MODELO DE REQUISITOS PARA LA GESTIÓN DE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

VERSIÓN 01

NOVIEMBRE DE 2021

DEPARTAMENTO GESTIÓN DOCUMENTAL

GERENCIA DE TECNOLOGÍA DE INFORMACIÓN

PROYECTO CONSOLIDACIÓN GESTIÓN DOCUMENTAL

ÍTEM	ELABORÓ	REVISÓ	APROBÓ
Nombre	Natalia Andrea Roldan Díaz Yenifer Cristina Cardona López Marcela López Gómez Olga Luz Cadavid Jinni Giovanni Arias Rom Jose Carlos Muñoz Morales	Julián Esteban Santamaría Claudia Durango Urrego Jaime Alberto Ruiz Jhon Dario Medina	Comité Interno de Archivo Comité Institucional de Gestión y Desempeño
Cargo	Profesional Servicios Administrativos Profesional Servicios Administrativos Profesional Servicios Administrativos Profesional Informático Profesional Informático Profesional Informático	Profesional Servicios Administrativos Profesional Informático Profesional Informático Profesional Informático	N/A

Contenido

Tabla de ilustraciones

1. INTRODUCCIÓN

El Archivo General de la Nación- AGN definió que las entidades públicas y privadas con funciones públicas deben desarrollar la gestión de sus documentos a partir de la formulación e implementación de ocho (8) instrumentos archivísticos, descritos claramente en el artículo 2.8.2.5.8 del Decreto 1080 de 2015. Entre los instrumentos, se encuentra el ***Modelo de Requisitos para la Gestión de Documentos Electrónicos de Archivo - MoREQ***; herramienta a través de la cual se planean rigurosamente los ítems funcionales y técnicos requeridos para desarrollar, adquirir e implementar un sistema de gestión de documentos electrónicos que cumpla con los parámetros establecidos en la normatividad vigente y que dé respuesta a las necesidades de la Organización respecto a la gestión, almacenamiento y conservación de la información oficial.

En relación con la información electrónica, es importante informar que EPM atendiendo sus necesidades particulares y ante los retos tecnológicos y las dinámicas mundiales, ha adquirido múltiples sistemas de información transaccionales que apoyan la ejecución de los procesos internos, dando como resultado un incremento significativo de los documentos de archivo en soporte electrónico y, de manera proporcional, la disminución de la producción documental en soportes análogos como el papel. Aunque esta situación claramente favorece la ejecución de las actividades administrativas y operativas al interior de la empresa; representa un nuevo reto para la gestión documental dado que estos sistemas de información que permiten adjuntar o generar documentos que soportan las transacciones, no tienen capacidades o servicios orientados al cumplimiento de funciones archivísticas y, por tanto, terminan generando islas de información y un control inadecuado de los documentos de archivo que impide el cumplimiento de las directrices internas en materia documental y de la normatividad vigente expedida por el Archivo General de la Nación.

Esta realidad devela la necesidad de desarrollar o adquirir un sistema de gestión de documentos electrónicos de archivo- SGDEA[1], en el cual se gestione la totalidad de información oficial de

[1] Definición entregada por el AGN y MINTIC en la guía G.INF.07. Se aclara que para EPM constituye un Sistema de Información para la Gestión de Documentos Electrónicos de Archivo que se incorpora al ecosistema tecnologico del proceso de Gestión Documental.

EPM durante su ciclo de vida; sistema que deberá responder a las necesidades tecnológicas manifiestas y que además, requiere de la completa articulación con las demás aplicaciones del dominio de gestión documental y con las directrices establecidas en el Programa de Gestión Documental, el Sistema Integrado de Conservación, las Tablas de Retención Documental y los demás instrumentos y estrategias que se adopten en la Organización.

Es preciso mencionar que la ausencia de un SGDEA corporativo y los riesgos que esto implica para la gestión de la información documental, fueron asuntos que se contemplaron en el marco de la formulación del Plan Institucional de Archivos- PINAR y que dieron como resultado la priorización de acciones para mitigar el siguiente aspecto critico " *No se ha implementado un Sistema de Gestión de Documentos Electrónicos de Archivo SGDEA que permita tener la integración tecnológica necesaria entre los sistemas de información y que garantice el cumplimiento de la normatividad asociada a la gestión de la información en formato diferente al papel*." Este aspecto, adicionalmente, fue clave para precisar la visión estratégica de la gestión de documentos en EPM la cual contempla el uso eficiente de las TIC´S como parte integral del desarrollo y posicionamiento del proceso.

De lo anterior, se puede concluir que para la Empresa es clave analizar y documentar sus necesidades, oportunidades, recursos, expectativas y demás variables que permitan seleccionar e implantar un Sistema de Gestión de Documentos Electrónicos de Archivo – SGDEA; orientado a la conformación y custodia del archivo electrónico institucional en sus diferentes fases y por ende, a constituir el patrimonio documental digital de la Organización, en concordancia con las instrucciones emitidas por el Archivo General de la Nación.

2. OBJETIVO

Establecer los requisitos funcionales y técnicos que orienten el proceso de adquisición, desarrollo, implementación y actualización de un SGDEA; propiciando la adopción de estándares de alta calidad para la gestión de los documentos electrónicos y digitalizados que conforman el fondo documental de EPM.

3. ALCANCE

Este modelo es aplicable exclusivamente a EPM y es compatible con las directrices, políticas y recursos tecnológicos internos. Incluye los requisitos obligatorios y opcionales que deben ser evaluados al momento de seleccionar un nuevo proveedor o para desarrollar el producto *in house*, así como, durante la evaluación del SGDEA con el que se encuentre operando en la actualidad en la Organización.

Respecto al alcance de los distintos Sistemas Tecnológicos en las organizaciones el Archivo General de la Nación ha descrito lo siguiente:*"Hoy en día, las entidades producen diferentes documentos como resultado de sus actuaciones administrativas, a través de diferentes aplicativos o soluciones tecnológicas diseñadas para fines particulares (sistemas de inventarios, nomina, contratos, sistemas académicos, entre otros)… Comúnmente se encuentra que este tipo de aplicativos son de uso transaccional y no están diseñados como un gestor documental que permita parametrizar las tablas de retención y administrar los documentos y expedientes*."

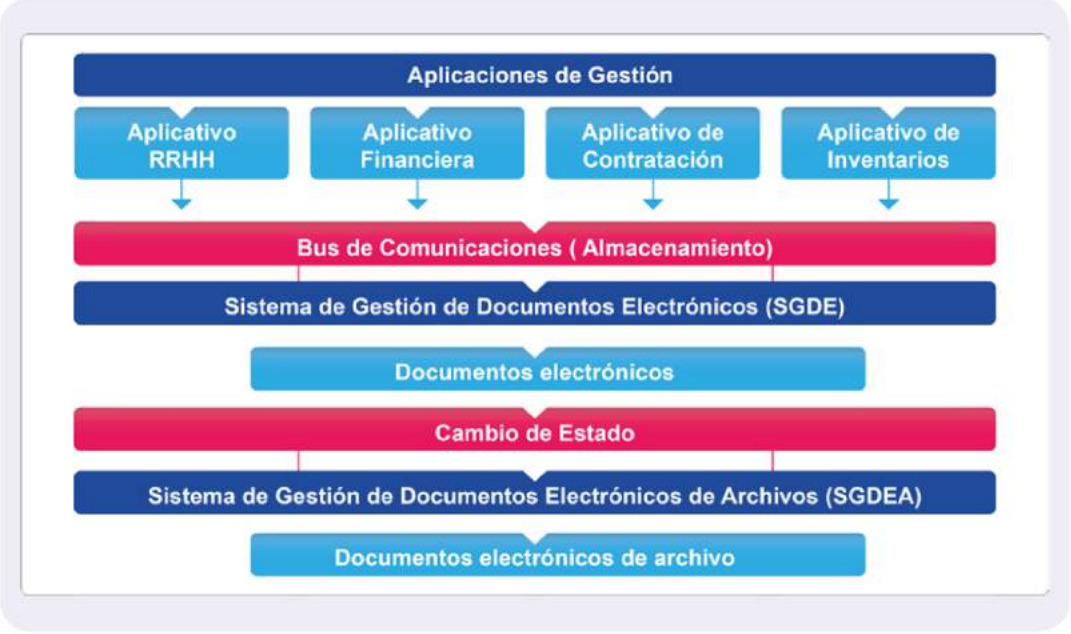


Ilustración 1. Integración del Gestor de Documentos. [2]

[2] Recuperado de: Archivo General de la Nación - Ministerio de Tecnologías de la Información y Comunicaciones. (2017) Guía de Implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo SGDEA. Bogotá.

Por lo anterior, es importante señalar que ninguno de los sistemas transaccionales que apoyan el desarrollo de los procesos en EPM podrá adoptarse como SGDEA, debido a que no cumplen con los requisitos mínimos obligatorios para la conformación y tratamiento archivístico de los expedientes. Además de ello, la administración de la información documental que se genera de manera física y electrónica es una función asignada oficialmente al Departamento De Gestión Documental; área que opera con diversos aplicativos tecnológicos que hacen parte de su dominio funcional.

4. ANTECEDENTES

Con base en el articulo 2.8.2.6.4 del Decreto 1080 de 2015, los sujetos obligados deben seleccionar un Sistema de Gestión de Documentos Electrónicos De Archivo que cumpla con lo reglamentado por el AGN y, que a la vez, responda a las necesidades de la Organización y a sus capacidades financieras, tecnológicas y documentales. Por lo anterior, la estructuración del presente Modelo tuvo fundamento en el resultado de las acciones descritas a continuación, las cuales fueron desarrolladas de manera previa en el Marco del proyecto Consolidación Gestión Documental y deberán ser revisadas y ajustadas en los futuros procesos de actualización del MoReq institucional:

a) Diagnóstico de necesidades

Para el Departamento de Gestión Documental, como responsable del proceso de Gestión Documental en la Organización, es fundamental integrar, estandarizar y homologar las actividades relacionadas con el manejo y disposición de la información que se genera de manera física y electrónica durante el cumplimiento de las funciones legalmente asignadas.

Por esta razón, se llevo a cabo la construcción de un diagnóstico en el que se evaluó y documentó de manera detallada la necesidad de adquirir una herramienta tecnológica para la administración centralizada de los documentos de archivo durante las distintas fases de su ciclo vital. Como parte del diagnostico se determinó que un SGDEA permitiría a EPM lo siguiente: administración centralizada de los expedientes electrónicos, gestion de metadatos, transferencias documentales automatizadas, administración integral de inventarios, foliado electrónico, integraciones tecnológicas con sistemas transaccionales, control de acceso a adoucmentos clasificados o reservados, entre otras funcionalidades con las que actualmente no se cuenta.

Adicionalmente, como parte del diagnostico se entregaron las siguientes recomendaciones, las cuales favorecen la adquisición de un sistema tecnologico adaptado a la realidad de la empresa:

- La solución SGDEA por ser una solución que apoya la gestión y control de los documentos de la Organización, se enmarca como parte del Dominio de Gestión Documental y por ende de la arquitectura objetivo definida para este dominio.

- SharePoint como ECM - Enterprise Content Management, es la herramienta que está definida en la arquitectura objetivo para Gestión Documental en el Grupo EPM y por tanto se propenderá por hacer énfasis en el uso de las aplicaciones asociadas al dominio de gestión al que pertenece el proceso, por lo tanto, la solución SGDEA objeto de estudio, deberá estar desarrollada sobre esta herramienta tecnológica.

- No se debe adquirir una solución SGDEA que esté desarrollada sobre un Enterprise Content Management diferentes a SharePoint.

- Si la solución SGDEA es a la medida y no sobre un ECM, se deberá garantizar su interoperabilidad con Sharepoint haciendo uso de servicios de integración de Azure - como API Management u otros válidos para la Organización, como Rest API.

- El repositorio para todos los documentos resultantes de la puesta en operación de los instrumentos archivísticos deberá continuar siendo la que se tiene actualmente sobre SharePoint.

- La solución deberá integrarse con la plataforma de aplicaciones de TI de la Organización, evitando la redundancia funcional y operativa.

- Las soluciones a evaluar deberán propender por el cumplimiento de la directriz de racionalización y estandarización de las aplicaciones, para lo cual se dará prioridad a las herramientas de proveedores incluidos en la ruta de arquitecturas objetivo o soluciones que estén habilitadas para apoyar un dominio funcional.

- La herramienta de SharePoint Online (solución Enter Online) está alojada en la nube de Azure, EPM cuenta con un tenant privado para todos los servicios que tiene suscritos

con MicroSoft. Por tanto, se debe buscar una solución SGDEA que sea alojada dentro del mismo tenant de EPM con el fin de facilitar la integralidad de las actualizaciones que Microsoft realice sobre sus servicios. No obstante, se deberán evaluar aquellas ofertas en las cuales el proveedor ofrezca la solución en un tenant diferente.

b) Rediseño del Proceso de Gestión Documental

La adquisición de sistemas de información para la gestión de documentos está supeditada a las definiciones registradas en la descripción del proceso. Por tal motivo, los cambios tecnológicos deberán estar alineados con la visión estratégica y el objetivo superior determinado para la gestión documental en la empresa.

Por lo anterior, es importante resaltar que para la formulación del Modelo de Requisitos se contó con un proceso de Gestión Documental recientemente rediseñado; el cual se enfoca en atender los retos archivísticos de la Organización y en cumplir con la regulación vigente en esta materia. Este nuevo proceso, aprobado en la Organización, no se centra exclusivamente en la ejecución de actividades operativas sino que incluye acciones de carácter estratégico, documenta la interacción con dependencias claves, redefine los indicadores y promueve el ajuste de algunos componentes de las dimensiones de la arquitectura empresarial. Esta restructuración se desarrolló en concordancia con las conclusiones del diagnostico realizado en EPM para identificar las necesidades no aatendidas en el ambito técnico, procedimental y tecnologico de la función archivística.

Esta información constituye un insumo sustancial para determinar las características o especificaciones a tener en cuenta para la selección, adquisición e implementación de un Sistema de Gestión de Documentos Electronicos de Archivo que, en articulación con los procedimientos y directrices internas, permita asegurar la disponibilidad, confiabilidad y completitud de la información documental que se produce o recibe en cumplimiento de las funciones institucionales.

c) Análisis de los requisitos AGN

El equipo interdisciplinario designado para la construcción del presente documento programó y realizó una serie de reuniones periódicas para el análisis de los requisitos funcionales y no funcionales propuestos por el Archivo General de la Nación. En estos espacios se logró determinar que, aproximadamente el 95% de los requerimientos publicados, se ajustan a los retos institucionales y a las expectativas de la Organización para el fortalecimiento del proceso de gestión documental.

Un pequeño porcentaje de los requisitos AGN se descartó debido a que corresponde a funcionalidades que ya ejecutan otros sistemas de información del dominio de gestión documental.

5. CONTEXTO NORMATIVO

EPM como sujeto obligado, adopta lo establecido en la normatividad vigente asociada a la gestión de los documentos electrónicos de archivo y, además, en su firme propósito de avanzar en la modernización del proceso y el control de la información institucional se compromete con la implementación de las normas y las buenas prácticas relativas al *documento electrónico*, que se encuentran registradas en las normas técnicas nacionales e internacionales que se describen a continuación:

N°	RANGO	NÚMERO	OBJETO
1	Ley	527 de 1999	Acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.
2	Ley	594 de 2000	Ley General de Archivos y otras disposiciones
3	Ley	1581 de 2012	Disposiciones generales para la protección de datos personales
4	Ley	1712 de 2014	Transparencia y acceso a la información pública
5	Decreto	1080 de 2015	Decreto único reglamentario del sector cultura
6	Decreto	2106 de 2019	Normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.
7	Acuerdo	002 de 2014	Parámetros a tener en cuenta para la conformación de expedientes e implementación de nuevas Tecnologías en los archivos públicos
8	Acuerdo	003 de 2015	Lineamientos para la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos
9	Circular E.	002 de 1997	Parámetros a tener en cuenta para la implementación de nuevas Tecnologías en los archivos públicos
10	Directiva Presidencial	004 de 2012	Eficiencia administrativa y Cero Papel en la administración pública.
11	Norma Internacional	MoReq2	Publicación europea. Presenta una recopilación de requisitos funcionales para gestionar los documentos electrónicos de archivo.
12	Norma Internacional	ISO 15489	Información y documentación. Gestión de registros: Metadatos para registros (5.2.3).

13	Norma Técnica	NTC-ISO 30300	Información y documentación. Sistemas de gestión para registros. Fundamentos y vocabulario
14	Norma Técnica	ISO 27001	Tecnología de la información. Seguridad de la información.
15	Norma Técnica	NTC-ISO 16175-1	Información y documentación. Principios y requisitos funcionales para los registros en entornos electrónicos de oficina

6. MARCO CONCEPTUAL

6.1 Documentos y expedientes electrónicos de archivo: Definición y características principales.

El SGDEA, cumpliendo con los estándares y principios normativos, deberá gestionar la totalidad de documentos electrónicos de archivo producidos y recibidos por la Organización. Para efectos de este modelo, el Documento Electrónico se define como la información generada, enviada, recibida, almacenada y comunicada por medios electrónicos, ópticos o similares (AGN, 2018). Estos "serán de archivo cuando por su valor administrativo, fiscal, legal, científico, histórico, técnico o cultural, adquieran esa naturaleza. En cuyo caso, deberán ser tratados conforme a los principios y procesos archivísticos y permanecer almacenados electrónicamente durante todo su ciclo de vida".[3]

En este sentido, un documento electrónico de archivo estará conformado por diferentes elementos (estructura física y estructura lógica) y características que deberán ser incorporadas y gestionadas de forma integral en el proceso de gestión documental, con el fin de garantizar y asegurar su tratamiento adecuado.

La estructura física del documento hace referencia a la parte material, representada en el *formato* que permite contener la información, los *medios de almacenamiento y reproducción (hardware y software)* que son utilizados para producir/recibir los documentos y que garantizan su conservación y recuperación en el tiempo.

La estructura lógica, por su parte, hace referencia a la forma en que se identifica y registra el documento electrónico en el SGDEA a través de los metadatos, la autenticación y el contenido (Ver figura 1).

3 Artículo 6º del Acuerdo 003 de 2015 Recuperado de: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=61731

A través del fortalecimiento de estos elementos, los documentos electrónicos de archivo adquieren como características; la autenticidad, la fiabilidad, la integridad y la disponibilidad [4]. A continuación, se describen algunas premisas asociadas a cada uno de ellos:

- Para garantizar que un documento sea *autentico* se debe acreditar que no haya sido alterado, a través de la verificación de los distintos metadatos que garantizan la confianza o seguridad sobre la información que contienen y que están asociados a información del contexto, estructura y contenido.

- El concepto de *fiabilidad* hace referencia a la capacidad de un documento de asegurar su contenido, el cual es la representación completa y fidedigna de las operaciones realizadas y que le dieron origen.

- Por su parte para que un documento electrónico sea *integro,* este siempre debe estar completo y sin alteraciones, por lo cual se debe asegurar su "inalterabilidad" a través de distintos mecanismos de protección para que el contenido y sus atributos se encuentren protegidos durante todo el ciclo vital.

- El atributo de *disponibilidad* establece que el documento y sus metadatos asociados deben estar siempre en la capacidad actual y futura de ser consultados, localizados, interpretados y legibles para el uso de la información que contienen cuando estos sean requeridos.

4 Decreto 1080 de 2015, artículo 2.8.2.7.2.

Ilustración 2. Estructura lógica del documento

En consideración de lo anterior, es importante resaltar que existen otras características adicionales sobre los documentos electrónicos de archivo definidas por el *Consejo Internacional de Archivos*, a saber: la forma documental fija, el contenido estable y el vínculo archivístico con otros documentos de archivo, descritas en la figura 2.

Ilustración 3. Características complementarias D.E.A

Por otra parte, bajo la premisa de que los documentos siempre deberán integrarse a un expediente de archivo y que estos pueden estar conformados por un sinnúmero de documentos, se toma la siguiente definición para el concepto de expediente electrónico de archivo desarrollado por el AGN como: "Conjunto de documentos y actuaciones electrónicos producidos y recibidos durante el desarrollo de un mismo trámite o procedimiento, acumulados por cualquier causa legal, interrelacionados y vinculados entre sí, manteniendo la integridad y orden dado durante el desarrollo del asunto que les dio origen y que se conservan electrónicamente durante todo su ciclo de vida, con el fin de garantizar su consulta en el tiempo".[5]

En este sentido, los documentos electrónicos de archivo deberán ser ordenados de acuerdo con el trámite que le dio origen y agrupados conformando series y subseries documentales de acuerdo con el esquema de clasificación definido en el Cuadro de Clasificación Documental y las Tablas de Retención Documental parametrizadas en el SGDEA. Así mismo, los expedientes deberán contar con algunos elementos y mecanismos tecnológicos que permitan un manejo adecuado sobre la información que contienen, tales como; Documentos electrónicos de archivo, el foliado electrónico, el índice electrónico, firma del índice y los metadatos o información virtual contenida en ellos. A continuación se registran algunas particularidades de cada uno de ellos:

5 Acuerdo 003 de 2015, artículo 3. AGN Recuperado de: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=61731

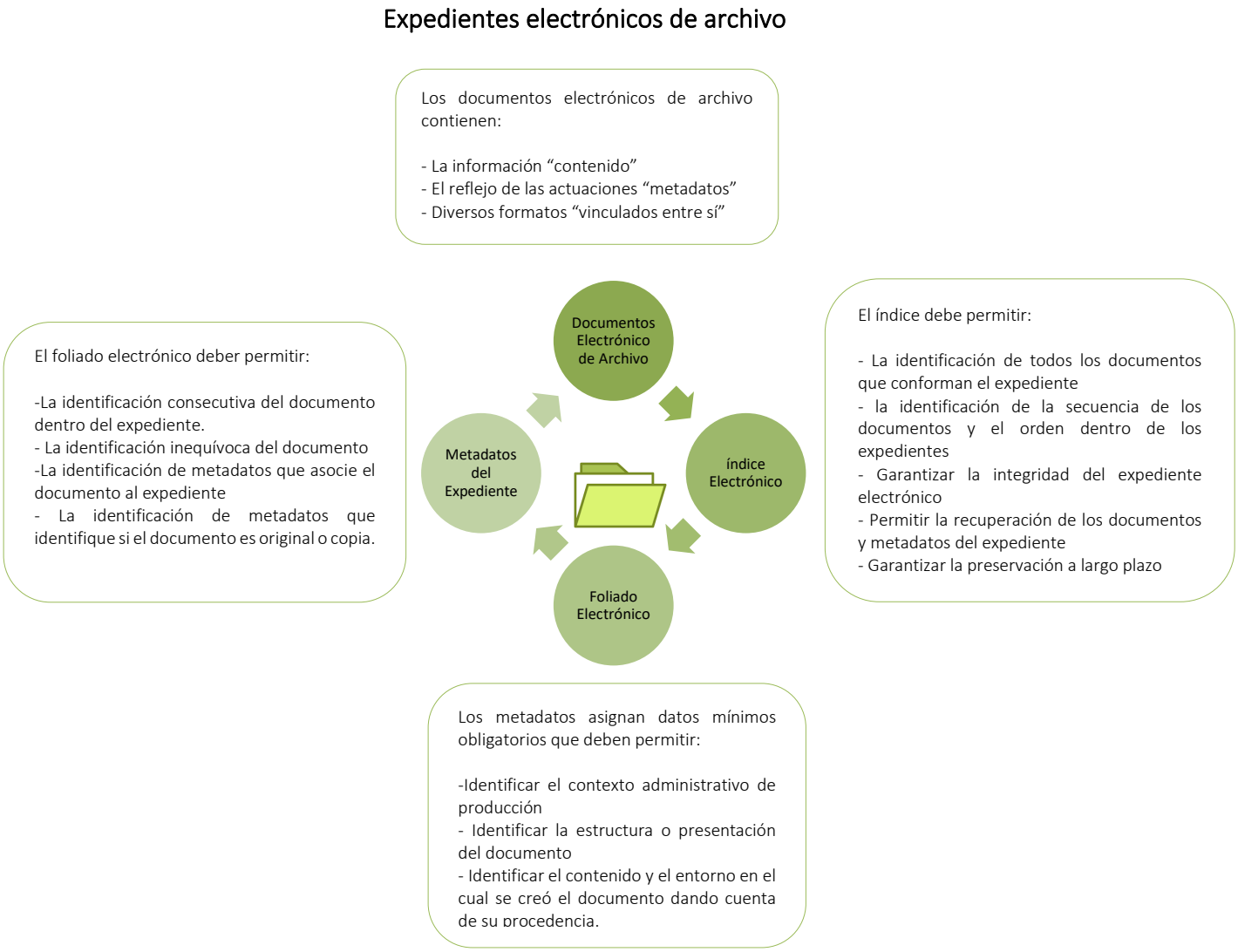


Ilustración 4. Elementos del Expediente electrónico de archivo

6.2 Sistema de Gestión de Documentos Electrónicos de Archivo. Definición y beneficios.

Un sistema de Gestión de Documentos Electrónicos de Archivo – SGDEA es una herramienta o conjunto de herramientas tecnológicas que por sus características y funcionalidades especificas gestionan de manera adecuada los documentos durante el ciclo de vida, asegurando su integridad, fiabilidad, autenticidad y accesibilidad.

Este tipo de soluciones tecnológicas aplicadas a la gestión documental permiten realizar una articulación estratégica entre las dependencias productoras, las políticas internas y los instrumentos archivísticos; de forma tal que la Organización puede evidenciar la trazabilidad en

el desarrollo de sus actividades y logra acceder a información real y actualizada para la toma de decisiones.

Con su implementación, el SGDEA aportará los siguientes beneficios[6]:

Estratégicos:

-Generación de condiciones que faciliten el desarrollo e implementación de soluciones estratégicas que aporten al proceso de la gestión documental como soportes para la toma de decisiones, rendiciones de cuentas, transparencia y acceso a la información.

- Control sobre la producción documental y los accesos sobre los mismos.

Financieros:

- Disminución de costos asociados al almacenamiento físico, a la impresión de copias y a los insumos que de ellas se derivan.

- Reducción de tiempo asociado a las búsquedas y recuperación de información, a través de la indexación de metadatos propios del documento y a los resultantes de las acciones sobre los mismos.

Administrativos:

- Facilitar la administración de los procesos de negocio, a través de la automatización.

- Mejora en los tiempos de gestión y tramite de los documentos enviados y recibidos, pues se tiene un control completo del proceso y de los documentos que a partir de ellos se generan.

Operativos:

- Reducción de tiempos de consultas y tareas de archivo.

- Facilitar el acceso a la información (agilidad en procesos de localización, control total sobre la documentación e información).

- Normalización y estandarización de formas y formatos que contribuyen a la creación, gestión y control, conservación y acceso a los documentos.

6Recuperado de: https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Recursos/Publicacionees/ImplementacionSGDEA.pdf

Tecnológicos:

- Garantía de seguridad para documentos según su clasificación (confidenciales, restringidos, entre otros) a través de la parametrización de roles y permisos.
- Auditoria y trazabilidad sobre las diferentes actividades concernientes a la gestión de la información y la documentación.
- Control de la documentación, evitando duplicidad.
- Definición y aplicación de permisos de acceso sobre los documentos según las políticas definidas en la empresa.

6.3 Glosario

Acceso: Derecho, oportunidad, medio de encontrar, usar o recuperar información.

Autenticidad: Característica técnica para preservar la seguridad de la información que busca asegurar su validez en el tiempo, forma y distribución. Así mismo, garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Captura: Acción por medio de la cual se incorpora el documento de archivo al SGDEA.

Contenido estable: Concepto que indica que el contenido del documento no cambia en el tiempo y que, los cambios deben estar autorizados conforme a reglas establecidas, limitadas y controladas por la entidad, o el administrador del sistema. De forma que, al ser consultado cualquier documento, una misma pregunta, solicitud o interacción genere siempre el mismo resultado.

Cuadro de clasificación documental: 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.

Digitalización: Proceso tecnológico que permite convertir un documento en soporte análogo (papel, video, casettes, cinta, película, microfilm) en uno o varios archivos digitales que contienen la imagen codificada, fiel e íntegra del documento.

Disponibilidad: Característica de seguridad de la información, que garantiza que los usuarios autorizados tengan acceso a la misma y a los recursos relacionados, toda vez que lo requieran asegurando su conservación durante el tiempo exigido por ley.

Documento de apoyo a la gestión: Conjunto de documentos recopilados por la oficina como apoyo informativo para la realización de un trámite especifico. No hacen parte de las series documentales de la dependencia y, por tanto, no le aplican las directrices archivísticas emitidas en la Organización.

Documento electrónico de archivo: Registro de información generada, recibida, almacenada y comunicada por medios electrónicos, que permanece en estos medios durante su ciclo vital. Es producida por una persona o entidad en razón de sus actividades y debe ser tratada conforme a los principios y procesos archivísticos.

Documento nativo electrónico: Información creada o recibida electrónicamente en las entidades, fruto de la automatización de procesos.

Esquema de metadatos: Instrumentos que facilitan la interoperabilidad y ayudan a asegurar el mantenimiento de los documentos a largo plazo. Su 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.

Expediente: Unidad documental compleja formada por un conjunto de documentos generados orgánica y funcionalmente por una instancia productora en la resolución de un mismo asunto.

Expediente digitalizado: Copia exacta de un expediente físico cuyos documentos originales, tradicionalmente impresos, son convertidos a formato electrónico mediante un proceso de digitalización.

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.

Firma digital: Una firma digital es un tipo específico de firma electrónica. Las firmas digitales utilizan ID digitales basados en certificados para autenticar la identidad del firmante y demostrar la prueba de la firma vinculando cada firma con el documento mediante un código cifrado. La validación se produce mediante autoridades de certificación de confianza o proveedores de servicios de confianza.

Firma electrónica: Termino general que se refiere a cualquier proceso electrónico que indica aceptación de un acuerdo. Las soluciones de firma electrónica típicas utilizan métodos comunes de autenticación electrónica para verificar la identidad del firmante, como una dirección de correo electrónico, un ID empresarial o un código PIN de teléfono.

Foliado electrónico: Asociación de un documento electrónico a un índice de un mismo expediente con el fin de garantizar su integridad, orden y autenticidad.

Forma documental fija: Cualidad del documento de archivo que asegura que su contenido permanece completo y sin alteraciones, a lo largo del tiempo, manteniendo la forma original que tuvo inicialmente.

Gestión Documental: Es el conjunto de actividades administrativas y técnicas tendientes a la planificación, procesamiento, manejo y Organización de la documentación producida y recibida

por los sujetos obligados, desde su origen hasta su destino final con el objeto de facilitar su Organización y conservación.

Índice electrónico: Relación de los documentos electrónicos que conforman un expediente.

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. / Hace referencia al carácter completo e inalterado del documento electrónico. Es necesario que un documento esté protegido contra modificaciones no autorizadas.

Metadatos: Descriptores a través de los cuales se identifica el contenido, calidad, condición y otras características de los documentos de archivo.

Migración: Acción de trasladar documentos de archivo de un sistema a otro, manteniendo la autenticidad, integridad, fiabilidad y disponibilidad de los mismos.

Patrimonio digital: Recursos de carácter cultural, educativo, científico o administrativo e información técnica, jurídica, médica o de otras clases, que se generan directamente en formato digital o se convierten a este a partir del material analógico ya existente.

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.

Seguridad de la información: Proceso mediante el cual las organizaciones aseguran la confidencialidad, integridad y disponibilidad de la información que producen, reciben y controlan en cumplimiento de sus funciones.

Transferencia documental: Remisión de los documentos del archivo de gestión al central y de este al histórico, de conformidad con las tablas de retención y de valoración documental vigentes.

Trazabilidad: Registros que dan cuenta de los procesos de producción, trámite, captura y conservación de los documentos de archivo.

Vinculo archivístico: La red de relaciones que cada documento de archivo tiene con otros documentos de archivo que pertenecen a la misma agregación (expediente, serie, fondo).

7. PREREQUISITOS

La formulación e implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo-SGDEA requiere previamente que la Organización cuente con instrumentos de clasificación documental actualizados y aprobados por la instancia correspondiente. Asimismo, se debe tener como base una Política de Gestión Documental que refleje el compromiso de la alta dirección frente a la correcta gestión de la información documental que se genera en la empresa y, por último, es necesaria la construcción y socialización a interesados del documento Habilitador de TI en el que se establecen las pautas generales que orientan el proceso de adquisición e implantación de herramientas tecnológicas en la Organización.

Además de los tres elementos anteriormente mencionados, es de vital importancia programar capacitaciones para el personal involucrado en la implementación del SGDEA y contar con el acompañamiento de personal experto en Gestión del Cambio antes, durante y después de la puesta en producción del sistema tecnológico.

8. MODELO DE REQUISITOS

8.1 Descripciones Generales

El Departamento Gestión Documental tiene entre sus responsabilidades *"Liderar la gestión electrónica de documentos de archivo en EPM"* y para su cumplimiento, se apoya en la implementación de habilitadores tecnológicos que promuevan la materialización de la estrategia de la Organización, plasmada en el modelo definido en la Arquitectura Empresarial.

Por tanto, se hace imprescindible enmarcar la gestión documental de EPM dentro de dos focos que se articulan estratégicamente para generar valor desde la información y los datos: *Gestión Electrónica de Documentos y Transformación Digital.* El análisis del proceso desde ambos puntos de vista evidenció la necesidad de adquirir e implementar las herramientas tecnológicas del Dominio funcional de Gestión Documental, cuyas capacidades están determinadas por el tratamiento técnico que requieren los contenidos, en concordancia con los asuntos normativos y las características inherentes a los tipos de formato (*Ver ilustración de capacidades y servicios del dominio de gestión documental)*.
A continuación se describen los aplicativos actualmente en uso:

- Mercurio: sistema de información corporativo para la Gestión de comunicaciones oficiales. Cuenta con capacidades especializadas para la gestión de radicados internos y externos tal como lo establece el Archivo General de la Nación a través del Acuerdo 060 de 2001. En este sentido, Mercurio permite radicar, registrar y direccionar al competente las comunicaciones oficiales, tutelas y derechos de petición recibidas en la Organización. Además, permite proyectar, distribuir, aprobar, firmar y enviar a los destinatarios correspondientes las comunicaciones producidas.

- Vault: herramienta que soporta la documentación técnica de los activos físicos productivos de los negocios durante su etapa constructiva y durante su operación y mantenimiento. Este sistema permite manejar el detalle de cada diseño, evidenciando las relaciones entre los diferentes componentes técnicos de los activos físicos, y la

gestión de las ordenes de cambio y las ordenes de ingeniería que se emiten sobre estos elementos.

- Enter: sistema de información corporativo para la gestión de documentos en EPM. Su función principal es la de soportar la construcción colaborativa, aprobación, publicación y el almacenamiento de archivo. Se ha constituido en el Enterprise Content Management System (ECM) de la Organización. Actualmente, los servicios de Enter están distribuidos en los siguientes módulos: Actos Administrativos, Expediente del Cliente, Expediente de Historias Laborales, Planotecas digitales, donde reposan las imágenes digitalizadas de las antiguas planotecas físicas de los negocios; y Documentos de la Arquitectura Empresarial, donde se controlan los documentos y registros de procesos y sistemas de gestión.

  Enter fue sometido a una evaluación detallada por parte de un equipo interdisciplinario, quien concluyó que este gestor de contenidos no cumple funcionalmente con los requisitos mínimos establecidos para la implantación de un Sistema de Gestión de Documentos Electronicos de Archivo – SGDEA. Asimismo, no se contempla su adaptación debido a que por políticas internas, la primer alternativa de solución para satisfacer una necesidad de tecnología es investigar si esta disponible en el mercado y proceder a adquirirla cuando esta cumple con el 80% de los requisitos estipulados en la empresa. En caso de que no existiera el aplicativo en el mercado sería necesario proceder a desarrollarlo, opción menos recomendable debido a que requiere una mayor inversión de tiempo y recursos. En este caso, en Colombia si existen múltiples proveedores de sistemas de información para el control integral de los documentos durante su ciclo de vida, los cuales favorecen la implementación de estrategias para asegurar los atributos de la documentación generada en la Organización.

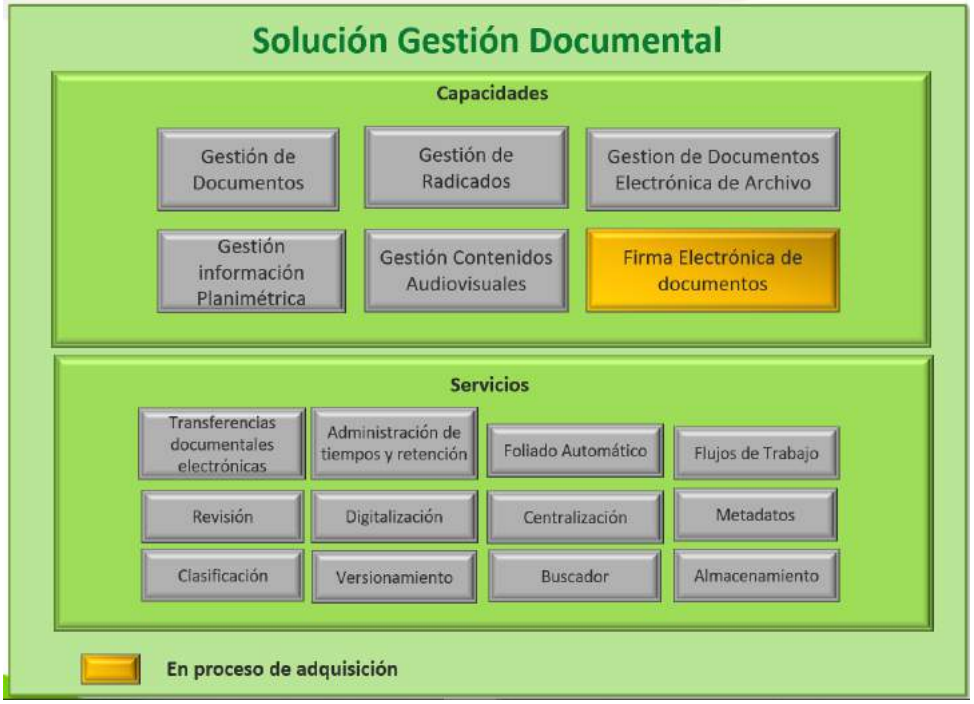


Ilustración 5. Capacidades y servicios GD

a. Arquitectura objetivo

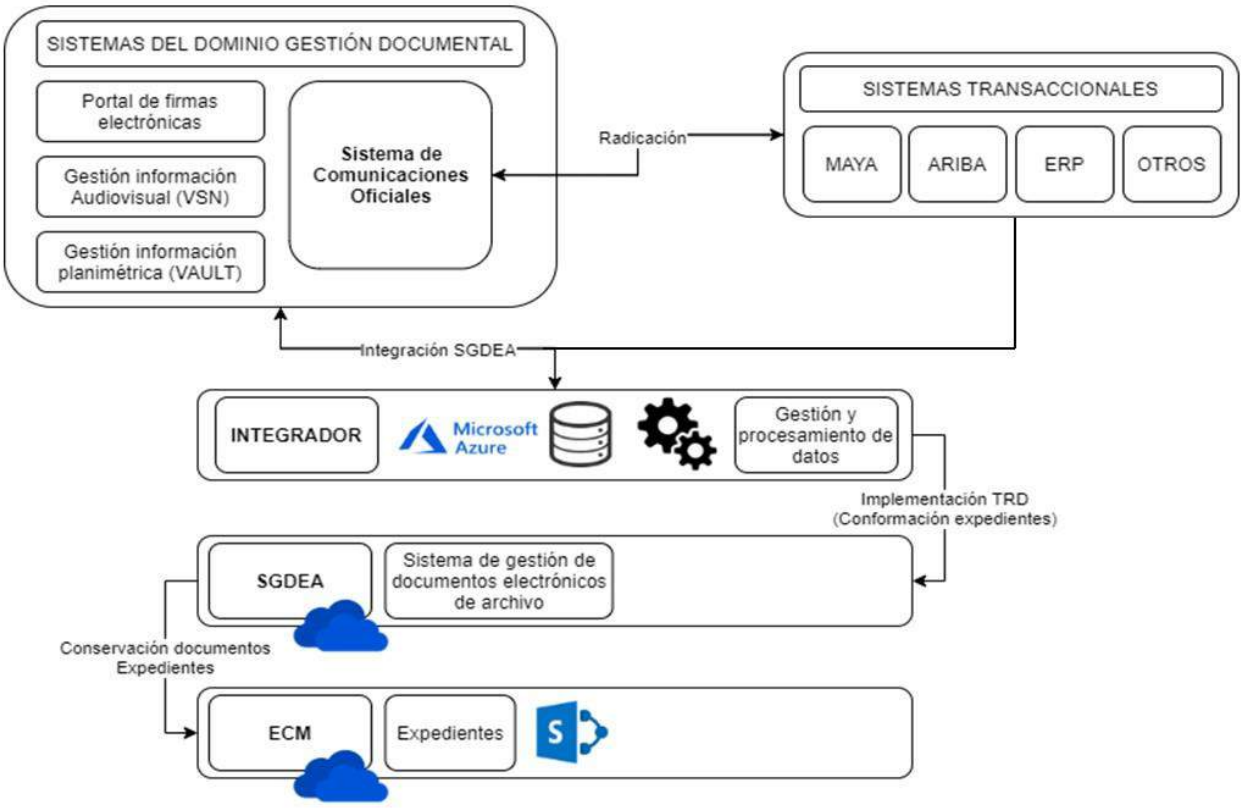


Ilustración 6. Arquitectura objetivo de alto nivel

En la ilustración se representan todos los sistemas de domino de gestión documental que hacen parte de la arquitectura objetivo. En ella se refleja como los sistemas transaccionales se comunican a través de interfaces con el Sistema de Comunicaciones Oficiales con el propósito de radicar los Derechos de Petición, Quejas, Reclamos, Denuncias o Felicitaciones que se reciban o produzcan en la Organización.

El Sistema de Gestión de Documentos Electrónicos de Archivo será la herramienta que soporte la implementación de las TRD en la Organización. Los sistemas del dominio funcional para la gestión de documentos de archivo de tipo planimétrico y audiovisual y el ECM se deberan integrar a él partir de la función que ejecuta de manera automática el componente integrador. Este ecosistema será el oficial para el almacenamiento de los documentos de archivo en EPM.

A continuación se presenta una breve descripción y se establecen los requisitos funcionales de los sistemas de información que conforman la arquitectura objetivo de Gestión Documental en EPM:

b. Gestor de comunicaciones oficiales en el entorno tecnológico

Las comunicaciones oficiales son aquellas que se intercambian entre EPM y sus grupos de interés en cumplimiento de una actividad, un proceso organizacional, o en cumplimiento de su objeto social. Su tratamiento archivístico deberá ejecutarse conforme a lo establecido en el Acuerdo 060 del año 2001 y el *Manual de Gestión y Trámite de Comunicaciones Oficiales Escritas* que ha sido elaborado, publicado y difundido por el Departamento Gestión Documental.

Es relevante mencionar, que aquellas comunicaciones que por asuntos administrativos o legales tengan que ser generadas y transmitidas en *soportes análogos, como el papel,* deberán cumplir con los protocolos archivísticos establecidos en la Organización y adicionalmente, deberán ser digitalizadas e incorporadas electrónicamente al expediente que pertenece según su naturaleza.

El sistema actual que soporta la producción, trámite y conservación de las comunicaciones en EPM es Mercurio. Este sistema de información asigna de manera automática un código único (radicado) que identifica los documentos y sus respuestas asociadas y, cuenta con mecanismo de firma electrónica que permite asegurar que la persona que firma la comunicación es quien dice ser. Allí se encuentran configurados los flujos de trabajo necesarios para la creación, aprobación y despacho de las comunicaciones oficiales de la Empresa.

Respecto a la clasificación de las comunicaciones oficiales, es importante mencionar que Mercurio no cumple con los parámetros mínimos exigidos para asegurar el Vinculo Archivístico, característica señalada en el literal i del artículo 2.8.2.5.5 del Decreto 1080 de 2015, la cual constituye el principio primordial para garantizar la integridad de los expedientes documentales registrados en el Cuadro de Clasificación Documental y las respectivas TRD de cada dependencia. Por lo anterior, EPM deberá emprender acciones orientadas al cumplimiento de los requisitos para la conformación integral de los expedientes electrónicos, disponiendo de

herramientas tecnológicas que permitan vincular las comunicaciones por razones de procedencia, proceso o función y que posibiliten que dicho vinculo se mantenga en el tiempo, a través de metadatos que reflejen el contenido, el contexto y la estructura tanto del documento como de la serie, subserie y expediente al que pertenecen. Adicionalmente, las auditorías internas al sistema han revelado fallas técnicas que vulneran la seguridad de la información, ponen en riesgo la continuidad de las operaciones y complejizan la interacción del usuario con la herramienta durante el proceso de producción, recepción y tramite de las comunicaciones oficiales.

Por lo anterior y en cumplimiento de las pautas establecidas por el Archivo General de la Nación, EPM deberá seleccionar un nuevo gestor de comunicaciones oficiales que atienda a los requisitos funcionales mínimos obligatorios descritos a continuación:

N°	REQUISITO
GESTIÓN DE COMUNICACIONES OFICIALES	
1	El SGDEA permite administrar las comunicaciones oficiales de acuerdo con los lineamientos establecidos en el Acuerdo 060 de 2001 del AGN.
2	El SGDEA permite realizar reportes de las distintas operaciones tales como: devoluciones a radicación, radicados por asunto, radicados por flujos de trabajo, radicados por dependencia, radicados por usuario entre otros.
3	El SDEA permite distribuir las comunicaciones oficiales a cada una de las dependencias responsables
4	El SGDEA permite archivar automáticamente las comunicaciones en el expediente correspondiente
ASUNTO	
5	La solución debe permitir configurar nuevos asuntos, administrar, modificar e inactivar los asuntos de las comunicaciones oficiales
6	La solución debe permitir asignar un código a cada asunto automáticamente en la configuración
7	La solución debe permitir asociar un asunto a una dependencia, a una ruta o que sea usado de manera genérica con cualquier dependencia (Cuando no trae un destino asociado al asunto)
8	La solución debe permitir que al generar la(s) respuesta(s) a partir del radicado recibido, queden asociados y relacionados a un mismo asunto.
9	La solución debe permitir asociar un asunto a una o varias filiales
10	La solución debe permitir marcar si los asuntos requieren respuesta o no.

11	La solución debe permitir que al asunto de un radicado recibido se le pueda configurar el tiempo definido por ley para dar la respuesta. (Tutelas, Acciones populares, Notificaciones Judiciales)
AUDITORÍA	
12	La solución debe permitir generar log de auditoría (trazabilidad) de las acciones (metadatos, documentos, asignaciones, repositorios de imagenes y bases de datos) realizadas por cada uno de los usuarios que ingresan al sistema.
REPORTE	
13	La solución debe permitir configurar los reportes de manera dinamica y de acuerdo a las necesidades corporativas tanto de historicos como documentos vigentes ejemplo: devoluciones a radicación, radicados por asunto, radicados por flujos de trabajo, radicados por dependencia, radicados por rutas, estados de atención, respuesta asociada, tiempo de atención, radicados por usuario, entre otros.
14	La solución debe permitir la extracción de información (reportes) en formatos .CSV, .PDF, XLSX, .TXT u otros
CONFIGURACIÓN	
15	La solución debe permitir hacer devoluciones a radicación en el caso de que se requiera cambiar el asunto o el destinatario para la atención de comunicación recibida
16	La solución debe permitir configurar perfiles, roles de usuario y permisos de forma dinámica
17	La solución debe permitir personalizar su entorno gráfico de acuerdo con el manual de marca definido por Identidad corporativa. Y debe ser independiente para cada una de las filiales de Grupo EPM
18	La solución debe permitir configurar el calendario local, franja horaria, Idioma por defecto (Español)
19	La solución debe permitir ingresar los datos básicos de identificación para cada tipo de documento cuando se recibe, además permitir la adición de otros campos. Ejemplo: Numero de radicado y fecha de origen, Nombre del radicador, Nombre, Nit, y ciudad de remitente, Asunto, Requiere o No respuestas, Tiempo de respuesta y unidad de medida, Prioridad, Tipo de documento – serie/subserie TRD, Destinatario o Ruta si no esta relacionado al asunto, entre otros
20	La solución debe permitir ingresar los datos básicos que debe tener cada tipo de documento cuando se genera, además permitir la adición de otros campos. Ejemplo: Plantilla, Radicado por (automatico asociado al usuario la solución) Datos del Remitente; nombre y municipio, Datos del destinatario Nombre, Nit, y ciudad (predefinido cuando es una respuesta) Asunto (predefinido cuando es respuesta) Tipo de documento – serie/subserie TRD

21	La solución debe permitir que cuando se ingresen los datos basicos en el formulario de radicación para produccion de radicados externos, internos y memorandos, se carguen los datos a la plantilla correspondiente de manera automatica
22	La solución debe permitir configurar en la plantilla de radicación de los diferentes tipos de documentos, campos adicionales o complementarios a los predefinidos inicialmente
23	La solución debe permitir la clasificacion o reserva de los documentos por un tiempo definido (durante ese tiempo la imagen queda oculta y solo la puede ver la dependencia del destinatario) y debe tener un mecanismo automatico que permita levantar la clasificación o reserva de un documento cuando cumpla el tiempo
24	La solución debe permitir la indexación y asociación masiva de las imágenes a cada uno de los radicados a partir de su número de identificación (Aplica para documentos en soporte fisico que son previamente digitalizados)
25	La solución debe permitir la radicación masiva de documentos producidos a partir de plantilla y combinación de correspondencia, generando un consecutivo para cada comunicación
26	La solución debe permitir al perfil administrador transferir de manera masiva las comunicaciones que una persona tiene pendiente por atender a otra persona
27	La solución debe permitir configurar las funcionalidades que puede realizar cada perfil de acuerdo al tipo de documento
28	La solución debe permitir configurar el cargo de "encargado" para tener la opcion de elegir al momento de firmar documentos
29	La solución debe permitir que al radicar cualquier tipo de documento traiga por defecto el usuario logueado
30	La solución debe permitir a un usuario que tenga acceso a las diferentes filiales, por ejm: Si atiende comunicaciones oficiales recibidas visualizarlas en una misma vista.
31	La solución debe permitir que las comunicaciones recibidas, asignadas a una dependencia puedan ser visualizadas y atendidas por varias personas de la dependencia
32	La solución debe permitir la configuración de las alertas asociadas a los términos de vencimiento
33	La solución debe permitir enviar los radicados desde la herramienta a través de correo electrónico a usuarios internos o externos y que quede la trazabilidad y como remitente el usuario logeado
34	La solución debe permitir la confirmación de lectura del correo electronico enviado desde la herramienta de radicación
CONTROL	

35	La solución debe mostrar la trazabilidad que ha tenido un radicado
36	La solución debe permitir hacer comentarios a quien tenga asignada una comunicación para el trámite y dejar registrado el usuario, fecha y hora del comentario, estos no podran ser modificados o eliminados
FIRMAS	
37	La solución debe permitir la aprobacion de los documentos por medio de firmas solo por las personas autorizadas, ya sea que el documento requiera 1 o multiples firmas
38	La solución debe permitir firmar los documentos de manera secuencial o en paralelo.
39	La solución debe permitir firmar documentos a través de firmas electrónicas, con minimo doble factor de autenticación, o haciendo uso de certificados digitales emitidos por PKI de EPM o por entidades acreditadas
GENERAL	
39	La solución debe permitir administrar las comunicaciones oficiales de acuerdo con los lineamientos establecidos en el Acuerdo 060 de 2001 del AGN
40	La solución debe permitir la radicación de comunicaciones oficiales en sus diferentes tipos: documento recibido, producido, interno, memorando, entre otros
41	La solución debe permitir distribuir las comunicaciones oficiales a cada una de las dependencias responsables
42	La solución debe registrar trazabilidad de la fecha, hora y usuario que haga uso de la radicación de las comunicaciones
43	La solución debe evitar la eliminación o cambio de la imagen asociada a un radicado una vez indexada
44	La solución debe garantizar la proteccion de las imagenes y bases de datos sin que se vulnere los perfiles de seguridad
45	La solución debe permitir subir anexos al radicado y visualizarlos
46	La solución debe permitir en una vista principal del radicado visualizar la gestión o estado de atención del documento
47	La solución debe imprimir los datos del radicado para los documentos recibidos fisicos través de un codigo QR / barras o similar
48	La solución debe permitir asignar un número de radicado con un procedimiento rapido, con el objetivo de agilizar la recepción de las comunicaciones en soporte fisico en las taquillas de correspondencia, de tal forma que el radicado se asigme sin diligenciar la ficha de radicación y en un momento posterior permita completar los datos, indexar imágen y enrutar al competente para su atención.
PLANTILLA	
49	La solución debe permitir que al generar respuesta desde el radicado recibido se recuperen datos de manera automatica como destinatario, asunto, entidad…) en una plantilla correspondiente

50	La solución debe permitir configurar multiples plantillas para cada tipo de comunicación
51	La solución debe garantizar que la radicacion de documentos externos, internos y memorando sea exclusivamente a partir del uso de plantillas controladas
52	La solución debe permitir que cuando la última persona de un flujo de aprobación firme el documento se produzca el PDF con número de radicado, fecha, firma, cargo y dependencia
53	La solución debe permitir al usuario relacionar en las plantillas varios firmantes en el flujo de aprobación de un documento
SUPLENCIA	
54	La solución debe permitir al responsable de atender las comunicaciones que llegan a una dependencia, programar las suplencias (reemplazo temporal por una novedad como vacaciones, encargos , entre otras) y que se restablezca automaticamente con la fecha definida de terminación de la suplencia y que tenga alcance aplicación o funcionalidades donde un usuario tenga acceso, incluyendo los flujos de trabajo
TRD	
55	La solución debe permitir asociar la comunicación al expediente al que pertenece, según lo establecido en la Tablas de Retención Documental
RUTAS	
56	La solución debe permitir configurar de acuerdo con las necesidades de la organización, los flujos de atención de las comunicaciones oficiales especificando: Pasos del flujo, personas que participan en cada paso, tareas a realizar en cada paso y distribución de la tareas basados en condiciones en cada paso, asignación de tareas en flujos de aprobación de acuerdo con la distribución de cargas de trabajo, distribución por asuntos, distribución por peso de la tarea, distribución por condicion, distribución diaria
57	La solución debe permitir que en una misma ruta ingresen y se asignen los radicados de diferentes filiales, manteniendo la independencia en los consecutivos de la numeración de cada filial
58	La solución debe permitir activar e inactivar los pasos, tareas, personas o flujos de trabajo configurados previamente
IMPRESIÓN	
59	La solución debe permitir generar e imprimir en las comunicaciones fisicas el código QR / barras a través de multiples fabricantes y tecnologías de impresión

c. Gestión de documentos audiovisuales: audios, videos y fotografías

El uso incremental de medios tecnologicos para apoyar el desarrollo de los procesos en la Organización ha generado un aumento siginificativo del volumen de información electrónica que se produce en EPM, representada no solo en documentos tipo texto sino también audios, fotografías y videos que dan cuenta del cumplimiento de las funciones misionales, estratégicas y de apoyo. Su masificación esta imponiendo nuevos retos y es necesario que estos contenidos se clasifiquen y controlen de tal forma que puedan estar disponibles para los distintos grupos de interés y a su vez, que puedan ser preservados en el largo plazo de acuerdo con el valor legal, administrativo e histórico que posean según su naturaleza.

Por ello, se debe informar que la Organización ha adquirido un sistema para la gestión de los documentos audiovisuales que permitirá el almacenamiento, gestión y control de las fotografías, videos y audios que hacen parte integral de los expedientes, las series y las subseries identificadas en la tabla de retención vigente, así como aquellos contenidos que conforman el archivo audiovisual institucional. Este sistema deberá asegurar la interoperabilidad con el SGDEA corporativo y con los demás sistemas de información del dominio de gestión documental, de manera que se pueda cumplir con los principios de procedencia, orden original y vinculo archivístico reglamentados en la normatividad vigente.

Para su implementación se debe asegurar que se cumpla con las directrices y mejores prácticas registradas en el programa especifico de documentos especiales de la empresa.

A continuación se detallan los requisitos funcionales mínimos evaluables para la adquisición e implementación del sistema de gestión de documentos audiovisuales:

N°	REQUISITO
GENERAL	
1	La solución debe soportar multicompañía, es decir, permitir la gestión de datos para múltiples compañías
2	La solución debe permitir gestionar videos, audios y fotografías

3	La solución debe permitir el cambio de extensión de los archivos cargados (wmv a mp4)
4	La solución debe permitir la carga de archivos, superiores a un 1 Gb de tamaño
5	La solución debe permitir la carga masiva de archivos
6	La solución permite personalizar su entorno gráfico de acuerdo con los colores e imágenes corporativas
7	La solución permite reproducir y/o descargar un video o una fotografía en el que se incluya una marca de agua configurable
8	La solución permite la identificación automática de la ubicación geográfica del material grabado (si el contenido trae esta ubicación)
9	La solución genera subtítulos para los vídeos y audios
10	La solución permite la transcripción de audios o vídeos
11	La solución debe permitir parametrizar y configurar la herramienta para la operación de múltiples compañías de manera centralizada
12	La solución tiene pluggins para acceso externo al material audiovisual
INGESTA	
13	La solución debe permitir cargar y reproducir los siguientes formatos de archivos de audio, fotografía y video : Videos: •.mov, .wmv, .mp4, .flv, .mts, .mpg, .AVI, .MPEG, .H264, .mxf, .mkv, .XVID, .mj2, .mjp2 Audio: •.mp3, .wav, .AAC, .WMA, .OGG, .aiff, .opus, .mpeg, .Aif, MP3Pro, Vorbis, RealAudio, .bwf .VQF, .AIFF, .FLAC, .WAV, .MIDI, .mka, .OGG. Fotografía o imagen: • .jpg, .gif, .tiff, .png, .bmp, raw, .ILBM, .jpg2, .jpg, .odg, HD Pro
14	La solución debe permitir configurar formatos adicionales para los archivos a cargar en el momento en que se requiera
15	La solución permite ingestar el audio por canales separados cuando sea necesario.
CONTENIDO AUDIOVISUAL	
16	La solución permite la carga de Rushes o material en bruto

17	La solución debe permitir incluir marcaciones o metadatos en el timeline de los audios o videos para su clasificación y búsqueda, y poder hacer búsquedas sobre esos contenidos, con el fin de extraer desde el mismo sistema segmentos de video y audio (sin necesidad de recurrir al video completo)
18	La solución debe permitir almacenar el contenido en su formato original y generar una versión de baja resolución que optimice su tamaño para su consulta
CLASIFICACIÓN	
19	La solución debe permitir configurar metadatos asociados a tipos de archivos audiovisuales, los cuales permitan su organización y búsqueda y que sean diferentes por secciones o agrupaciones de contenido
20	La solución debe permitir realizar el almacenamiento de contenido audiovisual en sitios por empresa y por secciones o agrupaciones de contenidos con sus respectivos metadatos, roles y permisos
21	La solución debe permitir clasificar el contenido audiovisual como reservado o público de manera granular (por archivo) o por sección o agrupación de contenido
22	La solución permite importar bases de datos para completar desde allí los metadatos de un contenido audiovisual que se vaya a cargar
23	La solución permite la reclasificación o cambio de nombres y metadatos en bloque (por ejemplo, cuando cambie el nombre de una dependencia de la Organización)
BUSQUEDA/CONSULTA	
24	La solución permite hacer búsquedas utilizando los metadatos de los archivos audiovisuales como criterios de búsqueda
25	La solución debe permitir previsualizar los archivos audiovisuales sin que ello implique descargarlos
26	La solución debe permitir descargar los contenidos audiovisuales en formatos predefinidos, diferentes a los de carga
27	La solución permite filtrar búsquedas a través de varios criterios que logren búsquedas avanzadas
28	La solución permite retornar al menos 1000 registros como resultado de las búsquedas.
AUDITORÍA	
29	La solución debe permitir generar log de auditoría de las acciones realizadas por los usuarios que ingresan al sistema
30	La solución debe permitir generar log de auditoría de las acciones realizadas por cada archivo audiovisual
REPORTES	
31	La solución permite la extracción de metadatos de los audiovisuales masivamente y su correspondiente acceso (ruta) al archivo
DISTRIBUCIÓN	
32	La solución debe permitir distribuir el contenido, ya sea compartiendo un enlace para descarga o descargándolo directamente.

ALMACENAMIENTO	
33	El sistema debe permitir definir el lugar donde se almacenan los videos, audios, fotografías y contenido multimedia en general: SAN o NAS. Nota: Tener en cuenta el apartado de “Infraestructura y despliegue” para proporcionar datos técnicos en caso de sugerir otro tipo de tecnología.
AUTENTICACIÓN	
34	La solución debe integrarse con el Directorio Activo o ADFS usando protocolos SAML 2.0 o OAuth 2 para el proceso de autenticación de usuarios
DATOS	
35	El sistema debe permitir inactivar los contenidos audiovisuales que cumplan con la regla de negocio enviada por otro sistema
36	La solución debe ofrecer mecanismos para evitar la eliminación o borrado de información en la base de datos de contenidos audiovisuales.
37	La solución debe permitir configurar periódicamente tareas de eliminación de contenidos audiovisuales inactivos
DISPONIBILIDAD	
38	La solución debe garantizar una disponibilidad de la solución no menor al 99.5%
39	La solución cuenta con mecanismos de recuperación de datos o información ante eventos inesperados de falla
ESCALABILIDAD	
40	La solución debe tener la flexibilidad y capacidad de crecer en respuesta a las necesidades del Grupo EPM según número de contenidos media sin ver afectada su funcionalidad, desempeño, fiabilidad y disponibilidad
INTEGRACIÓN	
41	La solución debe permitir extraer metadatos y contenido audiovisual para envío a otros sistemas.
42	La solución debe permitir el consumo y exposición de servicios web de sus funcionalidades básicas mediante protocolos de integración REST o SOAP
43	La solución soporta estándares de intercambio de datos tales como XML o JSON.
44	La solución almacena la información sensible de tokens y claves de acceso a los servicios bajo métodos seguros
45	La solución está en la capacidad de realizar carga masiva de contenidos audiovisuales y metadata usando diferentes fuentes de metadata como archivos xml, Excel o una base de datos.
46	La solución tiene transacciones implementadas en forma asíncrona, lo que implica que debe exponer un servicio para recibir la respuesta de forma posterior
47	La solución registra la información (Fecha y otros datos) en que se envío el registro (evento) en una integración asíncrona
48	La solución puede establecer fecha máxima para recibir la respuesta definitiva en una integración asíncrona

49	La solución registra información(datos y fecha con horas) en que se recibió la respuesta en una integración asíncrona.
50	La solución tiene la capacidad para actualizar los registros de datos con la respuesta de una integración asíncrona.
51	La solución tiene un sistema de registro de logs del proceso de integración y estos se pueden consultar o exportar
52	La solución cuenta con un diccionario de manejo de errores y códigos de error de integración
53	La solución al realizar la exportación de datos informa que los datos fueron exportados al sistema de staging o temporal
54	La solución al importar datos informa que los datos fueron importados al sistema de staging
55	La solución importa datos a tablas de interoperabilidad o a una area de staging
56	La solución exporta datos a tablas de interoperabilidad o a una área de staging
57	La solución se conecta a servicios de nube como almacenamientos, colas y otros.
58	La solución cuenta con el protocolo smb última versión de uso compartido de recursos de red o tecnología NDI que permita una integración con el tricaster.
59	La solución de estar en la capacidad de enviar mensajes compuestos por múltiples registros cuando consume un servicio de notificación de eventos
60	La solución tiene la capacidad de procesar respuestas con mensajes compuestos por uno y/o múltiples registros luego de consumir un servicio de notificación de eventos
SEGURIDAD	
61	La solución debe permitir el intercambio de datos entre soluciones externas y la solución por medio de protocolos seguros como HTTPS
62	La solución debe contar con control de acceso y registro de auditoría para el acceso a los contenidos audiovisuales, ya sea por usuarios, programas, servicios web, servicios de integración con otras aplicaciones o entidades
63	La solución cuenta con prácticas de DevOps para validación de seguridad, análisis estático de código y vulnerabilidades del sistema
SERVIDORES VIRTUALES	
64	La solución debe poderse desplegar en servidores virtuales
USABILIDAD	
65	La solución debe permitir la carga de contenido audiovisual masiva desde pantallas de usuario (capa de presentación – importación de datos).
66	La solución debe permitir la descarga de contenido audiovisual masiva desde pantallas de usuario (capa de presentación – exportación de datos)
67	La solución debe permitir el movimiento de contenidos en bloque entre medios de almacenamiento de media o alta disponibilidad.

68	La solución es compatible con los navegadores MS Edge y Google Chrome
ARQUITECTURA	
69	La solución debe cumplir con las especificaciones de WEB Enabled que permite ejecutarse desde cualquier dispositivo.
70	La solución soporta un esquema multi-tenant, administrado desde una instancia única de la solución del software, usando una configuración base y reglas de negocio que pueda ser compartida por todas las filiales nacionales del grupo EPM.
71	Bajo una misma instancia de la solución del software se habilitan niveles de visibilidad de información por filiales. Una filial no tiene visibilidad de la información de otra filial en su mismo nivel.
72	La solución tiene la capacidad de realizar upgrades de la aplicación una sola vez y que el cambio se vea reflejado en todas las filiales gestionadas al tiempo.
GESTIÓN DE VIDEOS	
73	La solución cuenta con analítica de contenidos generando reportes con la metadata (cantidad de videos por sección, usuarios que cuentan con permisos en cada sección, cantidad de videos sobre tema x)
ALERTAS	
74	La solución permite alertas que informen al usuario sobre los errores que se presentan durante la búsqueda o ingesta de contenido (Ejemplo: Inconsistencia de datos, error en formato)
FLUJOS	
75	La solución permite configurar flujos para tareas automáticas como transcodificación, ingesta masiva, aprobación o eliminación de contenido
DERECHOS DE USO	
76	La solución permite ingestar documentos en formato pdf, en este caso imágenes de los permisos de uso de derechos del material.
MANTENIBILIDAD	
77	La solución es "basada en reglas" donde se permita al usuario configurar y mantener el software sin requerir mayor intervención de analistas técnicos
78	La solución permite la actualización de versiones o "releases" sin impactar las configuraciones del usuario
79	La solución registra los errores con los detalles de la causa raíz del error, el usuario, el proceso que lo generó y la excepción generada
80	El sistema muestra al usuario claramente el error o errores presentados
ACCESIBILIDAD	
81	La solución cumple con el estándar de accesibilidad web NORMA NTC5854 - basada en los lineamientos internacionales WCAG 2.0 -Nivel A y el doble AA de la norma-. (Opcional)
EFICIENCIA	

82	La solución debe tener la capacidad de ejecutar diferentes módulos de ésta, en servidores diferentes para distribuir la carga y evitar pugna de recursos - Esquema de alta disponibilidad.

d. Portal de firmas

Con el objetivo de tener en EPM una solución de largo plazo que permita inmaterializar los documentos, avanzar en la estrategia corporativa de gestión electrónica de documentos, mitigar los riesgos y vulnerabilidades en los procesos frente al repudio por debilidades en la identificación del firmante, la trazabilidad de la firma y la integridad del contenido, además, corregir los procedimientos no controlados que se llevan a cabo por fuera de los sistemas de gestión documental corporativos para la aprobación y firma de documentos, se requiere de una herramienta tecnológica que permita aprobar documentos oficiales a través de mecanismos de firma electrónica y firma digital, según lo ampara la norma en la ley 527 de 1999 y los decretos reglamentarios 2364 de 2012 y 333 de 2014, respectivamente, de manera segura y controlada.

A partir del análisis de las necesidades actuales se concluye que la Organización requiere disponer de una herramienta informática que permita:

- Obtener el consentimiento de los firmantes y la aprobación del contenido de forma no presencial.
- Garantizar un procedimiento controlado de firma de documentos, de manera electrónica y digital, que cumpla con los criterios de integridad, trazabilidad y confiabilidad.
- Conectar tecnológicamente los diferentes actores que intervienen en la aprobación y firma de los documentos, agregando agilidad en la ejecución de los procesos.
- Mitigar el riesgo de fuga de información evitando la intermediación de personas no involucradas o autorizadas en el envío, recepción y firma de documentos oficiales.
- Oficializar hacia entidades externas la veracidad de la firma en caso de ser requerido.
- Firmar usando certificados emitidos por la PKI de EPM o por terceros acreditados por la ONAC.

A partir de lo expuesto, se evidencia con claridad la necesidad de adquirir, implementar y mantener un Portal de Firmas en el cual se gestionen los flujos de trabajo para la firma electrónica y se autentique el firmante a partir de los datos suministrados durante el enrolamiento y verificación de la identidad de la persona, actividad que es de total responsabilidad del proceso de negocio.

La adquisición o desarrollo del aplicativo tecnologico deberá estar basada en los siguientes requisitos:

N°	REQUISITO
1	La solución debe permitir firmar documentos electrónica y digitalmente que se gestionan con diferentes públicos de interés tanto internos como externos, tales como: proveedores, contratistas, empleados, inversionistas, gobierno, clientes, junta directiva.
2	La solución debe permitir la marcación de los campos en un documento donde debe firmar y/o aprobar cada firmante.
3	La solución debe tener la capacidad de iniciar y gestionar un flujo para la aprobación y firma de un documento con características como: envío de documentos por correo electrónico y orientación para firmar o aprobar.
4	La solución debe permitir el envio de notificaciones a través del correo a los participantes y otros destinatarios en la aprobación o firma del documento.
5	La solución debe tener la capacidad de especificar el orden en el que se debe firmar.
6	La solución debe tener la capacidad de firmar diferentes documentos de manera independiente y simultánea.
7	La solución debe permitir firmar documentos de forma masiva
8	La solución debe permitir asignar diferentes acciones a los participantes como entrega (copia), aprobación (VoBo) o firma del documento.
9	La solución debe tener la capacidad de adjuntar al documento que se va a firmar: imágenes u otros documentos de manera complementaria al procedimiento de firma.
10	La solución debe tener la capacidad de poder visualizar el estado de un proceso de firmado de un documento.

11	La solución debe registrar todos los eventos y las acciones realizadas por las personas que han participado en la transacción, permitiendo realizar auditoría. Especificar donde queda almacenada esta información y por cuanto tiempo.
12	La solución debe permitir la consulta de los registros de trazabilidad de los documentos para realizar auditorias.
13	La solución debe permitir que los firmantes y remitentes tengan acceso a los documentos en cualquier momento y lugar, 24 horas al día, es decir disponibilidad 7 x 24.
14	La solución debe permitir que el documento final tenga un certificado que garantice que no ha sido manipulado (integridad).
15	La solución debe tener la capacidad de garantizar que los firmantes no puedan repudiar su firma como consecuencia de los controles de autenticación. Describir como se realiza este proceso.
16	La solución debe permitir que se registre y certifique la trazabilidad y auditoría de las acciones ejecutadas por los firmantes. La información debe quedar incorporada en el documento firmado.
17	La solución debe garantizar el cumplimiento legal del Decreto 2364 de 2012 y de seguridad de la firma electrónica.
18	La solución debe tener la capacidad de almacenar los documentos firmados en un entorno seguro.
19	La solución debe tener la capacidad de almacenar los documentos firmados tanto en la aplicación que lo invoca como en el firmador, en los casos que se presenten integraciones.
20	La solución debe permitir al menos dos factores de autenticación para la firma electronica de los siguientes:• La solución debe permitir el factor de autenticación que certifique lo que soy: Huella Digital, grafo o firma manuscrita digitalizada, escribir en la pantalla, dibujar, usar pad de firma u otro mecanismo biométrico que permita autenticar al firmante de acuerdo con sus propias características. Describir como se hace este proceso de certificación. • La solución debe permitir el factor de autenticación que certifique lo que soy: Huella Digital, grafo o firma manuscrita digitalizada, escribir en la pantalla, dibujar, usar pad de firma u otro mecanismo biométrico que permita autenticar al firmante de acuerdo con sus propias características. Describir como se hace este proceso de certificación. • La solución debe permitir el factor de autenticación que certifique lo que sé: Contraseña de acceso al correo electrónico del firmante, ya sea de uso personal o corporativo, o contraseña de firma registrada en la solución informática o ambas. • La solución debe permitir el factor de autenticación que certifique lo que tengo:Token o algo equivalente que represente lo que posee. Describir como se hace este proceso de certificación.

21	La solución debe garantizar que exista una única persona detrás de cada firma electrónica.
22	La solución debe dejar evidencia de la identificación del firmante. Esto puede ser, capturando audio de la voz del firmante o representacion grafica de la huella, su geolocalización, los datos del dispositivo desde donde firma, la captura de su imagen, de su voz, o de su documento de identidad. Describir las formas como se puede realizar.
23	La solución debe garantizar que cuando se realice la creación de la firma electrónica, se usen los datos que el firmante puede utilizar, bajo su control exclusivo. Esto es, identificando el dispositivo del firmante, o si sólo se puede acceder a la firma a través de su cuenta privada (correo electrónico) y/o linea móvil.
24	La solución debe garantizar que la firma esta vinculada con los datos firmados por la misma, de tal modo que, cualquier modificación o alteración posterior del documento sea detectable.
25	La solución debe tener la capacidad de que se registre y certifique la trazabilidad y auditoría de las acciones ejecutadas por los firmantes como información complementaria del documento aprobado.
26	La solución debe tener la capacidad de que el documento sea recibido en su integridad por el destinatario, y que puede cumplirse tecnológicamente, el “sellamiento” del documento. En otras palabras, al final del proceso de firma, el documento debe estar protegido contra edición o sustracción de información.
27	Cada documento firmado tiene una URL para validación del proceso de firma
28	La solución debe permitir la firma de documentos a través de firma electrónica o firma digital (haciendo uso de certificados digitales emitidos por terceros)
29	La solución debe permitir que despues de creado el documento en Microsoft Word o PDF, insertar los campos para la firma y poder iniciar el proceso de firma sin necesidad de ingresar a la consola de firma o firmador.
30	La solución debe permitir la integración de tal forma que se puedan incorporar los campos de firma y correos electrónicos de los firmantes con aplicaciones como: Office 365, Ariba, JDE, AuraCuantic (BPMS), Dynamics 365, APIs Rest o WEB Services que permitan integraciones con otras aplicaciones.
31	Describir con cuales si tiene integración y que tan complejo es el proceso de integración.
32	La solución debe permitir firmar documentos desde un dispositivo móvil Android/IOS.
33	La solución debe permitir analítica descriptiva o generación de reportes para hacer seguimiento por tipo de documento, estado del documento.
34	La solución debe permitir la personalización de las listas de entidades de certificación de confianza permitidas para firmas digitales.
35	La solución debe permite integrar una autoridad de estampa de tiempo (TSA) de acuerdo con el RFC3161 de manera que quede en el documento sellado.

36	La solución debe permitir de 1 a 20 (o mas) firmantes por cada documento
37	La solución debe permitir registrar usuarios que inicien el proceso de firmado, desde los sistemas integrados o desde la misma solución
38	La solución debe poder entregar vía email la evidencia o documento final después de haberse frimado.
39	La solución debe poder recibir el documento de firma directamente desde el sistema corporativo integrado y entregarlo a dicho sistema después de firmado.
40	La solución permite conectarse al servicio de envío de mensajes de texto con Tigo o cualquier operador celular (doble factor de autenticación)
41	La solución está en idioma Español

A partir de los planteamientos presentados a lo largo del presente documento se puede concluir de manera categórica que EPM requiere de la adquisición e implantación de un Sistema de Gestión de Documentos Electrónicos que responda a lo establecido por el Archivo General de la Nación en articulación con el Ministerio de Tecnologías de la información y las Comunicaciones y además, que se adapte a las necesidades organizacionales y a sus particularidades respecto a estructura orgánica, avance del modelo documental, capacidad financiera, madurez tecnológica, etc. Por esta razón, a continuación, se plantean los requisitos funcionales a tener en cuenta durante el proceso de adquisición, actualización o desarrollo de un SGDEA corporativo:

8.2 REQUISITOS FUNCIONALES SGDEA CORPORATIVO

Implementar un Sistema de Gestión de Documentos Electronicos de Archivo no requiere exclusivamente el desarrollo de componentes tecnológicos, es una tarea que exige el fortalecimiento de la gestión de información desde las dimensiones de procesos y personas. Por ello, es importante que la herramienta no se conciba como un fin sino como un medio a través del cual se puedan concatenar una serie de estrategias que tienen como propósito la conformación del archivo electrónico institucional, el cual es de gran importancia para la toma de decisiones, la ejecución de las actividades organizacionales, la defensa jurídica de la empresa y la preservación de la memoria institucional, entre otros.

En consecuencia, antes de la adquisición de un SGDEA se debe diagnosticar el estado de madurez del proceso de Gestión Documental en EPM garantizando que se cumplan con las condiciones mínimas y los prerrequisitos para el despliegue de un sistema transversal. Adicionalmente, durante la planeación para la contratación de la herramienta, se deben evaluar los siguientes requisitos y asegurar que la solución seleccionada cumpla con al menos el 80% de ellos:

a. Producción, captura e ingreso de documentos

N°	REQUISITO
1	El SGDEA debe permitir tener un control sobre la *creación de los documentos electrónicos* de archivo, de manera que se asegure que los creadores de los mismos estén autorizados e identificados y que los documentos estén protegidos frente a cualquier adición, supresión, modificación, utilización u ocultación no autorizadas.
2	El proceso de captura de documentos del SGDEA debe contar con los controles y la funcionalidad adecuados para garantizar que los documentos se identifiquen dentro del cuadro de clasificación documental, y así sean asociados con la Tabla de Retención Documental.
3	El SGDEA, no debe limitar el número de documentos que pueden ser capturados en cualquier serie, subserie, expediente; ni el número de documentos que se pueden almacenar.
4	Para la captura de documentos que tienen anexos el SGDEA deberá gestionarlos como unidad, restringiendo el uso de formatos comprimidos.
5	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.
6	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.
7	El SGDEA debe disponer de una opción o servicios de conversión de documentos a formatos establecidos por el Archivo General de la Nación.
8	El SGDEA debe ofrecer opciones de gestión de notificaciones y avisos por medio de correo electrónico.
9	Cuando el usuario captura un documento que tiene más de una versión, el SGDEA debe permitir al usuario elegir:
	- Que todas las versiones son de un solo documento
	- Una sola versión como documento oficial
	- Cada versión como documento individual

10	El SGDEA debe generar una alerta al intentar capturar un registro que este incompleto o vacío.
11	El SGDEA debe contar con una plataforma estándar compatible con la definición de estructuras de datos (XML), que brinden la posibilidad de realizar la importación de información del mismo y de otros sistemas garantizando su interoperabilidad.

b. Organización documental de expedientes híbridos y electrónicos (clasificación, ordenación y descripción)

N°	REQUISITO
1	El SGDEA debe permitir la creación, importación, parametrización, automatización, administración y versionamiento de las Tablas de Retención Documental TRD, a partir de las planillas predefinidas, asistentes de configuración cargue de archivos planos o a través de la incorporación de otros mecanismos que faciliten la administración y gestión de la TRD
2	El SGDEA debe permitir que el CCD y las TRD sean controladas únicamente por un rol de administrador y que pueda agregar, modificar y reorganizar la estructura
3	El SGDEA debe garantizar que los documentos electrónicos de archivo que se capturen se asocien a una TRD configurada en el sistema.
4	El SGDEA debe garantizar que los documentos producidos y asociados a una TRD, mantendrán criterios de tiempo y de disposición final de la versión correspondiente.
5	El SGDEA debe registrar como metadatos la fecha y hora del registro del cargue de un documento al expediente electrónico.
6	El SGDEA debe permitir ingresar los datos de localización de un expediente híbrido (referencia cruzada al expediente físico). El sistema debe permitir diligenciar los metadatos de ubicación que luego van a permitir su localización a nivel de unidades documentales, para el caso de los expedientes híbridos.
7	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 los metadatos asociados e incluyendo pistas de auditoria.
8	El SGDEA debe permitir a los usuarios autorizados, la selección y uso de las diferentes versiones de la Tabla de Retención Documental.
9	El SGDEA debe proporcionar a los administradores las herramientas para informes estadísticos de la actividad dentro de la Tabla de Retención Documental.
10	El SGDEA debe permitir la generación de expedientes electrónicos y todos sus componentes (Documento electrónico, foliado, índice firmado y metadatos asociados)

11	El SGDEA debe permitir múltiples firmas electrónicas o digitales en los documentos electrónicos.
12	El SGDEA debe representar la organización de los expedientes y documentos, incluyendo sus metadatos, a partir del esquema del cuadro de clasificación documental.
13	El SGDEA debe permitir otorgarle un número único de identificación a un documento cuando es cargado a un expediente.
14	El SGDEA debe permitir establecer niveles de seguridad del expediente de acuerdo con los niveles de seguridad establecidos por la entidad.
15	El SGDEA debe permitir la reubicación de una carpeta (o conjunto de carpetas) o documento, a un lugar distinto dentro de la estructura de clasificación, y garantizar que se mantengan los metadatos y demás atributos (permisos). Sin que esto signifique la duplicidad del documento.
16	El SGDEA debe permitir que los documentos que componen el expediente, hereden los tiempos de conservación establecidos en la TRD. Así como los metadatos de la serie y subserie documental.
17	El SGDEA debe permitir que todas las acciones efectuadas sobre el expediente, queden registradas en un historial de eventos que puede ser consultado por los usuarios que tengan acceso al expediente electrónico. El SGDEA debe permitir que el historial de eventos del expediente electrónico pueda ser exportado.
18	El SGDEA debe permitir exportar el índice electrónico a formato XML
19	El SGDEA debe permitir la incorporación de la firma electrónica para la generación del índice del expediente electrónico.
20	El SGDEA debe permitir el foliado de los expedientes mediante un índice electrónico firmado digitalmente *por la autoridad, órgano o entidad actuante, según* proceda cuando el expediente se cierre. Este índice garantizará la integridad del expediente electrónico y permitirá su recuperación cuando se requiera. A partir de los siguientes requisitos:
	1. Identificación consecutiva del documento dentro del expediente acorde con el tipo de ordenación que se elija.
	2. Identificación inequívoca del documento
	3. Metadato(s) que asocie el documento al expediente
	4. Metadato(s) que identifique que el documento es Original o Copia.
21	La estructura del índice electrónico debe contener cada uno de los siguientes elementos;
	- Índice Contenido
	- Fecha Índice Contenido
	- Documento Foliado
	- Nombre Documento
	- Tipología Documental
	Fecha Creación Documento / Fecha de declaración de documento de archivo

	- Fecha Incorporación Expediente
	- Valor Huella
	- Función Resumen
	- Orden Documento Expediente
	- Página Inicio
	- Página Fin
	- Nota
	- Formato
	- Tamaño:
	- Origen
	- Expediente Foliado
22	El SGDEA debe hacer accesible el contenido de los expedientes de acuerdo con los roles y permisos
23	Una vez terminado el trámite administrativo, el SGDEA debe incorporar opciones para el cierre del expediente (manual-automático)
24	Una vez cerrado el expediente, el SGDEA deberá restringir la adición la supresión carpetas o documentos. Excepciones: Cuando por disposiciones legales o administrativas sea necesario reabrir un expediente, esta acción debe realizarse mediante un perfil administrativo y debe quedar registro en las pistas de auditoria, con la explicación del motivo por el cual se realizó la acción.
25	El SGDEA debe impedir la eliminación de un expediente electrónico o su contenido. Sin embargo, existen dos excepciones a este requisito: 1. La eliminación de acuerdo con lo establecido en la TRD. 2. Eliminación por un rol administrativo como parte de un procedimiento auditado.

c. Retención y disposición

N°	REQUISITO
1	El SGDEA debe permitir sólo al rol administrador crear, gestionar y modificar los tiempos de retención y disposición para un grupo de series y/o expedientes.
2	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.
3	Los SGDEA deben permitir como mínimo las siguientes acciones de disposición para cualquier regla de retención y disposición: - Conservación permanente - Eliminación automática - Eliminación con autorización del rol administrador - Transferencia - Selección
4	El SGDEA no debe limitar la duración de los tiempos de retención.
5	El SGDEA debe gestionar las alertas para las transferencias y eliminación documental, activando automáticamente una alerta al rol administrador y aprobador transferencia, cuando el periodo de retención aplicable está a punto de cumplir con

	el tiempo establecido (cronograma de transferencias documentales elaborado en el sistema)
6	El SGDEA debe suministrar el inventario documental automático (transferencia y eliminación)
7	El SGDEA debe permitir a un usuario autorizado aplazar la eliminación de una serie, subserie, expediente determinado. Cuando esto ocurra, el SGDEA debe solicitar y almacenar como mínimo la siguiente información en la pista de auditoria. - La fecha de inicio de la interrupción - La identidad del usuario autorizado - El motivo de la acción
8	Cuando el SGDEA está transfiriendo o exportando expedientes y/o documento y algunos de ellos incluyen referencias a documentos almacenados en otros expedientes, el SGDEA deberá transferir o exportar el documento completo, no sólo la referencia y almacenarlos de acuerdo al flujo de trabajo correspondiente
9	El SGDEA debe emitir una alerta al administrador en el caso en que un expediente electrónico se encuentre listo para ser eliminado y alguno de sus documentos esté vinculado a otro expediente. El proceso de eliminación debe aplazarse para permitir una de las siguientes acciones correctivas: - Solicitar confirmación para continuar y cancelar el proceso - Esta acción deberá quedar en las pistas de auditoria relacionando mínimo los siguientes datos: fecha 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
10	Cuando por motivos de obsolescencia tecnológica, seguridad de la información causal administrativa o judicial, se requiera exportar, transferir o migrar los documentos se debe garantizar la integridad de los expedientes respecto a: - Componentes del expediente (Documento electrónico, foliado, índice firmado y metadatos). - Estructura de los documentos, preservando las relaciones correctas entre ellos.
11	Durante un proceso de migración entre diferentes sistemas o plataformas tecnológicas, se debe garantizar que: - Exportar o transferir los documentos correspondientes con las reglas de retención y disposición, y sus respectivos controles de acceso (seguridad para la consulta) para que puedan seguir aplicándose en el sistema de destino - Imprimir uno más informes o reportes que muestren las reglas que se aplicaran a cada conjunto de documentos con sus características - Garantizar la estructura del expediente Asegurando que los vínculos archivísticos se conserven en todo momento.
12	Conservar todos los documentos electrónicos de archivo (DEA) que hayan sido objetivo de transferencia secundaria, al menos hasta que se reciba la confirmación de que el proceso transferencia ha concluido satisfactoriamente.

d. Búsquedas, consultas y reportes

N°	REQUISITO
1	El SGDEA debe permitir al usuario buscar y recuperar información que se encuentre dentro de los documentos, listas de documentos y metadatos de acuerdo al perfil de acceso.
2	El SGDEA debe permitir:
	• Ver la lista de resultados de una búsqueda
	• filtrar expedientes o documentos a partir de los resultado de una búsqueda
	• Ver la lista de todos los expedientes y documentos relacionados a cualquier serie determinada, con su respectivo contenido.
	• Mostrar miniaturas de imágenes digitalizadas como una ayuda para la navegación y búsqueda.
3	El SGDEA debe proporcionar herramientas para la generación de informes y reportes que incluyan como mínimo gráficos y tablas.
4	El SGDEA debe permitir generar informes sobre errores presentados en el sistema (Cargue de documentos fallidos, procesos y procedimientos incompletos, número de intentos fallidos al sistema)
5	El SGDEA debe proporcionar al usuario maneras flexibles de imprimir los documentos de archivo y sus correspondientes metadatos
6	El SGDEA de permitir que se impriman las listas de los resultados de búsqueda
7	El SGDEA debe permitir que los resultados de búsqueda se presenten únicamente las carpetas y documentos a los que el usuario tiene acceso de acuerdo a los niveles de permisos definidos.
8	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.
9	El SGDEA debe permitir que ninguna función de búsqueda revele jamás al usuario información como contenido o metadatos, que se le tengan restringidos por permisos de acceso.
10	El SGDEA debe permitir la previsualización de los documentos del expediente, sin que eso implique la descarga de los mismos.
11	El SGDEA no tiene limitaciones en el número de registros de los resultados de las búsquedas

e. Esquema de metadatos

N°	REQUISITO
1	EL SGDEA debe permitir incorporar diferentes esquemas de metadatos
2	El SGDEA debe permitir al usuario autorizado parametrizar, modificar y aplicar las reglas de los elementos del esquema de metadatos.
3	El SGDEA debe permitir que los valores de los metadatos se hereden automáticamente de forma predeterminada desde el nivel inmediatamente superior en la jerarquía de la clasificación
4	El SGDEA debe presentar en pantalla los metadatos de los documentos capturados.
5	El SGDEA debe permitir la asignación previa de palabras claves en las series, subseries, expediente y/o documentos, basados en bancos terminológicos, tesauros, taxonomías, entre otros.
6	El SGDEA debe permitir que al momento de la captura o en una etapa posterior de procesamiento, se puedan ingresar metadatos adicionales.
7	El SGDEA debe validar y controlar la entrada de los metadatos mínimos obligatorios.
8	El SGDEA permite la extracción automática de metadatos de los documentos al momento de la captura o cargue al sistema.

f. Roles y permisos

N°	REQUISITO
1	El SGDEA debe permitir la creación, administración de usuarios, revocación de privilegios, roles y permisos de un grupo o usuarios seleccionados.
2	El SGDEA debe permitir configurar controles, restringir el acceso de acuerdo a los perfiles configurados por el administrador del sistema.
3	El SGDEA debe tener la capacidad de actualizar y revisar los contactos apropiados con grupos de interés especiales, autoridades pertinentes y demás (contactos externos), que cuentan con autorización mediante acuerdos de confidencialidad o de los acuerdos de no- divulgación de la información. El SGDEA deberá cumplir con todos los requisitos de seguridad de la información a través de acuerdos con terceras partes.
4	El SGDEA debe permitir programar rutinas de copia de seguridad (backup) y su recuperación cuando sea necesario.
5	El SGDEA debe permitir la parametrización de copias de seguridad de los documentos en conjunto con los metadatos.
6	El SGDEA debe permitir la creación gestión y configuración de niveles de clasificación de información a la que haya lugar (Clasificada, reservada, confidencial de acuerdo con la normatividad existente), y permitir acceso a esta dependiendo del rol de usuario.

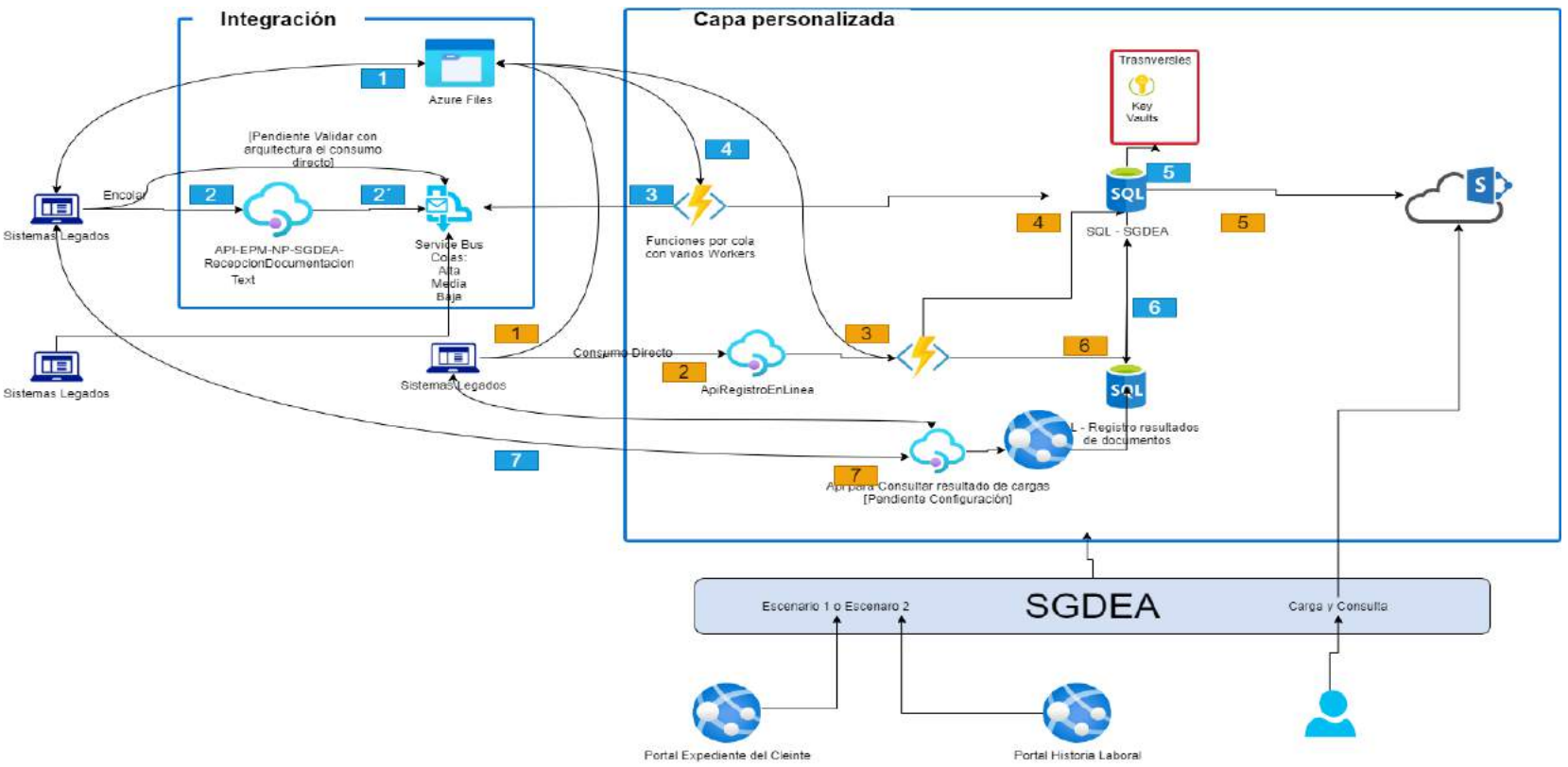
7	EL SGDEA debe garantizar que las operaciones realizadas en el sistema esten rotegidas contra adulteración, supresión, ocultamiento y demás operaciones que atenten contra la autenticidad, integridad y disponibilidad de la información.
8	El SGDEA debe permitir la inclusión en los reportes generados de un rótulo que permita identificar su nivel de clasificación (Clasificado, reservado, restringido, entre otros), de acuerdo con la clasificación.
9	El SGDEA debe permitir manejar los siguientes estados para las cuentas de usuario: Habilitado, deshabilitado, bloqueado, suspendido.

8.3 REQUISITOS TÉCNICOS SGDEA CORPORATIVO

En este apartado se presenta la arquitectura de alto nivel para el SGDEA y se registran los requisitos mínimos que este debe cumplir para lograr la integración e interoperabilidad. Así mismo, se presentan los requisitos que deben cumplir los distintos sistemas de información transaccionales, con el fin de que estos se integren a través de interfaces para garantizar la captura y tratamiento de los documentos electrónicos de archivo que se producen y reciben en cada uno de ellos.

- Arquitectura de alto nivel:

  (Ver gráfica en pagina siguiente)



Escenario 1

PASOS ESCENARIO MASIVO
1 - Subir Archivos al File Share
2 - Enviar metadata de los archivos
2´ - Encolar Metadata
3 - Desencolar Mensaje
4 - Descargar archivo
5 - Enviar Metadata y Archivo al SGDEA
6 - Almacenar archivo en Sharepoint
7 - Registrar resultado de la carga del archivo

Escenario 2

PASOS ESCENARIO EN LINEA
1 - Subir Archivos al File Share
2 - Enviar metadata de los archivos
3 - Descargar archivo
4 - Enviar Metadata y Archivo al SGDEA
5 - Almacenar archivo en Sharepoint
6 - Registrar resultado de la carga del archivo
7 - Consultar resultados de las cargas

Ilustración 7. Arquitectura de alto nivel SGDEA

Capa genérica de integración:

Es un grupo de componentes transversales en la nube de azure, los cuales se requieren para el envío de los documentos y la metadata asociada a cada uno de estos.

Capa personalizada de integración:
Es un grupo de componentes de nube que se encargan de obtener los metatados y archivos de la capa genérica, para ser procesados y clasificados a través de las tablas de homologación del SGDEA, para luego ser almacenados en las bibliotecas en SharePoint Online.

ESCENARIO N° 1

1. Carga de Documentos: El sistema origen a través de una utilidad de programación (SDK), envía los documentos a un servicio de almacenamiento de nube (File Share) a la carpeta correspondiente. Existe una carpeta por cada sistema o legado.

   Nota: Los sistemas que no tengan la capacidad de enviar directamente los archivos, deberán desarrollar una funcionalidad que les permita realizar la carga de los documentos al servicio de almacenamiento en nube.

2. Envío de Metadata: El sistema origen debe enviar a través del consumo de un servicio REST o por medio de conexión directa con el servicio de Mensajeria de nube (Service Bus) utilizando el SDK del lenguaje de programación del legado, la metada correspondiente a cada archivo enviado en el punto anterior, en formato Json.

2.1 Encolar mensajes: El servicio de mensajería (Service Bus) recibe los mensajes de todos los sistemas o legados, los encola dependiendo de la prioridad donde se encuentra registrado el legado.

3. Desencolar mensajes: Las funciones de la capa personalizada realizan el desencolamiento de los mensajes recibidos, para enviar a la base de datos y procesar la carga en el SGDEA.

4. Descargar archivo: Las funciones de la capa personalizada realizan el desencolamiento de los documentos recibidos, para enviar a la base de datos y procesar la carga en el SGDEA.

5. Enviar metadata y archivos al SGDEA: Mediante un proceso de homologación de la metadata se realiza la clasificación documental, para el registro del documento en la TRD correspondiente en el SGDEA.

6. Almacenar archivo en SharePoint Online: Internamente el SGDEA crea una estructura de bibliotecas por expedientes en SharePoint donde quedarán almacenados los documentos recibidos

7. Registrar resultado de la carga: El sistema SGDEA registra en una base de datos de respuesta, el resultado de la carga de los archivos en el sistema.

8. Consultar resultados de las cargas: El Sistema SGDEA expone un servicio Web, el cual puede ser consumido por las sistemas o legados para la consulta de los resultados de las cargas.

ESCENARIO N° 2

1. Carga de Documentos: El sistema origen a través de una utilidad de programación (SDK), envía los documentos a un servicio de almacenamiento de nube (File Share) a la carpeta correspondiente. Existe una carpeta por cada sistema o legado.
   Nota: Los sistemas que no tengan la capacidad de enviar directamente los archivos, deberán desarrollar una funcionalidad que les permita realizar la carga de los documentos al servicio de almacenamiento en nube.

2. Envío de Metadata: El sistema origen debe enviar a través del consumo de un servicio REST o por medio de conexión directa con el servicio de Mensajeria de nube (Service

Bus) utilizando el SDK del lenguaje de programación del legado, la metada correspondiente a cada archivo enviado en el punto anterior, en formato Json.

3. Descargar archivo: La función de la capa personalizada para escenario online realiza el procesamiento de los documentos recibidos, para enviar a la base de datos y procesar la carga en el SGDEA.

4. Enviar metadata y archivos al SGDEA: Mediante un proceso de homologación de la metadata se realiza la clasificación documental, para el registro del documento en la TRD correspondiente en el SGDEA.

5. Almacenar archivo en SharePoint Online: Internamente el SGDEA crea una estructura de bibliotecas por expedientes en SharePoint donde quedarán almacenados los documentos recibidos.

6. Registrar resultado de la carga: El sistema SGDEA registra en una base de datos de respuesta, el resultado de la carga de los archivos en el sistema.

7. Consultar resultados de las cargas: El Sistema SGDEA expone un servicio Web, el cual puede ser consumido por las sistemas o legados para la consulta de los resultados de las cargas.

a. Requisitos de arquitectura tecnológica:

ARQUITECTURA TECNOLÓGICA	
1	El SGDEA debe estar implementado sobre SharePoint online como Enterprise Content Management o ECM
2	El SGDEA será un complemento del sistema de Gestión Documental para EPM, por tanto, debe integrarse con este.
3	El SGDEA debe trabajar en ambientes Web o o Web Based
4	El SGDEA debe tener una solución en WEB Enabled

5	Los usuarios deben acceder al SGDEA a través de los navegadores más populares y mínimo que funcione en Google Chrome o MS Edge sin necesidad de un software dedicado.
6	El SGDEA de funcionar bajo la modalidad Software como Servicio - SaaS
7	El Data Center del SGDEA alterno debe cumplir con:
	- Mínimo TIER3 en diseño y construcción
	- Mínimo dos Data Center con servidores redundantes estado activo – activo ubicados en regiones geográficas diferentes. Proveer información de cuál es su proveedor de servicios Nube y la ubicación de los Data Center
	- Replicación de datos entre sus propios Data Center
8	El SGDEA debe tener un data center certificado TIER III
9	El SGDEA debe contar con un modelo de datos Conceptual, Lógico y Físico de la solución.
10	Las extensiones creadas por EPM pueden ser usadas en las nuevas versiones de la solución, sin necesidad de volverlos a desarrollar y sin mayores impactos en desarrollo o configuración.
11	El SGDEA deberá soportar un esquema multi-tenant, administrado desde una instancia única de la solución del software, usando una configuración base y reglas de negocio que pueda ser compartida por todas las compañías o "tenants".
12	El SGDEA deberá tener la capacidad de realizar upgrades de la aplicación una sola vez y que el cambio se vea reflejado en todas las compañias o "tenants" gestionadas al tiempo, independiente de la forma como se tenga almacenada la información de la compañía o "tenant".
13	El SGDEA deberá tener establecida un End-of-support o un end-of-life de la solución presentada.
14	El SGDEA debe proveer de un ambiente de pruebas (Sandbox) para probar los cambios, contra un ambiente de los datos del cliente, configuraciones y código.

b. Requisitos de integraciones / interoperabilidad

INTEGRACIONES E INTEROPERABILIDAD	
1	El SGDEA debe tener mecanismos de administración, ejecución y control de reintentos por falla en el llamado a un servicio de integración en procesos de carga de documentos.
2	El SGDEA deberá garantizar su interoperabilidad con Enter OnLine (SharePoint OnLine) y otros sistemas de haciendo uso de servicios de integración de Azure - como API Management, Logic Apps, Service bus, Event Grid, Data Factory, SKD u otros válidos para la Organización.
3	El SGDEA expone los servicios ofrecidos con protocolos REST usando el estándar Swagger del OPEN API Initiative
4	El SGDEA debe marcar en su sistema el registro como "envío exitoso" cuando hay éxito en el llamado de Servicios
5	El SGDEA debe marcar en su sistema el registro como "envío fallido" cuando hay falla en el llamado de Servicios
6	El SGDEA debe exponer servicios de integración de consulta que involucren un solo registro
7	El SGDEA expone servicios de integración de consulta que involucren múltiples registros
8	El SGDEA debe consumir servicios REST.
9	El SGDEA tiene la capacidad de ejecutar diferentes módulos de esta en servidores diferentes para distribuir la carga y evitar pugna de recurso

c. Integración de otros sistemas transaccionales con el SGDEA

N°	REQUISITO
1	El sistema de información debe tener la capacidad de consumir servicios tipo REST
2	El sistema de información debe tener la capacidad de consumir servicios con autenticación OAUTH 2.0
3	El sistema de información debe tener la capacidad de subir archivos al repositorio de Nube (File Share) de Azure Storage Account de Microsoft.

4	El sistema de información debe tener la capacidad de establecer conexiones nativas con servicios nube como Azure Service Bus y File Share de Microsoft, a través de SDK, para enviar los mensajes de la metada y los documentos.
5	El sistema de información debe incluir un mecanismo de verificación que valide que el archivo ya fue subido al Azure Storage Account (file share de la nube) de manera exitosa antes del envío del mensaje con la metadata del archivo.
6	El sistema de información debe incluir un mecanismo para consultar el servicio del SGDEA que entrega el resultado de la carga de documentos, si fue exitosa o fallida, en caso de que necesite guardar dicho resultado o realizar acciones con base en el resultado (Reintentos).
7	El sistema de información debe tener la capacidad de empaquetar multiples registros en un mensaje (enviar metadata varios archivos)
8	El sistema de información debe tener mecanismos de administración, ejecución y control de reintentos por falla en el llamado a un servicio de integración en procesos de carga de documentos.
9	El sistema de información debe consumir los servicios ofrecidos con protocolos REST usando el estándar Swagger del OPEN API Initiative
10	El sistema de información debe marcar en su sistema el registro como "envío exitoso" cuando hay éxito en el envío de información.
11	El sistema de información debe marcar en su sistema el registro como "envío fallido" cuando hay falla en el envío de información.
12	El sistema de información debe consumir servicios de integración de consulta que involucren un solo registro.
13	El sistema de información debe consumir servicios de integración de consulta que involucren múltiples registros.

d. Mantenimiento

N°	REQUISITO
1	El SGDEA debe permitir la fácil instalación y despliegue de plugins y desarrollos personalizados.
2	El SGDEA debe hacer actualización de versiones o "releases" sin impactar las configuraciones del usuario.
3	El SGDEA debe registrar la causa raíz de los errores técnicos o funcionales presentados durante su ejecución, (sistema, usuario, proceso, excepción generada).

4	El SGDEA debe ser una solución "basada en reglas" donde se permita al usuario configurar y mantener el software sin requerir mayor intervención de analistas técnicos.
5	Las configuraciones realizadas previamente en ambiente de pruebas deben poder ser migradas al ambiente de producción.

e. Usabilidad y experiencia de usuario

USABILIDAD Y EXPERIENCIA DEL USUARIO	
1	El SGDEA debe permitir que los usuarios modifiquen o configuren la interfaz gráfica a su gusto. Con elementos de personalización sencillos, que abarquen, al menos las siguientes opciones, sin limitarse necesariamente a estas:
	- Contenidos de los menús,
	- Disposición de las pantallas,
	- Uso de teclas de funciones y atajos de teclado,
	- Colores y tamaño de las fuentes que se muestran en pantalla
2	El SGDEA debe permitir el cumplimiento de la norma NTC5854 (estrategia del Gobierno Digital), estándares de accesibilidad.
3	El SGDEA debe contar con un diseño web responsive que permita funcionar en la mayoría de los dispositivos y navegadores reconocidos en el mercado.
4	El SGDEA debe proveer documentación en línea para el usuario o ayudas en línea que le permitan determinar las causas de errores o cómo operar el sistema
5	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.
6	El SGDEA debe contar con un módulo de ayuda en línea.
7	El SGDEA debe permitir acceso a todas las funcionalidades y a cualquier interfaz de la aplicación a través del teclado.
8	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.

f. Infraestructura

INFRAESTRUCTURA	
1	El SGDEA debe ofrecer soporte para sistemas de almacenamiento tipo NAS, DAS y SAN.
2	El SGDEA debe proveer al menos dos interfaces para la Gestión del ECM y sus componentes: • Interface de comandos • Interface gráfica de usuario

g. Confidencialidad, integridad y disponibilidad de la información

N°	REQUISITO
1	El SGDEA debe contar con mecanismos de recuperación de datos o información ante eventos inesperados de falla.
2	El SGDEA debe garantizar que, en el evento de presentarse caídas del sistema, se haga rollback de todas las transacciones afectadas por la falla y se evite pérdida de información.
3	El SGDEA debe permitir desplegarse de manera redundante para garantizar continuidad y disponibilidad en el servicio ante la presencia de fallas.
4	El SGDEA debe garantizar el tiempo de actividad del servicio (disponibilidad), incluso si las operaciones del centro de datos se subcontratan con un tercero. 99.5% o superior.
5	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.
6	El SGDEA debe permitir hacer copias de respaldo de la información y del software, y se deben poner a prueba con regularidad de acuerdo con la política de respaldo acordada.
7	El SGDEA debe tener el reloj sincronizado al de todos los sistemas de procesamiento de información pertinentes dentro de la Organización o del dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta y acordada.
8	El SGDEA deberá estar disponible las 24 horas del día, 7 días de la semana, 365 días del año.
9	Tiempo máximo para desplegar o refrescar páginas o pantalla debe ser de 5 segundos
10	Tiempo máximo para respuesta de servicios de consulta de información de 5 segundos

11	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.
12	Toda funcionalidad del sistema y transacción de negocio realizada en el SGDEA debe responder al usuario en menos de 5 segundos.
13	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.
14	El tiempo de inactividad previsto del SGDEA, no debe superar las 10 horas al trimestre y 40 horas al año.
15	El tiempo de inactividad no prevista del SGDEA, no debe superar las 10 horas al trimestre y 40 horas al año.
16	El SGDEA deberá tener la flexibilidad y capacidad de crecer en respuesta a las necesidades del Grupo EPM según número de registros o volumen de datos sin ver afectada su funcionalidad, desempeño, fiabilidad y disponibilidad.
17	El SGDEA debe incluir la normatividad del proveedor de servicios en la nube, sobre la transferencia de información del cliente entre data centers del proveedor

h. Migración

N°	REQUISITO
1	El SGDEA deberá diseñarse de modo que se garantice la autenticidad, la fiabilidad y el uso de los documentos, aunque se produzcan cambios en el sistema; incluyendo la conversión del formato, la migración entre hardware y sistemas operativos o aplicaciones específicas de software durante todo el periodo de su conservación.
2	Los soportes de almacenamiento del SGDEA deberán ser utilizados y conservados en entornos compatibles, previa identificación del tipo de formatos y soportes con esperanza de vida prolongada.
3	El SGDEA debe permitir la conversión en masa de los documentos de archivo, con sus metadatos y pista de auditoría, a otros soportes o sistemas acordes con las normas sobre el formato o los formatos en uso correspondientes.
4	El proveedor del SGDEA debe haber instalado un programa verificable de actualización de la tecnología básica del sistema que permita acceder a la información existente sin que se produzcan cambios en el contenido.

5	El SGDEA debe permitir que las configuraciones realizadas previamente en ambiente de pruebas pueden ser migradas al ambiente de producción

i. Anexos técnicos requeridos. (Desarrollador o vendedor del SGDEA)

N°	REQUISITO
1	El SGDEA debe contar con manuales de usuario estructurados adecuadamente.
2	El desarrollador o vendedor del SGDEA deberá aportar un diagrama con la arquitectura de solución del sistema que evidencie los principales componentes y el esquema de integración con otros sistemas, así como herramientas utilizadas en el desarrollo de la misma.
3	El desarrollador o vendedor del SGDEA deberá incluir una propuesta de la infraestructura con sus características técnicas y de almacenamiento que se requiere para implementar y operar su solución integral y correctamente en los distintos ambientes.
4	El desarrollador o vendedor del SGDEA deberá brindar información detallada sobre la extensión y desarrollo de nuevas funcionalidades, la cual describa las capacidades del sistema para desarrollar extensiones y nuevas funcionalidades, detallando el lenguaje utilizado y la arquitectura empleada para este propósito.
5	El desarrollador o vendedor del SGDEA deberá proveer el roadmap de la solución que refleje las funcionalidades y versiones planeadas para los próximos años.
6	El desarrollador o vendedor del SGDEA formular un cronograma detallado de ejecución contemplando las actividades y recursos requeridos para dar cumplimiento al alcance planteado en el proceso de implementación del SGDEA. Allí deberán quedar registrados los hitos más importantes del proyecto. Este cronograma, una vez aprobado por EPM, se convertirá en referente para hacer seguimiento al cumplimiento del contrato.
7	El desarrollador o vendedor del SGDEA deberá brindar información detallada sobre los servicios de instalación y configuración que contemple las siguientes actividades:
	- Creación de los App Services en Windows Azure para la instalación del API IOIP
	- Despliegue del API IOIP en Windows Azure
	- Configuración de autorización del tenant de Office 365 para permitir la conexión con el API IOIP de Windows Azure
	- Creación del Site Collection en donde quedaran los documentos como repositorio del SGDEA en SharePoint Online de Office 365

	- Verificación de la autenticación por medio del Azure Active Directory
8	El desarrollador o vendedor del SGDEA deberá brindar información detallada sobre los servicios de personalización, para la parametrización se deberán contemplar las siguientes actividades:
	- Parametrización de las TRD de EPM, con sus respectivos Tipos documentales.
	- Creación de los perfiles a través de los roles y asociación con los usuarios del sistema
	- Asociación de Plantillas Word, si se requiere para algunos tipos documentales.
9	El desarrollador o vendedor del SGDEA deberá brindar información detallada sobre los servicios de personalización, para los servicios de soporte y ayuda en línea se deberán contemplar las siguientes actividades; • Verificación de una página de recursos dentro del SGDEA que contenta ayudas en línea a través de videos que describan las funcionalidades más importantes del sistema y como se operan.
10	El desarrollador o vendedor del SGDEA deberá brindar información detallada sobre los servicios de personalización, para los servicios de Arquitectura se deberán contemplar las siguientes actividades; - Publicación de los servicios WEB del SGDEA en el Bus de Integración que EPM tenga dentro de Arquitectura de referencia. - Entrega a satisfacción del documento de arquitectura de la solución de SGDEA.
11	El desarrollador o vendedor del SGDEA deberá brindar información detallada sobre los servicios de personalización, para los servicios de desarrollo se deberán contemplar las siguientes actividades:
	- Desarrollos para lograr especificaciones técnicas con las cuales no cuenta la herramienta
12	El desarrollador o vendedor del SGDEA deberá entregar información de cada componente nuevo desarrollado para cumplir con la arquitectura objetivo propuesta (ver anexo 1) y que actualmente no sea parte de la solución, así como aquellos requerimientos solicitados por EPM para satisfacer la normatividad del AGN.
13	El desarrollador o vendedor del SGDEA deberá brindar información detallada sobre los servicios de capacitación que inlcuya la siguiente información:
	- La capacitación se hará en sitio
	- Se estima una capacitación para 5 técnicos y 15 funcionales, con una intensidad horaria de 8 horas.

14	El desarrollador o vendedor del SGDEA deberá brindar información detallada sobre los servicios de capacitación mediante Plataforma e-learning que se realizará de manera paralela a las capacitaciones de tal manera que facilite su refuerzo y aprendizaje, estará para los perfiles de usuarios finales.
15	El desarrollador o vendedor del SGDEA deberá brindar información detallada sobre los servicios de capacitación para garantizar la transferencia de conocimiento a los usuarios, mediante la información para el Gestor Expedientes, que debe incluir la descripción paso a paso el uso del Aplicativo SGDEA orientado en detallar el proceso que llevan a cabo los funcionarios de las dependencias. Serán capacitados en los siguientes temas:
	Expediente Electrónico:
	- Crear Expediente Electrónico
	- Buscar un expediente
	- Carga documento a expediente
	- Cambiar responsable de expediente
	- Permisos de consulta sobre el expediente
	- Permisos de edición sobre el expediente
	- Genera índice electrónico
	Metadatos:
	- Crear metadatos
	- Asociar metadatos a una SubSerie o tipo documental
	Flujos de trabajo:
	- Crear un flujo de trabajo o Reglas de trabajo
	- Validación de actividades
	- Asociar roles y usuarios a los flujos
	- Editar y modificar un flujo de trabajo
16	El desarrollador o vendedor del SGDEA deberá brindar información detallada sobre los servicios de capacitación para garantizar la transferencia de conocimiento a los usuarios, mediante la información para el Gestor de Archivo, que debe incluir la descripción del paso a paso del uso del Aplicativo, orientado en detallar el proceso que lleva a cabo el funcionario del responsable del Archivo Central y administración. Serán capacitados en los siguientes temas:
	- Configuración de Perfiles
	- Configuración de Usuarios
	- Configuración de Tablas de Retención Documental
	- Uso de la herramienta de carga masiva
	- Carga de plantillas

17	El desarrollador o vendedor del SGDEA deberá brindar información detallada sobre los servicios de capacitación para garantizar la transferencia de conocimiento a los usuarios, mediante la información para los líderes técnicos que describa los detalles de la arquitectura del proyecto, al igual que la topología de conectividad entre Windows Azure y Office 365.
18	El desarrollador o vendedor del SGDEA deberá brindar información detallada sobre los servicios especializados que inlcuya información sobre la cotización del valor hora de desarrollo cuya finalidad será suplir necesidades propias de EPM, en cuyo caso se solicitarán a través de actas de trabajo. En estas, se especificará la necesidad y se deberá estimar las horas para su desarrollo y se hará solo en el momento de recibir aprobación por parte de EPM.

j. Seguridad de la Información

	1. POLÍTICAS DE SEGURIDAD
1	El proveedor de la solución debe contar con modelo de gestión de seguridad de la información con políticas de seguridad de la información, y de privacidad de datos personales; y roles y responsabilidades frente a la seguridad de la información, así como las funciones asignadas a cada rol.
	2. ORGANIZACIÓN DE LA SEGURIDAD
2	El proveedor de la solución deberá tener documentada, formalizada y en operación una estructura organizacional en la que se defina los roles y responsabilidades frente a la seguridad de la información, así como las funciones asignadas a cada rol de esta estructura organizacional.
3	El proveedor de la solución deberá definir un rol dentro de la Organización que sea el punto de contacto oficial para todos los temas relacionados en el presente anexo.
	3. GESTIÓN DE RIESGOS Y GESTIÓN DE ACTIVOS
4	El proveedor de la solución debe realizar periódicamente un análisis de riesgos de Seguridad de la información que permita identificar riesgos potenciales que afecten la confidencialidad, integridad y/o disponibilidad de la información durante la ejecución de los servicios contratados, así como definir planes de acción para mitigar dichos riesgos.
5	Toda la información transaccional objeto del contrato, información de usuarios y contraseñas para acceso a los sistemas de información, información de gestión o administración de los sistemas de información es de carácter CONFIDENCIAL, por lo que el proveedor de la solución deberá garantizar e implementar los controles necesarios para mantener su confidencialidad, integridad y disponibilidad en todo momento y sin limitarse a lo descrito en el presente documento.

	4. SEGURIDAD DEL PERSONAL
6	El proveedor de la solución debe garantizar que los procesos de administración de personal ponen en práctica los aspectos relacionados con la seguridad de la información tales como (pero sin limitarse a) verificaciones e investigaciones sobre referencias personales, laborales, experiencia laboral, pruebas de polígrafo, examen aptitud y conocimientos, de tal manera que apoyen las políticas de seguridad dEl proveedor de la solución.
7	El proveedor de la solución contará con controles y tomará las medidas de seguridad para que el personal asignado al desarrollo del presente contrato, no divulgue la información de EPM o la utilice para un fin diferente al desarrollo de las actividades contratadas.
8	El proveedor de la solución deberá contar con un plan de capacitación permanente en seguridad de la información que permita mantener a todo su personal informado acerca de las políticas y las responsabilidades de seguridad de la información, y continuas amenazas que ponen en riesgo la información que administra y/o procesa.
	5. SEGURIDAD FÍSICA Y AMBIENTAL
9	El proveedor de la solución deberá tener implantados controles de acceso físico y mecanismos de identificación y autenticación que protejan contra acceso físico no autorizado a las áreas que almacenan información usados para la prestación de (los) servicio(s) ofrecido(s).
	6. GESTIÓN DE VULNERABILIDADES Y REMEDIACIÓN
10	El proveedor de la solución utiliza una herramienta actualizada de escaneo de vulnerabilidades para escanear automáticamente todos los sistemas en la red semanalmente o con mayor frecuencia para identificar todas las vulnerabilidades potenciales en los sistemas de la organización.
11	El proveedor de la solución implementa procedimientos de actualización de software para garantizar que los sistemas operativos ejecuten las actualizaciones de seguridad más recientes proporcionadas por el proveedor de software.
12	El proveedor de la solución implementa procedimientos de actualización de software para garantizar que el software de terceros en todos los sistemas ejecute las actualizaciones de seguridad más recientes proporcionadas por el proveedor de software.
13	El proveedor de la solución compara regularmente los resultados de los análisis de vulnerabilidades consecutivos para verificar que las vulnerabilidades se hayan corregido de manera oportuna.
14	El proveedor de la solución utiliza un proceso de calificación de riesgo para priorizar la reparación de vulnerabilidades descubiertas.
	7. GESTIÓN DE PRIVILEGIOS ADMINISTRATIVOS

15	El proveedor de la solución utiliza procedimientos para la gestión de todas las cuentas administrativas, incluidas las cuentas de dominio y locales, para garantizar que solo las personas autorizadas tengan privilegios elevados.
16	Antes de implementar cualquier activo nuevo, el proveedor de la solución cambia todas las contraseñas predeterminadas de cuentas de nivel administrativo.
17	El proveedor de la solución se asegura de que todos los usuarios con acceso de cuenta administrativa utilicen una cuenta dedicada o secundaria para actividades elevadas. Esta cuenta sólo debe usarse para actividades administrativas y no para navegar por Internet, correo electrónico o actividades similares.
18	El proveedor de la solución usa autenticación multifactor y canales encriptados para el acceso a la cuenta administrativa.
19	El proveedor de la solución se asegura de que los administradores usen una máquina dedicada para todas las tareas administrativas o tareas que requieren acceso administrativo. Esta máquina estará segmentada de la red principal de la organización y no se permitirá el acceso a Internet. Esta máquina no se utilizará para leer correos electrónicos, redactar documentos o navegar por Internet.
20	El proveedor de la solución configura los sistemas para emitir una entrada de registro y una alerta cuando se agregue o elimine una cuenta de cualquier grupo de privilegios administrativos asignados.
21	El proveedor de la solución configura los sistemas para emitir una entrada de registro y alertar sobre inicios de sesión fallidos en una cuenta administrativa.
	8. CONFIGURACIONES SEGURAS EN HARDWARE / SOFTWARE
22	El proveedor de la solución mantiene estándares de configuración de seguridad documentados para todos los sistemas operativos y software autorizados.
23	El proveedor de la solución mantiene lineas base de seguridad para todos los sistemas de la empresa según los estándares de configuración aprobados por la organización.
	9. GESTIÓN DE REGISTROS DE EVENTOS DE SEGURIDAD
24	El proveedor de la solución habilita el registro del sistema para incluir información detallada, como un origen de eventos, fecha, usuario, marca de tiempo, direcciones de origen, direcciones de destino y otros elementos útiles.
25	El proveedor de la solución se asegura de que los registros apropiados se agreguen a un sistema central de administración de registros para su análisis y revisión.

26	El proveedor de la solución entrega a EPM la información de registros y eventos de seguridad, de tal forma que pueda ser integrada al SIEM de la empresa.
27	Regularmente, el proveedor de la solución revisa los registros para identificar anomalías o eventos anormales.
	10. PROTECCIONES CONTRA EL MALWARE
28	El proveedor de la solución utiliza software antimalware centralizado para monitorear y defender continuamente cada una de las estaciones de trabajo y servidores de la organización.
29	El proveedor de la solución se asegura de que el software antimalware de la organización actualice su motor de escaneo y su base de datos de firmas de manera regular.
30	El proveedor de la solución envía todos los eventos de detección de malware a las herramientas de administración antimalware de la empresa y a los servidores de registro de eventos para análisis y alertas.
	11. RESPALDO Y RECUPERACIÓN DE DATOS
31	El proveedor de la solución se asegura de que todos los datos del sistema se respalden automáticamente de forma regular.
32	El proveedor de la solución prueba la integridad de los datos en los medios de respaldo de forma regular realizando un proceso de restauración de datos para asegurarse de que el respaldo funcione correctamente.
33	El proveedor de la solución se asegura de que las copias de seguridad estén protegidas adecuadamente mediante seguridad física o cifrado cuando se almacenan, así como cuando se mueven a través de la red. Esto incluye copias de seguridad remotas y servicios en la nube.
34	El proveedor de la solución se asegura de que todas las copias de seguridad tengan al menos un destino de copia de seguridad offsite (es decir fuera del sitio principal).
	12. CONFIGURACIÓN SEGURA EN EQUIPOS DE RED
35	El proveedor de la solución mantiene estándares de configuración de seguridad documentados para todos los dispositivos de red autorizados.
36	El proveedor de la solución compara todas las configuraciones de dispositivos de red con las configuraciones de seguridad aprobadas definidas para cada dispositivo de red en uso, y avisa cuando se descubran desviaciones.

37	El proveedor de la solución instala la última versión estable de cualquier actualización relacionada con la seguridad en todos los dispositivos de red.
38	El proveedor de la solución administra la infraestructura de red a través de conexiones de red que están separadas del uso comercial de esa red, confiando en VLAN separadas o, preferiblemente, en conectividad física completamente diferente para sesiones de administración para dispositivos de red.
	13. SEGURIDAD PERIMETRAL
39	El proveedor de la solución mantiene un inventario actualizado de todos los perímetros de red de la organización.
40	El proveedor de la solución bloquea las comunicaciones con direcciones IP de Internet maliciosas o no utilizadas conocidas y limita el acceso solo a los rangos de direcciones IP confiables y necesarios en cada uno de los perímetros de red de la organización.
41	El proveedor de la solución bloquea la comunicación a través de puertos TCP o UDP no autorizados o tráfico de aplicaciones para garantizar que sólo los protocolos autorizados puedan cruzar el perímetro de red dentro o fuera de la misma.
42	El proveedor de la solución implementa sistemas de prevención de intrusiones (IPS) basados en la red para bloquear el tráfico de red malicioso en cada uno de los perímetros de red de la organización.
43	El proveedor de la solución se asegura de que todo el tráfico de red hacia o desde Internet pase a través de un proxy de capa de aplicación autenticado que esté configurado para filtrar conexiones no autorizadas.
	14. PROTECCIÓN DE DATOS
44	El proveedor de la solución mantiene un inventario de toda la información confidencial almacenada, procesada o transmitida por los sistemas tecnológicos de la organización, incluidos los ubicados en el sitio o en un proveedor de servicios remotos.
45	El proveedor de la solución implementa una herramienta automatizada en los perímetros de la red que supervisa la transferencia no autorizada de información confidencial y bloquea dichas transferencias mientras alerta a los profesionales de seguridad de la información.
46	El proveedor de la solución monitorea todo el tráfico que sale de la organización y detecta cualquier uso no autorizado de cifrado.
47	Cuando se requieran dispositivos de almacenamiento USB, el proveedor de la solución utiliza un software empresarial que pueda configurar sistemas para permitir el uso de dispositivos específicos. Se debe mantener un inventario de dichos dispositivos.
	15. GESTIÓN DE CUENTAS DE USUARIO

48	Las cuentas de usuario de los sistemas de información del proveedor de la solución deben utilizar roles y perfiles, y los permisos de acceso al sistema deben están segregados con base al principio de menor privilegio (los permisos o privilegios mínimos necesarios para ejecutar las acciones requeridas dentro del sistema)
49	La solución debería integrarse con el Directorio Activo o ADFS usando protocolos SAML 2.0 o OAuth 2 para el proceso de autenticación de usuarios internos.
50	La solución debería integrarse con el Directorio Activo Azure B2C usando protocolos Open ID y OAuth 2 para el proceso de autenticación y autorización de usuarios externos.
51	Los sistemas de información del proveedor de la solución deben contar con un módulo de administración de seguridad que permita la gestión de usuarios y perfiles, parámetros de seguridad, y generación de reportes (usuarios, perfiles, etc.).
	16. PROGRAMA DE CONCIENTIZACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD
52	El proveedor de la solución implementa un programa de concientización sobre seguridad para que todos los empleados lo completen regularmente para asegurarse de que comprenden y exhiben los comportamientos y habilidades necesarios para ayudar a garantizar la seguridad de la organización. Este programa debe ser actualizado con frecuencia al menos una vez al año.
	17. SEGURIDAD EN LAS APLICACIONES
53	El proveedor de la solución establece prácticas de codificación seguras apropiadas para el lenguaje de programación y el entorno de desarrollo que se utiliza.
54	El proveedor de la solución aplica herramientas de análisis estático y dinámico para verificar que se cumplan las prácticas de codificación segura para el software desarrollado internamente.
55	El proveedor de la solución mantiene entornos separados para sistemas de producción y no producción. Los desarrolladores no deberían tener acceso sin supervisión a los entornos de producción.
	18. GESTIÓN DE RESPUESTA A INCIDENTES DE SEGURIDAD
56	El proveedor de la solución se asegura de que haya planes escritos de respuesta a incidentes que definan los roles del personal, así como las fases de manejo / gestión de incidentes.
57	El proveedor de la solución designa personal de gestión, así como copias de seguridad, que apoyarán el proceso de manejo de incidentes actuando en roles clave de toma de decisiones.

58	El proveedor de la solución crea un esquema de calificación de incidentes y priorización basado en el impacto conocido o potencial para su organización. Utilice la puntuación para definir la frecuencia de las actualizaciones de estado y los procedimientos de escalación.
	19. PRUEBAS DE PENETRACIÓN Y RED TEAM
59	El proveedor de la solución establece un programa para pruebas de penetración que incluya un alcance completo de ataques combinados, como ataques inalámbricos, basados en el cliente y aplicaciones web.
60	El proveedor de la solución realiza pruebas de penetración internas y externas periódicas para identificar vulnerabilidades y vectores de ataque que puedan utilizarse para explotar con éxito los sistemas empresariales.
61	El proveedor de la solución realiza ejercicios periódicos del Equipo Rojo para evaluar la preparación de la organización para identificar y detener ataques o para responder de manera rápida y efectiva.
62	El proveedor de la solución utiliza las herramientas de escaneo de vulnerabilidades y pruebas de penetración en concierto. Los resultados de las evaluaciones de escaneo de vulnerabilidad deben usarse como un punto de partida para guiar y enfocar los esfuerzos de prueba de penetración.
	REQUERIMIENTO DE PROTECCÓN DE DATOS PESONALES
	1. ROL DEL PROVEEDOR
63	El proveedor de la solución deberá detallar los tipos de datos personales a los que tendrá acceso y/o procesará, recopilará, manejará, almacenará, transferirá o mantendrá en la provisión de sus productos o servicios a EPM.
64	El proveedor de la solución deberá garantizar que la solución cumple el principio de protección de datos personales de la Ley Estatutaria 1581 de 2012 del Estado colombiano y su reglamentación.
65	El proveedor de la solución deberá indicar los países de los que se recopilan o acceden los datos personales.
	2. PROGRAMA DE PRIVACIDAD
66	El proveedor de la solución deberá tener documentada, formalizada y en operación una política documentada que aborde la protección de la información de identificación personal (PII) / datos personales.
67	El proveedor de la solución deberá tener definido un programa para implementar los requisitos de la política.

68	El proveedor de la solución deberá tener definido y en operación un programa de capacitación a todos los empleados sobre el manejo adecuado de PII / datos personales.
	3. PLAN DE RESPUESTA A INCIDENTES DE PRIVACIDAD
69	El proveedor de la solución debe tener definido, documentación y en operación un plan de respuesta a incidentes de privacidad.
70	El proveedor de la solución debe tener definido, documentado y en operación una política y/o procedimiento de notificación de incidentes de privacidad de datos personales a sus clientes y/o asociados.
71	El proveedor de la solución deberá indicar si ha tenido un incidente de privacidad / violación de datos en los últimos 5 años que requirió notificación a los reguladores o las personas afectadas. En caso afirmativo, indicar si ha implementado procedimientos para corregir la causa raíz del incidente / incumplimiento.
	4. TRANSFERENCIA DE DATOS PERSONALES
72	El proveedor de la solución debe indicar si se transfieren datos personales de EPM y/o sus subsidiarias dentro de Colombia hacia otros países como Estados Unidos o dentro del Espacio Económico Europeo (EEE).
73	El SGDEA debe permitir el acceso a los datos y documentos exclusivamente desde los módulos o componentes funcionales de la misma.
74	El SGDEA debe tener controles que impidan a los usuarios con privilegios borrar definitivamente los datos, documentos y/o modificar la información almacenada en la base de datos.
75	El SGDEA debe limitar y restringir el acceso a las bases de datos usando herramientas de usuario final.
76	El SGDEA debe realizar el intercambio de datos entre soluciones externas y la solución por medio de protocolos seguros como HTTPS.
77	El SGDEA debe utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones y funcionalidades de alto riesgo.
78	El SGDEA debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.
79	El SGDEA debe permitir el uso de firmas electrónicas y certificados de autenticación con fines específicos.
80	El SGDEA debe cumplir con la certificación de seguridad para computación en nube ISO 27001.

81	Se debe proteger el acceso a las herramientas de auditoría del SGDEA para evitar su uso inadecuado o ponerlas en peligro, para ello se deberá tener un control de acceso y registro de auditoría para el acceso a la información, ya sea por usuarios, programas, servicios web, servicios de integración con otras aplicaciones o entidades.
82	El SGDEA debe generar y mantener evidencias de auditoria inalterables de las acciones realizadas por cada uno de los usuarios que ingresan al sistema.
83	El SGDEA debe tener la capacidad de generar auditoría de cambios sobre campos sensibles de la misma, dejando el rastro del cambio, especialmente información de usuario, máquina, fechas de aprobación.
84	El SGDEA debe impedir desactivar la generación y almacenamiento de pistas de auditoria.
85	El SGDEA debe permitir elaborar y mantener durante un periodo acordado las grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso.
86	El SGDEA deberá ofrecer el informe de la auditoría de terceros, por lo general un informe SOC 1 tipo 2 (basado en SSAE 16).
87	El SGDEA debe contar con un procedimiento para el monitoreo del uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deben revisar con regularidad.
88	El SGDEA debe utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.
89	El SGDEA debe tener un procedimiento de verificación periódica para determinar el cumplimiento con las normas de implementación de la seguridad.
90	El SGDEA deberá ofrecer mecanismos para evitar la eliminación o borrado de información en la base de datos, garantizando que los datos nunca sean eliminados físicamente, sino marcados como inactivos. Así como permitir configurar periódicamente tareas de eliminación de datos inactivos en la base de datos.

9. CONCLUSIONES

- Los repositorios oficiales para el almacenamiento de documentos de archivo en EPM son los del dominio de GD. Estos se utilizarán teniendo en cuenta las funcionalidades ofrecidas para cada tipo de contenido. (Se exceptúan los documentos Georeferenciados por temas de capacidad actual).

- Ningún sistema de información transaccional podrá ser considerado SGDEA, debido a que las funcionalidades que este ofrece deben garantizar el cumplimiento de la normatividad archivística vigente, la centralización de la información documental y su preservación durante el tiempo establecido en las TRD.

- Los sistemas transaccionales que requieran integración tecnológica con el SGDEA deberán cumplir con los requisitos de interoperabilidad registrados en el numeral 8.3 literal b.

- La adquisición de tecnología para el proceso de Gestión Documental deberá estar enmarcada en las definiciones determinadas en el Modelo de requisitos. Por tanto, este documento deberá permanecer articulado con la arquitectura de referencia del dominio funcional y las demás directrices que se emitan desde TI y que tengan relación directa o indirecta con la Gestión de Documentos recibidos o producidos en los sistemas de información de la organización.

- Los requisitos técnicos para la adquisición, actualización e implementación del SGDEA deberán ser revisados y ajustados por Tecnología de Información y Gestión Documental, en atención a las necesidades de la organización y la normatividad legal aplicable

- La conformación del ecosistema tecnológico alrededor del SGDEA, según la arquitectura objetivo del dominio funcional de gestión documental, debe partir de una transición en la que los sistemas de información que apoyan otros dominios funcionales de la organización habiliten las capacidades tecnológicas para articularse con las directrices establecidas por el proceso de Gestión Documental.

10. BIBLIOGRAFÍA

- Archivo General de la Nación. (2015, febrero 17) Acuerdo N° 03 Por el cual se establecen lineamientos generales para las entidades del Estado en cuanto a la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el capítulo IV del Decreto 2609 de 2012. Bogotá: Archivo General de la Nación.

- Archivo General de la Nación - Ministerio de Tecnologías de la Información y Comunicaciones. (2018) Guía para la gestión de documentos y expedientes electrónicos. Bogotá.

- Archivo General de la Nación - Ministerio de Tecnologías de la Información y Comunicaciones. (2017) Guía de Implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo SGDEA. Bogotá.

- Presidencia de la República de Colombia. (2015, mayo 26). Decreto N 1080 Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura. Bogotá. Presidencia de la República de Colombia.

- Modelo de requisitos para un SGDEA. Publicación AGN recuperada de https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Recursos/Publicacionees/ModeloDeRequisitosSistemaDeGestionElectronicos.pdf el 04 de agosto de 2021.

11. ANEXOS

- Actas de Trabajo TI – Gestión Documental
- Plan de elaboración e implementación MoREQ – EPM
- Requisitos técnicos y funcionales (Excel).