes analógicos) a través de procesos de digitalización, reconocimiento, clasificación y etiquetado de documentos; captura de documentos adjuntos, fax o correos electrónicos; captura de datos y documentos desde otros sistemas de información Ej.: CRM, ERP, soluciones misionales y de apoyo, en formatos estándar como XML, CSV o producción de documentos generados a través de herramientas ofimáticas y formas electrónicas.

- **Gestión:** es lo que se debe hacer, para que el contenido pueda ser administrado, encontrado y utilizado por la persona correcta, este componente comprende las herramientas que permiten de forma integral soportar la administración de documentos, indexación de contenidos y metadatos, versionado de documentos, ciclos de vida del documento a partir de la parametrización de tablas de retención documental, flujos de trabajo, entre otras funcionalidades.

- **Almacenamiento:** significa poder resguardar o almacenar en un lugar tecnológicamente apropiado el contenido, ya sea un sistema de gestión de contenido formal u otra solución de información.

- **Entrega o distribución:** se trata de poner la información o el contenido en las manos correctas de las personas justo en el momento correcto. Este componente comprende el tratamiento eficiente y eficaz de la información, los datos y los documentos, facilitan el intercambio de información entre las aplicaciones organizacionales internas y externas, la transparencia, rendición de cuentas y acceso a la información pública.

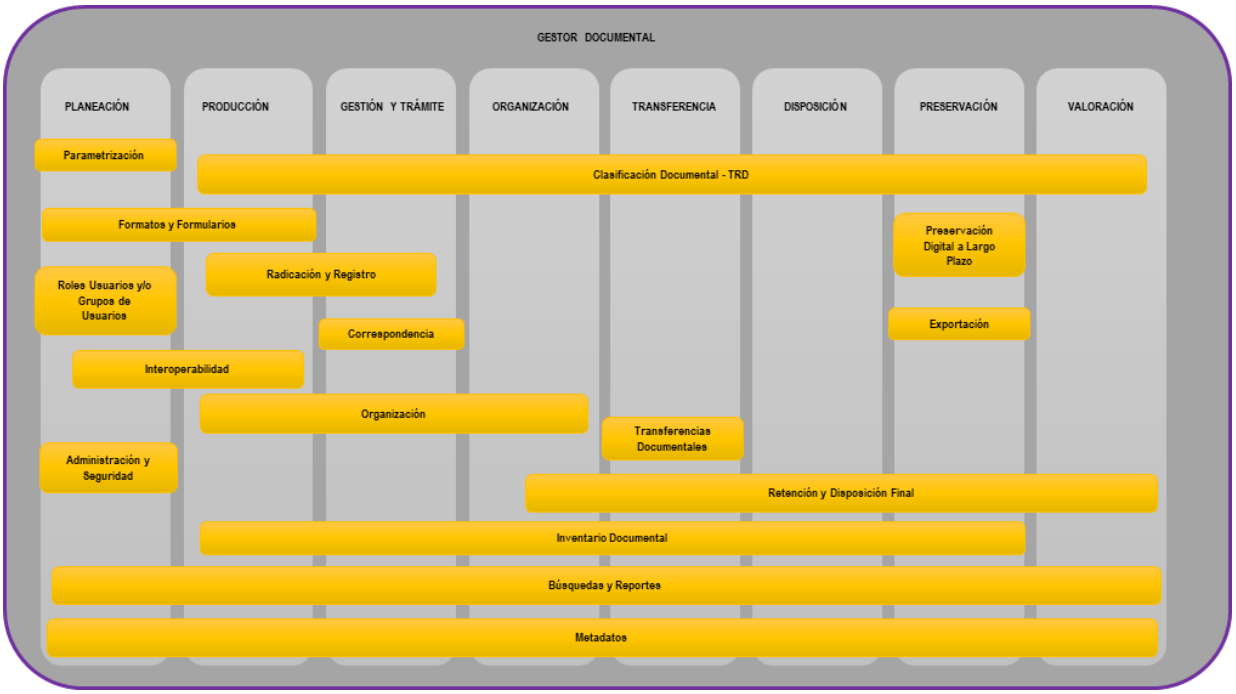
Gráfica 2. Componentes funcionales del SGDEA,
Fuente: Guía de Implementación de un SGDEA, AGN

2.1.12. Procesos de Gestión Documental

El sistema de gestión documental deberá ser la base documental de todas las soluciones de la UAE-DIAN, teniendo en cuenta que todos los procesos generan documentos que deben ser agrupados en expedientes, los cuales son alimentados por los registros que se producen en ejecución de los procedimientos y deben ser conformados y controlados con base en la Tabla de Retención Documental desde que se planean hasta su disposición final.

La solución deberá permitir la administración de manera integral del proceso de gestión documental de conformidad con lo establecido por el Archivo General de la Nación, enfocado en los procesos documentales:

1. **Planeación**. “Conjunto de actividades encaminadas a la planeación, generación y valoración de los documentos de la entidad, en cumplimiento con el contexto administrativo, legal, funcional y técnico. Comprende la creación y diseño de formas, formularios y documentos, análisis de procesos, análisis diplomático y su registro en el sistema de gestión documental.”
2. **Producción.** “Actividades destinadas al estudio de los documentos en la forma de producción o ingreso, formato y estructura, finalidad, área competente para el trámite, proceso en que actúa y los resultados esperados.”
3. **Gestión y trámite.** “Conjunto de actuaciones necesarias para el registro, la vinculación a un trámite, la distribución incluidas las actuaciones o delegaciones, la descripción (metadatos), la disponibilidad, recuperación y acceso para consulta de los documentos, el control y seguimiento a los trámites que surte el documento hasta la resolución de los asuntos.”
4. **Organización.** “Conjunto de operaciones técnicas para declarar el documento en el sistema de gestión documental, clasificarlo, ubicarlo en el nivel adecuado, ordenarlo y describirlo adecuadamente”.
5. **Transferencia.** “Conjunto de operaciones adoptadas por la entidad para transferir los documentos durante las fases de archivo, verificando la estructura, la validación del formato de generación, la migración, refreshing, emulación o conversión, los metadatos técnicos de formato, los metadatos de preservación y los metadatos descriptivos”.
6. **Disposición de documentos.** “Selección de los documentos en cualquier etapa del archivo, con miras a su conservación temporal, permanente o a su eliminación, de acuerdo con lo establecido en las tablas de retención documental o en las tablas de valoración documental.”
7. **Conservación y Preservación a largo plazo.** “Conjunto de acciones y estándares aplicados a los documentos durante su gestión para garantizar su preservación en el tiempo, independientemente de su medio y forma de registro o almacenamiento.”
8. **Valoración.** “Proceso permanente y continuo, que inicia desde la planificación de los documentos y por medio del cual se determinan sus valores primarios y secundarios, con el fin de establecer su permanencia en las diferentes fases del archivo y determinar su destino final (eliminación o conservación temporal o definitiva) Fuente: República de Colombia. Decreto 1080 de 2015 (AGN - Archivo General de la Nación, 2015).



Gráfica 3. Procesos de Gestión Documental vs Componentes
Fuente: Elaboración Propia

2.1.13. Formatos de Archivo

Se debe garantizar la Preservación Digital a Largo Plazo de los Documentos Electrónicos de Archivo, por lo que se establecen los siguientes formatos, según recopilación de la Guía Técnica G.INF.07 Guía para la gestión de documentos y expedientes electrónicos elaborada por Ministerio de Tecnologías de la Información y las Comunicaciones y el Archivo General de la Nación.

Tipo de Contenido	Formato	Características	Extensión	Estándar
Contenido de Texto	PDF/A	Formato de archivo de documentos electrónicos para la Preservación a largo plazo.	.pdf	ISO 19005
Contenido de Texto	PDF/A-1	PDF/A-1 Restricciones en cuanto al uso del color, fuentes, y otros elementos. 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	ISO 19005-1

Tipo de Contenido	Formato	Características	Extensión	Estándar
Contenido de Texto	PDF/ A-2	PDF/A-2 Características adicionales que no están disponibles en formato PDF/A-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	ISO 19005-2 ISO 32000-1
Contenido de Texto	PDF/A-3	PDF/A-3 Ofrece soporte para archivos incrustados. 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.	Pdf	ISO 19005-3 ISO 32000-1
Contenido de Texto	XML	Es un estándar abierto, flexible y ampliamente utilizado para almacenar, publicar e intercambiar cualquier tipo de información.	.xml	W3C HTML Estándar Abierto
Imagen de Mapa de Bits	JPEG2000	JPEG2000 (con pérdida) Permite obtener imágenes aproximadamente cinco veces menos pesadas. 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
Imagen de Mapa de Bits	OpenDocument	Formato de archivo abierto y estándar de la familia ODF para el almacenamiento de gráficas	.odg	OASIS ISO/IEC 26300
TIFF		Formato de archivo para imágenes panorámicas y en tercera dimensión TIFF (con compresión) Realiza compresión de imagen sin pérdidas, por tanto, devuelve la imagen descomprimida exactamente igual a la original. TIFF (sin compresión) Archivos más grandes que un formato comprimido.	.tiff	ISO 12639

Tipo de Contenido	Formato	Características	Extensión	Estándar
Imagen Vectoriales	SVG	Formato para describir gráficos vectoriales bidimensionales, tanto estáticos como animados en formato XML.	.svg .svgz	W3C
Contenido de audio	BWF	Formato de archivo que toma la estructura de archivos WAVE existente y añade metadatos adicionales	.bwf	EBU – TECH 3285
Contenido de video	JPEG 2000-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
Contenido geoespacial	GML	Geography Markup Language (GML) Formato basado en XML para el modelaje, transporte y almacenamiento de información geográfica.	.gml	ISO 19136 Estándar Abierto
Contenido geoespacial	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).
Formato de compresión	GZIP	Formato de compresión de datos	.gz	RFC 1952 Estándar Abierto
Bases de Datos	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
Bases de Datos	SQL	Structured Query Language, de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en ella	.sql	ISO 9075-1
Páginas Web	Web ARChive	Utilizado para almacenar “Web crawls” como secuencias de bloques de contenido recolectados de la World Wide Web	.warc	ISO 28500
Correo electrónico	EML	Diseñado para almacenar mensajes de correo electrónico en forma de un archivo de texto sin formato	.eml	RFC 822
Correo electrónico	MBOX	Formato utilizado para almacenar conjuntos de correos electrónicos.	.mbox, .mbx	N/A

Tabla 2. Formatos de Archivo.
Fuente: Adaptada de la Guía Técnica Guía para la Gestión de Documentos y Expedientes Electrónicos.

2.2. REQUERIMIENTOS

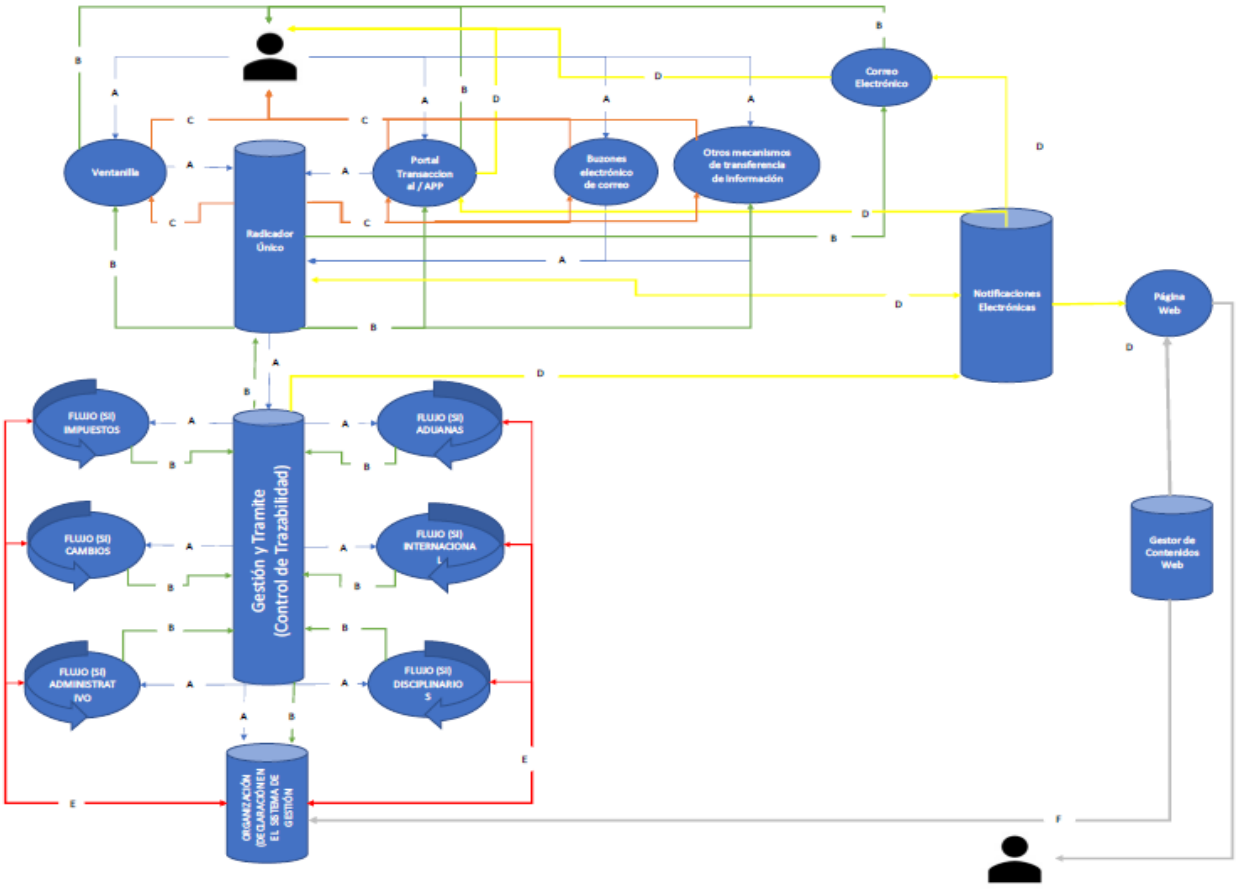
2.2.1. Requerimientos Funcionales

De manera general, la solución tecnológica debe cumplir con las siguientes características y funcionalidades básicas:

1. El SGDEA debe establecer mecanismos que permitan verificar los documentos presentados con firmas digitales, a fin de garantizar que son auténticos.
2. El SGDEA debe permitir la administración y gestión de los instrumentos archivísticos (tablas de retención, tabla de control de acceso, los cuadros de clasificación, entre otros) que permita su modificación cuando cambie la estructura orgánica de la DIAN o se cree o suprima alguna dependencia o cambien o reasignen funciones.
3. El SGDEA debe garantizar el registro y control de trazabilidad de cada documento y unidad documental.
4. El SGDEA debe permitir la gestión de unidades documentales complejas (expedientes) y simples, sean físicas, electrónicas o hibridas.
    - Creación
    - Reapertura
    - Cierre
    - Traslado
    - Transferencias
    - Eliminaciones
    - Preservación digital a largo Plazo
    - Conservación Documento
5. El SGDEA debe permitir el trabajo colaborativo de documentos electrónicos (acceso de varios funcionarios a un mismo documento).
6. El SGDEA debe contar con un Módulo de Administración que permita al usuario autorizado parametrizar, modificar y aplicar las reglas de los elementos del esquema de metadatos.
7. El SGDEA debe permitir administrar la información que se crea, captura y conserva y debe ser el vehículo a través del cual los usuarios pueden acceder a la información.
8. EL SGDEA debe permitir la creación, gestión y configuración de niveles de clasificación de información a que haya lugar (Clasificada, reservada, confidencial, de acuerdo con la normatividad existente) y permitir acceso a esta dependiendo el rol del usuario.
9. Estructura Orgánico funcional:

El SGDEA debe contar con una funcionalidad que permita al funcionario responsable a nivel nacional crear, actualizar y parametrizar las dependencias (códigos, niveles Jerárquicos, funciones de las dependencias, etc.) y garantizar la conservación histórica por cada periodo institucional, establecida en los decretos y/o resoluciones que la cree o modifique.

El SGDEA debe generar una base de conocimiento, asociada a las estructuras orgánicas, que debe contener asuntos, responsables, tiempos de respuesta; clasificada por trámites, peticiones, recursos, quejas, reclamos, felicitaciones, sugerencias y denuncias; esta debe permitir ser parametrizable y debe admitir carga de nuevos asuntos.



Gráfica 4. Diagrama general del Proceso Documental
Fuente: Elaboración Propia

10. El SGDEA debe permitir la creación del Banco Terminológico (asignación previa de palabras clave a las series, subseries, unidades documentales y/o documentos, basados en bancos terminológicos, tesauros, taxonomías, entre otros)

11. El SGDEA debe permitir parametrizar dentro del banco terminológico por cada período institucional las series, subseries y tipos documentales. Los bancos terminológicos permiten conocer el significado y contexto de cada una de las series, subseries y tipologías documentales definidas en los CCD y TRD, constituyendo un instrumento indispensable en la identificación y las relaciones de cada agrupación documental dentro del SGDEA. En efecto, los bancos terminológicos deben vincularse con el CCD dentro del SGDEA para una correcta denominación de cada agrupación documental. En las utilidades de la vinculación de los bancos terminológicos al sistema se encuentran:

    - Vocabularios que controlan los términos descriptivos y normalizados a ser admisibles en el SGDEA.
    - Establecer relaciones entre los términos descriptivos y normalizados.
    - Respaldan la recuperación de documentos a partir de su búsqueda por series, subseries o palabras claves definidas y normalizadas en el banco termológico integrado al sistema.

12. El SGDEA debe permitir al usuario autorizado parametrizar, modificar y aplicar las reglas a los elementos del esquema de metadatos, incorporar diferentes esquemas de metadatos según la transacción, los tiempos y obligatoriedad, tanto del documento nativo digital, como al digitalizado y a las unidades documentales (captura, modificación, inactivación).
13. El SGDEA debe proveer capacidades de organización, clasificación y distribución de las comunicaciones oficiales de entrada, internas y salida con las tablas de Retención Documental.
14. El SGDEA debe permitir incorporar metadatos manuales y automáticos (Ej. Información del RUT) sobre los documentos generados por la entidad, con destino interno y externo.
15. El SGDEA debe asociar todos los tipos documentales, especialmente cada formato y formulario, a un proceso, procedimiento y/o tramite.
16. El SGDEA debe contar con las consultas, informes o reportes a los diferentes niveles y estados, necesarios para la operación, control y supervisión de la gestión de las unidades documentales, tablas de retención documental, cuadros de clasificación, estructura organizacional, pistas de auditoría, cumplimiento de tiempos de trámite, entre otros.
17. El SGDEA debe contar con el Tablero de Control que permita a los funcionarios de las dependencias competentes y directivos la toma de decisiones, con la generación de indicadores (KPI), reportes y estadísticas de gestión, resultados, consulta, auditoría, trazabilidad, usabilidad y demás que requiera la entidad.
18. El sistema debe permitir la búsqueda por contenido y metadatos, aplicados al documento, así como la visualización de los documentos que hacen parte de cada radicado y cada respuesta al mismo.

19. El SGDEA debe ofrecer una clasificación de los resultados de la búsqueda, según su pertinencia, relevancia, fechas, nombre, autor, creador, modificador, tipo de documento, tamaño, entre otros.
20. El SGDEA debe controlar que ninguna función de búsqueda revele jamás al usuario información como contenido o metadatos, que se le tengan restringidos por permisos de acceso.
21. El SGDEA debe permitir la anonimización de la información clasificada o información sensible de los Documentos que tengan esta clasificación.
22. El SGDEA debe permitir controlar el préstamo de unidades documentales de Archivo de Gestión y Archivo Central, identificando la trazabilidad de las unidades documentales en préstamo y generando alertas para su devolución, de acuerdo con los tiempos parametrizados.
23. Control topográfico o ubicación (a partir de identificar como mínimo tipo de archivo, área de ubicación, estante o mueble, caja y carpeta donde se encuentra la unidad documental o el documento).
24. El SGDEA debe permitir la definición y parametrización de formatos de captura y el mantenimiento de estos, teniendo en cuenta las necesidades del negocio, los estándares, formatos abiertos y formatos recomendados por el AGN Captura e ingreso de documentos.
25. El SGDEA debe integrarse como mínimo con una solución de digitalización y debe permitir:
    - El escaneo monocromático, a color o en escala de grises
    - El escaneo de documentos en diferentes resoluciones (resolución mínima de 300 dpi)
    - Manejar diferentes tamaños de papel estándar
    - Debe reconocer y capturar documentos individuales en un proceso de digitalización masiva .
    - Guardar imágenes en formatos estándar.
26. El SGDEA debe estar orientado a identificadores únicos (IDs) por tipo de documento, con una estructura de codificación normalizada bajo los lineamientos del grupo de documentación conforme a la normatividad.
27. El SGDEA debe evitar la generación de datos “basura” que generen registros duplicados, cuando se poseen datos claros del administrado o interesado.
28. El SGDEA debe generar el cuadro resumen (Propuesta de CCD), el cual debe contener las agrupaciones documentales definidas bajo las cuales se parametrizará el sistema: fondo(s), subfondo(s) sección(es), subsección(es), series, subseries y tipologías documentales categorizadas y acordes con niveles jerárquicos existentes en la

organización, funciones, procesos y procedimientos, ayudando a soportar los metadatos tanto de las unidades documentales como de cada uno de los documentos electrónicos.

29. El SGDEA debe permitir la creación, importación, parametrización, automatización, administración y versionamiento de las Tablas de Retención Documental – TRD, a partir de plantillas predefinidas, asistentes de configuración, cargue de archivos planos o a través de la incorporación de otros mecanismos que faciliten la administración y la gestión de la TRD.
30. El SGDEA debe validar la información que se ingresa en el esquema de la Tabla de Retención Documental a través de generación de alertas o incorporación de opciones que incluyan asistentes paso a paso (listas desplegables, alertas, listas de chequeo, ventanas de ayuda, entre otras) que indiquen si existe información similar o igual en el sistema.
31. El SGDEA debe permitir el cargue de las Tabla de Retención y valoración Documental, de los períodos institucionales anteriores al actualmente vigente, en un formato abierto y editable. Las tablas tienen vigencia dentro del periodo institucional correspondiente, así (Gráfico 4).
32. El SGDEA debe permitir la importación y exportación total o parcial de la Tabla de Retención Documental, en un formato abierto y editable, teniendo en cuenta:

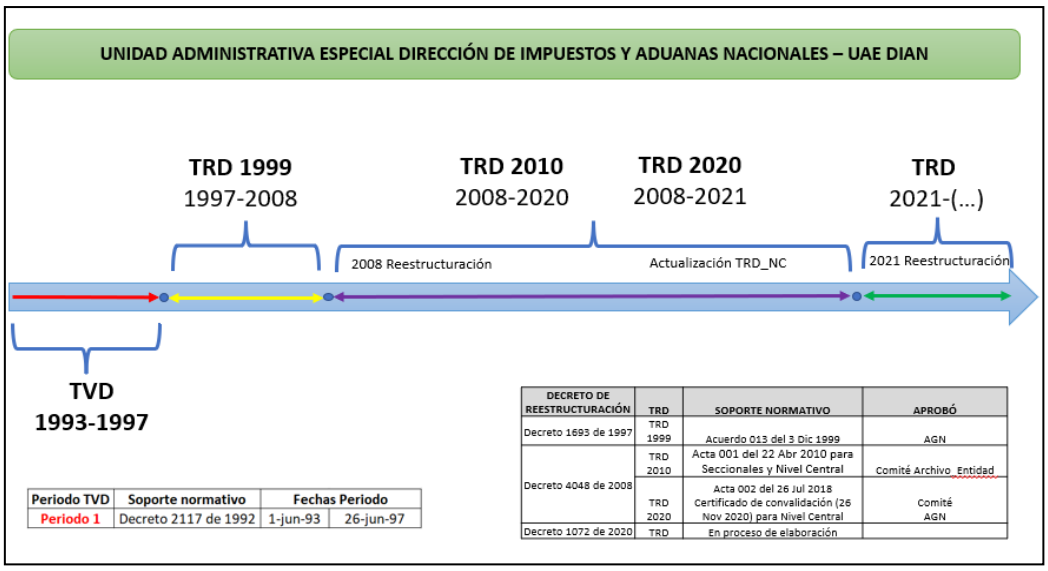
    - Para la importación:

    Permitir la importación de los metadatos asociados.

    Cuando se importen la TRD o TVD y sus metadatos, el SGDEA debe validar y arrojar los errores de estructura y formato que se presenten.

    - Para la exportación:

    Permitir la exportación de metadatos asociados, incluyendo pistas de auditoría.

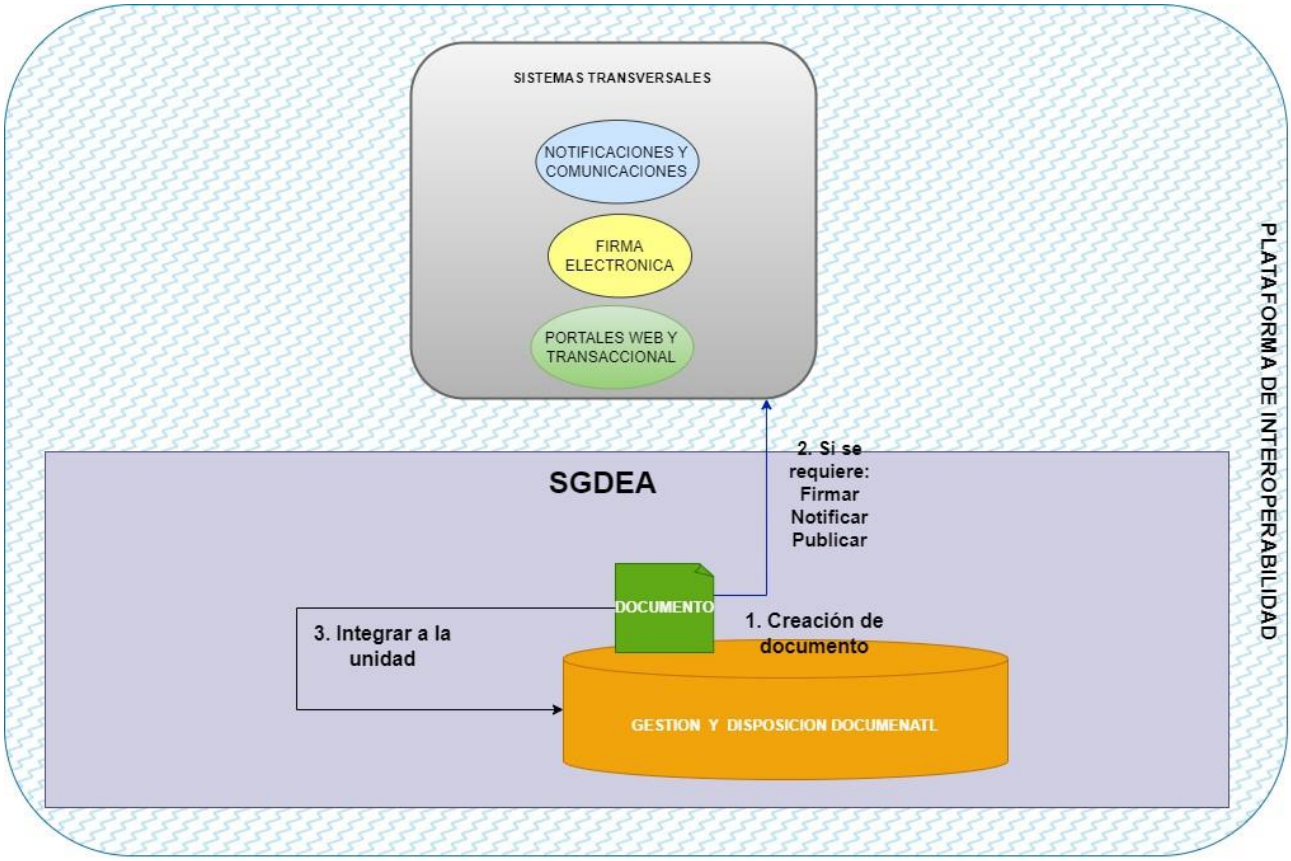


Gráfica 5. Vigencia de TRD por Versión
Fuente: Elaboración Propia

33. El SGDEA debe proporcionar a los administradores herramientas para informes estadísticos de la actividad dentro de la Tabla de Retención Documental.
34. El SGDEA debe permitir modificar los tiempos de retención para un conjunto de series y/o unidades documentales.
35. El SGDEA debe permitir la generación y asignación de ID único a nivel nacional de unidades documentales electrónicas y sus componentes (documentos electrónicos de archivo, índice electrónico, firma del índice electrónico y metadatos o información virtual contenida en ellos, Art. 9 del Acuerdo 001 de 2021 AGN).
36. El SGDEA debe permitir la creación de las Unidades Documentales Híbridas, con la correspondiente referenciación de sus documentos físicos.
37. El SGDEA debe permitir establecer niveles de seguridad de la unidad documental de acuerdo con los establecidos por la entidad y generar los reportes correspondientes.
38. El SGDEA debe impedir la eliminación de una unidad documental electrónica o de su contenido. Sin embargo, existen dos excepciones a este requisito:
    - La eliminación de acuerdo con lo establecido en las TRD
    - Eliminación por un rol administrativo como parte de un procedimiento auditado, conservando la correspondiente huella de auditoría.
39. El SGDEA debe permitir que todas las acciones efectuadas sobre la unidad documental deben ser registradas en un historial de eventos que puede ser consultado por usuarios que tengan acceso a la unidad documental electrónica; como mínimo debe registrar entre

otros la fecha y la hora de registro de la carga en la unidad documental, dependencia origen, usuario y demás metadatos asociados.

40. El SGDEA debe permitir la reubicación de una unidad documental (o conjunto de carpetas) o documento, garantizando la pista de auditoría, a un lugar distinto dentro de la estructura de clasificación, y garantizar que se mantengan los metadatos y demás atributos (permisos), cuando por equivocación se haya errado en el momento de la creación de la unidad documental, registrando las razones por las que se realiza la reubicación.
41. El SGDEA debe contar con una funcionalidad que permita al funcionario responsable, la creación en forma manual de las unidades documentales.
42. El SGDEA debe generar en forma automática los índices electrónicos de las unidades documentales, garantizando la integridad, orden y autenticidad de los documentos que la conforman. El índice electrónico se deberá generar cada vez que se asocie un documento electrónico a la unidad documental y se deberá firmar al cierre de la unidad documental, sin perjuicio de los estándares y seguridad de la información que deberán adoptar las autoridades respecto de los folios y unidades documentales (Artículo 11, Acuerdo 0001 de 2024 – AGN)
43. El SGDEA debe permitir exportar el índice electrónico a formato XML o según lineamientos del Archivo General de la Nación y en formato Excel.
44. El índice electrónico debe contener los elementos definidos en el numeral 3.1.3.1. “Estructura Índice Electrónico” de la Guía para la gestión de documentos y expedientes electrónicos, pág.51.
45. El SGDEA debe proveer una funcionalidad que permita a los usuarios autorizados acceder a la unidad documental, consultar la unidad documental para incorporarle nuevos documentos, bien sea recibidos por cualquier medio (ventanilla única, correo electrónico, redes sociales, mensajes de texto, app, etc.) o producidos por el responsable del asunto, una vez han sido firmados electrónicamente en el caso de las comunicaciones oficiales o digitalmente en el caso de actos administrativos.
46. El SGDEA debe habilitar un servicio que, en el marco de la modernización, realice en forma automática el envío de Documentos Electrónicos de Archivo y los incorpore en la correspondiente Unidad Documental.
47. El SGDEA debe permitir a un perfil administrador, actualizar y adicionar información de contexto (metadatos) a los datos importados que presenten inconsistencias o que lo requieran, y se debe llevar un registro detallado de auditoría de estas operaciones en una estructura independiente.
48. El SGDEA debe permitir que un documento pueda estar ubicado en diferentes partes de la estructura de clasificación, sin que esto signifique la duplicación del documento (Guía para la gestión de documentos y expedientes electrónicos, pág. 49 y 50).

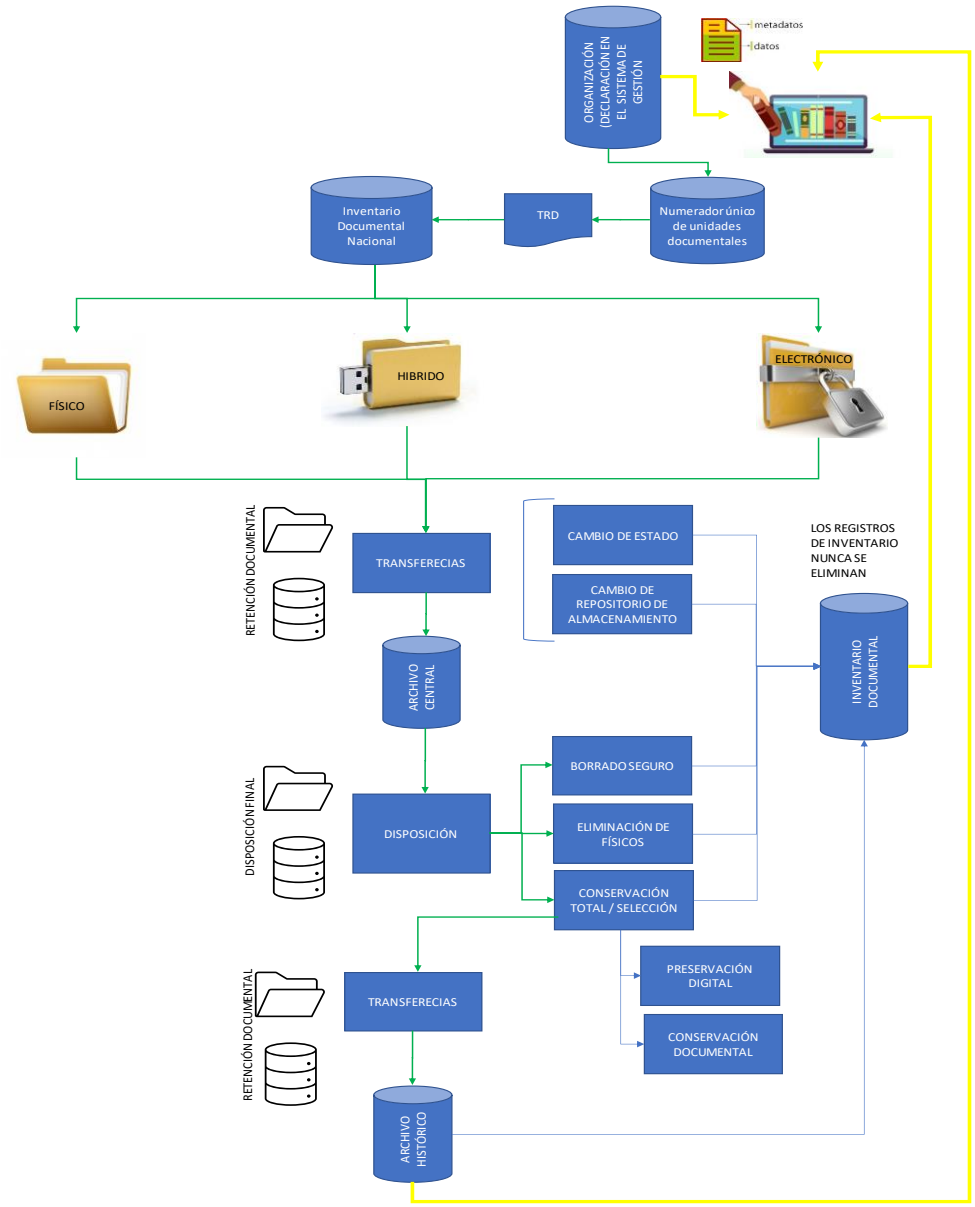


Gráfica 6. Generación documental en el SGDEA
Fuente: Elaboración Propia

49. El SGDEA debe otorgarle un número único de identificación a cada documento cuando es incorporado a la unidad documental (Guía para la gestión de documentos y expedientes electrónicos, pág.66).
50. Para la captura de documentos que tienen anexos el SGDEA deberá gestionarlos como unidad, restringiendo el uso de formatos comprimidos. Cada vez que un archivo adjunto se captura como un documento por separado, el sistema debe permitir asignar el vínculo archivístico en el registro de metadatos.
51. Se requiere que el SGDEA permita a los usuarios autorizados trasladar la unidad documental, en cuyo caso la administración de la unidad documental quedará a cargo del destinatario del traslado.
52. El SGDEA debe permitir traslado de unidades documentales entre dependencias, entre seccionales y nivel central, en la etapa de gestión de los documentos, entre:
    - Dependencias de la misma seccional
    - Dependencias del nivel central

- Dependencias de seccionales diferentes
- Dependencias de seccionales a dependencias de Nivel Central o viceversa

53. El SGDEA debe actualizar automáticamente el Inventario Documental por nuevo responsable, cuando se realicen estos traslados.
54. El SGDEA debe permitir a los usuarios registrar el estado de la unidad documental de forma manual o automática.
55. El SGDEA debe garantizar que una vez cerrado la Unidad Documental se deberá restringir la adición o supresión de carpetas o documentos. Artículo 4.3.2.4, Acuerdo 001 de 2024 – AGN: "Cierre del expediente electrónico. Cuando finalice la actuación o procedimiento administrativo, el funcionario autorizado por procedimiento deberá cerrar el expediente y firmar el índice electrónico".
56. Cuando la unidad documental se archive, se debe generar o convertir en un formato que permita asegurar su autenticidad, integridad, recuperación, conservación y preservación a mediano y largo plazo, conforme a los criterios de valoración documental establecidos por el Archivo General de la Nación y los lineamientos tecnológicos establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones.
57. Cuando por disposiciones legales o administrativas sea necesario reabrir una unidad documental, esta acción deberá realizarse mediante un perfil administrativo y debe quedar registro de ello en las pistas de auditoría, con la explicación del motivo por el cual se realizó la acción.
58. El SGDEA no deberá permitir la eliminación de documentos que hayan sido incorporados en la unidad documental al momento de reabrirla.
59. El SGDEA debe activar automáticamente alerta al rol administrador cuando el período de retención aplicable está a punto de cumplir el tiempo establecido.
60. El SGDEA deben permitir realizar transferencias primarias del Archivos de Gestión a Archivo Central y transferencias secundarias del Archivo Central al Archivo General de la Nación.
61. El SGDE debe realizar el cambio de Custodio de la Unidad Documental transfiriendo del Archivo de Gestión al Archivo Central.
62. El SGDEA debe mantener una historia inalterable de modificaciones (pistas de auditoría) que se realizan en los tiempos de retención y disposición, incluida la fecha del cambio o eliminación y el usuario que lo registra.
63. Cuando el SGDEA está transfiriendo o exportando unidades documentales y/o documentos y alguno de ellos incluye referencias a documentos almacenados en otras unidades documentales, El SGDEA deberá transferir o exportar el documento completo, no solo la referencia y almacenarlos, de acuerdo con el flujo de trabajo correspondiente.

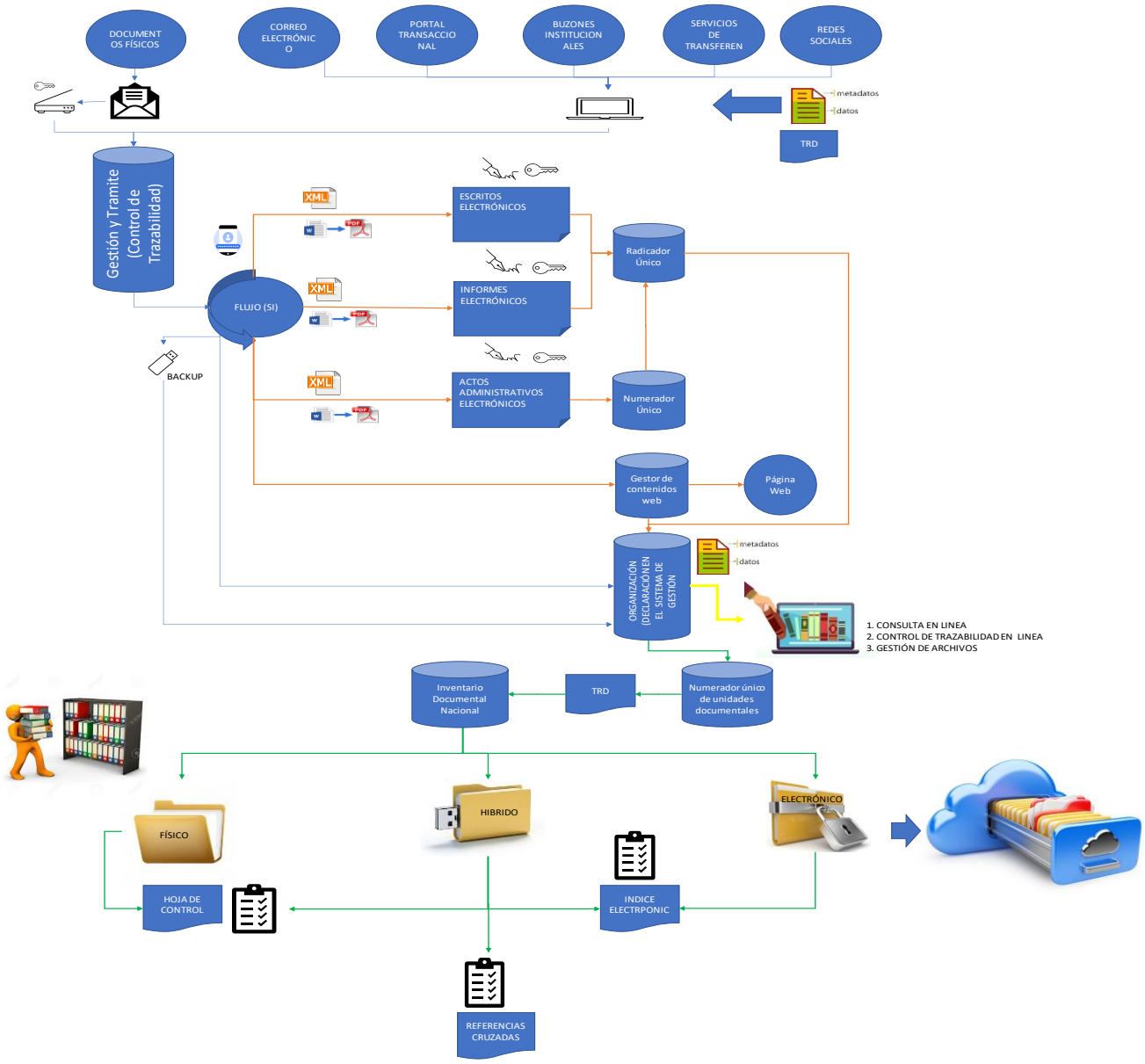


Gráfica 7. Transferencias y disposición final
Fuente: Elaboración Propia

64. El SGDEA debe conservar todos las Unidades Documentales con sus Documentos Electrónicos de Archivo (DEA) que se hayan transferido de acuerdo con la relación en el Inventario Documental correspondiente, donde se registran las Unidades Documentales Electrónicas e Híbridas.

65. El SDEA debe proporcionar al funcionario que recibe en el Archivo Central, una herramienta para la aceptación satisfactoria de la transferencia.
66. El SGDEA debe permitir que en los resultados de búsqueda se presenten todas las unidades documentales y documentos de acuerdo con los criterios de búsqueda; aunque solo puede permitir el acceso a las unidades documentales a los que el usuario que realiza la consulta tiene permiso de acuerdo con los niveles definidos.
67. El SGDEA debe permitir al funcionario autorizado buscar y recuperar información que se encuentre dentro de documentos, listas de documentos y metadatos, de acuerdo con el perfil de acceso.
68. El SGDEA debe permitir como mínimo las siguientes acciones de disposición para cualquier regla de retención y disposición:
    - Conservación permanente
    - Eliminación automática
    - Eliminación con autorización del rol administrativo
    - Selección para eliminación
    - Selección para conservación total
69. El SGDEA debe garantizar que los documentos producidos y asociados a una TRD, mantengan los criterios de tiempos y de disposición final de la versión correspondiente.
70. El SGDEA debe permitir de acuerdo con lo parametrizado en la TRD, que el usuario seleccione las Unidades Documentales a conservar según el criterio cualitativo o cuantitativo. Las unidades documentales que no se conservan pasarán a la propuesta de eliminación de la vigencia correspondiente.
71. El SGDEA debe emitir una alerta al administrador en el caso en que un expediente electrónico esté listo para ser eliminado y alguno de sus documentos esté vinculados a otra unidad documental. El proceso de eliminación debe aplazarse para permitir una de las siguientes acciones correctivas:
    - Solicitar confirmación para continuar o cancelar el proceso;
    - Esta acción deberá quedar en las pistas de auditoria relacionando mínimo los siguientes datos: fecha de inicio; identidad del usuario autorizado; motivo de la acción.
    - Deberá permitir copiar el documento a un expediente determinado y actualizar las referencias correspondientes, con el fin de garantizar la integridad del expediente.

72. El SGDEA debe realizar la eliminación de Unidades Documentales mediante procesos de Borrado Seguro de la información (Artículo 4.3.2.5. Acuerdo 001 de 2024).

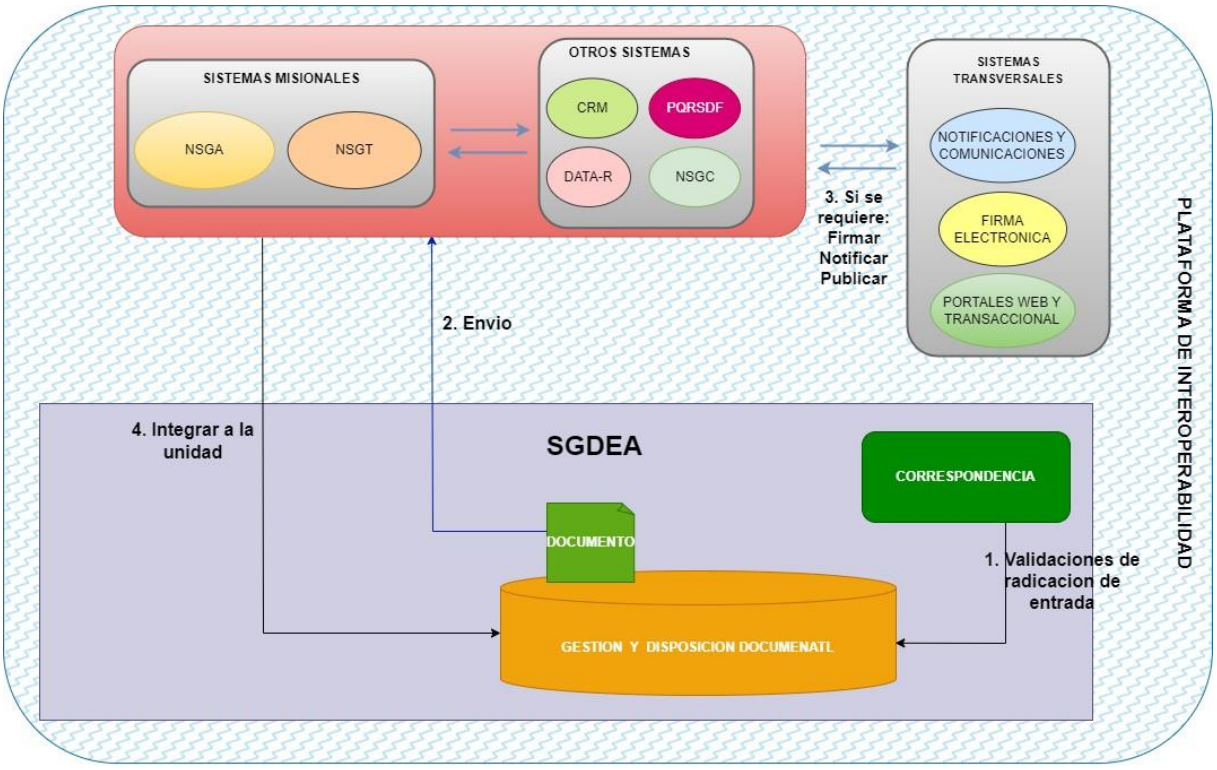


Gráfica 8. Gestión y conservación de unidades documentales
Fuente: Elaboración Propia

73. El SGDEA debe garantizar que el registro de la unidad documental repose en el inventario documental, aunque haya sido eliminada, registrando la trazabilidad del acta de eliminación correspondiente.
74. Debe permitir visualización y reproducción (imagen, audio, audiovisual) de los Documentos Electrónicos de Archivo que carecen de la aplicación o licencia para generarlos o visualizarlos. (por ejemplo, planos de AutoCAD, Videos, Grabaciones de Audio).
75. En el proceso de captura el SGDEA debe permitir la conversión a formato de preservación digital a largo plazo del documento a un formato previamente parametrizado en el sistema, Tabla 2. (Guía para la gestión de documentos y expedientes electrónicos, anexo 1. Formatos de archivo de uso común. pág.60).
76. El SGDEA por razones de obsolescencia tecnológica, preservación a largo plazo, debe permitir realizar cambios por personal autorizado dejando evidencia en el documento (a través de metadatos) conforme a reglas establecidas, limitadas y controladas por la entidad.
77. El SGDEA debe garantizar la relación sistemática y detallada de las Unidades Documentales electrónicas, físicas e híbridas asignadas a cada funcionario y dependencia, indicando la información desde la creación de la unidad documental, descripción, conformación, gestión y trámite, transferencias, ubicación topográfica, disposición final, entre otras.
78. El SGDEA debe proveer las funcionalidades de referenciación, debe crear y mantener automáticamente los inventarios de las unidades documentales de documentos electrónicos y físicos que se administren en el mismo, teniendo en cuenta que hacen referencia a los instrumentos de recuperación de la información de manera precisa y exacta.
79. El SGDEA debe permitir a los usuarios autorizados o asignados a través de los inventarios automatizados (para unidades documentales físicas, electrónicas e hibridas), realizar búsquedas que permitan la identificación, localización y recuperación de los documentos almacenados en el SGDEA en concordancia con los niveles de agrupación y descripción documental.
80. El SGDEA debe permitir la consulta y reportes a los diferentes niveles y estados de las unidades documentales registradas en el Inventario Documental de cada dependencia productora.
81. El SGDEA debe incluir un módulo de digitalización en la que se pueda configurar las siguientes características:
    - Resolución (resolución mínima de 300 dpi)
    - Profundidad de bits (blanco y negro, escala de grises, color)

- Escala (tamaño papel)
- Compresión
- OCR Reconocimiento Óptico de Caracteres.
- ICR Reconocimiento Inteligente de Caracteres
- Guardar en varios formatos electrónicos (PDF/A, TIFF, JPG, entre otros)

82. El SGDEA debe permitir la creación y administración de usuarios, roles y permisos.
83. El SGDEA debe permitir que el administrador restrinja el acceso a carpetas, documentos y metadatos a determinados usuarios del sistema.
84. El SGDEA debe permitir restringir el acceso a funciones como la lectura, modificación y eliminación de documentos y/o metadatos.
85. El sistema de correspondencia contará con una Ventanilla Única de Radicación para todos los documentos, solicitudes y/o trámites que los administrados y/o grupos de interés que presenten ante la Entidad, la cual estará habilitada a través del Portal Transaccional y durante el periodo de transición a la modernización de la entidad se deberá desarrollar la interoperabilidad con el sistema de PQRSD vigente.



Gráfica 9. Radicación e Interacción entre sistemas internos y SGDEA
Fuente: Elaboración Propia

86. El sistema deberá dejar auditoria de la trazabilidad de los diferentes estados, transacciones en el Sistema, reflejando fecha, hora, usuario e identificación del mismo y movimientos del mismo dentro del sistema.

87. El sistema de correspondencia deberá permitir a los administrados y/o grupos de interés, el seguimiento y/o consulta a través del portal transaccional (Sede electrónica, muisca, entre otros), de los trámites y/o documentos presentados ante la Entidad. El sistema debe permitir la consulta y seguimiento a través de los siguientes parámetros:

    - Cuando el ciudadano en calidad de anónimo presente ante la Entidad un documento, el sistema le asignará, un "Usuario anónimo" el cual hará las veces de identificador único de usuario. Este estará asociado a los consecutivos únicos de radicación y le permitirá realizar seguimiento a sus solicitudes a partir del correspondiente consecutivo único de radicación. Teniendo en cuenta los parámetros establecidos en la resolución 1519 de 2020 y sus anexos.

88. El sistema deberá permitir a través de la vista 360 (servidor público): Para todos los funcionarios DIAN, facilitar la producción, gestión y trámite de las comunicaciones oficiales, el ingreso acorde a los permisos del servicio de identidades debe permitir la publicación de información actualizada en tiempo real para conocimiento de los servidores públicos.

89. El sistema deberá permitir la gestión de comunicaciones oficiales permitiendo adjuntar documentos en las diferentes extensiones, así como la firma de los mismos de forma electrónica o digital según el mecanismo habilitado en la Entidad.

90. El sistema debe permitir la omnicanalidad asignando un consecutivo de radicación único, cronológico en el trámite de solicitudes, consultas y/o requerimientos allegados por los diversos canales existentes y habilitados por la Entidad.

91. El Sistema debe proveer herramientas de seguimiento y control, a nivel de usuario, dependencia, seccional y a nivel nacional, a través de la Vista 360, que permitan hacer control y seguimiento a las comunicaciones oficiales.

    1- Para el administrado o interesado también deberán diseñarse tableros de control en el ambiente privado, donde podrá ver:

    - Comunicaciones recibidas
    - Responder requerimientos
    - Plazo para responder o interponer recurso
    - Fecha máxima para interponer recurso o responder.

    2- Tableros de Control o módulos de seguimiento, trazabilidad y control, que permitan determinar solicitudes a cargo del área y del funcionario, con fechas límites de respuesta y semáforo de advertencia de vencimiento.

3- Generador de KPI y reportes sobre el estado de las comunicaciones oficiales, que le permitan presentar a la alta dirección la gestión institucional sobre la materia, estos módulos deben generar informes e indicadores dinámicos.

4- Módulo de administración para hacer correcciones controladas, cargue de nuevos asuntos o trámites, modificación de plazos de respuesta, destinatarios, liquidaciones de contratos de correo, etc.

5- El sistema debe permitir la generación de los reportes para la facturación de los envíos por Unidad Administrativa, por forma de envío electrónico y físico (Local, Nacional, Regional, etc.) por tipo de contrato del envío realizado.

92. El sistema debe contar con funcionalidades de radicación de comunicaciones de salida e interna a nivel nacional, en el cual se registren de manera unificada todos los documentos que salen de la UAE-DIAN o se generen entre dependencias; esto permite un control unificado de radicación y trazabilidad, así como mecanismos intuitivos de seguimiento para el administrado y cada una de las dependencias de la entidad.

    Tal servicio llevará control de todos las comunicaciones oficiales y actos administrativos que deben salir hacia los administrados, que hayan sido generados por los flujos y servicios informáticos; no bastando con dar un número consecutivo, deberá contar con fecha y hora de radicación y asociarse al radicado de entrada y unidad documental, si es una respuesta al administrado, enviando de forma automática al procedimiento de envío de correspondencia certificada.

    La radicación de salida e interna se deberá realizar desde cada área, la radicación debe ser prevista como la última actividad del flujo de generación de respuesta, en el cual la asignación del número y fecha se dará al momento en el cual el jefe del área o quien este delegue apruebe un documento definitivo, integrándose con el mecanismo de firma definido por la Entidad, asegurando las condiciones de documento electrónico de archivo, debe ser simultáneo la radicación del Documento y la firma, con el fin de evitar la alteración de documento, pérdida de consecutivos de radicado; garantizando la autenticidad de este.

    La radicación de salida e interna física deberá radicarse por las ventanillas únicas disponibles en cada Unidad Administrativa, para su respectivo trámite.

    Cuando la radicación de salida sea respuesta a una radicación de entrada, el sistema previo a la radicación debe permitir la asociación de los números de radicación y su respectiva unidad documental, para que la comunicación oficial tome de manera automática los datos del registro de entrada y dé cierre a la solicitud o trámite a través de metadatos, conformándola en la respectiva unidad documental.

93. El sistema deberá realizar la distribución y asignación automática de las comunicaciones oficiales radicadas, a través de un algoritmo de distribución inteligente del documento, que identifique y clasifique de acuerdo al asunto, destinatario y Unidad Administrativa a la que pertenece según la estructura orgánico-funcional de la entidad.

1- El sistema deberá tener en cuenta los siguientes aspectos para la asignación y distribución:

- Validar el lugar de domicilio fiscal, según su registro.
- Validar y asociar el asunto a la(s) dependencia(s) correspondiente(s), según la estructura orgánico funcional de la Entidad.
- Validar destinatario y coherencia con el asunto, previa a la radicación y asignación correspondiente.
- El sistema debe parametrizar los términos de cada trámite de acuerdo a normatividad vigente ligado a la estructura orgánico funcional y priorizar aquellas comunicaciones al momento de la recepción y envío de comunicaciones oficiales con origen y destino, especialmente para aquellos casos que prime la determinación del vencimiento de términos para la DIAN o para el administrado.

2- Interoperar con el servicio de identidades, con el fin de asociar el asunto con la(s) dependencia(s) responsable(s), para realizar la asignación efectiva.

3- El sistema debe permitir asociar el número de radicado inicial o unidad documental, de existir, citado en el documento recibido para radicado.

4- El sistema debe permitir asignar o reasignar a una o varias dependencias de la Entidad que tengan competencia de los diferentes trámites o solicitudes que estén inmersas dentro de este mismo trámite.

5- El sistema debe permitir manejar criterios de asignación automática de comunicaciones oficiales a funcionarios responsables en las diferentes dependencias, basándose en criterios predefinidos como roles, carga laboral, y novedades de situaciones administrativas.

6- El sistema debe garantizar la distribución de las comunicaciones oficiales mediante pantallas o tableros de control, que usarán los servidores públicos de cada una de las dependencias a Nivel Nacional para gestionarlos. Las comunicaciones oficiales radicadas por los diferentes canales habilitados por la UAE-DIAN, viajarán de manera inmediata al área responsable de su atención, salvo que el administrado o interesado no conozca el destinatario de su solicitud, caso en el cual, las solicitudes se enviarán a un centro de despacho para su clasificación.

7- Los documentos enviados por el sistema al centro de despacho, podrán ser clasificados manualmente y realizar la Distribución. Así mismo el sistema deberá mediante IA y herramientas de autoaprendizaje, reprogramarse identificando el criterio para futuras asignaciones.

94. El Sistema debe permitir generar alertas a través de la vista 360 a la dependencia productora o de radicaciones de las comunicaciones oficiales que han sido proyectadas, validadas y firmadas y que no se han tramitado.

1- Se debe generar alertas por un término continuo y máximo de dos meses, para documentos que iniciaron proyección, y de continuar su trámite, deben ser eliminados del servicio, dejando la auditoria correspondiente de todos los accesos, fecha, hora y trazabilidad.

2- Debe generarse alertas diarias, de no tramitarse el envío después de firmado, al día hábil siguiente de firma.

95. Entrega de la prueba de radicación al Administrado o Interesado.

    Cuando el documento físico se debe registrar, se le adicionará el sello de radicación, antes de asegurar el documento y al documento físico se le registrarán los datos de la radicación exigidos o se generará tirilla de radicación.

    Cuando la radicación se realice por Portal transaccional, el sistema deberá informarle que el documento ya fue radicado y permitirle guardar su radicado.

    El radicado a entregar será de formato estandarizado sin importar el medio de radicación.

96. Para los casos excepcionales donde se requiera radicación de salida de documentos o elementos en físico, el sistema debe permitir:

    - Realizar aceptación de los oficios enviados para remisión física.
    - Realizar la Devolución al área competente por inconsistencias en los datos o los anexos no correspondientes.
    - Cuando se trate de respuestas, solicitudes u oficios que no son actos administrativos, deben ser radicados, impresos y entregados al Courier.
    - Permitir registrar la Guía (fecha de imposición, numero guía, observación de la entrega o devolución y la causal), entregado por el Courier.

97. El sistema debe permitir la interoperabilidad con la empresa de mensajería contratada para la entrega de la información (metadatos) de la correspondencia de salida, para la distribución física/virtual de la misma al destinatario, así como, recibir la información de las pruebas de entrega o acuses de recibido o información de las devoluciones con su respectiva causal, asociándolo al radicado de salida correspondiente. Disponer de la capacidad de importación y exportación de archivos en formatos que defina la Entidad para este fin.

    1- El sistema debe permitir que la la prueba de entrega o devolución migre de manera automática a la unidad documental que reposa en el gestor documental.

98. El sistema debe permitir la digitalización certificada (PDF/A) de los documentos físicos que llegan por ventanilla, para que estos fluyan de forma electrónica al interior de la entidad, permitiendo la devolución del físico al administrado o interesado. Los documentos digitalizados por ventanilla de forma certificada deberán ser firmados por el mecanismo e firma habilitado por la Entidad, para asegurarlos desde su entrada.

99. El sistema deberá permitir el registro de observaciones adicionales durante el flujo de las comunicaciones oficiales:

    1- El sistema deberá permitir habilitar un campo de observaciones durante la radicación para facilitar el seguimiento de los documentos.

    2- El sistema deberá permitir, en cualquier momento del proceso, habilitar este campo de observaciones, con el fin de registrar las diferentes novedades presentadas para facilitar el seguimiento de los documentos.

    Todas las observaciones hacen parte del historial de eventos, pistas de auditoría y deben contener como mínimo el usuario, la fecha, el texto de la observación y récord de observación.

100. El sistema de correspondencia asignará un número de radicado único y cronológico, por tipo de radicado, en cada Dirección Seccional y Nivel Central, conservando la siguiente estructura:

- DIAN: Un (1) Dígito
- Seccional: Campo automático, según domicilio fiscal en el registro de tres (3) dígitos / según sede de radicación / si es un usuario anónimo indicar sede N.C.
- Año: Cuatro (4) dígitos
- Indicativo de tipo de radiación: (S-salida, I-interna, E-entrada)
- Consecutivos: Ocho (8) dígitos
- El sistema asignará un consecutivo independiente por tipo de radicación: (S-salida, I-interna, E-entrada)
- El sistema asignará un consecutivo único por Unidad administrativa (D.S. a Nivel Nacional y Nivel Central).
- En cada anualidad (01 de enero a las 12:00:00 am) se deben reiniciar los consecutivos únicos por tipo de radicación, de forma automática

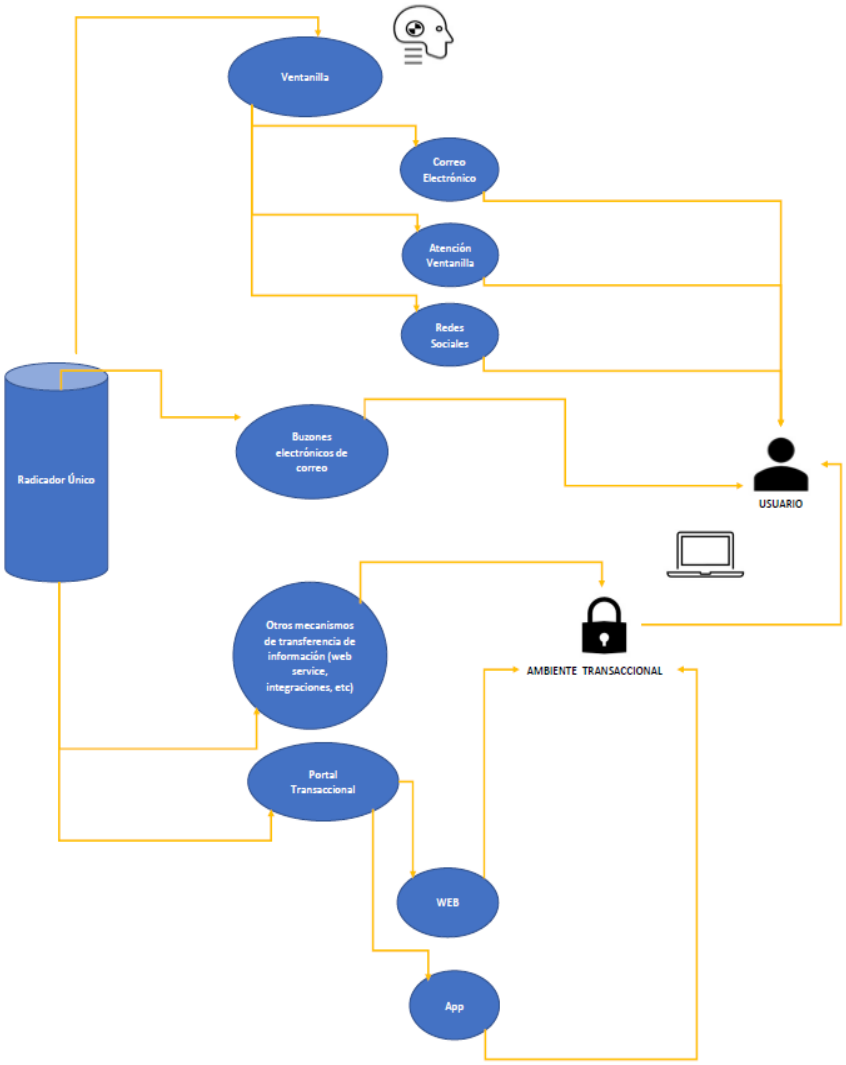
En cada anualidad (31 de diciembre a las 11:59:59 p.m.) se deben cerrar los consecutivos únicos por tipo de radicación, de forma automática

Todos los documentos de salida y entrada a la entidad a través del Portal Transaccional, el sistema deberá estampar un rótulo en el documento con la siguiente información:

- UAE DIAN (LOGO)
- Número de radicado asignado
- Fecha y hora de radicación: yyyy/mmm/dd (el mes debe ser expresado en letras) y la hora oficial colombiana hh/mm/ss
- Asunto y toda la información señalada, anteriormente.

- Remitente / Origen del documento: el rótulo deberá reflejar el nombre de la persona registrada Natural, Jurídica, Nombre Empresa o Entidad.
- Destinatario (dependencia - sede):el rótulo deberá contener la dependencia, sede, a la que se asignará la solicitud o trámite, de acuerdo a la competencia.
- Número de Folios y/o anexos: Con ayuda de la inteligencia artificial el sistema deberá incorporar estos metadatos en el rótulo como en el formulario de radicación, haciendo distinción en los diferentes formatos allegados (tipos de anexos).

Los datos contenidos en el rótulo serán metadatos asignados a cada comunicación oficial.



Gráfica 10. Entrega del radicado
Fuente: Elaboración Propia

101. El sistema deberá permitir a los administrados y/o grupos de interés presentar o radicar documentos de forma física o virtual, a través de los diferentes canales habilitados por la Entidad en el Portal Transaccional (buzones autorizados por la ley, redes sociales, PQRSD, Ventanilla presencial.

102. El sistema de correspondencia deberá permitirle a los administrados y/o grupos de interés, el acceso para la radicación de los documentos presentados ante la Entidad.

1- La autenticación se basa en los registros del Portal Transaccional: Para usuarios registrados en el portal transaccional (toma las credenciales de ingreso al Portal Transaccional) no permite anonimidad. Permite que los apoderados y/o representantes legales y/o terceros autorizados, puedan ingresar al Portal Transaccional con permiso de acceso a nombre propio y seleccionar la calidad en la que actúa y realizar la radicación de los documentos correspondientes (a nombre propio, a nombre de tercero, representante legal, apoderado, agente oficioso, liquidador, entre otros).

2- Permite presentación anónima de escritos, está habilitado de forma libre en el portal transaccional (con autenticación que garantice la anonimidad del usuario).

3- Interfaz entidades estatales, para Entidades de carácter gubernamental (Autoridades Administrativas, Autoridades Judiciales, Entes de Control y Congreso), la base de datos de autenticación se construye a partir de cada registro o radicación recibida por parte de cada entidad, se accede por página web principal.

4- Habilitar una funcionalidad para que las Entidades de carácter gubernamental (Autoridades Administrativas, Autoridades Judiciales, Entes de Control y Congreso) puedan remitir documentos, trasladar y solicitar información ante la Entidad, las cuales serán asociadas automáticamente por el sistema como correspondencia de entrada.

5- Las comunicaciones que ingresen a través de la funcionalidad dispuesta para radicaciones de carácter judicial, deberán conectarse con el Gestor Documental, para la asignación del consecutivo único de comunicaciones oficiales, el cual deberá visualizarse en la funcionalidad a cargo del proceso o área correspondiente.

103. El sistema debe permitir descargar y cargar información que se encuentra en dispositivos como CDS, USB, dispositivos móviles, u otros dispositivos que contengan información y que son presentados por el usuario ante la Entidad en ventanillas presenciales para la radicación de documentos anexos u otros.

1- En la vista 360 del funcionario el sistema deberá contar con una funcionalidad que permita descargar, cargar y almacenar la información en la vista 360, para adjuntar dicha información en el trámite de radicación de correspondencia.

2- En el Portal Transaccional el administrado el sistema deberá contar con una funcionalidad que permita descargar, cargar y almacenar la información en el Portal Transaccional, para adjuntar dicha información en el trámite de radicación de correspondencia.

3- El sistema deberá permitir que la información almacenada sin contar con limitantes de tamaño o peso, continue con el flujo de distribución y asignación correspondiente.

104. El Sistema debe permitir en caso de requerirse generación de planillas de distribución físicas, para los casos que se requieran entregas físicas por su naturaleza.

1- El sistema de permitir la distribución física por medio de la planilla de entrega para los casos excepcionales que se deben tramitar en soporte físico como muestras de laboratorio y se requiere su distribución a las diferentes áreas facilitando así la gestión interna de la Entidad.

105. El sistema debe permitir la implementación de protocolos de seguridad avanzados para proteger la información sensible, garantizando la privacidad de los datos personales y documentación confidencial de acuerdo a las políticas de la OSI y a la normatividad vigente.

106. El sistema deberá contar con la capacidad concurrente para el total de los usuarios internos y externos, sin afectar el funcionamiento y garantizando tiempos de respuesta permanentes.

107. El sistema debe asegurar una disponibilidad permanente (24/7) a través de la vista 360 y de la ventanilla única habilitada en el portal transaccional, con soporte para operaciones continuas y sin interrupciones.

108. El sistema deberá permitir la incorporación de futuras funcionalidades y requerimientos sin necesidad de un rediseño completo, facilitando su evolución con el tiempo.

109. El Sistema debe contener:

1- Administrado Registrado: si el administrado se encuentra registrado en el portal transaccional, permitirá la radicación a través de la opción habilitada para los diferentes trámites o solicitudes, así como visualizar el estado de la solicitud y/o respuestas emitidas por la Entidad.

2- Ventanilla Presencial (usuario externo): si el administrado se presenta en los puntos de radicación para correspondencia (entrada) habilitados por la Entidad en las diferentes sedes, el sistema le habilitará al funcionario en cargado de la función de radicación, el acceso a través del Portal Transaccional, para la radicación correspondiente.

3- Ventanilla Presencial (usuario interno): si el funcionario se presenta en los puntos de radicación para correspondencia (salida e interna) habilitados por la Entidad en las diferentes Unidades Administrativas, el sistema le habilitará al funcionario en cargado de la función de radicación, el acceso a través del Portal Transaccional, para la radicación correspondiente.

4- El sistema deberá permitir la interacción con el Portal Transaccional para la opción de presentación de solicitudes anónimas.

2.2.2. Características del Sistema

1. El SGDEA debe cumplir lo establecido en el capítulo VI “El Sistema de Gestión Documental” y VII “La Gestión de Documentos Electrónicos de Archivo” del Decreto 1080 de 2015, respecto de la gestión de documentos electrónicos de archivo y normatividad posterior que lo modifique, para las Entidades Públicas de Orden Nacional.
2. El SGDEA debe estar alineado a la guía de implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo – SGDEA del Archivo General de la Nación.
3. El SGDEA debe proveer interfaces gráficas para clientes externos (administrados e interesados) y para clientes internos (áreas de radicación y áreas responsables), centralizadas, independientemente de que haya más de un servicio informático (SI) en capacidad de recibir documentación.
4. El SGDEA no debe limitar el número de documentos que pueden ser capturados en cualquier serie, subserie, expediente ni sobre el número de documentos que se pueden almacenar.
5. El SGDEA debe proporcionar una función de búsqueda que permita utilizar combinaciones de criterios de búsqueda:
    - Operadores booleanos (y, o, exclusivo, o, no);
    - Coincidencias aproximadas;
    - Intervalos de tiempo;
    - Permitir búsqueda con comodines (*, ? , $, = , + , -);
    - Por agrupaciones (Código, Serie, subseries, asunto, usuario, área responsable, palabras clave…);
    - Tipos de formatos
    - Cualquier combinación valida con un número limitado de criterios de búsqueda, utilizando cualquier combinación de contenido textual o de metadatos.
    - Opción de autocompletar.
6. El SGDEA debe permitir el control de versiones de cada uno de los documentos.
7. El SGDEA debe disponer de una opción o servicio para la conversión de documentos a los formatos establecidos por el Archivo General de la Nación.
8. El SGDEA debe permitir la asignación previa de palabras clave a las series, subseries, expedientes y/o documentos, basados en bancos terminológicos, tesauros, taxonomías, entre otros.

9. El SGDEA debe garantizar la integración de los documentos y expedientes con Mi DIAN Digital para su consulta. Seguimiento por parte de los usuarios, vía web, de los radicados ingresados físicamente o por Mi DIAN Digital.
10. El SGDEA debe proveer servicios de consulta y préstamo de expedientes (para los casos que se encuentren en el archivo central o en los archivos de gestión, y sean requeridos por usuarios internos y externos).
11. El SGDEA debe permitir la generación de informes y reportes de auditoría y trazabilidad.
12. El SGDEA debe permitir gestionar contenidos como: videos, audio, imagen, entre otros, de la misma forma que los documentos electrónicos de texto. Teniendo en cuenta que se puede convertir en parte probatoria de un expediente.
13. El SGDEA debe admitir el control topográfico o ubicación (a partir de identificar como mínimo tipo de archivo, área de ubicación, estante o mueble, caja y carpeta donde se encuentra la unidad documental o el documento, para el caso de unidades híbridas o físicas).
14. El SGDEA debe soportar formatos de firma digital tales como CADES, PADES Y XADES.
15. El SGDEA debe dar cumplimiento al Decreto No. 2364 de 2012. Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones. Diario Oficial de la República de Colombia, Bogotá, 22 de noviembre de 2012.
16. El SGDEA debe contar con manuales de usuario estructurados adecuadamente.
17. El SGDEA debe proveer módulos de contingencias que permitan sostener la operación en las diferentes funcionalidades, en caso que no exista disponibilidad del sistema, permitiendo posterior registro de documentos o unidades documentales.
18. El SGDEA debe contar con un Módulo de administración para hacer correcciones controladas, cargue de nuevos asuntos o trámites, modificación de plazos de respuesta, destinatarios, etc.
19. El SGDEA debe desconectar los usuarios que hayan permanecido inactivos en el sistema durante un tiempo definido mediante un parámetro que especifique este tiempo.
20. El SGDEA debe permitir la inclusión en los reportes generados de un rótulo que permita identificar su nivel de clasificación (clasificado, reservado, restringido, entre otros), de acuerdo con la clasificación asignada mediante parámetro al momento de su creación.
21. El SGDEA debe permitir la creación y administración de usuarios, roles y permisos y alinearse con el Servicio de Identidad de la DIAN.
22. El SGDEA no debe limitar el número de roles o grupos que se puedan configurar.
23. El SGDEA debe permitir revocar privilegios de un grupo o usuarios seleccionados.

24. El SGDEA debe ofrecer opciones de configuración para asignar o eliminar roles después de un período predefinido automáticamente.
25. El SGDEA debe permitir configurar controles restringir el acceso de acuerdo con los perfiles configurados por el administrador del sistema.
26. El SGDEA debe hacer accesible el contenido de las unidades documentales de acuerdo con los roles y permisos.
27. El SGDEA debe heredar los permisos de acceso a las Unidades Documentales de acuerdo con el permiso que tenía en los servicios de Modernización (NSGT, NSGA, NSGC, entre otros).
28. El SGDEA debe garantizar que solamente el usuario que apertura o gestiona una unidad documental y su jefe inmediato puedan reasignar permisos a las unidades documentales o de acuerdo con los accesos y permisos parametrizados a nivel nacional.
29. El SGDEA debe contar con rol de usuario para el módulo de administración.
30. El SGDEA debe permitir al jefe de cada dependencia realizar la asignación de permisos de consulta, acceso y gestión a unidades documentales, a los funcionarios de su dependencia, para su respectiva gestión.
31. El SGDEA debe permitir que se definan perfiles o roles de usuarios y que a cada perfil se le asignen varios usuarios.
32. El SGDEA debe cumplir el Lineamiento General para todos los servicios “Restricciones de impresión” de acuerdo con los usuarios y perfiles autorizados.
33. El SGDEA debe contener como mínimo los metadatos establecidos en el Art. 2.8.2.7.9. del Decreto 1080 del 2015.
34. El SGDEA debe validar y controlar la entrada de los metadatos mínimos obligatorios.
35. El SGDEA debe permitir la creación de formatos y formularios que contengan como mínimo los siguientes metadatos:
    - Identificador del sistema
    - Título
    - Descripción
    - Fecha / hora creación
    - Fecha / hora primer uso
    - Código
    - Versión
    - Lista de control de acceso
    - Historial de eventos

- Metadatos contextuales

36. Mediante interfaz gráfica el SGDEA debe permitir la edición de formatos y formularios
37. El SGDEA debe permitir a un usuario autorizado modificar el “Título”, la “Descripción” y los “Metadatos contextuales” de los formatos y formularios que puedan producirse en formato XML.
38. El SGDEA debe permitir que los formatos y formularios puedan producirse en formato XML, JSON u otro formato estándar.
39. El SGDEA debe permitir a un usuario autorizado las funciones de edición de formatos y formularios.
40. En el SGDEA las formas y formularios deben estar disponibles solo para los usuarios que intervienen en el proceso al que están asociados.
41. El SGDEA debe auto complementar los campos definidos en los formularios al momento de registrar datos por parte del usuario. Por ejemplo, generar listas desplegables para los campos que así lo requiera.
42. El SGDEA debe poder definir los campos como requeridos o no requeridos para un formato y/o formulario.
43. El SGDEA para la elaboración de los documentos, el sistema debe garantizar el uso de los formatos y/o formularios definidos en la entidad.
44. El SGDEA debe permitir:
    - Ver la lista de resultados de una búsqueda
    - Listar documentos que componen un resultado de la búsqueda
    - Ver la lista de todas las unidades documentales a cualquier serie determinada.
    - Incluir funciones para presentar en los medios adecuados la salida de los documentos, por ejemplo, documentos de audio y video.
    - Mostrar miniaturas de imágenes digitalizadas como una ayuda para la navegación y búsqueda.
45. El SGDEA debe permitir previsualizar documentos de la unidad documental, antes de realizar la descarga del documento.
46. El SGDEA debe permitir su asociación con los servicios ciudadanos digitales, especialmente con los servicios de autenticación digital.
47. El SGDEA debe incluir tecnologías de reconocimiento de datos, (de acuerdo a las necesidades y las que sean requeridas por la entidad):

    (OCR) Reconocimiento óptico de caracteres

    (HCR) Huella de la mano de reconocimiento de caracteres

(ICR) Reconocimiento inteligente de caracteres

(OMR) Reconocimiento óptico de marcas

Reconocimiento de código de barras

Reconocimiento de código QR

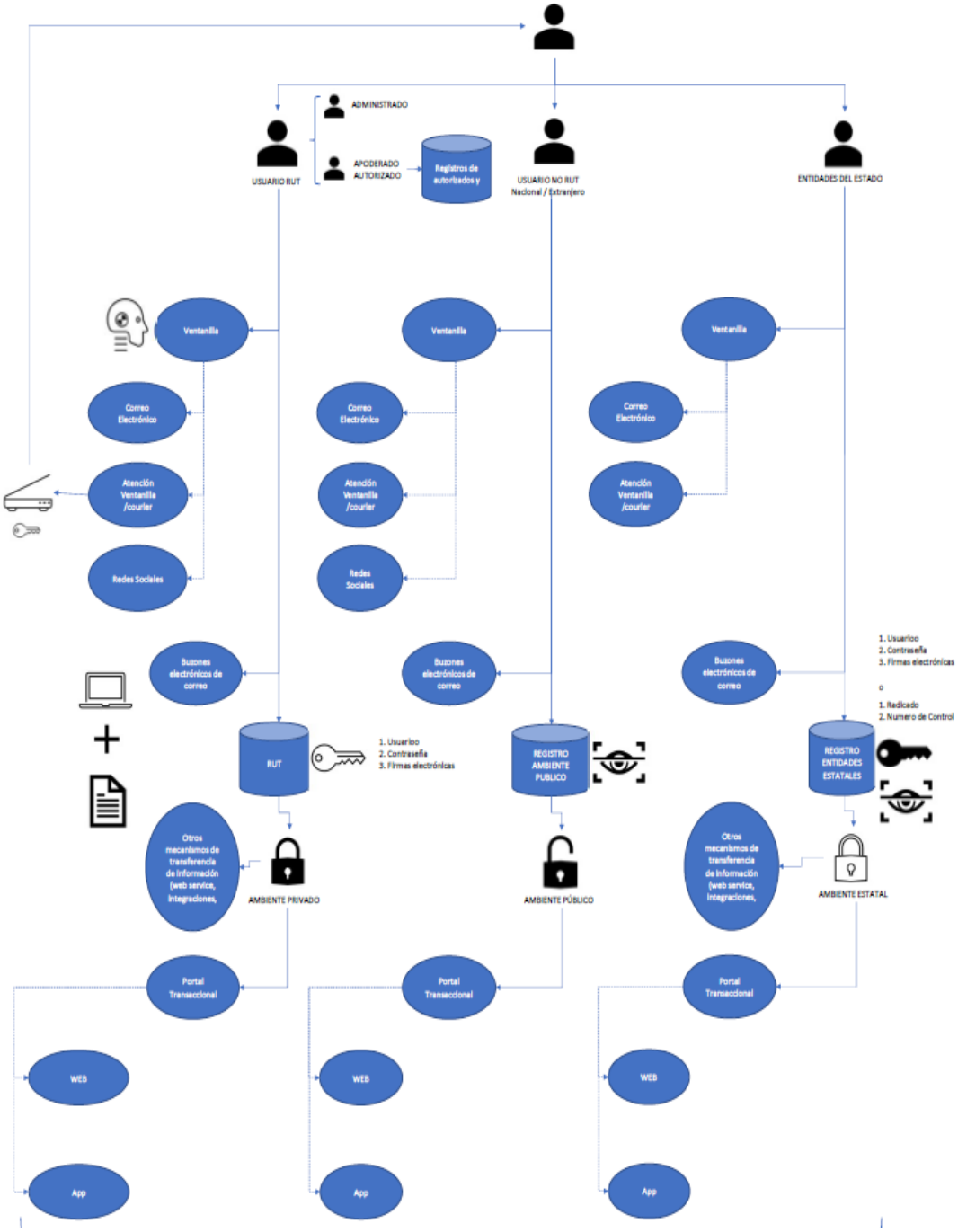
48. Seguimiento. El SGDEA debe permitirle al administrado o interesado realizar consulta por número de Radicación con numero de verificación (Numeral 104)
49. El SGDEA debe permitir que el Cuadro de Clasificación Documental - CCD y las Tablas de Retención Documental - TRD sean controladas únicamente por un rol administrador y que pueda agregar, modificar y reorganizar la estructura.
50. El SGDEA debe incorporar la producción documental conforme la estructura orgánico funcional en todos sus niveles según el esquema del Cuadro de Clasificación Documental.
51. El SGDEA debe garantizar que los documentos producidos y asociados a una TRD, mantengan los criterios de tiempos y de disposición final de la versión correspondiente.
52. El SGDEA debe permitir que las Tablas de Retención Documental tengan asociados los siguientes campos, entre otros: una descripción y/o justificación; Versión de la TRD, Fecha de creación y actualización de la TRD en el sistema, Identificador único cuando se crea, Fondo y codificación, Subfondo y codificación, sección y codificación, subsección y codificación, Dependencia y codificación, Serie y codificación, Subserie y codificación, Procedimiento, Definición, Disposición Final, Tiempos de Retención en Archivo de gestión y Central, Tipo de Soporte, nombre y firma de responsables, entre otros.
53. El SGDEA debe permitir a usuarios autorizados la selección y uso de las diferentes versiones de la Tabla de Retención Documental.
54. El SGDEA debe permitir exportar el directorio, de todas las unidades documentales y/o carpetas clasificadas en diferentes criterios y series documentales, indicando su contenido.
55. El SGDEA debe permitir la transferencia de la estructura la TRD mediante un archivo XML, XROAD, JSON o el reglamentado por el Archivo General de la Nación.
56. El SGDEA debe garantizar que cualquier cambio a un tiempo de retención y disposición se aplique inmediatamente a todas las series, subseries a las que se asigna.
57. El SGDEA debe contar con control de trazabilidad de cada documento
58. La unidad documental creada en el sistema debe quedar asociada a una serie y/o subserie contenida en las tablas de retención parametrizadas.
59. El SGDEA debe permitir que los documentos que componen la unidad documental hereden los tiempos de conservación establecidos en la TRD.

60. El SGDEA debe garantizar la estructura de la unidad documental asegurando que los vínculos archivísticos se conserven en todo momento.
61. El SGDEA debe restringir y generar una alerta cuando se importe un documento en un formato no configurado en el sistema e indicar al usuario los formatos permitidos.
62. Se deberán utilizar mecanismos electrónicos seguros, para garantizar la integridad, autenticidad y disponibilidad en el tiempo de manera que no puedan ser modificados, eliminados o reemplazados conforme a los lineamientos tecnológicos establecidos por el Ministerio de las Tecnologías de la Información y las Comunicaciones y los lineamientos archivísticos establecidos por el Archivo General de la Nación.
63. El SGDEA debe permitir que el administrado o interesado pueda realizar consultas del estado de sus escritos y solicitudes por medio de ventanilla, canales de atención telefónico y por los ambientes transaccionales desde la web o la app, en Ambiente Público, Ambiente Privado y Ambiente Entidad Estatal, según se requiera e integrado con las soluciones destinadas para este fin.
64. El SGDEA debe permitir identificar a través de una marca la opción de impresión física de los documentos. De lo contrario, se atenderá por los canales electrónicos informados por el administrado y/o interesado.
65. El SGDEA no debe limitar la duración de los tiempos de retención para parametrizar las Tablas de Retención Documental.
66. El SGDEA debe asegurar la disponibilidad y preservación a largo plazo de las Unidades Documentales que tengan como disposición final “Conservación Total” de acuerdo con la TRD.
67. El SGDEA debe cumplir con el Acuerdo 003 de 2015, Artículo 13°. Garantías de conservación y preservación a largo plazo, AGN. Los documentos electrónicos podrán conservarse, ya sea en el mismo formato a partir del que se originó el documento o en otro cualquiera que asegure su originalidad, así como la autenticidad, la integridad, la disponibilidad y confiabilidad necesaria para reproducirlo. Así mismo la autoridad deberá garantizar que la migración de los documentos electrónicos a otros formatos y soportes que garanticen la conservación y preservación a largo plazo, el acceso y la disponibilidad en el tiempo establecido en las Tablas de Retención Documental.
68. Utilizar formatos que garanticen la preservación a largo plazo de los documentos electrónicos (Tabla 2).
69. Permitir impresión y descarga de adjuntos desde la página web (en los ambientes público, privado y entidad estatal y en las interfaces graficas de usuario externo, no debe permitir impresiones al interior de la entidad, de acuerdo con la parametrización y restricción de uso de papel).
70. Cuando se requiera exportar, transferir, migrar y visualizar los documentos se debe garantizar la integridad de las unidades documentales, respecto a:

- Componentes de la unidad documental (documento electrónico, foliado, índice firmado y metadatos);
- Contenido de la unidad documental (documentos, videos, audio, imagen, entre otros)
- Estructura de los documentos, preservando las relaciones correctas entre ellos.
- Debe permitir vistas de los Documentos Electrónicos de Archivo que carecen de la aplicación utilizada para generarlos (por ejemplo, planos de AutoCAD)
- Debe permitir dentro de la unidad documental la conservación de correos electrónicos de entrada y de salida que contengan o no archivos adjuntos, considerándolos como un solo Documento Electrónico de Archivo, respetando su contenido, contexto y estructura.

71. En SGDEA debe tener implementados todos los flujos de la Gestión documental mencionados en el presente documento.
72. El SGDEA debe permitir la administración y control de los procesos por lotes y los procesos automáticos programados.
73. Los flujos con los que viene diseñada la solución no debe tener limitaciones.
74. El SGDEA debe permitir al usuario del flujo de trabajo electrónico:
    - Visualizar las actividades que tiene pendientes por realizar
    - Priorizar por diferentes criterios
    - Visualizar información en tiempo real sobre el desempeño de sus procesos.
75. El SGDEA debe tener posibilidad de integrarse con una herramienta BPMS que eventualmente pudiera proveer la DIAN.

76. El SGDEA debe permitir la creación, administración y ejecución de flujos de trabajo electrónicos.



Gráfica 11. Entradas al proceso documental
Fuente: Elaboración Propia

77. El SGDEA debe permitir diagramar y modelar flujos de trabajo electrónicos.
78. El SGDEA debe permitir diagramar tareas que componen un proceso y/o procedimiento.
79. El SGDEA debe permitir parametrizar los tiempos de ejecución y respuesta de los procesos ejecutados.
80. El SGDEA debe permitir incorporar un mecanismo de simulación para analizar los flujos de trabajo modelados.
81. El SGDEA debe permitir la parametrización de Reglas para la configuración y gestión de:
    - Estados del Flujo de Proceso
    - Validación de Actividades
    - Definición y asignación de usuarios
82. El SGDEA debe permitir parametrizar los accesos, creación, modificación o control total para usuarios o grupos de usuarios de los flujos de trabajo electrónicos.
83. El SGDEA debe permitir visualizar de manera gráfica el estado de cada flujo de trabajo electrónicos.
84. El SGDEA no debe limitar el ingreso de acciones que componen cada flujo de trabajo electrónico.
85. El SGDEA debe permitir contener múltiples versiones de un mismo proceso y/o procedimiento. Debe permitir al administrador seleccionar la última versión.
86. El SGDEA debe generar los flujos de trabajo electrónicos en un formato estándar.
87. El SGDEA debe generar un identificador único para cada flujo de trabajo electrónico.
88. El SGDEA debe generar una trazabilidad de las acciones de los flujos de trabajo electrónicos e incluirla en las pistas de auditoría
89. El SGDEA debe permitir solo a un rol administrador autorizado a crear, parametrizar, administrar y poner en ejecución flujos de trabajo electrónicos

    Duración real de los procesos versus el tiempo estimado de duración

    Actividades que tienen mayor porcentaje de retraso.
90. El SGDEA debe permite definir los flujos de trabajo electrónicos basado en plantillas.
91. El SGDEA debe permitir detener un flujo de trabajo electrónico.
92. El SGDEA debe permitir definir los tiempos límite de ejecución de los flujos y de cada una de sus actividades enviando alertas de incumplimiento.
93. El SGDEA debe permitir contar con semáforos que muestran el cumplimiento de tiempos en cada una de las actividades de un flujo.

94. El SGDEA debe ofrecer opciones de alertas de vencimientos de términos, tiempos de retención y demás, según se detallan en cada flujo. Con las opciones de correo electrónico, pop-up.
95. El SGDEA debe proveer información de contexto e información del estado del usuario en todo momento.
96. El SGDEA debe permitir al usuario gestionar las ventanas (modificar el tamaño y posición, minimizar, maximizar, cerrar la ventana, etc.), y que se guarden estas especificaciones en un perfil de usuario.
97. El SGDEA debe proveer al menos dos interfaces para la Gestión del ECM (Enterprise Content Management o Gestión de Contenido Empresarial) y sus componentes:
    - Interface de comandos
    - Interface gráfica de usuario
98. El SGDEA debe garantizar que se estandarice el manejo de las excepciones por capa del sistema, errores del sistema, mensajes al usuario final, alertas o confirmaciones; con el fin de informar al usuario final el estado de su sesión en el sistema.
99. El SGDEA debe permitir la personalización de los mensajes de error que se presentan a los usuarios y la personalización de los diferentes mensajes de correos que se envían a los usuarios en los diferentes eventos.
100. El SGDEA debe permitir la parametrización (nombres, ocultamiento y visualización, orden de presentación, tipo de información, reglas o lógica) de los campos en pantallas, formularios, formas, y consultas creadas y/o pre-automatizados.
101. El SGDEA debe almacenar los objetos digitales de forma separada a la base de datos con los controles y permisos establecidos en cada servicio en el que sea requerida dicha función.
102. El SGDEA debe permitir incorporar documentos sonoros, visuales y audiovisuales.
103. El SGDEA debe garantizar para todo el sistema, un esquema de URL limpios el cual se debe caracterizar por lo siguiente: o Corresponder a la jerarquía del sitio. o No incluir caracteres especiales como $, &, ?,= entre otros
104. El SGDEA debe funcionar en diferentes modos de comunicación y tipologías de red. Debe estar en la capacidad de funcionar correctamente en conexiones LAN, WAN, Internet o Wifi.
105. El SGDEA debe contar con un módulo de ayuda en línea.
106. El SGDEA deberá estar disponible las 24 horas del día, 7 días de la semana, 365 días del año.

107. El SGDEA debe ser escalable y no permitir ninguna característica que impida su uso en organización de pequeño o gran tamaño, permitiendo aumentar la capacidad del sistema para ofrecer más servicios a un mayor número de usuarios sin degradar la calidad del servicio.

108. El SGDEA debe ofrecer soporte para sistemas de almacenamiento tipo NAS, DAS y SAN.

109. El SGDEA de garantizar que cuando se produzca un fallo del software o del hardware, debe resultar posible devolver el sistema a un estado conocido (más reciente que la copia de seguridad del día anterior) en menos de 02 horas de trabajo con el hardware disponible.

110. El SGDEA debe proporcionar en todo momento al usuario final y al administrador funciones de uso fácil e intuitivo.

111. El SGDEA debe ser 100% web y su administración y parametrización debe realizarse desde el navegador. Se deben proveer interfaces de escritorio opcionales.

112. El SGDEA debe poseer un diseño “Responsive” a fin de garantizar la adecuada visualización en múltiples computadores personales, dispositivos, tabletas y teléfonos inteligentes.

113. El SGDEA se debe ejecutar y visualizar correctamente sobre los siguientes navegadores y las últimas versiones de: Firefox Mozilla, Edge, Chrome, Opera.

114. El SGDEA debe ser diseñado y construido con los mayores niveles de flexibilidad en cuanto a la parametrización de los tipos de datos, de tal manera que la administración del sistema sea realizada por un administrador funcional del sistema.

115. El SGDEA debe permitir acceso a todas las funcionalidades y a cualquier interfaz de la aplicación a través del teclado.

116. El SGDEA debe permitir que las interfaces gráficas del sistema puedan ser parametrizables y por tanto permita actualizar, cambiar o crear los logos, imágenes, fondos, etiquetas, títulos, banners y mensajes de acuerdo con las características de diseño DIAN.

117. El SGDEA debe auto complementar los campos definidos en los formularios al momento de registrar datos por parte del usuario. Por ejemplo, generar listas despegables para los campos que así lo requiera.

118. El proveedor deberá proveer un diseño de la interfaz del SGDEA versión escritorio y móvil centrado en la experiencia del usuario. Se deben considerar aspectos como la accesibilidad, seguridad y usabilidad, de acuerdo con los lineamientos establecidos por la entidad.

119. El proveedor de la solución deberá entregar a la Entidad un prototipo antes de la implementación. Este prototipo se utilizará para llevar a cabo pruebas de usabilidad y

accesibilidad, identificar posibles barreras y considerar mejoras que puedan ser incorporadas en la solución final.

120. El SGDEA debe poder adaptarse y cumplir rigurosamente con los lineamientos gráficos de Experiencia de Usuario (UX) de la DIAN, sin admitir ninguna excepción, particularmente en lo que respecta a los componentes transversales como lo son: la barra de accesibilidad, la barra GOV.CO, el cabezote, los colores, los enlaces y las pestañas, la iconografía, la marca DIAN, el pre pie y pie de página GOV.CO y las tipografías. Estos componentes desempeñan un papel esencial para mantener la coherencia visual y la identidad de las soluciones tecnológicas asociadas. Asimismo, se requiere a los contratistas interesados en la adjudicación que adopten, en la medida de lo posible, los componentes generales y de formularios, con el fin de garantizar una experiencia de usuario consistente y de calidad.

121. El SGDEA debe ser capaz de realizar una búsqueda sencilla en 3 segundos y una búsqueda compleja (combinando criterios) en máximo 5 segundos, con independencia de la capacidad de almacenamiento y el número de documentos en el sistema.

122. Toda funcionalidad del sistema y transacción de negocio realizada en el SGDEA debe responder al usuario en menos de 5 segundos.

123. El SGDEA debe ser capaz de soportar el Número de Usuarios: Total de funcionarios de la DIAN.

124. El SGDEA debe permitir cargue de adjuntos de 50 mb o más, tanto por parte de los usuarios externos como internos.

125. El SGDEA debe permitir la expansión controlada del sistema mínimo de 4.000 usuarios sin perjudicar la continuidad y eficacia.

126. El SGDEA debe estar en la capacidad de operar con infraestructura de clustering a nivel de servicio, debe ser escalable y dispuesta a través de balanceador de carga.

127. El SGDEA debe estar en capacidad de almacenar y gestionar grandes volúmenes de contenido de manera rápida, segura y eficiente. Ejemplo: backups de base de datos, repositorios electrónicos, información contenida en discos duros, memorias extraíbles, CD, DVD, cintas.

128. El SGDEA debe evolucionarse tecnológicamente de acuerdo con las nuevas versiones.

129. El SGDEA debe permitir programar rutinas de copia de seguridad (backup) y su recuperación cuando sea necesario.

130. El SGDEA debe permitir la parametrización de copias de seguridad de los documentos en conjunto con los metadatos.

131. El SGDEA debe alertar al usuario encargado, fallas críticas en los servicios del sistema en el instante en que se presentan.

132. El SGDEA debe permitir la fácil instalación y despliegue de plugins y desarrollos personalizados.

133. El SGDEA debe integrarse con el Sistema de Identidad de la DIAN, entre otros debe cumplir, heredar e interoperar las siguientes funcionalidades:

- El SGDEA debe estar vinculado al Servicio de Identidad de la DIAN, para controlar los permisos y accesos.
- El SGDEA se debe acoplar a las funcionalidades que permiten autenticación, autorización, administración y almacenamiento de datos de usuarios.

134. El SGDEA debe soportar diferentes mecanismos de autenticación.

135. El SGDEA debe permitir la definición por parámetro y controlar la longitud mínima y máxima de las contraseñas.

136. El SGDEA debe permitir la definición por parámetro y controlar el número de contraseñas a recordar (Histórico de contraseñas).

137. El SGDEA debe permitir la definición de un diccionario de contraseñas no válidas y controlar que las contraseñas no coincidan con las existentes en dicho diccionario.

138. El SGDEA debe controlar mediante parámetro la complejidad de la contraseña. Cuando se habilita la complejidad, la contraseña debe tener una combinación de caracteres numéricos, alfabéticos (Mayúsculas y Minúsculas) y signos o caracteres especiales.

139. El SGDEA debe permitir definir por parámetro y controlar la vigencia mínima, vigencia máxima y tiempo de aviso de vencimiento, de las contraseñas.

140. El SGDEA debe permitir manejar los siguientes estados para las cuentas de usuario: Habilitado, deshabilitado, bloqueado, suspendido.

141. El SGDEA debe permitir a un usuario autorizado parametrizar el número de intentos fallidos de ingreso a la sesión.

142. El SGDEA deberá bloquear al usuario una vez se hayan completado el número de intentos fallidos configurados por el usuario autorizado para el inicio de sesión y alertar mediante un mensaje.

143. El SGDEA debe permitir que las contraseñas nunca pueden ser almacenadas en formato texto. Deben ser almacenadas por medio de un algoritmo de encriptación de una sola vía reconocido por la industria como MD5 y SHA. Para estos procesos de cifrado se deben utilizar llaves cuya longitud mínima sea de 128 bits.

144. El SGDEA debe permitir marcar un usuario individual como inactivo, sin eliminarlo del sistema por medio del servicio de Identidad de la DIAN.

145. EL SGDEA debe contar con mecanismos de recuperación de credenciales de acceso obedeciendo las políticas de ingreso seguro.

146. El SGDEA debe permitir la generación de registros de control o hashes que permitan validar la integridad de los registros de seguridad generados.

147. El SGDEA debe generar y mantener pistas de auditoria inalterables de las acciones realizadas por cada uno de los usuarios que ingresan al sistema.

148. El SGDEA debe mantener las pistas de auditoría en el sistema durante el tiempo que se haya establecido en las políticas de la Entidad y las normas aplicables.

149. El SGDEA debe permitir rastrear de forma automática y sin ninguna intervención manual todas las acciones realizadas en el sistema, y almacenar los datos sobre estas en la pista de auditoría.

150. El SGDEA debe registrar cualquier intento de violación de los mecanismos de control de acceso en las pistas de auditoría.

151. El SGDEA debe impedir desactivar la generación y almacenamiento de las pistas de auditoría.

152. Las pistas de auditoría del SGDEA deben permitir identificar los errores en la ejecución de los procesos. (Mantenimiento en menor tiempo).

153. El SGDEA debe permitir generar informes con los datos almacenados en las pistas de auditoría, permitiendo filtros y selección de criterios establecidos por el usuario solicitante.

154. El SGDEA debe mantener la pista de auditoría durante el tiempo necesario, que al menos abarcará el ciclo de vida de los documentos de archivo o expedientes electrónicos a los que hace referencia.

155. El SGDEA debe permitir consignar en la pista de auditoría todas las modificaciones realizadas en los parámetros administrativos, como creación de usuarios, grupos, perfiles, modificación de derechos de acceso.

156. El SGDEA debe ser capaz de exportar la pista de auditoría de determinados documentos, sin que ello repercuta en la almacenada por el sistema.

157. El SGDEA debe mantener una pista de auditoría inalterable, capaz de capturar y almacenar de forma automática información sobre:

Todas las operaciones relacionadas con los documentos electrónicos y los metadatos.

El usuario que inicia o realiza la operación:

La fecha y la hora de la operación.

Debe consignar las pista de auditoría todas las operaciones que afecten a:

Documentos electrónicos de archivo ,Documentos electrónicos

Metadatos relativos a cualquiera de los elementos anteriores.

El SGDEA debe como mínimo se debe efectuar registro en la pista de auditoría de:

La fecha y la hora de la captura de todos los documentos electrónicos.

La reclasificación de un documento electrónico.

Cualquier modificación realizada en los metadatos asociados a los documentos electrónicos.

La fecha y la hora de creación, modificación y eliminación de los metadatos.

Los cambios realizados en los privilegios de acceso relativos a un documento electrónico o bien a un usuario.

158. El SGDEA debe capturar y almacenar en las pistas de auditoría, como mínimo información sobre:

Toda acción realizada sobre cada documento, unidad documental, usuario y metadatos;

Toda acción realizada en los parámetros de administración;

Usuario que realiza la acción;

Fecha y hora de la acción;

Cambios realizados a los metadatos;

Cambios realizados a los permisos de acceso;

Creación, modificación o eliminación de usuarios, grupos o roles del sistema;

País, navegador, dirección ip, tipo de dispositivo, sistema operativo, desde donde fue abierta la sesión del sistema.

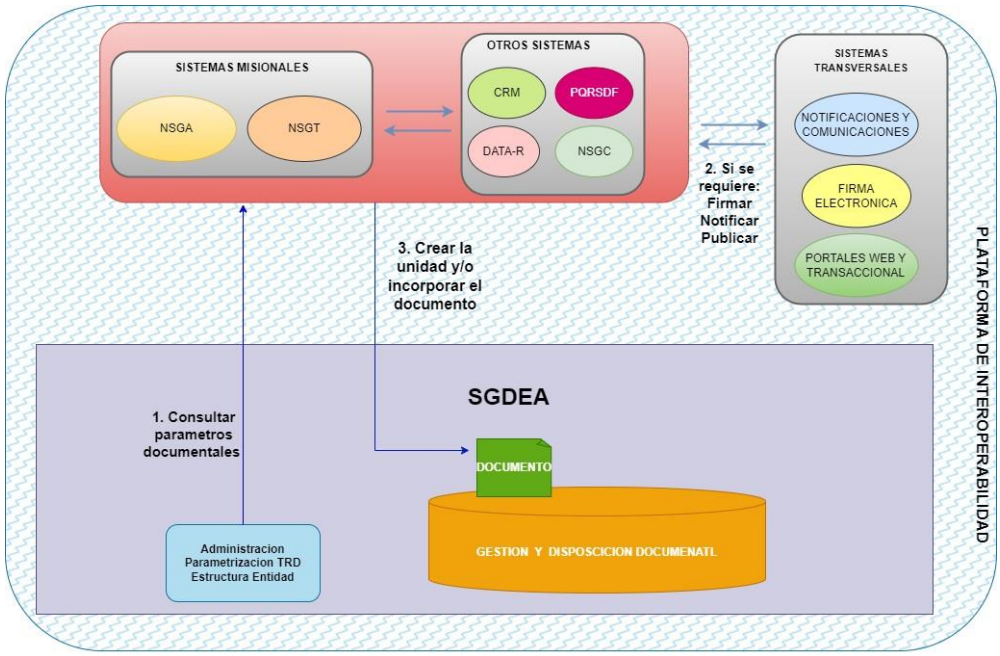
159. EL SGDEA debe aplicar técnicas criptográficas en las operaciones y/o transacciones críticas o sensibles para la organización.

160. Garantizar recuperación de documentos o registros eliminados incorrectamente.

161. Cuando el SGDEA realice procesos de importación o exportación de información, deberá realizarse a través de interfaces seguras y aplicar protocolos y mecanismos de seguridad.

162. EL SGDEA debe garantizar que las operaciones realizadas en el sistema deben estar protegidas contra adulteración, supresión, ocultamiento y demás operaciones que atenten contra la autenticidad, integridad y disponibilidad de la información.

163. El SGDEA debe permitir contar con procedimientos automáticos para copias de seguridad y restauración encaminados a realizar copias periódicas de seguridad de todos elementos dentro del sistema (carpetas, documentos, metadatos, usuarios, roles, permisos, configuraciones específicas).



Gráfica 12. Interacción entre sistemas internos y SGDEA
Fuente: Elaboración Propia

164. Debe permitir cifrar los documentos y hacer imposible su consulta por fuera del SGDEA

165. Debe cumplir con las políticas de seguridad y privacidad de la DIAN establecidas para los lineamientos de Protección de Datos Personales.

166. El SGDEA debe garantizar que las transacciones u operaciones que realice el sistema las cuales presenten fallos en su ejecución deben reversarse al estado inicial en la ejecución del proceso. (rollback) (evita envío de información incompleta y perdida de esta).

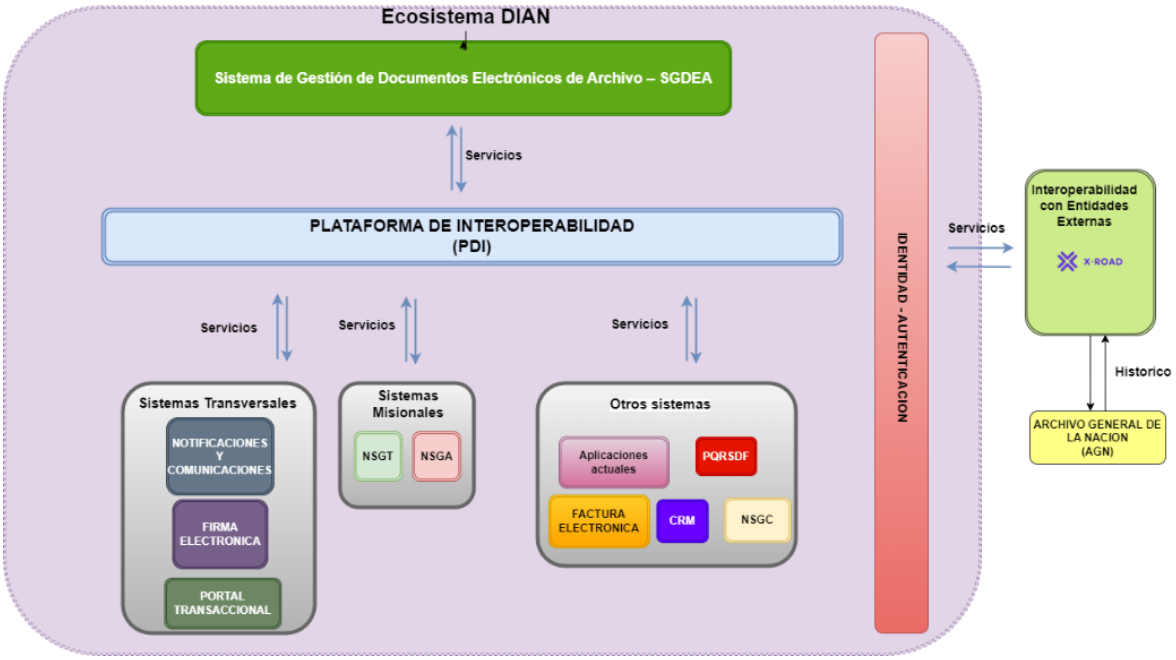
167. Gestión de Permisos de acceso mediante los servicios de identidades de la UAE-DIAN, conforme con los requerimientos establecidos por las áreas cliente.

168. Cuando el SGDEA realice procesos de importación o exportación de información, deberá realizarse a través de interfaces y aplicar protocolos y mecanismos de seguridad.

169. Se debe interoperar con las soluciones acordadas, al momento de la puesta en producción.

170. El SGDEA debe estar en capacidad de entregar los documentos recibidos a otros flujos de proceso y otros S.I. misionales y legados, para que estos puedan realizar la gestión y trámite de los documentos.

171. El SGDEA al realizar integraciones deben cumplir con el marco de interoperabilidad de la DIAN y los lineamientos y políticas de seguridad de la información de la DIAN.



Gráfica 13. Diagrama de Arquitectura DIAN relacionado con el SGDEA
Fuente: Elaboración Propia

172. El SGDEA debe ser interoperable con otros componentes definidos por la entidad, mediante la plataforma de interoperabilidad (PDI) provista por la entidad

173. El SGDEA debe cumplir como mínimo con los siguientes estándares de interoperabilidad: OAI-PMH y CMIS-OASIS, para garantizar la interoperabilidad con otros sistemas, requisito establecido por el AGN en el modelo de requisitos de documentos electrónicos (ejemplo transferencias históricas al AGN).

174. El SGDEA debe integrarse a la plataforma de correo utilizada por la entidad para el envío de los avisos de asignación o alertas a los usuarios.

175. La integración del módulo de gestión del SGDEA y los sistemas de gestión de orden superior debe garantizarse a través de mecanismos de interoperabilidad estándar como SNMP, XML SOAP - REST, X-ROAD etc.

176. Las comunicaciones externas entre servidores de datos, aplicaciones, repositorios deberán estar encriptadas mediante algoritmos de seguridad como AES (Estándar de encriptación avanzada) función SHA-256, IDEA (Algoritmo Internacional de Encriptación de datos), DES, 3DES, RSA, RC5.

177. El SGDEA debe integrarse con el servicio de identidad de la DIAN.

178. El SGDEA debe permitir la gestión de documentos en las diferentes aplicaciones (traslado de documentos entre aplicaciones, cambios de índices, anexo o eliminación de páginas, etc.).

179. El SGDEA debe facilitar procesos de interoperabilidad mediante el consumo de API's y/o web services con los sistemas de información de la entidad.

180. El SGDEA debe tener Interoperabilidad con otros sistemas externos, debe cumplir con el marco de interoperabilidad con otros sistemas de las entidades públicas dando cumplimiento al Marco de Interoperabilidad del Estado Colombiano, como por ejemplo, se señala en la Circular Externa Única del 15 de Julio de 2022 "Las entidades deberán adoptar las políticas, medidas y estándares necesarios para asegurar la preservación y conservación documental en el ciclo de vida de la información institucional (independientemente del sistema que los generó, tramitó o en el cual se conservan), con el fin de facilitar su consulta en el tiempo y realizar la disposición final de acuerdo con sus instrumentos archivísticos. Es responsabilidad de las Entidades Estatales la disposición final de las unidades documentales de los procesos de contratación, de acuerdo con sus Tablas de Retención Documental – TRD y su actividad derivada de la valoración documental - TVD, luego de cumplido el plazo de retención mínimo, de acuerdo con la normativa vigente, contados a partir de la terminación del plazo del contrato o de su liquidación cuando esta es obligatoria. En este sentido, la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente, en su función de administración del SECOP, es responsable de asegurar la inalterabilidad y disponibilidad de la información gestionada a través de las diferentes plataformas, y no está autorizada a realizar procesos de sustracción, destrucción, u ocultamiento de esta información."

181. El SGDEA debe estar orientado a asegurar los documentos que ingresan a la entidad, independientemente de su formato, permitir el tráfico masivo de información y el intercambio de datos y documentos con los sistemas legados de la entidad y sus nuevos desarrollos.

182. El SGDEA debe habilitar integraciones e interoperabilidades para la consulta y seguimiento de los documentos (trámites, comunicaciones, PQRS, denuncias, etc.) deberá poder adelantarla el SI de manera centralizada y uniforme (atendiendo las restricciones que otorguen los roles, permisos de acceso y ambientes transaccionales) de

cara al administrado, el interesado y los funcionarios de la UAE-DIAN, cada uno con tableros de control o semáforos de seguimiento y control de tiempos.

183. El SGDEA debe entregar los documentos recibidos a cada flujo documental, sea este desarrollado dentro del mismo servicio o en aplicativos legados o nuevos desarrollos, para que estos a su vez hagan la entrega al gestor documental.

184. El SGDEA debe permitir la elaboración de documentos desde la solución SGDEA, lo que le exige contar con integraciones a las herramientas ofimáticas, también debe permitir que los sistemas legados, así como las nuevas soluciones, le entreguen los documentos que estos elaboran; de manera automática deberá generar las certificaciones de notificación, certificaciones de ejecutoria y las constancias de comunicación.

185. El SGDEA debe permitir integración con la página web de la entidad, los sistemas legados de la DIAN y los nuevos desarrollos, independientemente de su enfoque (apoyo, misional, estratégico, etc.), lo mismo que con entidades externas con las que se requiera intercambio de información, siguiendo las políticas y lineamientos de la OSI. Estas integraciones deben permitir hacer trazabilidad de forma centralizada a todo documento (tramite, comunicación oficial, denuncia), independientemente del canal o SI por el que haya ingresado.

186. El SGDEA debe permitir la integración con los diferentes servidores de correo electrónico y otras plataformas como ventanilla única, portal web, redes sociales, APP, entre otros, y diferentes dependencias, cuando la unidad documental no proviene en su totalidad de un sistema.

187. El SGDEA debe proveer servicios de integración con herramientas de correo electrónico, para emitir advertencias de vencimiento de tiempo para responder requerimientos, envío automático de respuestas por correo electrónico a los usuarios que hayan solicitado tal servicio.

188. El SGDEA debe incorporar de funcionalidades que permitan la integración de soluciones de correo electrónico certificado.

189. El SGDEA debe tener integración con los servicios ciudadanos digitales en lo referente firmas, entrega de documentos en la carpeta ciudadana y consumos de documentos de la carpeta ciudadana y demás funcionalidades que los servicios ciudadanos digitales ofrezcan.

190. El SGDEA debe contar con una interfaz gráfica que permita al administrador del sistema crear o modificar las parametrizaciones de configuración del software y todos sus componentes, entre ellos puertos de comunicación, instancias de nombre de base de datos, IP's, URL de repositorios y los demás requeridos para la operación óptima del sistema en su totalidad.

191. El SGDEA en caso de presentarse fallas durante la restauración de las copias de seguridad debe permitir alertar sobre el fallo y los detalles del mismo, para que el administrador tome las decisiones necesarias para subsanar los errores.

192. El SGDEA debe permitir que los administradores de forma controlada y sin ningún esfuerzo innecesario, recuperen, visualicen y reconfiguren parámetros del sistema y opciones escogidas en el momento de la configuración, como los elementos que se indexan, así como la asignación de usuarios y funciones a otros perfiles de usuarios.

193. El SGDEA debe permitir supervisar el espacio de almacenamiento disponible y avisar a los administradores cuando convenga intervenir, ya sea por escasez de espacio, o porque sea necesario alguna otra medida de tipo administrativo.

194. El SGDEA debe permitir ser compatible con protocolo IPV6 tanto en la configuración del software, hardware y dentro del funcionamiento del sistema. En caso de almacenar, referenciar enlaces o almacenamiento de direcciones físicas IP debe ser transparente la interacción para toda la plataforma y el sistema en general. El cambio de direccionamiento IPV4 a IPV6 no debe generar errores o mal funcionamiento del software y sus componentes y en caso de presentarse, los corregirá o solucionará inmediatamente.

195. El SGDEA debe ser 100% web, es decir accedido mediante protocolo de transferencia https y debe estar en la capacidad para operar con protocolo de comunicación SSL implementado.

196. El licenciamiento debe cubrir todos los tipos de usuarios/roles necesarios para la operación, administración y mantenimiento de la Solución.

197. El licenciamiento debe cubrir la totalidad de usuarios, este número está dado por la total de funcionarios de la DIAN y previendo el crecimiento de la Planta a futuro.

198. Se deben entregar licencias, sin limitaciones al número de usuarios que accedan a los servicios a través de la Solución y de manera independiente al número de productos/componentes que la conformen.

199. La Solución debe incluir el licenciamiento de todos los componentes propios y de terceros necesarios para cumplir con los requerimientos descritos en este documento.

200. Se debe brindar un esquema de licenciamiento para los entornos/ambientes de Pruebas, Preproducción, Producción, Capacitación y Contingencia que se establezcan para la Solución, que cumpla con el número de Usuarios definidos por la DIAN o según el modelo de licenciamiento.

201. Se debe garantizar que la Solución ofrecida (y cualquiera de sus componentes) esté libre de restricciones y que pueda ser instalada y mantenida por el personal técnico de la DIAN o quien la DIAN designe.

202. El licenciamiento debe ser portable entre diferentes plataformas de manera que el DIAN pueda migrar la Solución a su propia infraestructura o a la de un tercero sin que esto implique un costo adicional.

203. No debe existir límite territorial para la instalación y el uso de la Solución y esta puede ser utilizada directa o indirectamente por la DIAN.

204. Todo el software que haga parte de la Solución debe tener licencia y estar registrado a nombre de la DIAN.

205. La DIAN podrá desarrollar, extender, adaptar, modificar y configurar el código fuente de la Solución de acuerdo con las necesidades de la entidad, sin costos adicionales.

206. En el caso en que el Contratista utilice total o parcialmente un nuevo software de su propiedad o de un tercero con posterioridad al inicio del Proyecto, deberá notificar y solicitar la autorización a la DIAN.

207. El licenciamiento de la solución adquirido por la DIAN es a perpetuidad.

208. El sistema deberá enviar mensajes automatizados tanto al remitente, al funcionario y/o dependencia asignada para atender estas solicitudes o requerimientos.

1- El sistema deberá generar alertas automatizadas al remitente sobre la recepción y radicación del documento, incluyendo detalles relevantes como el número de radicación y la fecha estimada de atención.

2-El sistema deberá generar alertas automatizadas a los funcionarios sobre la recepción y radicación de los documentos asignados.

3- El sistema deberá permitir generar alertas del funcionario a otros funcionarios competentes del trámite.

209. El sistema deberá contar con una funcionalidad que lo integre con los servicios ciudadanos digitales, especialmente con los servicios de autenticación digital.

1- El sistema deberá permitir una autenticación por medio de esta funcionalidad.

2- El sistema deberá permitir la parametrización de los diferentes métodos de autenticación, de acuerdo con lo determinado por la Oficina de Seguridad de la Información.

210. El sistema debe garantizar el enlace de las entradas, las salidas y las internas, cuando entre ellas exista una relación directa, que se debe ver en las trazas de seguimiento.

1- Cuando una radicación de entrada o salida no tiene relación con un documento previamente radicado, debe permitir ingresar el tipo de documento de identidad, número de identificación y con estos datos traer de Registro Único, la información requerida, editable ya que puede traer una dirección procesal.

2-Cuando se trate de una radicación de entrada, el sistema debe contemplar registro de datos del representado.

3- Cuando una radicación de entrada es respuesta a una radicación de salida, debe habilitarse el campo de referencia, para que al digitar el radicado de salida tome automáticamente los datos del emisor.

4- Cuando una radicación de salida es respuesta a una radicación de entrada, debe habilitarse el campo de referencia, para que al digitar el radicado de entrada tome automáticamente los datos del destinatario.

211. El sistema debe permitir visualizar el estado de cada comunicación oficial (Radicado, Asignado, en tránsito, pendiente, Finalizado, devuelto, entre otros) mediante un dashboard intuitivo.

212. El sistema debe integrarse con un sistema de correo electrónico certificado que refleje en la certificación: fecha, hora de envío, entrega y acceso y sean incorporados como metadatos según la estampa de tiempo de la misma.

1- El sistema debe generar constancias de entrega de correspondencia de salida, permitiendo la impresión o consulta de las constancias de entrega o devolución de la correspondencia.

2.2.3. Requerimiento de Operación del Servicio

1. Las soluciones y/o sistemas internos de la DIAN (misionales, de apoyo y demás), tendrán sus propios Flujos de Trabajo administrados y gestionados por cada una de las soluciones.
2. El tiempo de inactividad no prevista del SGDEA, no debe superar las 10 horas al trimestre y 40 horas al año.
3. El SGDEA debe contar con una mesa de servicio para los funcionarios y la atención de incidentes durante el periodo de garantía y soporte acordados entre las partes.
4. Cuando se realicen accesos directos a la base de datos del sistema SGDEA se deberá registrar cada transacción realizada por el usuario autenticado identificando como mínimo fecha y hora, dependencia, tipo de usuario, transacción realizada.
5. Se debe cubrir el mantenimiento del licenciamiento y actualización de versiones posteriores hasta la finalización del contrato. Se debe entregar a la DIAN las nuevas versiones sin que esto genere un costo adicional por el periodo de 3 años.

2.2.4. Requerimientos de Seguridad de la Información

Análisis de Riesgos

1. Modelado de amenazas de seguridad y privacidad de la información en los documentos de arquitectura de software
2. Plan de mitigación de vulnerabilidades de seguridad y privacidad de la información de los requisitos funcionales y no funcionales
3. Gestión de vulnerabilidades del software
4. Generar un plan de respuesta a incidentes del componente, producto o servicio desplegado

Registros de transacciones, Manejo de errores, logs y auditoria

5. Un mismo formato de logging debe ser utilizado en todo el sistema. Por ejemplo, [<timestamp>] [<log_level>] [<logger_name>] [<correlation id>] [<username>] - <message>
6. No difundir información sensible en respuestas de error, incluyendo detalles del sistema, identificador de sesión o información de la cuenta.
7. Implementar mensajes de error genéricos y utilizar páginas de error adaptadas.
8. La lógica para la gestión de errores debe estar asociada a que los controles de seguridad no permitirán acceso por defecto.
9. Todos los controles de registro de logs deben estar implementados en sistemas confiables.
10. El registro de logs para controles de acceso debe incluir tanto los casos de éxito como de falla.
11. Restringir el acceso a los logs solo a personal autorizado.
12. Restringir la funcionalidad de borrado de logs para cualquier usuario, incluido, el usuario super administrador.
13. No guardar información sensible en el registro de logs, incluyendo detalles innecesarios del sistema.
14. El registro de logs debe contener las fallas de validación de datos de entrada.
15. Registrar en un log todos los intentos de conexión con tokens inválidos o vencidos.
16. Registrar en un log todas las funciones administrativas, incluyendo cambios en la configuración de seguridad.
17. Registrar en un log, todas las fallas de conexión de SSL, TLS.
18. Utilizar una función hash para validar la integridad de los logs.
19. Generar y mantener pistas de auditoria inalterables de las acciones realizadas por cada uno de los usuarios que ingresan al sistema.

20. Mantener las pistas de auditoría en el sistema durante el tiempo que se haya establecido en las políticas de la Entidad y las normas aplicables.
21. Debe permitir rastrear de forma automática y sin ninguna intervención manual todas las acciones realizadas en el sistema, y almacenar los datos sobre estas en la pista de auditoría.
22. Debe registrar cualquier intento de violación de los mecanismos de control de acceso en las pistas de auditoría.
23. Impedir desactivar la generación y almacenamiento de las pistas de auditoría.
24. Generar informes con los datos almacenados en las pistas de auditoría, permitiendo filtros y selección de criterios establecidos por el usuario solicitante.
25. Mantener la pista de auditoría durante el tiempo necesario, que al menos abarcará el ciclo de vida de los documentos de archivo o expedientes electrónicos a los que hace referencia.
26. Permitir consignar en la pista de auditoría todas las modificaciones realizadas en los parámetros administrativos, como creación de usuarios, grupos, perfiles, modificación de derechos de acceso.
27. Exportar la pista de auditoría de determinados documentos, sin que ello repercuta en la almacenada por el sistema.
28. Debe capturar y almacenar en las pistas de auditoría, como mínimo información sobre:

    Toda acción realizada sobre cada documento, unidad documental, usuario y metadatos; Toda acción realizada en los parámetros de administración; Usuario que realiza la acción; Fecha y hora de la acción; Cambios realizados a los metadatos; Cambios realizados a los permisos de acceso; Creación, modificación o eliminación de usuarios, grupos o roles del sistema; País, navegador, dirección ip, tipo de dispositivo, sistema operativo, desde donde fue abierta la sesión del sistema.
29. Los datos de las transacciones y logs se deben guardar en lugares independientes a los datos de aplicación, con control de acceso independiente y no accesibles desde la red de usuarios.

Verificación de la administración de autenticación y contraseñas.

30. Soportar sistemas múltiples de autenticación, mínimo con los que cuente la Entidad o tenga en plan de adopción.
31. Se deben utilizar cuentas únicas en el sistema con el menor privilegio para todos los componentes de la aplicación, servicios y servidores.
32. Las cuentas que se usan para la comunicación entre los componentes de una aplicación deben estar asociado a una entidad o función específica.

33. No utilizar cuentas que tengan privilegios administrativos o cuentas por defecto para la comunicación entre los componentes de una aplicación, como cuentas de administrador por defecto de los sistemas operativos, bases de datos, entre otros.
34. Las cuentas genéricas de un software o aplicación, es decir, que no estén asociadas a una entidad o función deben ser deshabilitadas durante el despliegue y permanecer deshabilitadas en operación.
35. Todas las comunicaciones entre componentes, APIs, el middleware y las capas de datos, deben ser de forma autenticada. Los componentes deben tener los privilegios mínimos necesarios requeridos.
36. Todas las vías de autenticación y las APIs de gestión de identidad que se implementen deben tener una consistencia en la fortaleza en los controles de seguridad de autenticación, de manera que no existan alternativas más débiles según el riesgo de la aplicación.
37. Se deben establecer y utilizar servicios de autenticación y estándares probados.
38. Utilizar una implementación centralizada para todos los controles de autenticación, incluyendo librerías que llamen a servicios externos de autenticación.
39. Todos los controles de autenticación deben fallar de una forma segura. En caso de error o excepción el portal o sitio web no deberá proveer información relacionada con información de autenticación del usuario.
40. Se debe considerar como restringido el acceso a la administración del Portal.
41. Si la aplicación administra un almacenamiento de credenciales, se debe asegurar que únicamente se almacena el hash (salty hash) de las contraseñas y que el archivo/tabla que guarda las contraseñas y claves solo puede ser escrito por la aplicación.
42. El hash de las contraseñas debe implementarse en un sistema en el que se confíe.
43. Validar los datos de autenticación únicamente luego de haber completado todos los datos de entrada.
44. Las respuestas a los fallos en la autenticación no deben indicar cual parte de la autenticación fue incorrecta. Por ejemplo, en lugar de “Usuario inválido” o “Contraseña inválida”, utilizar “Usuario y/o contraseña inválidos” en ambos casos. Las repuestas a los errores deben ser idénticas tanto a nivel de lo desplegado como a nivel de código fuente.
45. Utilizar autenticación para conexiones a sistemas externos que involucren información o funciones sensibles. En lo posible, para estos sistemas debería emplearse 2FA o MFA.
46. Las credenciales de autenticación para acceder a servicios externos de la aplicación deben ser cifradas y almacenadas en ubicaciones protegidas.
47. Utilizar únicamente solicitudes de tipo POST para la transmisión de credenciales de autenticación.
48. Utilizar conexiones o datos cifrados para enviar contraseñas no temporales.

49. No se debe mostrar en pantalla la contraseña ingresada. A modo de ejemplo, en formularios web, utilizar tipo de entrada “password”.
50. Deshabilitar la cuenta luego de un número de intentos errados de ingreso al sistema.
51. El cambio y reinicio de contraseñas requieren los mismos niveles de control como aquellos asociados a la creación y autenticación de cuentas.
52. En el reinicio por correo electrónico, únicamente enviar un enlace o contraseña temporales a cuentas previamente registradas en el sistema.
53. Las contraseñas y enlaces temporales deben tener un periodo de validez corto.
54. Forzar el cambio de contraseñas temporales luego de su utilización.
55. Notificar a los usuarios cada vez que se produce un reinicio de la contraseña.
56. Prevenir la reutilización de contraseñas. De ser necesario, definir un historial de al menos las últimas 5 contraseñas utilizadas para que no se puedan repetir.
57. Deshabilitar la funcionalidad de “recordar” para los campos de contraseña.
58. El último acceso (fallido o exitoso) debe ser reportado al usuario en su siguiente acceso exitoso.
59. Implementar un monitoreo para identificar ataques a múltiples cuentas utilizando la misma contraseña. Este tipo de ataques debe quedar registrado en los logs que maneja el portal o sitio web.
60. Reautenticar usuarios antes de la realización de operaciones críticas.
61. Implementar mecanismos para confirmar los métodos alternativos de recuperación de contraseñas o envío de tokens de autorización para operaciones críticas.
62. Debe integrarse con el Sistema de Identidad de la DIAN, entre otros debe cumplir, heredar e interoperar las siguientes funcionalidades: - El SGDEA debe estar vinculado al Servicio de Identidad de la DIAN, para controlar los permisos y accesos, - El SGDEA se debe acoplar a las funcionalidades que permiten autenticación, autorización, administración y almacenamiento de datos de usuarios.
63. Debe permitir la definición por parámetro y controlar la longitud mínima y máxima de las contraseñas.
64. Debe permitir la definición por parámetro y controlar el número de contraseñas a recordar (Histórico de contraseñas).
65. Debe permitir la definición de un diccionario de contraseñas no válidas y controlar que las contraseñas no coincidan con las existentes en dicho diccionario.
66. Debe controlar mediante parámetro la complejidad de la contraseña. Cuando se habilita la complejidad, la contraseña debe tener una combinación de caracteres numéricos, alfabéticos (Mayúsculas y Minúsculas) y signos o caracteres especiales.

67. Debe permitir definir por parámetro y controlar la vigencia mínima, vigencia máxima y tiempo de aviso de vencimiento, de las contraseñas.
68. Debe permitir manejar los siguientes estados para las cuentas de usuario: Habilitado, deshabilitado, bloqueado, suspendido.
69. Debe permitir a un usuario autorizado parametrizar el número de intentos fallidos de ingreso a la sesión.
70. Deberá bloquear al usuario una vez se hayan completado el número de intentos fallidos configurados por el usuario autorizado para el inicio de sesión y alertar mediante un mensaje.
71. Debe permitir que las contraseñas nunca pueden ser almacenadas en formato texto. Deben ser almacenadas por medio de un algoritmo de encriptación de una sola vía reconocido por la industria como MD5 y SHA. Para estos procesos de cifrado se deben utilizar llaves cuya longitud mínima sea de 128 bits.
72. Debe permitir marcar un usuario individual como inactivo, sin eliminarlo del sistema por medio del servicio de Identidad de la DIAN.
73. Debe contar con mecanismos de recuperación de credenciales de acceso obedeciendo las políticas de ingreso seguro.

Criptografía

74. Todas las claves y contraseñas deben ser reemplazables y debe existir un proceso bien definido para volver a cifrar datos sensibles en caso de cambio de clave.
75. Las claves simétricas, contraseñas o tokens de API del cliente no deben ser utilizados para proteger o acceder a datos sensibles, estos recursos del cliente siempre deben ser tratados como inseguros.
76. Uso de cifrado asimétrico o mixto (Mezcla entre cifrado asimétrico y simétrico) para el intercambio de datos sensibles, como, por ejemplo, OpenPGP en los intercambios de datos a través de correo electrónico, FTPS/SFTP, directorios compartidos, Teams, etc.
77. Uso de certificados digitales (Identificación segura de origen y destino).
78. Uso de firma digital para garantizar las comunicaciones extremo a extremo y el no repudio.
79. Validación y verificación de autenticación en toda la cadena de transmisión.
80. El canal de comunicación es cifrado para garantizar la confidencialidad de las transmisiones.
81. La utilización de protocolos seguros de transmisión y almacenamiento.

Manejo de sesiones

82. El tamaño del Id de sesión debe ser mínimo de 128 bits para evitar ataques de fuerza bruta.
83. El valor de los identificadores de sesión debe proporcionar al menos 64 bits de entropía, es decir, debe ser lo bastante aleatorio para evitar vulnerabilidades de ataque de colisión de hash.
84. Se debe considerar ataques de tipo “Cookie Replay”. La aplicación o componente de software, para las zonas en las cuales se requiera autenticación del cliente, debe permitir el control de los identificadores de sesión “session_ID”. No deberá ser posible tener dos sesiones simultaneas con el mismo “session_ID”, en cuyo caso las dos sesiones deberán ser cerradas.
85. Los controles de administración de sesiones deben utilizar algoritmos que generen identificadores suficientemente aleatorios para evitar colisiones.
86. Definir el dominio y ruta para las cookies que contienen identificadores de sesión autenticados como un valor apropiadamente estricto para el sitio.
87. La función de Logout debe terminar completamente con la sesión o conexión asociada y debe estar disponible en todos los componentes protegidos por autenticación.
88. Se debe establecer un tiempo de vida de la sesión lo más corto posible, no debería ser superior a 15 minutos.
89. Si una sesión fue establecida antes del inicio de sesión (login), se deberá cerrar dicha sesión y establecer una nueva luego de un inicio de sesión exitoso.
90. Generar un nuevo identificador de sesión luego de cada reautenticación.
91. No permitir inicios de sesión concurrente con el mismo usuario.
92. No exponer identificadores de sesión en URLs, mensajes de error ni logs.
93. Proteger la información sobre las sesiones del lado del servidor implementando los controles de acceso apropiados.
94. Generar un nuevo identificador de sesión y desactivar el anterior de forma periódica.
95. Considerar el manejo de sesión complementario para operaciones sensible del lado del servidor, como los puede ser: gestión de cuentas o utilización de token o parámetros por sesión.
96. Manejo de sesión complementario para operaciones sensibles o criticas utilizando tokens o parámetros (per request) en lugar de que sea por sesión.
97. Configurar el atributo “Secure” para las cookies transmitidas sobre una conexión SSL, TLS.
98. Configurar las cookies con el atributo “HttpOnly”, salvo que se requiera específicamente scripts del lado del cliente en la aplicación, para leer o configurar una cookie.
99. Configurar las cookies con el atributo “SameSite” cuando se utilicen para uso exclusivo de la aplicación.

Control de acceso

100. Se debe utilizar un control de acceso basado en atributos o características, en el cual el código verifica la autorización del usuario para una característica o elemento de datos en lugar de solo su rol.

101. Utilizar un único componente para el chequeo de autorización para todos los componentes de un software, aplicación y/o servicio.

102. Los controles de acceso en caso de falla deben fallar en forma segura, es decir, no exponiendo información personal, de la aplicación o del error presentado.

103. Se debe denegar todos los accesos en caso de que la aplicación no pueda acceder a la información de configuración de seguridad.

104. Se debe requerir controles de autorización en cada solicitud o pedido.

105. Se debe separar la lógica privilegiada de otro código de la aplicación.

106. Restringir acceso a ficheros u otros recursos, incluyendo aquellos fuera del control directo de la aplicación, únicamente a usuarios autorizados.

107. Restringir el acceso a URLs protegidas, solo a usuarios autorizados.

108. Restringir el acceso a funciones protegidas, solo a usuarios autorizados.

109. Restringir las referencias directas a objetos, solo a usuarios autorizados.

110. Restringir el acceso a servicios, solo a usuarios autorizados.

111. Restringir el acceso a información de la aplicación, solo a usuarios autorizados.

112. Restringir el acceso a los atributos y política de información utilizada por los controles de acceso.

113. Restringir el acceso a información relevante de la configuración, solo a usuarios autorizados.

114. Se debe limitar el número de transacciones que un usuario común o un mismo dispositivo puede desarrollar en un cierto periodo de tiempo.

115. Utilizar el header “refer” solo como un chequeo complementario. Nunca debe usarse como chequeo de autorización, ya que se puede modificar.

116. Se debe implementar auditorias de cuentas.

117. La aplicación debe permitir deshabilitar y terminar cuentas una vez que se termina la autorización (Cambio de rol, estatus de empleo, etc.).

118. Las cuentas de servicio o cuentas que soportan conectividad deben tener los privilegios mínimos.

119. El portal deberá funcionar dentro de un contexto de mínimo privilegio. Por ejemplo, si se requiere una cuenta como parte de su conexión hacia la base de datos, esta cuenta debe tener los privilegios necesarios para su funcionalidad; por ningún motivo esta cuenta deberá tener privilegios DBA.

120. Debe integrarse con el Sistema de Identidad de la DIAN, entre otros debe cumplir, heredar e interoperar las siguientes funcionalidades: El SGDEA debe estar vinculado al Servicio de Identidad de la DIAN, para controlar los permisos y accesos. El SGDEA se debe acoplar a las funcionalidades que permiten autenticación, autorización, administración y almacenamiento de datos de usuarios.

121. Gestión de Permisos de acceso mediante los servicios de identidades de la UAE-DIAN, conforme con los requerimientos establecidos por las áreas cliente.

Entrada y salida de datos

122. Se debe especificar el set de caracteres apropiados, tales como UTF-8 para todas las fuentes de entrada.

123. Codificar los datos a un set de caracteres común antes de realizar la validación (Canonicalización).

124. Se deben validar todos los datos brindados por el cliente antes de procesarlos, incluyendo todos los parámetros, URL y contenidos de cabecera HTTP.

125. Se debe validar toda entrada con una lista “blanca” que contenga los caracteres aceptados, siempre que sea posible.

126. Si es necesario permitir el ingreso de algún carácter considerado peligroso, se debe asegurar la implementación de controles adicionales tales como la codificación de la salida, API de seguridad y el registro del uso de tales datos a lo largo de la aplicación. Entre los ejemplos de caracteres peligrosos podemos encontrar: < >”’ % ( ) & + \ / \’ \”.

127. Se deben comprobar si hay bytes nulos (%00).

128. Se deben comprobar si hay caracteres de nueva línea (%0d, %0a, \r, \n).

129. Se deben comprobar si hay caracteres de alteraciones de ruta “punto, punto, barra (../ o ..\). En los casos en que se soportan sets de caracteres UTF-8 extendidos, se debe implementar representaciones alternativas tales como: %c0%ae%c0%ae/ (utilizar la canonicalización como forma de implementar la doble codificación u otras formas de ofuscación de ataques).

130. No se debe almacenar información confidencial en un lugar accesible desde el explorador, como campos ocultos o cookies. Por ejemplo, no se debe almacenar una contraseña en una cookie.

131. Redirección segura.

132. Cuando el SGDEA realice procesos de importación o exportación de información, deberá realizarse a través de interfaces seguras y aplicar protocolos y mecanismos de seguridad.

Protección de datos y privacidad

133. Se debe implementar el mínimo privilegio, restringir el acceso de los usuarios solo a las funcionalidades, datos y sistemas de información necesarios para realizar la tarea.

134. Proteger los almacenamientos temporales (en memoria o caché) de los datos sensibles guardados en el servidor. Lo antes posible, se deben eliminar estos si no se requieren.

135. Se debe cifrar toda la información altamente sensible. Siempre utilizar algoritmos de cifrado que hayan sido chequeados, acorde a la arquitectura de la aplicación se define que información sensible deberá ser cifrada.

136. El código fuente de la aplicación debe protegerse en el servidor, para que usuarios sin acceso o no deseados no puedan alterarlo o descargarlo.

137. Los comentarios en código que puedan revelar información sensible o sobre servidores en la fase de producción deben ser removidos.

138. No se debe incluir información sensible en los parámetros de una petición HTTP GET.

139. Deshabilitar las funcionalidades de completar automáticamente en aquellos formularios que contienen información sensible, incluyendo la autenticación.

140. Deshabilitar el almacenamiento temporal del lado del cliente de páginas que contienen información sensible. “Cache-Control: no-store” debería ser utilizado en conjunto con el control en la cabecera HTTP “Pragma: no-cache”, que es menos efectivo, pero mantiene compatibilidad con HTTP/1.0.

141. La aplicación debe soportar la eliminación de datos sensibles cuando ya no sean requeridos. Por ejemplo, información personal o datos financieros.

142. Se debe implementar controles de acceso apropiados para los datos sensibles almacenados en el servidor. Esto incluye memoria temporal, archivos temporales y datos que solo pueden acceder usuarios específicos del sistema.

143. Debe permitir la creación, gestión y configuración de niveles de clasificación de información a que haya lugar (Clasificada, reservada, confidencial, de acuerdo con la normatividad existente) y permitir acceso a esta dependiendo el rol del usuario.

144. Debe permitir establecer niveles de seguridad de la unidad documental de acuerdo con los niveles de seguridad establecidos por la entidad y generar los reportes correspondientes.

145. En todos los componentes que realicen tratamiento de datos personales, se debe informar claramente a los usuarios sobre la política de tratamiento de datos personales antes de la recolección de cualquier dato y se debe obtener el consentimiento explícito de

los usuarios para el tratamiento de sus datos personales, asegurando que comprendan los fines específicos para los cuales se utilizarán sus datos.

146. Los usuarios deben tener la opción de seleccionar cómo desean que se traten sus datos personales. Esto incluye la posibilidad de optar por no participar en ciertos tipos de tratamiento de datos, proporcionando mecanismos fáciles de usar para que los usuarios puedan modificar sus preferencias de tratamiento de datos en cualquier momento.

147. Debe informar a los usuarios sobre cualquier cambio en la política de tratamiento de datos personales y se debe obtener su consentimiento para cualquier nuevo uso de sus datos.

148. Respetar y facilitar el ejercicio de los derechos de los usuarios, tales como el derecho de acceso, rectificación, cancelación y oposición (derechos ARCO), proporcionando canales de comunicación claros y accesibles en el software para que los usuarios puedan ejercer sus derechos y presentar quejas relacionadas con el tratamiento de sus datos personales.

Manejo de archivos

149. Se debe asegurar que los archivos subidos por los usuarios; si es necesario mostrarlos o descargarlos desde la aplicación, sean proporcionados ya sea como descargas de tipo "octet stream" o desde un dominio no relacionado.

150. No se debe utilizar directamente la información provista por el usuario en ninguna operación dinámica.

151. Para la realización de una transferencia de un archivo al servidor en caso de que se encuentre la función como parte de los RF debe exigir autenticación.

152. La transferencia de archivo al servidor únicamente debe soportar los tipos de archivos requeridos en el modelo de requisitos de documentos electrónicos.

153. Validar los tipos de archivo transferidos verificando la estructura de los encabezados.

154. Se debe evitar o restringir la transferencia de archivos que puedan ser interpretados por el servidor web. Por ejemplo, asp, php, jsp, etc.

155. Se debe comprobar que los archivos transferidos no tengan permisos de ejecución.

156. La ruta absoluta de un archivo no debe ser enviada al cliente.

157. Se debe asegurar que los archivos y recursos de la aplicación sean solo de lectura.

158. No se debe incluir nombres de directorio o rutas de archivos en parámetros. En su lugar, utilizar índices que internamente se asocien a directorios o rutas predefinidas.

159. Se debe validar los tipos de los archivos (Tipo MIME), extensiones, tamaños y cantidad de archivos concurrentes, Las validaciones deben realizarse tanto en el cliente como en el servidor.

160. Cuando se sirven archivos a través de HTTP, la respuesta debe contener la cabecera Content-Disposition y X-Content-Type-Options.

161. Debe cifrar los documentos para imposibilitar su consulta por fuera del sistema

162. Debe permitir que el administrador restrinja el acceso a carpetas, documentos y metadatos a determinados usuarios del sistema.

163. Debe permitir restringir el acceso a funciones como la lectura, modificación y eliminación de documentos y/o metadatos.

APIs REST seguras

164. Todas las APIs deben consumirse por canales seguros (HTTPS)

165. Todas las respuestas de las APIs deben contener las siguientes cabeceras de seguridad: Content-Security-Policy, Strict-Transport-Security, X-XSS-Protection: 1; mode=block;, X-Frame-Options: Deny;

166. Se deben remover las cabeceras que revelen información del servidor como Server, X-Powered-By, X-AspNet-Version, X-AspNetMvc-Version, etc.

167. Se deben restringir el acceso de un recurso a los verbos HTTP estrictamente necesarios, dependiendo del contexto de solicitud al recurso: HEAD obtener las cabeceras de respuesta del recurso solicitado, GET para consultar datos, POST para insertar datos, PUT para modificar datos, PATCH para actualizar datos, DELETE para eliminar datos.

Servicios web seguros

168. Todas los Servicios Web SOAP deben estar publicados en un transporte confiable TLS.

169. Verifique que la validación del esquema XSD tiene lugar para garantizar un documento XML formado correctamente, seguido de la validación de cada campo de entrada antes de que se realice cualquier procesamiento de esos datos.

170. Verifique que el payload del mensaje está firmada mediante WS-Security para garantizar un transporte fiable entre el cliente y el servicio.

171. Aplicar los servicios de Seguridad con X-Road para intercambios de información interinstitucionales.

Controles de Implementación y puesta en marcha

172. Desplegar últimas versiones soportadas de software adquirido en sistemas operativos, capa media y capa de base de datos en las últimas versiones soportadas y estables preferiblemente con soporte LTS.

173. Actualizar en versiones estables y estándar del Software.

174. Compatibilidad del software a instalar con el software existente.

175. Incluir los diagramas de arquitectura de solución de infraestructura física, arquitectura de infraestructura lógica, arquitectura de seguridad, arquitectura de lógica de negocio y los diagramas relacionados como flujos de datos y diagramas de secuencia en los documentos de arquitectura de software.

176. Generar los documentos técnicos para la instalación y configuración del software.

177. Crear, ejecutar y documentar set de pruebas para: requerimientos de seguridad de auditoria y log de eventos, penetración, fuerza bruta, suplantación de identidad, acceso denegado, manipulación de datos, corrupción de datos, cifrado, autenticación, integridad, inyección SQL, XSS, CSRF, administración de Cookies de sesión, complejidad de contraseñas, carga y estrés, cabeceras seguras HTTP, redirección segura, DDoS, APIS y Servicios Web, paginas web (Content-negotiation, CORS, HTTP Status Codes, HTTP Response Content, Iframes, Secure Redirection, etc.), de aceptación funcionales, técnicas y de seguridad aprobadas por los responsables funcionales, técnicos y de seguridad.

178. Debe garantizar que las operaciones realizadas en el sistema deben estar protegidas contra adulteración, supresión, ocultamiento y demás operaciones que atenten contra la autenticidad, integridad y disponibilidad de la información.

179. Debe permitir contar con procedimientos automáticos para copias de seguridad y restauración encaminados a realizar copias periódicas de seguridad de todos elementos dentro del sistema (carpetas, documentos, metadatos, usuarios, roles, permisos, configuraciones específicas).

180. Debe cumplir con las políticas de seguridad y privacidad de la DIAN establecidas para los lineamientos de Protección de Datos Personales.

181. Debe garantizar que las transacciones u operaciones que realice el sistema las cuales presenten fallos en su ejecución deben reversarse al estado inicial en la ejecución del proceso. (rollback) (evita envío de información incompleta y perdida de esta).

BIBLIOGRAFÍA

- ARCHIVO GENERAL DE LA NACIÓN. (2024). Acuerdo 001. Acuerdo Único de la Función Archivística. Disponible en: https://normativa.archivogeneral.gov.co/wp-content/uploads/2024/04/2024-02_29_AcuerdoAGN-FIRMADO.pdf

- ARCHIVO GENERAL DE LA NACIÓN. (2020). Guía de Implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo -SGDEA.

- ARCHIVO GENERAL DE LA NACIÓN Y MINISTERIO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y LAS COMUNICACIONES. (2018). G.INF.07 Guía Técnica para la Gestión de Documentos y Expedientes Electrónicos.

- COLOMBIA. PRESIDENCIA DE LA REPÚBLICA. (2015). Decreto 1080. Decreto Reglamentario Único del Sector Cultura.