



UAESP



ESPECIFICACIONES TÉCNICAS

REPÚBLICA DE COLOMBIA

ALCALDÍA MAYOR DE BOGOTÁ D.C.

UNIDAD ADMINISTRATIVA ESPECIAL DE SERVICIOS PÚBLICOS - UAESP

ANEXO No. 3

ANEXO TECNICO

MODALIDAD DE SELECCIÓN: Selección abreviada- Menor cuantía

OBJETO: SAF-091 Implementación y puesta en marcha de Sistema de Gestión Documental Electrónico de Archivo de la Unidad Administrativa Especial de Servicios Públicos - UAESP.

BOGOTÁ D.C., NOVIEMBRE 2025



SC-2000374

CONTEXTO Y NORMATIVA A APLICAR

La normatividad aplicable se relaciona con el manejo de información institucional, garantizando propiedad intelectual y el tratamiento adecuado de la información; con el fin de garantizar la eficiente y segura prestación de los servicios TI a sus usuarios internos y las normas archivísticas para el Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) se basa en avalar la organización, autenticidad, seguridad y accesibilidad de los documentos electrónicos para el cumplimiento de las funciones administrativas, la transparencia y la protección de los derechos ciudadanos, con el fin de asegurar un repositorio digital seguro y cumplir con la ley, la cual requiere que la documentación sea recuperable y sirva como fuente histórica y para el servicio al ciudadano.

- ✓ Decreto Ley 019 de 2019, por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública
- ✓ Ley 2069 de 2020 que tiene por objeto establecer un marco regulatorio que propicie el emprendimiento y el crecimiento, consolidación y sostenibilidad de las empresas, con el fin de aumentar el bienestar social y generar equidad.
- ✓ Ley 2195 de 2022, La presente Ley tiene por Objeto adoptar disposiciones tendientes a prevenir los actos de corrupción, a reforzar la articulación y coordinación de las entidades del Estado y a recuperar los daños ocasionados por dichos actos con el fin de asegurar promover la cultura de la legalidad e integridad y recuperar la confianza ciudadana y el respeto por lo público
- ✓ Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.
- ✓ Decreto 1078 de 2015, Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- ✓ Ley 1915 de 2018: Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
- ✓ Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
- ✓ Resolución 460 de 2022, por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación.
- ✓ Decreto 1041 de 2022, Por el cual se adiciona un párrafo transitorio al artículo 2.2.1.1.1.5.2. y se modifican los párrafos transitorios 1 y 2 del artículo 2.2.1.1.1.5.6. del Decreto 1082 de 2015, Único Reglamentario del Sector Administrativo de Planeación Nacional, con el fin de extender hasta el año 2023 la facultad de los oferentes de acreditar el mejor indicador financiero y organizacional de los últimos tres (3) años, para contribuir a la reactivación económica.
- ✓ Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
- ✓ Ley 594 del 2000. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
- ✓ Decreto 1080 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura.
- ✓ Acuerdo 001 del 2024. Por el cual se establece el Acuerdo Único de la Función Archivística, se definen los criterios técnicos y jurídicos para su implementación en el Estado colombiano y se fijan otras disposiciones.

1. OBJETO A CONTRATAR

SAF-091 Implementación y puesta en marcha de Sistema de Gestión Documental Electrónico de Archivo de la Unidad Administrativa Especial de Servicios Públicos - UAESP.

2. ALCANCE DEL OBJETO

Contratar la adquisición, implementación, parametrización, migración, capacitación, estabilización, puesta en operación y soporte técnico de un Sistema de Gestión de Documentos Electrónicos de Archivo - SGDEA de la Unidad Administrativa Especial de Servicios Públicos - UAESP, de acuerdo con las necesidades específicas de la entidad en cumplimiento de su función, de los instrumentos archivísticos y de conformidad con la normatividad archivística colombiana y capacitación sobre el funcionamiento de este.

3. ESPECIFICACIONES TÉCNICAS**3.1 ESPECIFICACIONES FUNCIONALES**

ÍTEM	CLASIFICACIÓN Y ORGANIZACIÓN DOCUMENTAL
1	El Sistema de Gestión de Documentos Electrónicos de Archivo - SGDEA debe permitir la utilización de un Cuadro de Clasificación en el que los expedientes se puedan representar dispuestos en una jerarquía.
2	El SGDEA debe incorporar múltiples niveles para el esquema del Cuadro de Clasificación Documental
3	El SGDEA debe permitir que el CCD (Cuadro de Clasificación Documental) y las Tablas de Retención Documental - TRD sean controladas únicamente por un rol administrador y que pueda agregar, modificar y reorganizar la estructura.
4	Debe permitir al sistema importar archivos CSV para valores de sección, subsección, serie, subserie y tipos documentales validando los datos y reportando los errores o inconsistencias de datos presentados. Estos valores son necesarios para la configuración de las TRD de la entidad.
5	EL SGDEA debe permitir la creación, importación, parametrización, automatización, administración y versionamiento de las Tablas de Retención Documental - TRD, a partir de las plantillas predefinidas, asistentes de configuración, cargue de archivos planos o a través de la incorporación de otros mecanismos que faciliten la administración y la gestión de las TRD.
6	El SGDEA debe permitir a los usuarios autorizados la selección y uso de las diferentes versiones de la Tabla de Retención Documental.
7	El SGDEA debe Permitir que las Tablas de Retención Documental tengan asociados los siguientes campos: * Una descripción y/o justificación. * Versión de las TRD. * Fecha de actualización de las TRD en el sistema. * Identificador único cuando se crea.
8	El SGDEA debe garantizar que los elementos producidos y asociados a una TRD, mantendrán

	Los criterios de tiempos y de disposición final de la versión correspondiente.
9	El SGDEA debe permitir que los documentos que componen el expediente hereden los tiempos de conservación establecidos en la TRD.
10	EL SGDEA debe validar la información que se ingresa en el esquema de la Tabla de Retención Documental a través de la generación de alertas o incorporación de opciones que incluyan asistentes paso a paso (listas desplegables, alerta, listas de chequeo, ventanas de ayuda entre otras) que identifiquen si existe información similar o igual en el sistema.
11	<p>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:</p> <p>Para la importación:</p> <ol style="list-style-type: none"> 1. Permitir la importación de los metadatos asociados. 2. Cuando se importe las TRD y sus metadatos, el SGDEA debe validar y arrojar los errores de estructura y formato que se presenten. <p>Para la Exportación:</p> <ol style="list-style-type: none"> 1. Permitir la Exportación de metadatos asociados, incluyendo pistas de auditoría. Los procesos de importancia en y exportación en deben generar reportes y estas acciones deben quedar registradas en las pistas de auditoría.
12	El SGDEA debe permitir la transferencia de la estructura la TRD mediante un archivo XML, CSV o XLS
13	El SGDEA debe proporcionar a los administradores herramientas para informes estadísticos de la actividad dentro de la Tabla de Retención Documental.
14	El SGDEA debe permitir la integración con los diferentes servidores de correo electrónico de acuerdo con las necesidades o políticas de la entidad.
15	El SGDEA debe hacer accesible el contenido de los expedientes de acuerdo con los roles y permisos
16	El SGDEA debe permitir la asignación de un vocabulario controlado y normalizado.
17	El SGDEA debe garantizar que los documentos electrónicos de archivo que se capturen se asocien a una TRD configurada en el sistema.
18	El SGDEA debe permitir otorgarle un número único de identificación a un documento cuando es cargado al expediente.
19	El SGDEA debe permitir ingresar los datos de localización de un expediente híbrido (referencia cruzada al expediente físico). El sistema debe permitir diligenciar metadatos de ubicación, que luego van a permitir su ubicación a nivel de unidades documentales, para el caso de los expedientes híbridos.
20	El SGDEA debe representar la organización de los expedientes y de los documentos incluyendo sus metadatos, a partir del esquema del cuadro de clasificación documental.
21	Una vez finalizado el trámite administrativo, el SGDEA debe incorporar opciones para el cierre del expediente. (manual o automático) configurable de acuerdo con la política de la entidad.
22	Una vez cerrado el expediente se deberá restringir la adición o supresión de carpetas o documentos.
23	Excepciones: Cuando por disposiciones legales o administrativas sea necesario reabrir un expediente, esta acción deberá realizarse mediante un perfil administrativo y debe quedar registro de ello en las pistas de auditoría, con la explicación del motivo por el cual se realizó la acción.
24	El SGDEA debe permitir la generación de expedientes electrónicos y sus componentes (documento electrónico, foliado, índice firmado y metadatos).

25	<p>El SGDEA debe impedir la eliminación de un expediente electrónico o de su contenido. Sin embargo, existen dos excepciones a este requisito:</p> <ol style="list-style-type: none"> 1. La eliminación de acuerdo con lo establecido en las TRD. 2. Eliminación por un rol administrativo como parte de un procedimiento auditado.
26	El SGDEA debe permitir la incorporación de la firma electrónica para la generación del índice del expediente electrónico.
27	El SGDEA debe permitir múltiples firmas electrónicas o digitales en los documentos electrónicos de acuerdo con la normalización de las series y subseries documentales de la entidad.
28	El SGDEA debe permitir cotejar la composición de los documentos electrónicos que integran el expediente electrónico, asegurando su integridad y autenticidad.
29	El SGDEA debe disponer de una opción o servicio para la conversión de documentos a los formatos establecidos por el Archivo General de la Nación.
30	El SGDEA debe permitir exportar el directorio, de todos los expedientes y/o carpetas clasificadas en una serie específica y su contenido.
31	El SGDEA debe permitir exportar el índice electrónico a formato XML y CSV.
32	Los documentos dentro del SGDEA deberán heredar los metadatos de serie o subseries.
33	El SGDEA debe permitir diligenciar metadatos de ubicación, que luego van a permitir su ubicación a nivel de unidades documentales, para el caso de los expedientes híbridos.
34	El SGDEA debe registrar como metadatos la fecha y la hora de registro de la carga de un documento al expediente electrónico.
35	El SGDEA debe permitir que todas las acciones efectuadas sobre el expediente sean registradas en un historial de eventos que puede ser consultado por usuarios que tengan acceso al expediente electrónico incluso la consulta.
36	El SGDEA debe registrar en la pista de auditoría, cuando se realice la reubicación de una carpeta (o conjunto de carpetas) o documento.
37	El SGDEA debe permitir que el historial de eventos del expediente electrónico pueda ser exportado.
38	El SGDEA debe permitir realizar la trazabilidad de los documentos electrónicos en el Cuadro de Clasificación Documental mostrando información como mínimo de que, quien, cuando y como realizaciones en el mismo.
39	El SGDEA debe permitir establecer niveles de seguridad del expediente de acuerdo con los niveles de seguridad establecidos por la entidad.
RETENCIÓN Y DISPOSICIÓN	
40	El SGDEA debe permitir sólo al rol administrador parametrizar y/o gestionar tiempos de retención y disposición.
41	El SGDEA debe en la aplicación de los tiempos de retención a partir de la firma del índice electrónico una vez cerrado el expediente
42	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.
43	<p>Los SGDEA deben permitir como mínimo las siguientes acciones de disposición para cualquier regla de retención y disposición final:</p> <ol style="list-style-type: none"> 1. Conservación Total. 2. Eliminación segura con autorización del rol administrador, conservando los metadatos producto de la eliminación. 3. Medio técnico (permitiendo describir la forma en la cual se elimina el documento ya

	<p>sea físico o digital).</p> <p>4. Selección.</p>
44	El SGDEA requiere que genere notificaciones periódicas al administrador de todas las normas de conservación que se apliquen en un periodo determinado, y proporcionar informes cuantitativos sobre los volúmenes y tipos documentales de archivo afectados.
45	El SGDEA debe activar automáticamente una alerta al rol administrador y al productor cuando el período de retención aplicable está a punto de cumplir el tiempo establecido. Debe informar por correo electrónico y en el sistema.
46	El SGDEA debe informar al administrador que expedientes han cumplido su tiempo de retención antes de aplicar las acciones correspondientes. Una vez que el administrador haya confirmado el procedimiento inicia de acuerdo con los lineamientos establecidos por la entidad.
47	<p>El SGDEA debe emitir una alerta al administrador y productor en el caso en que un expediente electrónico esté listo para ser eliminado y alguno de sus documentos esté vinculados a otro expediente. El proceso de eliminación debe aplazarse para permitir una de las siguientes acciones correctivas:</p> <ol style="list-style-type: none"> 1. Solicitar confirmación para continuar o cancelar el proceso. 2. Esta acción deberá quedar en las pistas de auditoria relacionando mínimo los siguientes datos: fecha de inicio; identidad del usuario autorizado; motivo de la acción. 3. Deberá permitir copiar el documento a un expediente determinado y actualizar las referencias correspondientes, con el fin de garantizar la integridad del expediente.
48	<p>El SGDEA debe permitir a un usuario autorizado aplazar la eliminación de una serie, subseries, expediente determinado, alineado al proceso de eliminación definido por la entidad:</p> <p>Cuando esto ocurra, el SGDEA debe solicitar y almacenar como mínimo la siguiente información en la pista de auditoría:</p> <ol style="list-style-type: none"> 1. La fecha de inicio de la interrupción. 2. La identidad del usuario autorizado. 3. La justificación de la acción.
49	El SGDEA debe grabar automáticamente e informar a administrador de todas las acciones relacionadas con el destino de los documentos de archivo.
50	El SGDEA debe mantener una historia inalterable de modificaciones (pistas de auditoría) que se realizan en los tiempos de retención y disposición, incluida la fecha del cambio o eliminación y el usuario que lo registra.
51	El SGDEA no debe limitar la duración de los tiempos de retención.
52	Cuando el SGDEA está transfiriendo o exportando expedientes y/o documentos y alguno de ellos incluye referencias a documentos almacenados en otros expedientes, el SGDEA deberá transferir o exportar el documento completo, no solo la referencia y almacenarlos de acuerdo con el flujo de trabajo correspondiente.
53	<p>Cuando por motivos de obsolescencia tecnológica, seguridad de la información, causal administrativo o judicial, se requiera exportar, transferir o migrar los documentos se debe garantizar la integridad de los expedientes, respecto a:</p> <ol style="list-style-type: none"> 1. Componentes del expediente (documento electrónico, foliado, índice firmado y metadatos). 2. Estructura de los documentos, preservando las relaciones correctas entre ellos.

54	<p>Durante un proceso de migración entre diferentes sistemas o plataformas tecnológicas se debe garantizar que:</p> <ol style="list-style-type: none"> 1. Exportar o transferir los documentos correspondientes con las reglas de retención y disposición y sus respectivos controles de acceso (seguridad para consulta) para que puedan seguir aplicándose en el sistema de destino. 2. Generar e Imprimir uno o más informes o reportes que muestren las reglas que se aplicarán a cada conjunto de documentos con sus características. 3. Garantizar la estructura del expediente asegurando que los vínculos archivísticos se conserven en todo momento.
55	El SGDEA deberá generar un reporte del estado de la transferencia o exportación realizada y guardar datos de la acción efectuadas en las pistas de auditoría.
56	Conserva todos los Documentos Electrónicos de Archivo (DEA) que se hayan transferido, al menos hasta que se reciba la confirmación de que el proceso de transferencia ha concluido satisfactoriamente.
TRANSFERENCIAS DOCUMENTALES	
57	Cuando se aplican las transferencias a los expedientes físicos y/o electrónicos, debe ser de acuerdo con los procedimientos establecidos por la Entidad.
58	El sistema debe monitorear el tiempo de conservación de los expedientes electrónicos y/o Físico, tomando como base la fecha del último documento que contiene el expediente conforme la disposición final de la TRD.
59	El SGDEA debe notificar la transferencia según el cronograma de transferencia, de acuerdo con los inventarios documental de la oficina.
60	<p>El SGDEA debe transferir un expediente o un volumen, la transferencia debe incluir:</p> <ol style="list-style-type: none"> 1. Todos los expedientes. 2. Todos los volúmenes de los expedientes. 3. Todos los documentos de archivo de los expedientes y volúmenes. 4. Todos los metadatos asociados al expediente, volúmenes y documentos de archivo.
61	El sistema debe facilitar la generación del inventario documental (F U I D) y su aprobación por archivo central.
62	El sistema debe permitir ingresar los diferentes tomos que hacen parte del expediente, de manera que se vean reflejados en el FUID.
63	<p>Cuando el SGDEA realice la transferencia de documentos electrónicos debe garantizar:</p> <ol style="list-style-type: none"> 1. Compatibilidad de formatos. 2. Compatibilidad de soportes. 3. Los metadatos del documento electrónico deben ser transferidos asociados al documento para permitir su identificación y autenticidad.
64	<p>El SGDEA debe ser capaz de transferir o exportar un expediente en una sola secuencia de operaciones, de modo que:</p> <ol style="list-style-type: none"> 1. No se degrade el contenido ni estructura de sus documentos electrónicos de archivo. 2. Se conservan todos los vínculos entre el documento de archivo y sus metadatos.
65	<p>El sistema debe permitir al usuario solicitar ampliación de plazo de transferencia. Debe registrarse una observación en el histórico del expediente, garantizando lo siguiente:</p> <ol style="list-style-type: none"> 1. La fecha de inicio de la interrupción. 2. El motivo de la acción.

66	En la transferencia o exportación de documentos electrónicos de archivo, el sistema debe ser capaz de incluir una copia de los datos de la pista de auditoría asociada a los documentos de archivo, volúmenes y expedientes objeto de la transferencia.
67	En la transferencia del expediente electrónico, el sistema no puede degradar el contenido ni la estructura de sus documentos electrónicos; conservando todos los vínculos entre el documento y sus metadatos.
68	El SGDEA debe conservar todos los expedientes electrónicos que se hayan transferido, al menos hasta que se reciba la confirmación de que el proceso de transferencia ha concluido satisfactoriamente.
69	Debe reflejar en el estado del expediente, de acuerdo con el ciclo de vida del documento. Eje: transferido "Archivo Central".
70	El sistema debe presentar al archivo central, los metadatos que faciliten la ubicación física para el caso de los expedientes híbridos.
71	El sistema debe presentar un informe en el que se detalle cualquier fallo que se haya producido durante la transferencia, la exportación o el borrado. El informe deberá indicar cuáles de los registros que estaba previsto transferir han generado errores durante la operación.
72	El sistema debe permitir para casos excepcionales de expedientes transferidos al Archivo Central, la reincorporación al Archivo de Gestión, mediante una operación monitoreada y realizada por usuarios autorizados.
73	El sistema debe permitir la carga masiva y consulta de inventarios documentales.
CAPTURA E INGRESOS DE DOCUMENTOS	
74	El SGDEA debe permitir registrar y gestionar todos los documentos electrónicos de archivo, con independencia del método de codificación empleado, la codificación está definida en el Cuadro de Clasificación Documental.
75	El SGDEA debe contar un repositorio centralizado de expedientes electrónicos.
76	El contenido del documento electrónico de archivo debe incluir la información que determine su forma de presentación y el comportamiento del documento electrónico de archivo.
77	El SGDEA debe permitir la definición y parametrización de formatos de captura y el mantenimiento de estos, teniendo en cuenta las necesidades del negocio, los estándares, formatos abiertos y formatos recomendados por el Archivo General de la Nación.
78	El SGDEA debe permitir gestionar contenidos como: videos, audio, imagen, de la misma forma que los documentos electrónicos de texto.
79	El SGDEA deberá ofrecer ayudas que permitan clasificar los documentos según la TRD y el CCD.
80	El proceso de captura de documentos del SGDEA debe contar con los controles y la funcionalidad adecuados para garantizar que los documentos se asocien con la Tabla de Retención Documental.
81	SGDEA debe asignar el documento electrónico de archivo a un único expediente según el flujo documental definido en la TRD.
82	El SGDEA no debe limitar el número de documentos que pueden ser capturados en cualquier serie, subseries, expediente ni sobre el número de documentos que se pueden almacenar.
83	Para la captura de documentos que tienen anexos el SGDEA deberá gestionarlos como unidad, restringiendo el uso de formatos comprimidos no nativos como ZIP, RAR, entre otros.
84	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.
85	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.

86	El SGDEA debe ofrecer opciones de gestión de notificaciones y avisos por medio de correo electrónico.
87	Cuando el usuario captura un documento que tiene más de una versión, el SGDEA debe permitir el versionamiento del documento, el cual evidencie la trazabilidad del documento.
88	<p>Cuando existe más de una versión de un documento, el SGDEA deberá permitir que los usuarios soporte al menos por una de las siguientes posibilidades:</p> <ol style="list-style-type: none"> 1. Registrar todas las versiones del documento como un solo documento de archivo. 2. Registrar una sola versión del documento como documento de archivo. 3. Registrar cada versión del documento como un documento de archivo distinto.
89	El SGDEA debe generar una alerta al intentar capturar un registro que este incompleto o vacío.
90	El SGDEA debe cumplir como mínimo con uno de los siguientes estándares de interoperabilidad: OAI-PMH o CMIS-OASIS en sus últimas versiones, para garantizar la interoperabilidad con otros sistemas.
91	<p>Cuando se realiza captura masiva de documentos, en el cual se requiere que al momento de iniciar un proceso masivo es necesario que muestre el avance del proceso de digitalización y cuáles de esos presentan inconvenientes de cargue y por ende se pueda realizar lo indicado:</p> <ol style="list-style-type: none"> 1. Ver cola. 2. Pausar la cola de un documento o de todos. 3. Reiniciar la cola. 4. Eliminar la cola.
92	<p>El SGDEA debe tener integrado o desarrollado como mínimo con una solución de digitalización y debe permitir:</p> <ol style="list-style-type: none"> 1. El escaneo monocromático, a color o en escala de grises. 2. El escaneo de documentos en diferentes resoluciones. 3. Manejar diferentes tamaños de papel estándar. 4. Debe reconocer y capturar documentos individuales en un proceso de digitalización masiva. 5. Guardar imágenes en formatos estándar.
93	<p>El SGDEA debe incluir tecnologías de reconocimiento de datos, (de acuerdo con las necesidades y las que sean requeridas por la entidad):</p> <ol style="list-style-type: none"> 1. (OCR) Reconocimiento óptico de caracteres. 2. (ICR) Reconocimiento inteligente de caracteres. 3. (OMR) Reconocimiento óptico de marcas. 4. Reconocimiento de código de barras.
94	<p>El SDGEA debe proporcionar asistencia automatizada para el registro de documentos electrónicos, extrayendo automáticamente los metadatos de los siguientes tipos de documentos, como mínimo:</p> <ol style="list-style-type: none"> 1. Documentos de oficina (formatos normalizados). 2. Correos electrónicos sin ficheros adjuntos, tanto recibidos como enviados. 3. Correo electrónico con ficheros adjuntos, tanto recibidos como enviados.
95	Debe permitir parametrizar los metadatos de acuerdo con lo establecido en la norma ISO 23081 y Guía de esquema de metadato para la Gestión Documental - Archivo General de la Nación.
96	En la captura, el SGDEA debe permitir la incorporación de todos los elementos de metadatos especificados en el momento de la configuración, así como su conservación, manteniéndolos

	asociados en todo momento a los documentos electrónicos de archivo correspondientes.
97	El SGDEA debe garantizar que solo los administradores y los usuarios autorizados puedan modificar el contenido de determinados elementos de metadatos del documento electrónico de archivo.
98	El SGDEA debe permitir la visualización de los metadatos que conforman el expediente o documento.
99	El SGDEA debe permitir la validación y control de los metadatos.
100	El SGDEA debe permitir la captura automática de metadatos pertenecientes a mensajes de correo electrónico y sus archivos adjuntos. Garantizando la autenticidad del documento.
101	El SGDEA debe permitir al usuario capturar un mensaje de correo electrónico asignándolo dentro de una serie, subseries o expediente.
102	El SGDEA debe tener la opción de capturar en una sola operación, varios correos electrónicos seleccionados manualmente.
103	El SGDEA debe permitir parametrizar firmas individuales, múltiples firmantes, firmas masivas de documentos y firmas por lotes de documentos, de acuerdo con la normalización de las series y subseries documentales de la entidad.
104	El SGDEA debe permitir la integración con mecanismos tecnológicos tales como: firmas digitales, estampado cronológico, mecanismos de encriptación, marcas digitales electrónicas. Se aclara que el sistema debe permitir la integración con cualquier proveedor de certificados de firmas digitales.
105	El SGDEA debe soportar formatos de firma digital tales como CADES, PADES o XADES:
106	El SGDEA debe permitir vistas de los Documentos Electrónicos tipo TIFF, PDF y JPG de Archivo DEA que carecen de la aplicación utilizada para generarlos.
107	El SGDEA debe permitir que los registros almacenados temporalmente sean modificados y completados para continuar con su proceso.
108	El SGDEA debe permitir la configuración de una lista de correos con el fin de identificar las cuentas que serán gestionadas de manera automatizada cada vez que se envíen y se reciban mensajes en las mismas.
109	El SGDEA debe permitir la activación o desactivación de las cuentas de correo que serán gestionadas de manera automatizada.
110	El SGDEA debe permitir la captura de correos electrónicos de entrada y de salida que contengan o no archivos adjuntos, considerándolos como un solo Documento Electrónico de Archivo - DEA, respetando su contenido, contexto y estructura.
111	El SGDEA debe permitir el registro de información básica de contexto (metadatos) automáticamente obteniéndola del encabezado del correo electrónico.
112	El SGDEA debe contar con una plataforma estándar compatible con la definición de estructuras de datos (XML), que brinden la posibilidad de realizar importación de información de este y de otros sistemas garantizando su interoperabilidad.
113	El SGDEA debe permitir a un perfil administrador, actualizar y adicionar información de contexto (metadatos) a los datos importados que presenten inconsistencias o que lo requieran, y se debe llevar un registro detallado de auditoría de estas operaciones en una estructura independiente.
114	En el proceso de captura el SGDEA debe permitir la conversión de formatos XLS, DOC, JPG y PPT, los cuales se almacenarán en formato PDF y PDF/A con excepción de los formatos audiovisuales.
115	El SGDEA debe permitir crear documentos basados en plantillas de office Word preestablecidas.
116	El SGDEA debe proporcionar una herramienta de edición / diseño de plantillas de Word que permite a los administradores de sistema, crear plantillas de acuerdo con las necesidades de la

	entidad.
117	<p>En relación con los documentos electrónicos de archivo con más de un componente, el SGDEA debe:</p> <ol style="list-style-type: none"> 1. Manejar el documento de archivo como una entidad única e indivisible, conservando las relaciones existentes entre sus componentes. 2. Respetar la integridad estructural del documento de archivo. 3. Permitir su recuperación, visualización y su gestión integrada.
118	<p>El SGDEA debe capturar documentos sobre transacciones generadas por otros sistemas, lo cual debe incluir:</p> <ol style="list-style-type: none"> 1. La posibilidad de importar transacciones de ficheros de lotes predefinidos. 2. La edición de reglas que permitan personalizar el registro automático de los documentos de archivo. 3. La validación de la integridad de los datos.
BÚSQUEDA Y PRESENTACIÓN	
119	El SGDEA debe permitir al usuario buscar y recuperar información que se encuentre dentro de documentos, listas de documentos y metadatos, de acuerdo con el perfil de acceso.
120	<p>El SGDEA debe permitir:</p> <ol style="list-style-type: none"> 1. Ver la lista de resultados de una búsqueda. 2. Listar documentos que componen un resultado de la búsqueda. 3. Ver la lista de todos los expedientes y documentos relacionados a cualquier serie determinada, con su respectivo contenido. 4. Incluir funciones para presentar en los medios adecuados la salida de los documentos que no se pueden imprimir. Por ejemplo, documentos de audio y video. 5. Mostrar miniaturas de imágenes digitalizadas como una ayuda para la navegación y búsqueda.
121	El SGDEA debe permitir que el usuario efectúe una búsqueda combinada en los metadatos y/o en el contenido de los documentos de archivo en una sola consulta.
122	El SGDEA debe permitir hacer búsquedas por conceptos, mediante el uso de tesauros (Diccionario que muestra la equivalencia entre los términos o expresiones del lenguaje natural y aquellos términos normalizados y preferentes del lenguaje documental, así como las relaciones semánticas que existen entre otros términos) como un índice en línea.
123	El SGDEA debe permitir que en los resultados de búsqueda se presenten únicamente las carpetas y documentos a los que el usuario tiene acceso de acuerdo con los niveles de permisos definidos.
124	El SGDEA debe permitir la búsqueda dentro de los niveles de jerarquía del cuadro de clasificación.
125	El SGDEA debe mostrar el número total de resultados de una búsqueda en la pantalla del usuario y permitir que éste visualice dichos resultados o bien afine sus criterios de búsqueda.
126	El SGDEA debe permitir visualizar los documentos de archivo recuperados como resultado de la búsqueda sin necesidad de cargar la aplicación de software asociada.
127	<p>El SGDEA permita que los usuarios y adiestradores configuren los formatos de visualización de los resultados de búsqueda, funciones como:</p> <ol style="list-style-type: none"> 1. Elegir el orden en que se muestren los resultados de una búsqueda. 2. Determinar el número de resultados que se muestran cada vez en pantalla en la visualización. 3. Determinar el número máximo de resultados de una búsqueda.

	4. Seleccionar los campos de metadatos que se muestra en la lista de resultados de la búsqueda.
128	El SGDEA debe permitir la búsqueda de texto libre y metadatos de forma integrada y coherente.
129	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.
130	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.
131	El SGDEA debe permitir la previsualización de documentos del expediente, sin que eso implique la descarga del documento.
132	El SGDEA debe restringir la impresión de los documentos, de acuerdo con los lineamientos de la entidad.
133	El SGDEA debe permitir a los administradores configurar y cambiar los campos de búsqueda: <ol style="list-style-type: none"> 1. Especificar como campo de búsqueda cualquier elemento de metadatos de los expedientes o documentos de archivo, de forma opcional. 2. Modificar la configuración del campo de búsqueda.
134	El SGDEA debe proporcionar herramientas para la generación de informes y reportes parametrizables.
135	El SGDEA debe permitir generar informes que incluyan como mínimo gráficos y tablas parametrizables.
136	El SGDEA debe permitir generar informes sobre los errores presentados en el sistema (Cargue de documentos fallidos, procesos y procedimientos incompletos, número de intentos fallidos al sistema, entre otros).
PRÉSTAMO DE DOCUMENTOS	
137	El flujo de préstamos documentales debe ser 100% a través de la plataforma.
138	El sistema debe permitir parametrizar el tiempo de vencimiento de los préstamos documentales.
139	El sistema debe ofrecer una funcionalidad que permita buscar y solicitar el préstamo de expedientes o radicado.
140	El sistema debe permitir al responsable del expediente o radicado aceptar o rechazar el préstamo.
141	El sistema debe controlar la devolución del préstamo mediante el envío de notificación en caso de vencimiento.
142	El sistema debe permitir realizar la devolución del préstamo al usuario solicitante.
143	El sistema debe registrar en el histórico del expediente el registro de la operación en torno al proceso de préstamo documental y generar informes y reportes de los préstamos documentales
144	El SGDEA debe habilitar vínculos de acceso temporales para los préstamos de los documentos digitalizados y cargados en la plataforma, deshabilitando el acceso al vencimiento de la temporalidad del préstamo.
RADICACIÓN	
145	El sistema de cumplir con lo establecido en el acuerdo 001 de 2024: <ol style="list-style-type: none"> 1. Firmas responsables. 2. Procedimientos para la radicación de comunicaciones oficiales. 3. Numeración de actos administrativos. 4. Comunicaciones internas.

	5. Control de comunicaciones oficiales. 6. Conservación documental. 7. Comunicaciones oficiales enviadas y recibidas.
146	El sistema debe contar con un módulo para generar comunicados internos.
147	Permite la selección de opción de tipo radicación de Entrada, Salida y Memorando (interna) y otros.
148	El sistema debe permitir identificar a través del número de radicado mediante un código identificador el tipo de radicado, entrada, salida e interno.
149	El sistema debe permitir en la radicación de documentos que ingresan por correspondencia, la impresión de rótulos de identificación para incorporar al documento físico el cual incluya códigos de barras, fecha, hora, oficina a la cual va dirigido el radicado, código de validación y usuario radicador.
150	Al momento de radicar un documento de entrada el sistema genera el número de radicado.
151	Al digitalizar el documento que entra por ventanilla (radicado de entrada) hay un aval electrónico que el documento es original (firma desatendida).
152	Los anexos que acompañan al radicado principal (entrada) al ser digitalizados, se tipifican y dan observaciones especiales para enviarlos organizados y divididos al área.
153	Radicación Masiva: Realizar radicación de 5 a 100 documentos, sin usar archivos CSV, utilizando un módulo integral de listados y el mismo generador de documento para Salida y Memorando.
154	Permite tipificar (Selección TRD) desde la ventana de radicación, para documentos internos y de salida.
155	Generar expedientes masivos en el momento de realizar una radicación masiva, permitiendo campos extra de información asociada a los radicados.
156	Después de radicado por el ciudadano, el sistema debe presentar un número de radicado único para posterior consulta.
157	Los comunicados internos, entradas y salidas deben permitir seleccionar múltiples destinatarios.
158	Debe permitir para todo tipo de radicado, la opción de referenciar otro número radicado del sistema, generando log en los históricos implicados.
159	Los destinatarios de comunicados internos pueden reasignar, incluir a expediente electrónico y responder a través mediante un comunicado interno electrónico.
160	El sistema debe permitir generar radicados de salida desde la dependencia productora.
161	Todo documento para radicado de salida debe permitir la previsualización en formato PDF/A y combinación de datos de la plantilla de Word.
162	Los radicados de salida deben permitir enviar copia a otros destinatarios externos, generando diferente número radicado.
163	El sistema debe permitir generar radicados de salidas digitales y físicas. Para el primero debe enviarlo al ciudadano o empresa destinataria.
164	Al momento de radicar un documento de salida el sistema genera el número de radicado asignado.
165	Respuesta aclaraciones, cierre de la entrada y posteriormente debe permitir referenciar el nuevo radicado del ciudadano como antecedente del nuevo trámite.
166	El sistema debe contar con un módulo integrado y expuesto desde el portal Web de la entidad, para la radicación de PQRS desde y hasta el aplicativo: El ciudadano puede seleccionar el tipo de requerimientos (Petición Queja, Reclamo, Sugerencia, Denuncia, Felicitación, etc.).

	<p>El módulo debe permitir la validación de la existencia del correo electrónico provisto por el ciudadano.</p> <ol style="list-style-type: none"> Validado el ciudadano, este puede formular requerimientos vía Web. El ciudadano puede seleccionar el tipo de requerimiento (Petición Queja, Reclamo, Sugerencia, Denuncia, Felicitación, etc.). El ciudadano puede seleccionar la temática general de que trata su requerimiento.
167	El sistema debe contar con un tipo de radicado de requerimientos para los usuarios que lo registran desde los puntos de atención.
168	El sistema debe permitir radicar requerimientos mediante documentos físicos y electrónicos.
169	El sistema debe permitir adjuntar a un requerimiento archivos anexos (correo electrónico, documentos, audios, videos, etc.)
170	Este sistema debe permitir la carga del oficio principal y anexos que pueda tener el requerimiento.
171	Después de cargado el documento digital, el sistema debe presentarlo en la bandeja de entrada del usuario responsable de gestionar el trámite del requerimiento.
172	Una vez radicado el requerimiento, el sistema debe cargarlo en la bandeja de entrada del usuario configurado como responsable del tema seleccionado por el ciudadano.
173	El sistema debe enviar copia del requerimiento registrado al correo electrónico suministrado por el ciudadano.
174	El sistema debe permitir delegar los requerimientos a uno o varios usuarios encargados de la gestión del trámite, de tal forma que cada usuario pueda aportar los soportes y comentarios necesarios para emitir respuesta consolidada.
175	El sistema debe permitir consultar las respuestas de los requerimientos en el sitio Web de la Entidad con el número de radicado y un mecanismo de verificación que valide que el usuario es el petionario.
176	El sistema debe permitir la carga del archivo digitalizado cuando los radicados se realizan de manera física, así como la carga de los anexos que soporten el requerimiento.
177	El sistema debe permitir referenciar un requerimiento con otro al momento de su creación.
178	Respuesta definitiva, es el cierre definitivo de la PQRSD y derechos de petición.
179	El sistema debe permitir la clasificación de tipos de requerimiento.
180	Las tutelas deben poder registrar la fecha máxima de respuesta en horas y minutos.
181	Las tutelas deben permitir asociar un rol, para que los usuarios que cuenten con este, pueden reasignar a cualquier usuario del sistema.
182	El sistema debe facilitar los análisis de antecedentes, proyección de respuesta y trámite que haya lugar hasta culminación del asunto.
183	Estas operaciones deben generar histórico en los radicados enlazados.
184	Cuando se radique un requerimiento para la Unidad de manera física, correo electrónico, fax o vía Web, debe consumir un número de radicado provisto por el SGDEA para la consulta del estado del trámite.
185	Permitir que se pueda seleccionar los vencimientos de términos para radicados que no sean PQRSD.
DISTRIBUCIÓN	
186	El sistema debe permitir con los radicados de entrada la función de asignación simple y múltiple. Ejemplo cuando un radicado debe ser tramitado por varios usuarios simultáneamente.
187	Los documentos que se requieran enviar a través de un módulo de correspondencia deberán ser marcados o identificados en el sistema, con el fin de evitar cambios o modificar el documento.

188	El sistema debe permitir la devolución de un radicado (marcar regreso) en caso de que el documento físico no llegue al área de correspondencia y hacer su inventario para el envío final.
189	Permitir la devolución o anulación de un radicado cuando este haya sido rechazado por falta de datos, por error u otras observaciones que correspondencia administre.
190	Los usuarios de ventanilla no pueden reasignar requerimientos a otra dependencia. Esta acción se debe realizar únicamente por los usuarios con el perfil designado para ello.
191	El sistema debe permitir la asignación de rutas de correspondencia y mensajería con terceros para radicados de salida en soporte físico, así como la generación de planillas de reparto.
FLUJO DE TRABAJO	
192	El plazo debe ser configurado de acuerdo con lo estipulado en los términos de ley por cada trámite.
193	Deberá finalizar el requerimiento cuando el tipo de respuesta sea traslado por competencia.
194	El sistema debe permitir sobre plantillas de Word la creación, asignación, modificación, preparación, aprobación secuencial. Todas estas funciones desde la misma plataforma.
195	Permite hacer modificación a los documentos que ya se generaron (editar) antes de ser enviado o aprobado definitivamente.
196	Los cambios efectuados deben sincronizarse automáticamente y guardarse, tipo guardado automático.
197	El sistema debe permitir construir documentos según el flujo de trabajo de radicados de entrada y salida. En todo caso debe gestionarse una sola versión del documento.
198	El sistema debe facilitar los análisis de antecedentes, proyección de respuesta y trámite que haya lugar hasta culminación del asunto.
199	Metadatos: Módulo donde se crean y editan los campos requeridos para los radicados y expedientes de cada área.
CONSULTA	
200	Los documentos radicados de entrada deben permitir ser consultados desde la bandeja del usuario seleccionado, aun cuando no tenga asociado el documento digitalizado.
201	El expediente debe contar con un organizador de vista de su contenido a través de filtros.
202	El sistema debe permitir consultar requerimientos asociadas a un peticionario por cedula, nombre, documento de identidad o palabras claves
203	Realizar búsquedas básicas por medio del número de radicado, nombre o número de expediente filtrado por fechas.
204	Realizar búsquedas avanzadas; por radicado: asunto, documento, nombre tercero, metadatos, filtrado por fechas. Por expediente: Metadatos, TRD.
205	El ciudadano debe contar con un módulo que permita consultar las respuestas emitidas por la entidad.
PARAMETRIZACIÓN	
206	El sistema debe permitir la creación y selección de un contacto, ya sea ciudadano o entidad.
207	La dirección del contacto debe ser creada bajo un formulario.
208	Se debe poder parametrizar asuntos de radicación de entrada por dependencia para facilitar el ingreso y ubicación del documento con la mayor información requerida.
209	Cuando se cuente con el diligenciamiento del formulario de radicación de entrada, el sistema de permitir su radicación, generando un RÓTULO Impreso donde no afecte el contenido del documento.
210	El RÓTULO debe contar con imagen corporativa de la entidad, código de barras, fecha, hora y usuario radicado.

	<ol style="list-style-type: none"> Número de Registro: Fecha: Hora: Registrado Por: Área: Responsable: Folios: Código de barras o Código QR: <p>El diseño de rótulo y los campos visibles deben poderse modificar por el administrador del sistema.</p>
211	El sistema debe tener el control de la entrega física del documento a través de un reporte que permita la recepción de documentos evitando la impresión de planillas físicas.
212	Al gestionar el radicado de salida, permite la selección de terceros, sin cruzar listado de los funcionarios de la entidad.
213	Al realizar una búsqueda de un tercero en el listado de selección, permite enlazar un radicado (asociado o anexo) que sea parte de una solicitud antes enviada.
214	El sistema debe permitir la creación y selección de un contacto, ya sea ciudadano o empresa.
215	Cuando se cuente con el diligenciamiento del formulario de radicación de salida, el sistema de permitir su radicación, generando un RÓTULO.
216	El sistema debe permitir asociar una plantilla de Word al comunicado interno, el cual debe ser el cuerpo del comunicado interno.
217	Las plantillas de Word después de radicadas, el sistema debe convertirlas en PDF/A para efectos de conservación.
218	La plantilla utilizada por el usuario debe alojarse nativamente en la plataforma, el cual debe permitir la edición del documento las veces que el usuario lo requiera.
219	Cuando se radica un documento de salida el sistema debe presentar metadatos directamente sobre las plantillas de Word con datos básicos de los destinatarios
220	Al realizar una búsqueda de un tercero en el listado de selección, permite enlazar un radicado (asociado o anexo) que sea parte de una solicitud antes enviada.
221	Se debe exponer un web services que permita integración con los sistemas de mensajería que realizan la entrega física de la correspondencia de salida de la entidad, para hacer que la Unidad se encargue de realizar la integración. Se aclara que la empresa de mensajería se cambia anualmente, el protocolo de integración será definido en conjunto con la empresa de mensajería con contrato vigente.
222	El sistema debe permitir que se realice un cargue de las guías de entrega de la correspondencia de salida por el grupo de Correspondencia.
223	Anular Radicados: Permitir por rol - perfil dar el permiso de solicitud de anulación de radicados, encaso de que no se dé el trámite final convenido al mismo.
224	Anular Radicados: Permitir por rol - perfil general un acta de los radicados anulados con el área encargada del caso.
225	Los comunicados internos deben permitir contar con roles de proyectores y aprobadores.
226	Los comunicados internos deben ser 100% electrónicos.
227	Debe permitir mediante rol, la opción de enviar masivamente comunicados internos a usuarios del sistema.
228	Al gestionar un radicado Interno, permite la selección de los funcionarios y sus áreas.

229	El sistema debe permitir configurar los consecutivos de correspondencia y creación de expediente.
230	El sistema debe permitir devolver a ventanilla, los radicados de entrada que no sea de su competencia, con la observación y trazabilidad sobre el mismo, el tiempo de devolución debe ser parametrizable.
231	El sistema debe contar con un rol que permita la modificación de algunos campos (folios, numero de anexos, dirección) del formulario, con el registro en el histórico del mismo.
232	El sistema debe Permitir a los usuarios (previamente autorizados para ello) reasignar radicados de un usuario a otro nuevo de la misma dependencia. el tiempo de reasignación debe ser parametrizable.
233	El sistema debe permitir reasignar un radicado de entrada respetando la jerarquía de la entidad (dependencia superior y dependencia inferior) omitiendo las áreas que no hagan parte de la misma línea de mando. Debe permitir seleccionar la dependencia responsable de consolidar la respuesta.
234	El sistema debe contar con un buscador que recupere los expedientes y tramites que faciliten la inclusión de radicados.
235	El sistema debe permitir el cálculo de la fecha de vencimiento de los radicados, cuando este se ha establecido.
236	El sistema debe permitir la carga de plantillas de Word para la generación de radicados de salida, que recuperen información del requerimiento.
237	Cuando se recibe en ventanilla un radicado de salida físico, el sistema debe permitir asignar numero definitivo, generación del RÓTULO, digitalizar el radicado de salida.
238	El sistema debe permitir asociar o desactivar los nombres y apellidos de los mensajeros de la empresa encargada de las entregas.
239	Se debe permitir la anulación de cualquier tipo de radicado de entrada, salida o interno según el rol asignado.
240	Los radicados anulados pueden ser consultados a través del buscador del sistema. En el histórico debe registrarse la operación de "Anulado".
241	El sistema debe permitir los radicados anulados los cuales se deben manejar como un estado adicional en el sistema, el cual al momento de ser modificado como ANULADO por el administrador del sistema, debe permitir el cargue de documento con la autorización del jefe del área pertinente, adicionalmente el radicado debe quedar sin responsable y debe desaparecer de la vista de pendientes de los funcionarios. Este estado debe permitirse filtrar dentro de los reportes de radicados.
242	Pueden solicitar anulación, todos los usuarios que hacen parte del flujo de revisión y aprobación del documento según el rol asignado.
243	El sistema debe permitir configurar sucursales, las cuales se asocian a dependencias y estas permiten el control de la correspondencia.
244	El contador de los consecutivos de radicación debe reiniciar automáticamente a partir del 1 de enero a las cero horas.
245	El sistema debe permitir configurar los tiempos respuesta según los términos de Ley predeterminados.
246	El sistema debe permitir configurar días y horas no laborales, los cuales se tienen en cuenta para el vencimiento de radicados.
247	El sistema debe permitir configurar motivos de devolución de la correspondencia enviada físicamente, de tal manera que se pueda establecer cual implica reprogramación o cancelación

	del envío.
248	El sistema debe permitir configurar alertas para los radicados, de tal manera se pueda asignar responsables de notificación y fecha de vencimiento.
249	El sistema debe permitir crear temáticas para la asignación de radicados.
250	El sistema debe permitir la creación de usuarios con los datos completos de la funcionalidad: tipo de usuario, login, nombres, documento, correo electrónico. Adicionalmente el sistema debe permitir la creación de puntos de radicación, entendiendo por puntos las sedes en las cuales la entidad considere habilitar radicación, estos puntos estarán conectados mediante VPN punto a punto o bien mediante MPLS como una LAN extendida.
251	EL SGDEA debe realizar la autenticación de los usuarios únicamente a través del directorio activo de Windows.
252	Creación de las respectivas dependencias de la entidad, con el número que la identifica según el sistema orgánico funcional (organigrama designado en la TRD de la Entidad).
253	Creación de nuevos tipos de radicación que requiera la entidad para sus procesos
254	Creación y edición de listados de roles.
255	Generar la relación de los roles vs las dependencias, con los respectivos permisos que cada área concrete para el funcionario (rol), manejando niveles de seguridad que permitan el escalonamiento de la información.
256	Permitir la visualización en información total o parcial según los roles, jerarquías o niveles definidos
257	<p>Crear una plantilla con la estructura de la serie de contratos y convenios de la que permita almacenar documentos digitales de los contratos y convenios.</p> <p>Identificando motores de búsqueda</p> <p>Borrador necesidades de herramienta tecnológica</p> <p>Documentos de patrimonios autónomos: Los documentos producidos en razón de la actividad propia de estos contratos no son obligatorios para custodia por parte de la Entidad, sin embargo, se tiene la necesidad de la consulta, por esta razón es importante que la herramienta brinda un módulo de consulta de contratos de la unidad, que cuente con motores de búsqueda como:</p> <p>Vigencia: No. de Contrato: Objeto de contrato Contratista Identificación del Contratista</p> <p>En donde se tengan los siguientes roles: el administrador quien podrá hacer seguimiento del flujo de la información y eliminación de información si es necesario, el consultor que únicamente podrá visualizar los archivos producidos, que están en vigencia y los liquidados y el Registrador quien será el encargado de alimentar el sistema y consultarlo.</p> <p>De igual forma poder habilitar el motor de búsqueda con la vigencia, No de contrato y tipo de contrato,</p> <p>Nota. Mantener los mismos requisitos funcionales, clasificación y organización documental, retención y disposición, transferencias documentales, captura e ingresos de documentos, búsqueda y presentación, préstamo de documentos, radicación, distribución, flujo de trabajo, consulta, parametrización, metadatos, controles y seguridad, usuario final reportes.</p>
METADATOS	
258	En el momento de parametrización, el SGDEA debe permitir que se definan varios conjuntos de elementos de metadatos adecuados a las distintas clases de documentos electrónicos de

	archivo.
259	<p>El SGDEA deberá permitir que el administrador defina, en el momento de la parametrización, que elementos de metadatos son obligatorios y cuales son facultativos, así como aquellos que podrán ser objeto de búsqueda.</p> <p>El SGDEA debe admitir, al menos, los siguientes formatos de elementos de metadatos:</p> <ol style="list-style-type: none"> 1. Alfabético. 2. Alfanumérico. 3. Número. 4. Fecha.
260	El SGDEA debe permitir incorporar diferentes esquemas de metadatos.
261	El SGDEA debe permitir la extracción automática de elementos de metadatos de los documentos tipo formulario estandarizado en el momento de su captura.
262	El SGDEA debe permitir que el administrador decida qué elementos de metadatos se pueden introducir y mantener manualmente a través del teclado y cuales se escogerán de una lista desplegable.
263	El SGDEA debe permitir al usuario autorizado parametrizar modificar y aplicar las reglas de los elementos del esquema de metadatos.
264	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 clasificación.
265	<p>El SGDEA debe permitir la validación de los metadatos cuando los usuarios se encargan de su introducción o bien cuando se importen. Dicha valoración deberá emplear, como mínimo los siguientes mecanismos:</p> <ol style="list-style-type: none"> 1. Formato del contenido del elemento. 2. Intervalo de valores. 3. Validación frente a una lista de valores mantenida por el administrador. 4. Referencias al cuadro de clasificación documental válido.
266	El SGDEA debe impedir cualquier modificación de los metadatos generados directamente por otros paquetes de aplicaciones. Ejemplo los datos de la transmisión del correo electrónico.
267	El SGDEA debe presentar en pantalla los metadatos de los documentos capturados.
268	El SGDEA debe impedir la modificación del contenido de ciertos campos de metadatos especificados en el momento de la parametrización
269	El SGDEA debe permitir la asignación previa de palabras clave a las series, subseries, expedientes y/o documentos, basados en bancos terminológicos, tesauros, taxonomías, entre otros.
270	El SGDEA debe permitir que al momento de la captura o en una etapa posterior de procesamiento, se puedan ingresar metadatos adicionales.
271	El SGDEA debe validar y controlar la entrada de los metadatos mínimos obligatorios.
272	El SGDEA permite la extracción automática de metadatos de los documentos al momento de la captura o cargue al sistema.
273	En la ventana de radicación de documentos, el sistema cuenta con una opción adicional de ingresar METADATOS que se ajustan a la necesidad de la entidad y las áreas que lo requieren.
274	El SGDEA debe permitir que se redefinan los conjuntos de metadatos establecidos por el administrador y debe consignar los cambios en la pista de auditoría
CONTROLES Y SEGURIDAD	
275	El SGDEA debe permitir que el administrador restrinja el acceso a los documentos de archivo expedientes a determinados usuarios o grupos de usuarios.
276	El SGDEA debe permitir que el administrador asocie al perfil del usuario ciertos atributos que determinaran las funciones, los campos de metadatos, los documentos de archivo y

	<p>expedientes a lo que el usuario tendrá acceso. Los atributos del perfil servirán para:</p> <ol style="list-style-type: none"> 1. Vetar el acceso al SGDEA cuando no se aplique un mecanismo de autenticación. 2. Restringir el acceso del usuario a ciertos expedientes o documentos de archivo. 3. Restringir el acceso del usuario a ciertas clases del cuadro de clasificación documental. 4. Restringir el acceso del usuario según la habilitación de seguridad de su perfil. 5. Restringir el acceso del usuario a ciertas funciones, como lectura, impresión de documentos y la actualización y la eliminación de determinados campos de metadatos. 6. Denegar el acceso después de una fecha concreta. 7. Asignar al usuario a uno o varios grupos de usuarios.
277	El SGDEA debe ser capaz de establecer grupos de usuarios asociados a un conjunto de expedientes o documentos de archivo.
278	El SGDEA debe permitir que un usuario pertenezca a más de un grupo.
279	Si un usuario lleva a cabo una búsqueda de texto íntegro, el SGDEA nunca debe incluir en los resultados documentos de archivo a los que el usuario no tenga derecho de acceder.
280	Cuando el SGDEA permita que los usuarios intenten acceder a expedientes o documentos de archivo sin la autorización debida, debe quedar constancia de tales intentos en la pista de auditoría y enviar correo al administrador del sistema y administrador de Gestión Documental.
281	<p>El SGDEA debe mantener una pista de auditoría inalterable, capaz de capturar y almacenar de forma automática información sobre:</p> <ol style="list-style-type: none"> 1. Todas las acciones relacionadas con los documentos de archivo electrónicos, los expedientes electrónicos y el cuadro de clasificación. 2. El usuario que inicia o realiza la acción, la fecha y la hora de la acción.
282	Una vez activada la funcionalidad de la pista de auditoría, el SGDEA debe ser capaz de rastrear sin intervención manual de todas las acciones y de almacenar en la pista de auditoría la información sobre ellas.
283	El SGDEA debe mantener la pista de auditoría durante el tiempo necesario, que al menos abarque el ciclo de vida de los documentos de archivo o expedientes electrónicos a los que hace referencia.
284	<p>El SGDEA debe permitir consignar en la pista de auditoría todas las modificaciones que afecten a:</p> <ol style="list-style-type: none"> 1. Grupos de expedientes electrónicos. 2. Expedientes electrónicos individuales. 3. Volúmenes electrónicos. 4. Documentos electrónicos de archivo. 5. Documentos electrónicos. 6. Metadatos relativos a cualquiera de los elementos anteriores.
285	El SGDEA debe permitir consignar en la pista de auditoría todas las modificaciones realizadas en los parámetros administrativos.
286	El SGDEA debe ser capaz de exportar la pista de auditoría de determinados documentos de archivo y expedientes electrónicos y también de grupos de expedientes.
287	El SGDEA debe poder capturar y guardar los intentos de los usuarios de acceder a un documento de archivo o expediente sin tener la debida autorización, y (cuando sea factible) de los intentos de violación de los mecanismos de control de acceso.
	USUARIO FINAL
288	Las consultas asociadas al centro de gestión para consultar pendientes y realizar reasignaciones debe ser responsive.

289	<p>Debe contar con un tablero de control, que muestra al usuario el número de solicitudes que están asignadas, agrupadas por tipo de solicitud, según el plazo establecido se encuentran:</p> <ol style="list-style-type: none"> 1. A tiempo (verde). 2. Próximas al vencimiento (amarillo). 3. Vencida (rojo).
290	El ribbon debe presentar los botones a que tiene acceso según el perfil asignado.
291	Debe presentar en la bandeja de entrada los radicados pendientes de trámite.
292	Garantizar que, si un usuario lleva a cabo una búsqueda de texto íntegro, NUNCA debe incluir en los resultados documentos de archivo a los que el usuario no tenga permisos de acceso.
293	El sistema debe proveer con una agenda propia del sistema que permita al usuario una ayuda gráfica de los radicados pendientes por tramitar
294	Proveer una bandeja de tareas pendientes donde encontrarán los trámites que tengan asignados provenientes de radicados.
295	Para la descarga de los envíos físicos, el sistema debe contar con un buscador por número de planilla, que, al consultar, presenta los radicados incluidos en esta.
296	Cuando se carga el acuse de recibido a un radicado asociado a la planilla, debe actualizar a cada uno de los registros, dejándolo como anexo a cada radicado.
297	El sistema debe permitir excluir los radicados de salida a los cuales no se les debe hacer cargar de acuse de recibido.
298	El sistema debe permitir a usuarios con privilegios reabrir PQRSD, aun cuando ya tenga una respuesta definitiva.
299	Cuando se reabra la PQRSD, debe abrir un formulario tipo texto, donde debe argumentar esta operación, la cual se registra en el histórico del radicado.
300	Cuando se consulta un radicado, debe generar un log en el histórico del éste.
301	El comunicado interno debe permitir la opción de marca como públicos o privados.
302	Los públicos pueden ser consultados por usuarios que tienen el rol o funcionalidad de consulta.
303	Para los radicado de entrada y salida, pueden ser públicos o privados. Estos últimos pueden ser consultados únicamente a través de un rol asociado al perfil del usuario.
304	Los radicado de salida digitales, pueden enviarse de manera física o digital al ciudadano.
REPORTES	
305	El sistema debe contar con un administrador de logs para reportes, notificaciones, inicio de aplicación entre otros.
306	Debe brindar servicios de Consultas paramétricas por rangos y filtros.
307	<p>El sistema debe contar con un módulo en la plataforma para generar reportes de los diferentes tipos de radicados, de manera que permita determinar el estado de estos y de las PQRS:</p> <ol style="list-style-type: none"> 1. Abiertos. 2. Cerrados. 3. Vencidos. 4. Asignados por dependencia. 5. Ejes temáticos. 6. Respondidos oportunamente. 7. Respondidos fuera del plazo máximo. 8. Clasificados según el medio de recepción. 9. Clasificados por Tipo.

308	<p>Los reportes deben ser parametrizables y permitir las siguientes condiciones:</p> <ol style="list-style-type: none"> 1. Permitir su exportación al menos a cuatro formatos diferentes de acuerdo con las necesidades de la entidad (XML, CSV, PDF o XLS). 2. Contar con gráficos y porcentajes de nivel gerencial, técnico y operativo; como son los indicadores de respuestas a PQRSD, cumplimiento de cronograma de transferencias, y cumplimiento de metas. 3. Expedientes por Series, subseries y en general por la estructura de las TRD. 4. Radicados de entrada por: Soporte, sucursal, dependencia, usuario. 5. Radicados de salida por: Soporte, sucursal, dependencia, usuario, enviados físicos, estado de entrega, devoluciones y reenviados.
309	Generar reportes exportables de datos en XML, CSV o XLSX para la presentación de informes a través de aplicaciones de terceros.
310	Debe brindar servicios de Consultas paramétricas por rangos y filtros
311	<p>Debe contar con reportes de expedientes según:</p> <ol style="list-style-type: none"> 1. Estado, abierto o cerrado. 2. Niveles de seguridad. 3. Fase de archivo. 4. Préstamos de expedientes. 5. Niveles de seguridad de los expedientes. 6. Transferencia documental. 7. Eliminación documental de expedientes.
312	El sistema debe presentar un reporte de los PQRSD físicos pendientes por entregar físicamente al usuario responsable de atenderla.
313	Cuando se trate de PQRSD físicos, el sistema debe contar con un reporte que permita seleccionar aquellos radicados que físicamente entrega ventanilla.
314	Este reporte debe contar con un check que le facilite al usuario, seleccionar aquellos PQRS que recibe.
315	El sistema debe proveer en la mayor cantidad posible, la generación de reportes para las distribuciones físicas de documentos, facilitando su control mediante formularios del sistema y evitando la impresión de planillas de entrega.
316	El sistema debe proveer desde el radicado de salida, en hipervínculo que, al presionarlo, abre la prueba de entrega.
317	Los documentos marcados como envío de correspondencia permitirán organizar y marcar los envíos externos de la documentación, generando planillas de entrega en formato CSV y PDF.
318	El sistema debe generar planillas en CSV para cruzar información con el Sistema del Proveedor de correspondencia, permitiendo obtener los números guías de cada radicado, asociado en los datos del mismo, permitiendo por medio del número guía redirigir una URL del proveedor y ver la ruta del documento.
319	En caso de que sea excluido un radicado físico de un expediente y sea incluido en otro, el sistema debe reportar esa novedad.
320	Los radicados de salida deben permitir generar notificaciones a usuarios internos que pueden presentar algún tipo de interés en la generación del mismo, mediante un correo electrónico que adjunte el documento de salida.
321	El sistema debe permitir establecer cuando ha sido entregada exitosamente un radicado de salida, en caso tal permitir su reprogramación.

322	El sistema debe presentar un reporte de los radicados físicos y PQRSD pendientes por entregar físicamente al usuario asignado.
323	Para los radicados, el sistema debe contar con un reporte que presente aquellos que esta pendiente de vinculación de imagen.
324	El sistema debe enviar en puntos críticos notificaciones al correo del usuario que tramita un documento
325	El sistema debe contar con alarmas o monitoreo mediante correo electrónicos que permita controlar los tiempos de los términos fijados. Activables por el usuario.
326	Los metadatos definidos en la Solución adquirida deberán contemplar atributos relacionados con protección y privacidad de la información, permitiendo almacenar si la información es pública clasificadas y sensible entre otros atributos que se definan
327	Garantizar en este componente (Sistema SGDEA) las características de los documentos electrónicos de la entidad (Autenticidad, Integridad, Fiabilidad y Disponibilidad).
328	Establecer niveles de seguridad a los documentos electrónicos contenidos en expedientes garantizando su acceso solamente a los usuarios, roles y perfiles establecidos.
329	Restringir el acceso a la información confidencial para que sólo pueda ser consultada por los perfiles autorizados.
330	Debe incluir el componente PQRSD con la parametrización y tipificación de las diferentes solicitudes, asociadas con los flujos de trabajo automáticos, escalamientos, control tiempos, acuerdos de servicio, eventos, alertas, trazabilidad, responsables; permitiendo generar los reportes de estado en línea y por diferentes criterios.

3.2 ESPECIFICACIONES NO FUNCIONALES

Ítem	Temática	Requerimiento	
1	Modalidad de compra	Compra a perpetuidad sin límite de usuarios, para ser desplegado en la infraestructura de TI de la entidad.	
2	Modalidad de compra	Opciones de licenciamiento aceptadas: <ul style="list-style-type: none"> Open Source (p. ej., licencias AGPL/GPL u otras compatibles) preferida/no excluyente; o Propietaria sin restricciones de uso sobre ningún componente del software comprado. 	
3	General	<ul style="list-style-type: none"> El SGDEA cubrirá gestión de documentos y expedientes electrónicos, desde la captura/recepción hasta la disposición final, con trazabilidad integral y seguridad por diseño. Debe permitir la administración centralizada por parte de los funcionarios 	

ESPECIFICACIONES TÉCNICAS

		<p>de la entidad que le de autonomía en su parametrización.</p> <ul style="list-style-type: none"> Principios: disponibilidad, integridad, confidencialidad, autenticidad, fiabilidad y preservación, interoperabilidad, portabilidad sin bloqueo de proveedor, accesibilidad y usabilidad. Todas las ayudas, herramientas y documentación de la Solución debe operar y entregarse en idioma español para administrador funcional y usuario final. 	
4	Requerimientos de arquitectura e infraestructura (Arquitectura de aplicación web)	<ul style="list-style-type: none"> Aplicación 100% web, accesible vía navegador moderno, responsiva, sin dependencias de plugins obsoletos. Separación por capas (frontend, backend, BD) y APIs. Compatibilidad con navegadores de uso institucional (Chrome/Edge recientes) y accesibilidad WCAG 2.1. Diseño responsivo, es decir, que se adapte correctamente a diferentes dispositivos (computadores, tabletas y teléfonos móviles). El sistema deberá contar con un servicio integrado de Gestión de Contenidos Empresariales (ECM) que soporte de manera nativa la Gestión Documental Electrónica de Archivo (SGDEA), respondiendo a las necesidades de gestión archivística, correspondencia, radicación, conservación, consulta, trazabilidad y disposición final de los documentos de la Unidad, en cumplimiento de los lineamientos del Archivo General de la Nación, el Acuerdo 001 de 2024 y la Política de Gobierno Digital 	
5	Requerimientos de arquitectura e infraestructura (Despliegue e infraestructura)	<ul style="list-style-type: none"> Despliegue contenedorizado (Docker) y orquestado (Kubernetes/Openshift) o máquinas virtuales en la infraestructura de la entidad, garantizando que todos los datos y procesos permanezcan bajo el control y la soberanía de la institución. Base de datos: Debe ser compatible con motores de bases de datos PostgreSQL 	

ESPECIFICACIONES TÉCNICAS

		<p>versión 16 o superior o MariaDB version 11 o superior.</p> <ul style="list-style-type: none"> Almacenamiento: Discos duros, NAS y azure blob storage o equivalentes proporcionados por la entidad. Sistema operativo servidores de aplicaciones: Linux con Kernel: ≥ 5.15, de preferencia Ubuntu 22.04 LTS. El sistema operativo elegido deberá tener soporte LTS vigente de mínimo 36 meses, con repositorios oficiales activos. Si el oferente requiere una distribución distinta de Ubuntu 22.04 LTS, deberá garantizar: <ul style="list-style-type: none"> a) Instalación guiada (manual paso a paso, scripts o Ansible) sobre las máquinas de UAESP; b) No generar costos adicionales para la Entidad en licencias/suscripciones del SO ni en soporte base del SO respecto del escenario Ubuntu 22.04. Librerías: todas las librerías y dependencias del software deben estar actualizadas y no deben tener vulnerabilidades reportadas. 	
6	Requerimientos de arquitectura e infraestructura (Requerimientos de interoperabilidad e integración)	<ul style="list-style-type: none"> Autenticación/SSO: Active Directory/LDAP y Azure AD/Entra ID. APIs REST (JSON), webhooks, conectores para correo (IMAP/SMTP/M365). Integración con sistemas SDQS Bogota te Escucha y VUC (Ventanilla única de la Construcción). Conectores/SDKs para exchange con herramientas ofimáticas (Microsoft 365/Outlook). Importación/Exportación masiva: CSV/JSON/XML; Exportación bulk de expedientes con metadatos y estructura de carpetas. Exportación total (datos, archivos, metadatos, bitácoras y configuraciones) para evitar vendor lock-in. Permitir el desarrollo e integración de funcionalidades, módulos y ajustes a la medida, de acuerdo con las necesidades de la Entidad. 	

ESPECIFICACIONES TÉCNICAS

7	Requerimientos de seguridad y privacidad (Desarrollo seguro y ciclo de vida)	<ul style="list-style-type: none"> El proveedor deberá implementar controles de seguridad durante todo el ciclo de vida de desarrollo (planificación, codificación, pruebas, despliegue y operación), en línea con la Resolución 1519 de 2020 – Anexo 3 y el MSPI y/o normas que las complementen o sustituyan. Adopción de buenas prácticas OWASP (Top 10 vigente). Análisis estático (SAST) y dinámico (DAST) obligatorios en preproducción; análisis de dependencias (SCA) y gestión de vulnerabilidades; reporte de hallazgos críticos/altos corregidos antes de pasar a producción. 	
8	Requerimientos de seguridad y privacidad (Controles técnicos mínimos)	<ul style="list-style-type: none"> Debe soportar SSL y el uso de certificados digitales. Canal seguro: TLS 1.2/1.3 vigente; HSTS (incl. subdominios) y deshabilitar protocolos/cifrados inseguros. Cabeceras de seguridad (mínimo): ContentSecurityPolicy (CSP), XContentTypeOptions: nosniff, XFrameOptions (o frameancestors en CSP), ReferrerPolicy, PermissionsPolicy, CrossOriginResourcePolicy/COOP/COEP cuando aplique. Protecciones OWASP Top 10: validación/normalización de entradas, consultas parametrizadas/ORM (prevención SQLi), salida escapada (XSS), protección CSRF, gestión segura de autenticación/sesiones (rotación de tokens, expiración, cookie Secure y HttpOnly), control de accesos RBAC/ABAC, registro y monitoreo de eventos de seguridad. CAPTCHA o mecanismos antiautomatización para formularios públicos expuestos (radicación, recuperación de contraseña, etc.). CSP para visor de documentos y restricciones de frame ancestors para evitar clickjacking en módulos de consulta pública. Política de contraseñas y MFA para perfiles administrativos; bloqueo progresivo y alertas ante intentos fallidos. 	

ESPECIFICACIONES TÉCNICAS

		<ul style="list-style-type: none"> Privacidad por diseño: clasificación de datos, minimización, mascaramiento en logs, bitácoras y exportaciones. Funciones para anonimización/pseudonimización cuando se requiera. 	
9	Requerimientos de seguridad y privacidad (Evidencias y pruebas de seguridad)	<ul style="list-style-type: none"> Pentest de caja gris en preproducción y posterior a cambios mayores (alcance sobre módulos críticos y APIs). Reporte de conformidad con Anexo 3 Res. 1519 (checklist) y OWASP ASVS (matriz de controles aplicados) y demás requisitos definidos en este numeral. 	
10	Acceso, autenticación e integración con Directorio	<ul style="list-style-type: none"> SSO con AD/Azure AD para las funcionalidades que permiten autenticación, autorización, administración y aprovisionamiento de información de usuarios. Permitir la creación de grupos de usuarios con sus respectivos permisos a los diferentes componentes y elementos de los mismos. Estados de usuario gestionados (activo, suspendido, baja, etc.), con revocación inmediata. Debe permitir al usuario administrador crear los perfiles requeridos de acuerdo con la necesidad de la entidad, sin necesidad de desarrollo adicional. Listas de control de acceso (ACLs). Guardar registros de auditoria que permita analizar actividades de usuario que mínimo se identifique dirección IP desde donde se conecta, usuario que realiza la conexión, fecha y hora, si el intento de conexión es exitoso o fallido, descripción del evento realizado por el usuario. Esto independiente de las acciones que el usuario realice sobre a cada radicado o parte del proceso de gestión documental dentro de la aplicación. Proporcionar un visor o gestión de consulta de estos logs con el fin de realizar el respectivo seguimiento, preferiblemente dentro de la misma aplicación 	
11	Condiciones generales	<ul style="list-style-type: none"> Debe evitar la existencia de puertas traseras o mecanismos de modificación directa de los esquemas de datos, para 	

ESPECIFICACIONES TÉCNICAS

		<p>cualquier tipo de labor, funcionalidad, requerimiento, parametrización y configuración, siendo realizado con una interfaz de usuario sujeta a las políticas de seguridad integral de la Solución.</p> <ul style="list-style-type: none"> • Debe generar logs de auditoría para hacer seguimiento a las operaciones y acciones realizadas por los usuarios, identificando tipo de transacción, tipo de operación realizada en los componentes de la solución, valores iniciales, valores actualizados; dejando así el rastro de estas. • Debe proveer la vista de consulta, al igual que la exportación del log de auditoría. • Tener facilidades como scripts pre-establecidos para realizar operaciones de copia de seguridad y recuperación de Backups. • Restringir el acceso a la información confidencial para que sólo pueda ser consultada por los perfiles autorizados. 	
12	Garantías y Soporte (Garantías del Sistema)	<p>Garantía de Funcionamiento</p> <ul style="list-style-type: none"> • Cobertura: El proveedor debe ofrecer una garantía sobre el software e implementación superior o igual a 24 meses, que cubra: <ul style="list-style-type: none"> ○ Fallos de funcionamiento derivados de errores en el código o diseño. ○ Incompatibilidades con la infraestructura de la entidad (siempre que se cumplan los requisitos técnicos acordados). ○ Actualizaciones y parches de seguridad durante el período de garantía. • Exclusiones: No cubre fallos causados por: <ul style="list-style-type: none"> ○ Modificaciones no autorizadas al software. ○ Uso inadecuado o fuera de los parámetros definidos en el contrato. 	

ESPECIFICACIONES TÉCNICAS

		<ul style="list-style-type: none"> Desastres naturales o eventos de fuerza mayor no atribuibles al proveedor. <p>Garantía de Cumplimiento Normativo</p> <ul style="list-style-type: none"> En caso de cambios normativos durante la vigencia del contrato que afecten los requisitos funcionales de la aplicación, el proveedor debe actualizar el sistema sin costo adicional para la entidad, siempre que los cambios sean razonables y aplicables a todos sus clientes. 	
13	Garantías y Soporte (Niveles de Servicio (SLA))	<p>Disponibilidad</p> <ul style="list-style-type: none"> SLO de disponibilidad del servicio $\geq 99\%$ mensual (aplicación) (este tiempo no contempla indisponibilidades a causa de la infraestructura de la entidad) <p>Tiempos de Respuesta y Resolución</p> <p>Los tiempos de resolución aplica para incidencias atribuibles al sistema o consultas sobre el sistema. Los tiempos de respuesta de parte del proveedor aplican independientemente de si la incidencia es atribuible o no al sistema.</p> <ul style="list-style-type: none"> Incidencias críticas (ej. caída total del sistema): <ul style="list-style-type: none"> Tiempo de respuesta: Máximo 1 hora (reconocimiento del incidente). Tiempo de resolución: Máximo 2 horas (restauración del servicio). Incidencias mayores (ej. fallos en módulos específicos): <ul style="list-style-type: none"> Tiempo de respuesta: Máximo 2 horas. Tiempo de resolución: Máximo 8 horas. Incidencias menores (ej. consultas o ajustes menores): 	

ESPECIFICACIONES TÉCNICAS

		<ul style="list-style-type: none"> ○ Tiempo de respuesta: Máximo 8 horas. ○ Tiempo de resolución: Máximo 48. <p>Rendimiento</p> <ul style="list-style-type: none"> • Tiempos de carga: En operaciones comunes (búsqueda simple de radicados, abrir expediente, listar bandejas, búsqueda simple, abrir visor de documento existente, guardar metadatos) debe ser inferior a los 2.5 segundos en condiciones normales de operación. • Capacidad de usuarios concurrentes: El sistema debe soportar al menos 100 usuarios concurrentes sin degradación del rendimiento, con capacidad para expansión. 	
14	Garantías y Soporte (Soporte Técnico)	<p>Modalidades de Soporte</p> <ul style="list-style-type: none"> • Soporte Nivel 1 (Básico): <ul style="list-style-type: none"> ○ Horario: 8:00 a.m. a 5:00 p.m. (días hábiles). ○ Canales (mínimo): Correo electrónico, chat en línea, teléfono. ○ Alcance: Resolución de consultas básicas, guía de uso, y escalamiento a niveles superiores. • Soporte Nivel 2 (Avanzado): <ul style="list-style-type: none"> ○ Horario: 24x7 (para incidencias críticas y mayores). ○ Canales (mínimo): Correo electrónico, chat en línea, teléfono. ○ Alcance: Diagnóstico y resolución de fallos técnicos, configuraciones avanzadas. <p>Equipo de Soporte</p> <ul style="list-style-type: none"> • Ubicación: El proveedor debe contar con un equipo de soporte local en Colombia, 	

ESPECIFICACIONES TÉCNICAS

		<p>con capacidad para brindar asistencia presencial en Bogotá si es requerido.</p> <ul style="list-style-type: none"> Idioma: Todo el soporte debe prestarse en español, con documentación y comunicaciones en el mismo idioma. 	
15	Garantías y Soporte (Métricas y Reportes de Desempeño)	<p>Métricas y Reportes de Desempeño</p> <ul style="list-style-type: none"> Indicadores Clave (KPIs) <ul style="list-style-type: none"> Tiempo promedio de resolución de incidencias (por nivel). Número de incidencias críticas/mayores/menores por mes. Cumplimiento de SLAs (porcentaje de incidencias resueltas en plazo). Reportes Periódicos <ul style="list-style-type: none"> Frecuencia: Mensual (para incidencias y rendimiento) y trimestral (para revisión de SLAs y mejoras). Tipo de contenido: <ul style="list-style-type: none"> Resumen de incidencias y tiempos de resolución. Estado del sistema. Recomendaciones para optimización. Avance en la implementación de mejoras o nuevas funcionalidades. 	
	Mantenimiento y Actualizaciones (Mantenimiento preventivo)	<ul style="list-style-type: none"> El proveedor debe garantizar actualizaciones del software, incluyendo nuevas funcionalidades y parches de seguridad durante la vigencia del contrato. El proveedor debe notificar con 48 horas de anticipación cualquier mantenimiento que pueda afectar la disponibilidad del sistema. Actualizaciones mayores: Las actualizaciones de versión del SGDEA deben planificarse con al menos 30 días de anticipación, incluyendo: <ul style="list-style-type: none"> Pruebas en entorno de staging. Plan de rollback en caso de fallos. 	<ul style="list-style-type: none">

ESPECIFICACIONES TÉCNICAS

16	Mantenimiento y Actualizaciones (Mantenimiento correctivo)	Resolución de fallos de cualquier componente del software de acuerdo con los tiempos definidos en los niveles de servicio, sin costo adicional.	
17	Mantenimiento y Actualizaciones (Evolución tecnológica)	El proveedor debe presentar un plan de evolución del SGDEA, incluyendo migración a nuevas versiones y adopción de tecnologías emergentes (ej. inteligencia artificial para clasificación automática de documentos).	
18	Migración desde el sistema actual (Alcance)	<ul style="list-style-type: none"> Incluye entre otros: documentos electrónicos, expedientes (abiertos y cerrados), metadatos (mínimos, condicionales y de preservación), radicados/folios, relaciones (vínculos entre docs/expedientes), historial de auditoría (eventos críticos), sellos de tiempo asociados, estados de trámite, transferencias y disposiciones registradas, etc. Migración consultiva/histórica y para cerrar radicados/transacciones/archivos pendientes desde el nuevo SGDEA. 	
19	Migración desde el sistema actual (Preservación de autenticidad y cadena de custodia)	<ul style="list-style-type: none"> Registro de cadena de custodia por lote (origen → extracción → transporte → almacenamiento temporal → carga); evidencias firmadas por responsable. Inmutabilidad de lotes entregados (WORM/objetolock) hasta cierre de auditoría de migración. 	
20	Migración desde el sistema actual (Calidad e integridad - pruebas y métricas)	<ul style="list-style-type: none"> Conteo 100%: documentos, expedientes y metadatos vs. origen. Huella: coincidencia SHA256 origen/destino $\geq 99,99\%$; discrepancias justificadas. Muestreo funcional estratificado ($\geq 95\%$ confianza, $\pm 5\%$ error) de expedientes completos: visualización, metadatos, relaciones, firmas, auditoría. KPIs: tasa de éxito de carga $\geq 99,5\%$ por lote; reintentos automáticos y bitácora de errores. 	
21	Migración desde el sistema actual (Seguridad y privacidad)	<ul style="list-style-type: none"> Tratamiento de datos conforme Ley 1581/2012 y políticas de la Entidad. Cifrado en tránsito (TLS 1.2/1.3) y en reposo (AES256); uso de KMS/HSM institucional si está disponible. Registro/auditoría inmutable de eventos de migración. 	

ESPECIFICACIONES TÉCNICAS

22	Migración desde el sistema actual (Entregables de migración)	<ul style="list-style-type: none"> • Inventario y diccionario de datos (origen). • Matriz de mapeo (origen → destino) + reglas de transformación. • Plan de pruebas (funcional, rendimiento, preservación, seguridad) y evidencias. • Manifiestos de lotes con hashes y actas de cadena de custodia. • Informe de reconciliación (conteo, huellas, discrepancias). • Acta de corte y salida a producción; Plan de reversa. 	
23	Migración desde el sistema actual (Criterios de aceptación (pruebas de aceptación de usuarios de la migración))	<ul style="list-style-type: none"> • Consulta exitosa en el nuevo SGDEA de expedientes históricos con documentos, radicados, registro de históricos de radicados, metadatos, índice electrónico y firmas visibles/validables. • Reconciliación 100% de conteos y $\geq 99,99\%$ de huellas coincidentes. • Posibilidad de cerrar transacciones/temas pendientes en el nuevo SGDEA (flujos operativos habilitados). • Evidencias de cadena de custodia. 	
24	Entregables/hitos mínimos del proyecto.	<ul style="list-style-type: none"> • Plan de Proyecto detallado. • Diseño y arquitectura aprobados. • Pruebas: plan, casos y evidencias (funcionales, rendimiento, seguridad, accesibilidad, interoperabilidad). • Ambiente montado y pruebas técnicas superadas. • Parametrización de funcionalidades aprobada. • Integraciones críticas operativas. • Migración de información piloto y validación. • Cierre de pruebas de aceptación del usuario y plan de paso a producción. • Capacitación • Puesta en producción y estabilización. • Entrega documental y cierre. 	
25	Pruebas y aceptación (pruebas)	<ul style="list-style-type: none"> • Pruebas de rendimiento: Simular cargas de hasta 200 usuarios concurrentes para validar tiempos de respuesta y estabilidad. • Pruebas de seguridad: Realizar pruebas de penetración y análisis de vulnerabilidades antes de la puesta en producción. • Pruebas de integración: Validar la interoperabilidad con VUC,SDQS, 	

ESPECIFICACIONES TÉCNICAS

		asegurando que los flujos de datos sean correctos y seguros.	
26	Pruebas y aceptación	<ul style="list-style-type: none"> Disponibilidad: 99% de uptime durante 30 días consecutivos. (no se tienen en cuenta indisponibilidades a causa de aspectos ajenos al propio software). Rendimiento: Tiempos de respuesta menores a 2.5 segundos para operaciones comunes (búsqueda simple de radicados, abrir expediente, listar bandejas, búsqueda simple, abrir visor de documento existente, guardar metadatos) en condiciones normales de operación. Seguridad: Sin incidentes ni vulnerabilidades críticas detectadas en pruebas de seguridad. 	
27	Capacitación y transferencia de conocimiento (Plan de Capacitación)	<ul style="list-style-type: none"> Duración: Mínimo 15 horas (presenciales o virtuales). Públicos objetivo: <ul style="list-style-type: none"> Administradores técnicos. Administrador funcional. Líder de proceso. Operador del proceso. Usuario estándar. 	
28	Capacitación y transferencia de conocimiento (Documentación Técnica)	<p>Documentación Técnica</p> <p>El proveedor debe entregar la siguiente documentación, en español y actualizada:</p> <ul style="list-style-type: none"> Manual de instalación y configuración (para el equipo de TI). Manual de administración (para gestores del SGDEA). Manual de usuario (para colaboradores y ciudadanos). Diagramas de arquitectura (física y lógica). Guía de integración con VUC y SDQS. Registro de pruebas y certificaciones de cumplimiento normativo. Diccionario de base de datos. 	
29	Licenciamiento y propiedad (Licencias de Software)	<ul style="list-style-type: none"> Tipo de licencia: Licencia de uso perpetuo con los siguientes derechos: <ul style="list-style-type: none"> Uso exclusivo: La entidad tendrá derecho a utilizar el software para fines 	

ESPECIFICACIONES TÉCNICAS

		<p>institucionales sin ninguna restricción.</p> <ul style="list-style-type: none"> Actualizaciones: Las actualizaciones menores (parches de seguridad) deben incluirse sin costo adicional durante la vigencia del contrato. Código fuente: <ul style="list-style-type: none"> Para sistemas de código libre, la entidad tendrá derecho a utilizar el código fuente de acuerdo con las condiciones establecidas por el proveedor. Los desarrollos a la medida que se realicen durante el proceso de migración, instalación y puesta en funcionamiento de la herramienta, así como actualizaciones posteriores, serán de propiedad, explotación y uso de la Entidad. 	
30	Licenciamiento y propiedad (Propiedad de los datos)	<ul style="list-style-type: none"> Titularidad: Todos los documentos y metadatos almacenados en el SGDEA son propiedad exclusiva de la entidad. Confidencialidad: El proveedor no podrá utilizar, compartir o comercializar los datos de la entidad sin autorización expresa, salvo para cumplir con obligaciones legales (ej. requerimientos judiciales). Portabilidad: La entidad tendrá derecho a exportar sus datos en formatos abiertos y estandarizados (ej. XML, JSON, SQL, CSV, PDF/A) en cualquier momento, sin restricciones ni costos adicionales. 	
31	Otros	<ul style="list-style-type: none"> El sistema que atiende este componente debe ser parametrizable en términos de las tablas maestras y proveer mecanismos de usuario final, como interfaces y accesos, para su configuración 	
32	Otros	<ul style="list-style-type: none"> debe proporcionar en todo momento al usuario final y al administrador funciones de uso fácil e intuitivo. 	
33	Otros	<ul style="list-style-type: none"> El proveedor de realizar todas las actividades relacionadas con la instalación, configuración y alistamiento de la plataforma (asistencia técnica suficiente a la entidad en las actividades 	

ESPECIFICACIONES TÉCNICAS

		relacionadas con el alistamiento de hardware, software y procesos)	
34	Otros	<ul style="list-style-type: none"> El proveedor de realizar todas las actividades necesarias para la implementación y puesta en operación de la solución ofrecida. 	
35	Otros	<ul style="list-style-type: none"> Debe contar con un equipo funcional para acompañar a la entidad durante la adopción del nuevo sistema 	
36	Otros	<ul style="list-style-type: none"> El sistema debe utilizar la infraestructura de la Entidad y debe adoptar la imagen gráfica de la organización (logos, colores, fuentes, etc). 	
37	Otros	<ul style="list-style-type: none"> Instalar y configurar la infraestructura tecnológica necesaria y los elementos necesarios para su funcionamiento en la sede principal de la entidad, asegurando conectividad desde cualquier punto de red dentro de la entidad. 	
38	Otros	<ul style="list-style-type: none"> El contratista deberá garantizar que el desarrollo, implementación y operación del Sistema de Gestión Documental Electrónico de Archivo (SGDEA) cumpla con los lineamientos de la Estrategia de Gobierno Digital del Gobierno Nacional, conforme a lo dispuesto en la Guía No. 6 – Sistema de Gestión de Documentos Electrónicos, asegurando la observancia de los principios de seguridad, trazabilidad, autenticidad, disponibilidad, interoperabilidad y preservación a largo plazo de la información institucional. 	

3.3 OTRAS CONSIDERACIONES

Ítem	Característica	Descripción
1	Características ECM	<p>El Sistema de Gestión Documental Electrónico de Archivo (SGDEA) deberá incorporar un componente ECM (Enterprise Content Management) robusto, que permita la administración integral del ciclo de vida de los documentos electrónicos de la UAESP y dos interfaces para la Gestión del ECM y sus componentes:</p> <ul style="list-style-type: none"> Interfaz de comandos Interfaz gráfica de usuario

ESPECIFICACIONES TÉCNICAS

2	Planeación	El SGDEA incluyen el diagnóstico inicial, donde se evalúa la situación actual de la gestión documental, la planificación estratégica, que define el alcance, metas y recursos necesarios, y el análisis de requisitos, que detalla las necesidades tecnológicas y funcionales del sistema.
3	Análisis	Realizar el diagnóstico de la situación actual, evaluar los sistemas existentes con los que cuenta la entidad, definir el modelo de parametrización del sistema en el Cuadro de Clasificación Documental, las Tablas de Retención Documental, los perfiles de acceso, un modelo de metadatos, bancos terminológicos, el control de formatos de preservación, las reglas de captura de información, reportes e informes teniendo en cuenta lo contemplado en el Decreto 2609 de 2012, en el Acuerdo 001 del 29 de Febrero de 2024 del AGN y en los lineamientos internacionales de Modelo de Requisitos para la Gestión de Documentos Electrónicos de Archivo MOREQ. Evaluar las capacidades de la plataforma tecnológica (hardware y software) existente para la implementación de la solución propuesta.
4	Diseño	De acuerdo con la información recolectada, el proveedor debe diseñar la mejor solución para la implementación en su plataforma.
5	Instalación y Configuración	El proveedor de realizar todas las actividades relacionadas con la instalación, configuración y alistamiento de la plataforma (asistencia técnica suficiente a la entidad en las actividades relacionadas con el alistamiento de hardware, software y procesos)
6	Modelaje y Parametrización	De acuerdo con los procesos definidos y los flujos establecidos, se deben modelar los diferentes procedimientos, junto con su parametrización de acuerdo con la normatividad y las necesidades de la entidad para la gestión de documentos.
7	Pruebas	Se deben realizar las diferentes pruebas y validaciones de la solución definida.
8	Implantación	El proveedor de realizar todas las actividades necesarias para la implementación y puesta en operación de la solución ofrecida.
9	Servicio Técnico	Debe contar con un equipo de soporte técnico y funcional para acompañar a la entidad durante la adopción del nuevo sistema.

ESPECIFICACIONES TÉCNICAS

10	Acompañamiento	Debe contar con un equipo funcional para acompañar a la entidad durante la adopción del nuevo sistema.
11	Personalización	El sistema debe utilizar la infraestructura de la Entidad y debe adoptar la imagen gráfica de la organización (logos, colores, fuentes, etc).
12	Administración	La administración del Sistema de Gestión Documental, Electrónica y de Archivo (SGDEA) depende directamente de la alta dirección, el Comité Institucional de Gestión y Desempeño, la Oficina de tecnologías de la Información y las Comunicaciones, la Subdirección Administrativa líder del proceso de Gestión Documental y los responsables de archivo de gestión en cada área.
13	Informes	El contratista deberá presentar los informes requeridos por la entidad, y un informe final de cumplimiento
14	Otro	Realizar todas las pruebas de funcionalidad necesarias para garantizar el óptimo estado y puesta en marcha de la solución. La configuración debe ser efectuada por personal certificado en la solución ofertada y garantizada por el fabricante.

Firma:



Nombre: DOLLY ARIAS CASAS

Cargo: Subdirectora Administrativa y Financiera.

Dependencia Solicitante: Subdirección Administrativa y Financiera.

Elaboró: Fernando Martin Romero Montilla- Profesional Universitario - SAF. 
William Alexis Villalobos Ballesteros - Técnico Operativo - SAL

Revisó: Jorge Alexis Rodríguez Meza - Jefe Oficina TIC 
José Dagoberto Cotes Guzmán -Contratista - SAF
Alexander López Palacios - Contratista - SAF