INVITACIÓN A COTIZAR No. 045 DE 2021

Objeto: Fiduprevisora S.A. requiere recibir cotización para realizar la implementación de un sistema de gestión electrónica de documentos de archivo – SGDEA que permita la centralización y control de la toda información física o electrónica de los diferentes procesos de negocios de la Entidad, garantizando su recuperación, conservación, disposición y preservación de la información contenida en los documentos de archivo (físicos/híbridos/electrónicos) en el ciclo vital del documento.

Apertura de la Invitación: 10 de noviembre de 2021.

Fecha límite para presentar observaciones: 16 de noviembre de 2021 hasta las 17:00 horas.

Respuesta a Observaciones: 19 de noviembre de 2021.

Recepción de Cotizaciones: 24 de noviembre de 2021 hasta las 17:00 horas a través del correo electrónico intdemercados@fiduprevisora.com.co y/o plataforma SECOP II.

Área Responsable: Gerencia de Gestión Documental.

Contacto: intdemercados@fiduprevisora.com.co y/o plataforma SECOP II.

1. INFORMACIÓN GENERAL

FIDUPREVISORA S.A. aclara que la presente invitación a cotizar en ningún caso podrá considerarse oferta para celebrar contrato; por lo tanto, no podrá deducirse relación contractual alguna.

Así las cosas, se precisa que el fin de esta solicitud es el de analizar las condiciones del mercado correspondiente, la viabilidad de la contratación mediante la medición de variables como la oportunidad, la calidad, el costo, etc. Adicionalmente, se realizarán las gestiones pertinentes si alguna de las cotizaciones allegadas cumple con las expectativas de la Fiduciaria, la cual debe satisfacer las necesidades de acuerdo con los requerimientos descritos en el documento respectivo o si se requiere, se reestructura la solicitud de acuerdo con el presupuesto definido o en el evento en el cual las entidades consultadas no cumplieren con los requisitos para la prestación integral de los servicios solicitados.

1.1. Régimen Jurídico

La presente solicitud de cotización se realiza conforme con lo establecido en el Artículo 15 de Ley 1150 de 2007 la cual establece lo siguiente: “DEL RÉGIMEN CONTRACTUAL DE LAS ENTIDADES FINANCIERAS ESTATALES. El parágrafo 1o del artículo 32 de la Ley 80 de 1993, quedará así: “Artículo 32. (...) Parágrafo 1°. Los contratos que celebren los Establecimientos de Crédito, las compañías de seguros y las demás entidades financieras de carácter estatal, no estarán sujetos a las disposiciones del Estatuto General de Contratación de la Administración Pública y se regirán por las disposiciones legales y reglamentarias aplicables a dichas actividades.
En todo caso, su actividad contractual se someterá a lo dispuesto en el artículo 13 de la presente ley”, especialmente a los principios de la función administrativa y de la gestión fiscal de que tratan los artículos 209 y 267 de la Constitución Política.

Sin perjuicio de lo anterior, la presente invitación está sujeta a las normas del derecho privado y al Manual de Contratación Bienes y Servicios de Fiduciaria La Previsora S.A.

1.2. Confidencialidad de la Información

Los interesados se obligan con Fiduprevisora S.A., a manejar y utilizar de manera confidencial cualquier información que le sea entregada o a la que tenga acceso con ocasión de la presente invitación, garantizando por todos los medios a su alcance, que los empleados a su servicio y demás personas autorizadas respetarán la obligación de guardar secreto y confidencialidad sobre cualquier información recibida u obtenida.

1.3. Protección de datos personales

Los interesados en desarrollo de las actividades previas, de ejecución, terminación y conexas a esta solicitud de cotización; reconocen y autorizan que podrán realizarse tratamiento de datos personales en los términos de Ley 1581 de 2012, sus decretos reglamentarios, y demás normas concordantes que la adicionen, aclaren o modifiquen, por las cuales se establecen disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos; y además, bajo la completa observancia de lo preceptuado en la Política de Protección de Datos Personales, manuales y procedimientos internos establecidos por FIDUPREVISORA S.A.

Así mismo, los proveedores interesados deberán manifestar en su cotización, que, para efectos de trámites relativos a consultas o reclamos relacionados con datos personales, tienen habilitados los siguientes medios de contacto: _____

Fiduprevisora S.A., informa que para el mismo efecto tiene habilitados los siguientes canales de atención: página WEB https://www.fiduprevisora.com.co/solicitudes-quejas-y-reclamos/; Teléfono: (1) 756 6633 y dirección física: calle 72 # 10-03, Bogotá, Colombia.

1.4. Criterios Ambientales

El proveedor deberá cumplir con la normatividad ambiental vigente que le aplique y aportar la documentación pertinente que solicite la Fiduciaria; además, deberá ceñirse a las políticas y lineamientos del Sistema de Gestión Ambiental de la Entidad, cuando sea aplicable al servicio a cotizar, el cual podrá ser consultado a través de la página web www.fiduprevisora.com.co, en el link que se relaciona a continuación:

https://www.fiduprevisora.com.co/wp-content/uploads/2019/12/Protocolo-de-buenas-practicas-1.pdf

1.5. Matriz Riesgos

N°	FUENTE	ETAPA	TIPO	DESCRIPCION	CONSECUENCIA DE LA OCURRENCIA DEL EVENTO	PROBABILIDAD	IMPACTO	VALORACION DEL RIESGO	CATEGORIA	A QUIEN SE LE ASIGNA
1	Interna	Planeación	Operacional	No contar con el presupuesto para la adquisición del bien y/o servicio	-No adquisición del bien y/o servicio -Demoras en el inició de la etapa de selección	3	3	6	Alto	Entidad
2	Interna	Planeación	Operacional	Errores en los pliegos de condiciones y/o en la invitación a cotizar	-Demoras en la adjudicación del contrato -Adquirir productos o servicios que no satisfacen las necesidades del área usuaria -Re procesos	3	2	5	Medio	Entidad
3	Externo	Ejecución	Operacional	Incumplimiento en las especificaciones técnicas contratadas	Afectación en la calidad del producto y/o servicio	4	4	8	Extremo	Contratista
4	Externo	Ejecución	Operacional	No cumplimiento en la entrega de los bienes y/o servicios contratados	Incumplimiento del contrato	3	3	6	Alto	Contratista

2. INFORMACIÓN PARA LA COTIZACIÓN.

2.1. ALCANCE

Se busca realizar la automatización e integración de los procesos de la administración de la información, para uso y aprovechamiento de las nuevas tecnologías (TIC) para mejorar la provisión de servicios digitales, el desarrollo de procesos internos eficientes, la toma de decisiones basada en datos, la interoperabilidad, el impulso y el desarrollo de una entidad inteligente, lograda a partir de la consolidación de competitividad, proactividad e innovación que generan un entorno de confianza digital para el cliente interno como para el cliente externo.

El proyecto está basado en cinco (5) ejes transversales:

- **a.** Administración de las comunicaciones oficiales en las entidades públicas – Ley 594 de 2000, Ley 1712 de 2014 y Acuerdo 060 de 2001 (Gerencia de Gestión Documental)).
- **b.** Arquitectura tecnológica (Gerencia de Tecnología e Información).
- **c.** Privacidad de la Información– Ley 1581 de 2012 - Decretos Reglamentarios (Gerencia de Riesgos).

d. Seguridad de la Información y Ciberseguridad (Gerencia de Riesgos).
e. Servicios digitales - Gobierno Digital – Min Tic (Todas las áreas).

2.2. CONDICIONES DEL SERVICIO REQUERIDO

2.2.1. Módulo de Ventanilla Única Virtual / Física:

2.2.1.1. Diseño

a. Diseño Tablas de Retención Documental: Contiene el ciclo de vida de la información, parametriza el gestor documental.
b. Diseño de la ventanilla única: Documentación física
c. Diseño de la ventanilla digital: Documentación electrónica, Seguridad y privacidad de la información.

2.2.1.2. Requerimientos funcionales:

a. Tablas de Retención Documental:

I. El SGDEA debe garantizar que los documentos electrónicos de archivo que se capturen se asocien a una TRD configurada en el sistema.
II. El SGDEA debe garantizar que los documentos producidos y asociados a una TRD, mantendrán los criterios de tiempos y de disposición final de la versión correspondiente.
III. El SGDEA debe permitir la creación, importación, parametrización, automatización, administración y versionamiento de las Tablas de Retención Documental – TRD, a partir de plantillas predefinidas, asistentes de configuración, cargue de archivos planos o a través de la incorporación de otros mecanismos que faciliten la administración y la gestión de la TRD.
IV. EL SGDEA debe permitir la importación y exportación total o parcial de la Tabla de Retención Documental, en un formato abierto y editable, teniendo en cuenta:

Para la importación:

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

Para la Exportación:

VII. Permitir la exportación de metadatos asociados, incluyendo pistas de auditoría.
VIII. Los procesos de importación y exportación deben generar reportes y estas acciones deben quedar registradas en las pistas de auditoria.
IX. El SGDEA debe permitir que el CCD y las TRD sean controladas únicamente por un rol administrador y que pueda agregar, modificar y reorganizar la estructura

de acuerdo con las actualizaciones que se realicen a estos instrumentos archivísticos.

X. El SGDEA debe permitir que las Tablas de Retención Documental tengan asociados los siguientes campos de manera opcional:

- **i.** Una descripción y/o justificación.
- **ii.** Versión de la TRD.
- **iii.** Fecha de actualización de la TRD en el sistema.
- **iv.** Identificador único cuando se crea.

XI. El SGDEA debe permitir que los documentos que componen el expediente, hereden los tiempos de conservación establecidos en la TRD.

XII. El SGEDEA debe permitir la transferencia de la estructura la TRD mediante un archivo XML.

XIII. Toda la información que ingresa o se produce debe ser debidamente clasificada de acuerdo a la TRD, con un sistema que controle y sea dinámico para manejar actualizaciones.

b. Radicación, distribución, Asignación y trámite:

I. Todas las comunicaciones de entrada a la Fiduciaria deben generar un radicado de entrada y cada documento debe estar clasificado dentro de la tabla de retención documental de la entidad.

II. El SGDEA debe generar un código único de radicado para cada comunicación ingresada al sistema (Recibida, Enviada e Interna), de forma centralizada y con la estructura definida.

III. Cada código debe contener un componente de secuencia numérica que el SGDEA debe reiniciar automáticamente cada 1ro. de enero (Acuerdo 060 de 2001 – AGN).

IV. El SGDEA no debe imponer límite para la cantidad de radicados (Recibida, Enviada e Interna) soportados por el sistema, por lo que se debe configurar una longitud de la secuencia de radicados, de acuerdo con las necesidades y volúmenes.

V. Los metadatos para radicación de un documento de (Recibida, Enviada e Interna) deben responder a las especificaciones de información que defina y la caracterización de uso que se haya establecido por el administrador del sistema.

VI. EL SGDEA debe permitir la creación, gestión y configuración de niveles de clasificación de información a que haya lugar (Etiquetas Clasificada, reservada, confidencial, de acuerdo a la normatividad existente) y permitir acceso a esta dependiendo el rol de usuario.

VII. El SGDEA debe disponer de una función de integración con aplicaciones externas, para radicar comunicaciones oficiales enviadas por canales distintos al sistema (páginas web, correos electrónicos u otros sistemas de información de la entidad etc.).

VIII. El SGDEA debe tener la capacidad de generar masivamente radicados de comunicaciones (Recibidas, Enviadas e Internas) de acuerdo con la necesidad para atender volúmenes de radicación.

IX. El SGDEA debe generar los consecutivos de correspondencia de forma automática, periodizada y ubicado en la posición del Cuadro de Clasificación que defina conforme la normatividad nacional.

X. La Ventanilla Virtual/física del SGDEA debe manejar formularios validados para garantizar una integridad básica en la radicación remota de comunicaciones oficiales.

XI. Toda radicación realizada a través de la Ventanilla Virtual/física debe informar al usuario radicador, el código oficial asignado a la comunicación ingresada al sistema.

XII. En el proceso de radicación debe poderse digitalizar (documento físico) y capturar información de manera automática de tal forma que permita distribuir la información en el flujo.

XIII. La Ventanilla Virtual/física debe disponer de mínimo dos criterios de búsqueda, para seguimiento a comunicaciones radicadas de forma remota: Código único de radicado - Metadato de uso personal del radicador.

XIV. El despliegue de respuesta de la Ventanilla Virtual del SGDEA, debe informar al usuario el estado en que se encuentra la comunicación.

XV. Cuando la radicación es de un documento electrónico, el código se debe poder reflejar como un metadato del SGDEA.

XVI. El SGDEA debe permitir la configuración de las cuentas de correo electrónico que serán asociados oficialmente a la Ventanilla Única de Comunicaciones.

XVII. Cuando se radique un correo electrónico, el SGDEA debe capturarlo en el formato nativo (EML o MSG) en que se genera la comunicación.

XVIII. La radicación del correo electrónico(web) o físico debe, a través del SGDEA, tener las siguientes funciones:

- **i.** Generar un número en la secuencia de radicación
- **ii.** Asegurar la captura de los datos de transmisión, como metadatos de la Radicación.
- **iii.** Crear el mensaje original de correo, como Anexo Principal del radicado.
- **iv.** Configurar respuesta de los adjuntos del correo, como Anexos Secundarios del mismo radicado con formato original.
- **v.** Debe permitir visualizar la guía y # de guía de la gestión de entrega de un radicado.
- **vi.** Debe permitir anular radicados dejando la traza del proceso y usuario que anuló. No debe permitir eliminar radicados.
- **vii.** Debe permitir reasignar, devolver, archivar o tramitar la respuesta física o electrónica de los radicados y así dejar trazabilidad de estos cambios y log de auditoria.

XIX. El SGDEA debe permitir crear documentos basados en plantillas prestablecidas y formularios.

XX. El SGDEA debe proporcionar una herramienta de edición / diseño de plantillas que permita administrar la radicación de un documento de (Recibida, Enviada e Interna) y crear plantillas de acuerdo a las necesidades de las áreas de la entidad.

XXI. Debe permitir manejar los tiempos de trámite de todos los radicados por tipo de solicitud, que se asignen por balance de carga cuando se requiera, que genere notificaciones y alertas de vencimiento a la respuesta. Igualmente, que se generen reportes exportables de solicitudes o radicados atendidos a tiempo, próximos a vencer y vencidos.

XXII. Una vez radicado y el documento, éste se debe distribuir para trámite de acuerdo a una matriz definida y parametrizable en el sistema (Estado, días de retención, recibida, enviada, términos para detener o activar, finalizar términos, clasificación, tipo documental, flujo al que pertenece, dependencia asociadas con el flujo o trámite, criterios de seguridad y permisos), ésta asignación debe ser automática y debe llegar a un centralizador por trámite o área para que este asigne al responsable de gestionar.

XXIII. El árbol de tipificación correspondiente a las PQRSD debe estar disponible en el formulario de la página web, para clasificar la comunicación según corresponda.

XXIV. Debe permitir la parametrización de los formularios web, por parte del área encargada de la entidad cuando se requiera de acuerdo a las necesidades

XXV. Debe permitir definir la Interoperabilidad del sistema de la entidad cuando se requiera.

XXVI. Captura: Servicios nativos o integración con terceros para: reconocimiento de caracteres ópticos (OCR) y reconocimiento inteligente de caracteres (ICR), reconocimiento de formularios / formatos, reconocimiento de código de barras y QR, así mejorar los procesos de búsqueda para radicados (Recibida, Enviada e Interna).

XXVII. El SGDEA debe registrar una estampa de tiempo (fecha y hora) asociada a cada número de radicado cuando se requiera (Recibida, Enviada e Interna).

XXVIII. Firma Digital/Electrónica: Servicios nativos y/o integración con terceros para firma digital/electrónica:

- **i.** Se debe garantizar que la firma implementada sea única, no falsificable, verificable, no repudio (innegable) y viable (que sea fácil de generar por el firmante).
- **ii.** Que la solución esté disponible y sea parametrizable para implementar en cualquier proceso futuro o documento nuevo que se genere.

XXIX. El SGDEA debe permitir múltiples firmas electrónicas o digitales en los documentos electrónicos.

XXX. El SGDEA debe permitir parametrizar firmas individuales, múltiples firmantes, firmas masivas de documentos y firmas por lotes de documentos.

XXXI. El SGD debe permitir la disposición de formularios de radicación de comunicaciones oficiales en las páginas web de la entidad, asegurando su asignación de consecutivo y debe permitir realizar seguimiento del estado de la misma a través de un módulo de consultas; estas funcionalidades se pondrán a

disposición de los usuarios en las páginas web de la entidad y el formulario deberá permitir realizar cambios o añadir según la necesidad de la entidad.

XXXII. Debe permitir parametrizar los ANS dentro del gestor documental, por servicio o por etapa, generar alertas por incumplimiento y reportes por rangos de fechas.

c. Expediente Electrónico:

I. Debe permitir consultar, controlar y generar reportes de inventarios del archivo físico con ubicación topográfica del sitio de custodia. Trazabilidad de consultas y préstamos y cargar inventarios (FUID).

II. El SGDEA debe incorporar múltiples niveles para el esquema del Cuadro de Clasificación Documental.

III. El SGDEA debe impedir la eliminación de un expediente electrónico o de su contenido. Sin embargo, existen excepciones a este requisito:

IV. La eliminación de acuerdo con lo establecido en las TRD o

V. Eliminación por un rol administrativo como parte de un procedimiento auditado.

VI. El proceso de captura de documentos del SGDEA debe contar con los controles y la funcionalidad adecuados para garantizar que los documentos se asocian con la Tabla de Retención Documental.

VII. El SGDEA debe permitir a usuarios autorizados la selección y uso de las diferentes versiones de la Tabla de Retención Documental.

VIII. El SGDEA debe permitir la búsqueda dentro de los niveles de jerarquía del cuadro de clasificación.

IX. 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 realizó acciones en el mismo.

X. El SGDEA debe proporcionar a los administradores herramientas para generar informes estadísticos de la actividad dentro de la Tabla de Retención Documental.

XI. El SGDEA debe representar la organización de los expedientes y documentos, incluyendo sus metadatos, a partir del esquema del cuadro de clasificación documental.

XII. El SGDEA debe validar la información que se ingresa en el esquema de la Tabla de Retención Documental a través de generación de alertas o incorporación de opciones que incluyan asistentes paso a paso (listas desplegables, alertas, listas de chequeo, ventanas de ayuda, entre otras) que indiquen si existe información similar o igual en el sistema.

XIII. 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.

XIV. El SGDEA debe permitir exportar el directorio, de todos los expedientes y/o carpetas clasificadas en una serie específica y su contenido.

XV. El SGDEA debe permitir la pre-visualización de documentos del expediente, sin que eso implique la descarga del documento.

XVI. El SGDEA debe permitir modificar los tiempos de retención para un conjunto de series y/o expedientes.

XVII. Una vez cerrado el expediente se deberá restringir la adición o supresión de carpetas o documentos.

XVIII. Una vez finalizado el trámite administrativo, el SGDEA debe incorporar opciones para el cierre del expediente. (manual o automático).

XIX. El SGDEA debe emitir un alerta al administrador 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:

i. 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 auditoria, con la explicación del motivo por el cual se realizó la acción.

XX. El SGDEA debe permitir cotejar la composición de los documentos electrónicos que integran el expediente electrónico, asegurando su integridad y autenticidad.

XXI. 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.

XXII. El SGDEA debe permitir la generación de expedientes electrónicos y sus componentes (documento electrónico, foliado, índice firmado y metadatos).

XXIII. El SGDEA debe permitir otorgarle un número único de identificación a un documento cuando es cargado al expediente.

XXIV. El SGDEA debe permitir que el historial de eventos del expediente electrónico pueda ser exportado.

XXV. El SGDEA debe permitir que todas las acciones efectuadas sobre el expediente, deben ser registradas en un historial de eventos que puede ser consultado por usuarios que tengan acceso al expediente electrónico.

XXVI. El SGDEA debe registrar como metadatos la fecha y la hora de registro de la carga de un documento al expediente electrónico.

2.2.2. Módulo Flujos Electrónicos:

2.2.2.1. Diseño

a. Del portal funcionario: Modulo integrado de gestión

2.2.2.2. Requerimientos funcionales:

I. Contar con semáforos que muestran el cumplimiento de tiempos en cada una de las actividades de un flujo.

II. Definir los tiempos límite de ejecución de los flujos y de cada una de sus actividades enviando notificaciones de incumplimiento.
III. El SGDEA debe generar los flujos de trabajo en un formato/ plantillas estándar.
IV. El SGDEA debe generar un identificador único para cada flujo de trabajo.
V. El SGDEA debe generar una trazabilidad de las acciones de los flujos de trabajo e incluirla en las pistas de auditoria.
VI. El SGDEA debe permitir al usuario del flujo de trabajo:
VII. Visualizar las actividades que tiene pendientes por realizar.
VIII. Priorizar por diferentes criterios.
IX. Visualizar información en tiempo real sobre el desempeño de sus procesos.
X. El SGDEA debe permitir detener un flujo de trabajo.
XI. El SGDEA debe permitir diagramar tareas que componen un proceso y/o procedimiento.
XII. El SGDEA debe permitir diagramar y modelar flujos de trabajo.
XIII. El SGDEA debe permitir incorporar un mecanismo de simulación para analizar los flujos de trabajo modelados.
XIV. El SGDEA debe permitir la parametrización de Reglas para la configuración y gestión de:
XV. Estados del Flujo de Proceso.
XVI. Validación de Actividades.
XVII. Definición y asignación de usuarios.
XVIII. El SGDEA debe permitir parametrizar los accesos, creación, modificación o control total para usuarios o grupos de usuarios de los flujos de trabajo.
XIX. El SGDEA debe permitir parametrizar los tiempos de ejecución y respuesta de los procesos ejecutados.
XX. El SGDEA no debe limitar el ingreso de acciones que componen cada flujo de trabajo.
XXI. El SGEDEA debe permitir contener múltiples versiones de un mismo proceso y/o procedimiento. Debe permitir al administrador seleccionar la última versión.
XXII. El SGDEA debe proporcionar facilidades de generación de informes/reportes para permitir que los usuarios autorizados con competencia para supervisar revisen las cantidades y el rendimiento del tipo de proceso en cada área.
XXIII. El SGDEA debe registrar en cada documento los datos del usuario quien proyectó, revisó y aprobó.
XXIV. El SGDEA debe permitir configurar flujos de trabajo que incluyan arboles de decisión, identificando que tipo de solicitud se va radicar (Petición, queja, reclamo, o sugerencia)
XXV. El SGDEA debe permitir el uso de correo electrónico como medio de notificación de las acciones que se realizan en el flujo.
XXVI. Debe permitir incorporar firmas electrónicas o digitales dentro del flujo.
XXVII. El sistema debe generar de manera automática las alertas a que haya lugar para brindar información de los pendientes de los documentos en cada instancia del flujo.

a. Formularios de registro y parametrización de flujos:

I. Este reporte debe exigir password al usuario que recibe la PQRS. Esta funcionalidad evita la impresión de planillas físicas para la entrega de los PQRS.
II. El sistema debe contar con un módulo integrado y expuesto desde el portal Web de la entidad, para la radicación de PQRS.
III. El módulo de PQRS Web debe permitir formular PQRS de manera anónima.
IV. El módulo de PQRS Web debe permitir registrar a ciudadanos que deseen ser identificados.
V. El sistema debe permitir la validación de la existencia del correo electrónico provisto por el ciudadano.
VI. Validado el ciudadano, este puede formular PQRS desde la Web.
VII. El ciudadano puede seleccionar el tipo de PQRS, Petición, queja etc.
VIII. El ciudadano puede seleccionar la temática general de que trata su PQRS.
IX. Después de radicado por el ciudadano, el sistema debe presentar un numero de radicado único para posterior consulta.
X. Una vez radicada la PQRS Web, el sistema debe enviarle la PQRS a la bandeja del usuario configurado como responsable del tema seleccionado por el ciudadano.
XI. El sistema debe enviarle la PQRS formulada desde la Web al correo electrónico registrado por el ciudadano.
XII. El ciudadano debe contar con un módulo que permita consultar las respuestas emitidas por la entidad.
XIII. El modulo del ciudadano debe permitirle cambiar sus datos personales.

2.2.3. Módulo Administración Documental:

2.2.3.1. Diseño

a. Del portal archivista: Parametrizar la normatividad vigente que aplica la entidad.

2.2.3.2. Requerimientos funcionales:

I. El SGDEA debe garantizar los permisos de acción sobre el expediente, respondiendo a las Tablas de Control de Acceso configuradas en el sistema.
II. El SGDEA debe permitir establecer niveles de seguridad del expediente de acuerdo con los niveles de seguridad establecidos por la entidad.
III. El SGDEA debe disponer de la búsqueda de información, parametrizado con base en la Tabla de Control de Acceso, para que los usuarios autorizados y con permisos asignados, acceden a los documentos permitidos.
IV. El índice electrónico se deberá firmar digitalmente al cierre del expediente, sin perjuicio de las garantías de seguridad de la información que deberá adoptar la entidad.
V. Todos los expedientes deberán contar con un índice electrónico, el cual debe ser firmado electrónicamente una vez se cierre el expediente.
VI. Los SGDEA deben permitir como mínimo las siguientes acciones de disposición para cualquier regla de retención y disposición:

ii. Conservación permanente.
iii. Eliminación automática.
iv. Eliminación con autorización del rol administrativo.
v. Transferencia.
vi. Selección.

VII. El SGDEA deberá generar un reporte del estado de la transferencia o exportación realizada y guardar datos de la acción realizada en las pistas de auditoria.

VIII. 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 al flujo de trabajo correspondiente.

IX. El SGDEA debe permitir realizar la solicitud de transferencias documentales e iniciar el proceso de transferencias seleccionando el tipo de transferencia que se desea realizar:

X. Transferencias documentales primarias.

XI. El SGDEA debe permitir filtrar por área los expedientes que cumplieron el periodo de retención primaria o secundaria y a los cuales se les va a realizar la transferencia documental.

XII. El SGDEA debe permitir escoger, dentro de la lista de expedientes que cumplieron un tiempo de retención específico, los expedientes a los cuales se les va a realizar la transferencia documental.

XIII. El SGDEA debe permitir transferir los documentos correspondientes con las reglas de retención y disposición y sus respectivos controles de acceso (seguridad para consulta).

XIV. El SGDEA debe permitir realizar el cambio de estado del expediente en el ciclo de vida indicando luego de una transferencia primaria del expediente que se encuentra en Archivo Central.

XV. El SGDEA debe permitir generar un acta de transferencia, asignando un número de acta, fecha y expedientes transferidos.

XVI. El SGDEA debe permitir gestionar el estado de los expedientes transferidos al Archivo Central.

XVII. El SGDEA debe permitir presentar un informe en el que se detalle cualquier falla que se produzca durante la transferencia, la exportación o el borrado. El informe deberá indicar cuáles de los registros que estaba previsto transferir generó errores durante la operación.

XVIII. Proporcionar tableros de control de todos los procesos que se encuentran implementados en el SGEDA, estos deben ser parametrizables a las necesidades de la entidad y estar disponibles para consulta.

XIX. Debe tener capacidad para compartir contenido con usuarios individuales y grupos, capacidad de recopilar contenido en alguna forma de espacio de trabajo al que se pueda invitar a otros participantes, capacidad para anotar y comentar el contenido en formato PDF (como mínimo)

XX. Debe permitir consultar la información por rangos flexibles de funciones que operen con los metadatos relacionados y los contenidos de los documentos, a través de parámetros definidos. Esta búsqueda debe traer agrupaciones de documentos electrónicos o no electrónicos asociados a la variable de búsqueda seleccionada.

2.2.4. Requerimientos Técnicos:

a. Autenticidad:

I. Implementación de estampas de tiempo o cronológicas que permitan certificar con fecha y hora el registro de un evento sobre un el documento electrónico, que garantice la creación, modificación, recepción sobre el mismo.
II. Implementación de Firma electrónica que permita relacionar la identidad y/o autorización de un usuario para firmar documentos.
III. Implementación de Firma Digital bajo certificados seguros que garanticen la autenticidad e integridad, para la gestión y creación de documentos.

b. Interoperabilidad:

I. Debe permitir la interoperabilidad a través de arquitectura orientada a servicios ofreciendo (Web Services) o consumiendo servicios web expuestos para generar y/o capturar documentos de archivo y gestionarlos en su respectivo ciclo de vida.
II. Debe permitir la integración con
III. El SGDEA debe implementar la funcionalidad de los siguientes servicios:

i. Servicio del sistema
ii. Servicio de usuarios y grupos
iii. Servicio de roles
iv. Servicio de radicación y registro
v. Servicio de formatos y formularios
vi. Servicio de flujos de trabajo
vii. Servicios de trabajo colaborativo y gestión de documentos
viii. Servicios de Clasificación
ix. Servicios Documentos Archivo
x. Servicio archivos físicos
xi. Servicios de Metadatos
xii. Servicios de retención y disposición documental
xiii. Servicios para búsqueda y reportes
xiv. Servicios de exportación.

IV. El SGDEA debe permitir la integración con datos de otras aplicaciones, tareas de negocio, web Services y otros mecanismos de interoperabilidad.

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

VI. 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

VII. El SGDEA debe permitir integrarse con los sistemas de Gestión de contenido CMS (Content Management System) haciendo uso del protocolo CMIS 1.1 (Content Management Interoperability Services").

VIII. Debe permitir utilizar HTTPS como protocolo de transporte de los mensajes generados y recibidos por los servicios.

IX. El SGDEA debe permitir recibir la información de los parámetros de entrada y los datos de salida de los servicios de interoperabilidad se realicen a través de SOAP (para interoperabilidad con aplicaciones web legadas) y REST (para interoperabilidad con aplicaciones web actuales).

X. El SGDEA debe estar en la capacidad de poder proveer una interfaz con los servicios disponibles de interoperabilidad para la interacción de una aplicación externa con el repositorio.

XI. El SGDEA debe permitir cuando los servicios sean utilizados mediante el protocolo de mensajería SOAP, se deben proveer sus interfaces de acceso mediante el protocolo de descripción del servicio WSDL. Para el caso que los servicios sean utilizados mediante el protocolo de mensajería REST, se debe hacer uso del protocolo de descripción del servicio Swagger para definir las interfaces de acceso.

XII. El SGDEA debe proveer servicios que permitan realizar consulta, inserción y/o modificación de la información de los documentos que están dentro del repositorio.

XIII. El SGDEA debe permitir que los servicios expuestos mediante el protocolo de mensajería SOAP, se utilizará el protocolo de descubrimiento estándar UDDI.

XIV. El SGDEA debe proveer el catálogo de los tipos de objetos, junto con sus atributos y tipos de dato de estos.

XV. El SGDEA debe proveer información acerca del fabricante del gestor y la versión del estándar CMIS que está implementando.

XVI. El SGDEA debe estar en la capacidad de poder proveer una interfaz con los servicios disponibles de interoperabilidad para la interacción de una aplicación externa con el repositorio.

XVII. El SGDEA debe proveer servicios que permitan realizar consulta, inserción y/o modificación de la información de los documentos que están dentro del repositorio.

XVIII. El SGDEA debe proveer servicios para navegar a través de la estructura jerárquica de carpetas y documentos que está definida en el repositorio del gestor documental.

XIX. El SGDEA debe proveer servicios que permiten hacer operaciones sobre documentos, carpetas y relaciones, tales como la creación, actualización y eliminación.

XX. El SGDEA debe proveer servicios que permiten efectuar búsquedas sobre objetos que no se tienen certeza de su ubicación, o que cumplen con unos criterios específicos

c. Fiabilidad:

I. Debe ser escalable y no permitir ninguna característica que impida su uso en organización de pequeño o gran tamaño, permitiendo aumentar la capacidad del sistema para ofrecer más servicios a un mayor número de usuarios sin degradar la calidad del servicio.
II. Debe ser escalable y no permitir ninguna característica que impida su uso en organización de pequeño o gran tamaño, permitiendo aumentar la capacidad del sistema para ofrecer más servicios a un mayor número de usuarios sin degradar la calidad del servicio.
III. Debe garantizar la alta disponibilidad mínimo un 99.96 estándar de los servicios SaaS
IV. Debe Permitir incluir instrumentos de seguridad y características que permitan restaurar el sistema a partir de dichas copias y de la pista de auditoría, sin perder la integridad del sistema
V. Cuando se produzca un fallo del software o del hardware, debe resultar posible devolver el sistema a un estado conocido (más reciente que la copia de seguridad)
VI. Debe garantizar que el tiempo de inactividad no prevista del SGDEA, no debe superar las 10 horas al trimestre y 40 horas al año.
VII. El SGDEA debe garantizar que las transacciones u operaciones que realice el sistema las cuales presenten fallos en su ejecución deben reversarse al estado inicial de la ejecución del proceso (Rollback) (evita envío de información incompleta y pérdida de esta).

d. Usabilidad:

I. Debe contar con manuales de usuario estructurados adecuadamente
II. Debe integrar contenidos explicativos, ejemplos y todos aquellos elementos que ayuden al autoaprendizaje.
III. Debe presentar ayudas en línea para las funcionalidades del sistema, sistemas guiados de consulta y tooltips para campos descriptivos en los formularios.
IV. Debe permitir atajos para las funcionalidades importantes.
V. Debe incluir ayudas en línea integradas al sistema, que permita al usuario encontrar con facilidad ayuda sobre una funcionalidad del sistema y permitir la navegación entre diferentes contenidos.
VI. El SGDEA debe proporcionar en todo momento al usuario final y al administrador funciones de uso fácil e intuitivo
VII. Debe garantizar un menú secundario el cual indica al usuario los lugares del sistema/sitio a los que se puede dirigir dentro de su nivel de navegación actual o local.

VIII. Debe garantizar el uso de tipográfico y de colores basado en la imagen corporativa de la Fiduprevisora.

IX. El sistema se debe ejecutar y visualizar correctamente sobre los siguientes navegadores y las últimas versiones de: Firefox Mozilla, Internet Explorer, Chrome.

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

XI. La interfaz de usuario del sistema deberá cumplir con el nivel AAA descrito en el manual de usabilidad de Gobierno en Línea.

XII. Debe auto complementar los campos definidos en los formularios al momento de registrar datos por parte del usuario. Por ejemplo generar listas despegables para los campos que así lo requiera

XIII. Las interfaces de usuario del sistema SGDEA deben ser intuitivas, rápidas, ágiles, estéticas, autoajustable a las características de las pantallas en cuanto a tamaño y resolución.

e. Eficiencia:

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

II. Debe soportar la concurrencia de usuarios y las peticiones a las diferentes funcionalidades sin sacrificar la disponibilidad y disponibilidad del sistema en terminado momento.

f. Mantenibilidad:

I. Debe permitir que los administradores realicen cambios masivos en la estructura de clasificación, incluyendo la completa manipulación de todos los metadatos y dejando la respectiva pista de auditoría, de forma que sea posible realizar en la estructura de clasificación la combinación de dos o más carpetas en una sola

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

III. Debe garantizar la flexibilidad a los cambios que se requieran hacer de manera ágil y que no impliquen cambios estructurales o de ajuste al código de la aplicación.

g. Portabilidad:

I. Debe ser compatible con protocolo IPV6 tanto en la configuración del software, hardware y dentro del funcionamiento del sistema. En caso de almacenar, referenciar enlaces o almacenamiento de direcciones físicas IP debe ser

transparente la interacción para toda la plataforma y el sistema en general. El cambio de direccionamiento IPV4 a IPV6 no debe generar errores o mal funcionamiento del software y sus componentes y en caso de presentarse, los corregirá o solucionará inmediatamente.

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

III. Debe funcionar en diferentes modos de comunicación y tipologías de red. Debe estar en la capacidad de funcionar correctamente en conexiones LAN, WAN, Internet o Wifi.

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

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

2.2.5. Requerimientos No Funcionales

a. Roles Y Permisos:

I. El SGDEA debe permitir solo a un rol administrador autorizado a crear, parametrizar, administrar, actualizar y eliminar la ejecución para flujos de trabajo, TRD, CCD, TVD.

II. El SGDEA debe permitir la creación y administración de usuarios, roles y permisos.

III. El SGDEA debe permitir sólo al rol administrador crear y/o gestionar tiempos de retención y disposición.

IV. El SGDEA debe activar automáticamente una alerta al rol administrador cuando el período de retención aplicable está a punto de cumplir el tiempo establecido.

V. Debe permitir controlar los perfiles y roles de los usuarios que ejecutan o consultan los flujos de información, parametrizar necesidades de negocio o requerimientos de entes externos y obtener log de auditoria.

VI. El SGDEA debe permitir la creación, administración y ejecución de flujos.

VII. El SGDEA debe ofrecer opciones de configuración para asignar o eliminar roles después de un período predefinido automáticamente.

VIII. El SGDEA no debe limitar el número de roles o grupos que se puedan configurar.

IX. El SGDEA debe permitir la administración y control de los procesos por lotes y los procesos automáticos programados.

X. Se requiere tener perfiles de consulta por roles de acuerdo a necesidades de negocio.

XI. El SGDEA debe permitir que los roles administrativos agreguen y eliminen usuarios desde y hacia los roles y grupos en cualquier momento.

XII. El SGDEA debe permitir definir y parametrizar los grupos, roles y permisos de las dependencias y los usuarios de la Entidad que intervienen en el proceso

documental, con los privilegios de acceso a los archivos y expedientes. Los cuales pueden ser totales, parciales por tipos documentales.

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

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

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

b. Seguridad y auditoria del sistema

Administración de sesiones

I. El sistema no debe permitir realizar el guardado automático de contraseña.

II. La función de logout del sistema debe terminar completamente con la sesión o conexión asociada.

III. La función de logout del sistema debe estar disponible en todas las páginas protegidas por autenticación.

IV. El sistema debe contar con una validación del tiempo de vida de la sesión lo más corto posible, balanceando los riesgos con los requerimientos del negocio. En la mayoría de los casos, nunca debería ser superior a cinco minutos.

V. Si una sesión fue establecida antes del login, el sistema debe cerrar dicha sesión y establecer una nueva luego de un login exitoso.

VI. El sistema debe generar un nuevo identificador de sesión luego de cada re autenticación.

VII. El sistema no debe permitir logeos concurrentes con el mismo usuario.

VIII. Los controles de acceso en caso de falla del sistema, deben actuar en forma segura.

IX. Denegar todos los accesos en caso de que la aplicación no pueda acceder a la información de configuración de seguridad.

X. En el sistema se debe restringir el acceso a información relevante de la configuración a usuarios no autorizados.

Administración De Logs

I. El sistema debe almacenar en un registro de auditoría cada cambio en cada parámetro con la información de fecha, hora, valor anterior, valor nuevo, usuario del sistema e IP, actividad (ingreso/borrado/modificación).

II. El sistema debe permitir el acceso a los logs, solo a personal autorizado.

III. El sistema deberá utilizar una rutina centralizada para todas las operaciones de logging.

IV. El sistema no deberá guardar información sensible en logs, incluyendo detalles innecesarios del sistema.

V. Asegurar que existen mecanismos para conducir un análisis de los logs.

VI. El sistema deberá registrar en un log todas las fallas de validación.
VII. El sistema deberá registrar en un log todos los intentos de autenticación, en particular los fallidos.
VIII. El sistema deberá registrar en un log todas las fallas en los controles de acceso.
IX. El sistema deberá registrar en un log todos los intentos de conexión con tokens inválidos o vencidos.
X. El sistema deberá registrar en un log todas las excepciones del sistema.
XI. El sistema deberá registrar en un log todas las funciones administrativas, incluyendo cambios en la configuración de seguridad.
XII. El sistema deberá registrar en un log, todas las fallas de conexión.
XIII. El sistema deberá registrar en un log las fallas de los módulos criptográficos. (Si aplica)
XIV. El sistema deberá utilizar una función de hash para validar la integridad de los logs.

Administración De Seguridad

I. El sistema debe contar con un módulo para la administración de la seguridad del sistema.
II. El sistema debe contar con conexiones TLS para todo el contenido que requiera acceso autenticado y para todo otro tipo de información sensible.
I. El sistema proporcionara una herramienta que haga parte del módulo de Seguridad y Auditoria que facilite el análisis de datos de acceso a las aplicaciones.
II. Los componentes del sistema propuesto deben correr sobre protocolos seguros https.
III. El sistema debe tener una administración centralizada de los sistemas de Seguridad y Auditoria.
IV. El proveedor debe entregar el detalle de los roles y funciones asociadas a cada rol, describiendo detalladamente el alcance de cada función para así poder identificar internamente el rol que se debe asignar a cada funcionario de acuerdo a sus funciones.
V. Autenticación contra el LDAP/Directorio Activo de la compañía.
VI. El sistema debe tener un mecanismo de control de acceso que permita asignación o denegación de privilegios solo al rol que cumple un usuario autorizado.
VII. El sistema debe limitar las opciones de menú y submenú de cada uno de los usuarios que utilizan los sistemas de información de acuerdo al perfil.
VIII. El sistema generará informes que permitan visualizar los roles por aplicación, usuarios del sistema, privilegios de cada rol por opción, opciones con permisos por rol.
IX. Se debe garantizar que la aplicación está libre de vulnerabilidades de seguridad de la información, realizando pruebas de revisiones de código estático y dinámico y análisis de vulnerabilidades, realizando ejercicios completos de Ethical Hacking para validar la posibilidad de aprovechamiento de las mismas, en el caso que se identifiquen.

Continuidad De Servicio

- **I.** El proveedor debe contar con un servidor alojado en un DATA CENTER con domicilio nacional o internacional que garantice alta disponibilidad, confidencialidad y seguridad de la información.
- **II.** El oferente debe contar con planes de continuidad de negocio que aseguren la disponibilidad del sistema ante una interrupción de la operación de su infraestructura tecnológica.
- **III.** El SGDEA debe permitir la parametrización de copias de seguridad de los documentos en conjunto con los metadatos.
- **IV.** Cuando el SGDEA realice procesos de importación o exportación de información, deberá realizarse a través de interfaces seguras y aplicar protocolos y mecanismos de seguridad.
- **V.** El SGDEA debe permitir contar con procedimientos automáticos para copias de seguridad y restauración encaminados a realizar copias periódicas de seguridad de todos elementos dentro del sistema (carpetas, documentos, metadatos, usuarios, roles, permisos, configuraciones específicas).
- **VI.** El SGDEA en caso de presentarse fallas durante la restauración de las copias de seguridad debe permitir notificar sobre el fallo y los detalles del mismo, para que el administrador tome las decisiones necesarias para subsanar los errores.

2.3. DURACIÓN.

Plazo de ejecución veinticuatro (24) meses.

2.4. FORMA DE PAGO

Fiduprevisora S.A. bajo ninguna circunstancia realizará anticipos o pagos anticipados, el pago del valor estimado del servicio se hará conforme a los servicios prestados.

Nota: *FIDUPREVISORA S.A., conforme a su portafolio de servicios financieros, lo invita a invertir en un Fondo de Inversión Colectiva administrado por ésta, con el fin de que los pagos derivados del eventual contrato, sean generados a través de dicho medio. Para lo anterior, podrá solicitar información al correo electrónico operacionesfic@fiduprevisora.com.co.*

3. INFORMACIÓN ESPECÍFICA DE LA COTIZACIÓN.

3.1. Forma de presentación de la Cotización

Los interesados deben presentar sus ofertas por medio de correo electrónico y/o plataforma SECOP II, en idioma español, dentro de las fechas establecidas para cada etapa del proceso relacionadas en el cronograma y acompañadas de los documentos solicitados.

3.2. Documentos de carácter jurídico y financiero

Las respectivas cotizaciones deberán estar acompañadas de los documentos que se relacionan a continuación, con el fin de realizar un análisis de tipo jurídico y financiero de cada interesado; veamos:

I. Certificado de Representación Legal con fecha de expedición no mayor a 30 días calendario.
II. Registro Único Tributario – RUT.
III. Estados Financieros con corte a diciembre de (año).

3.3. Experiencia Específica

El interesado debe relacionar experiencia de ejecución de contratos cuyo objeto contemple las actividades citadas en el objeto de esta invitación.

N°	EMPRESA O ENTIDAD CONTRATANTE	OBJETO	FECHA INICIO	FECHA FIN	VALOR TOTAL EJECUTADO INCLUIDO IVA
1					
2					
3					

Nota* se recomienda que preferiblemente la experiencia relacionada no sea superior a 5 años respecto de la actual vigencia.

4. VALOR DE LA COTIZACIÓN

El valor de la propuesta debe presentarse en pesos colombianos, debe incluir impuestos, tasas y/o contribuciones a los que haya lugar, así como costos directos e indirectos.

Costos de Implementación:

IMPLEMENTACIÓN	Módulo Ventanilla Única Digital/Física	Módulo Flujos Electrónicos	Módulo Administración Documental
Costos Implementación ($COL)	$	$	$
Duración (meses)			

Costos de Mantenimiento Mes:

Costos Soporte y Mantenimiento ($COL)	Módulo Ventanilla Única Digital/Física	Módulo Flujos Electrónicos	Módulo Administración Documental
Soporte Mes	$	$	$
Usuarios mes (valor unitario)			
1 a 1.000	$	$	$
1.001 a 2.000	$	$	$

3.001 a 4.000	$	$	$
Almacenamiento mes			
1 a 5 Teras	$	$	$
6 a 10 Teras	$	$	$
11 a 20 Teras	$	$	$

Para Fiduprevisora S.A., es importante contar con su cotización teniendo en cuenta su experiencia y reconocimiento en el mercado; de esta manera, conoceremos las mejores prácticas que se están llevando a cabo, con el fin de establecer condiciones equitativas y factores objetivos de selección dentro de los procesos de contratación.

Agradecemos su participación.

Elaboró: Jose Dayan Duque Cadena – Técnico Gerencia de Adquisiciones y Contratos
Revisó: Rodrigo Alfonso Alvarez Torres Profesional Inteligencia de Mercados
Revisó: Enrique Carlo Badel Kerquelen – Director de Contratos Empresas
Aprobó: Luz Maria Molina Tovar – Coordinadora Centro de Recursos de Información - Gerencia de Gestión Documental
Aprobó: Juan Gabriel Barrera Cardenas – Director de Proyectos Especiales