INVITACIÓN A COTIZAR No. 028 DE 2024

Objeto: Fiduprevisora S.A. está interesada en recibir cotizaciones para la implementación de un Sistema de Gestión Electrónica de Documentos de Archivo – SGDEA que permita la administración, centralización y control de la toda información documental física y electrónica de los diferentes procesos de negocios de la entidad, los cuales se producen en los sistemas de información de la organización o directamente en el SGDEA, 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: 12 de diciembre de 2024.

Fecha límite para presentar observaciones: 17 de diciembre de 2024 hasta las 18:00 horas.

Respuesta a Observaciones: 20 de diciembre de 2024.

Recepción de Cotizaciones: 28 de diciembre de 2024 hasta las 18:00 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 de 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/wpcontent/uploads/2021/11/Lineamientos_del_SIG_proveedores_contratistas.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 -Reprocesos	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. 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.

La solución debe garantizar la administración de la documentación que se generan en todos los procesos de la Fiduprevisora, que cuente con una arquitectura y taxonomía dinámica que permita realizar la producción, distribución, consulta, retención, almacenamiento, preservación y disposición final de los documentos que se originen en los sistemas de información de la organización y/o directamente en el SGDEA, por lo que debe contar con la capacidad de integrarse con los canales de comunicación, sistemas y/o aplicaciones propios y/o terceros, los cuales sean utilizados por la organización para su gestión

Adicionalmente, se debe contemplar la migración de los datos y documentos del sistema actual, con el fin de mantener los datos y documentos consolidados y disponible para consulta y gestión.

El proyecto está basado en ocho (8) ejes transversales:

1. Administración de las comunicaciones oficiales en las entidades públicas – Ley 594 de 2000, Ley 1712 de 2014 y Acuerdo 01 de 2024 (Gerencia de Gestión Documental)), MOREQ y demás normas vigentes y que llegue a expedir el Archivo General de la Nación.
2. Ventanilla Única de Radicación.
3. Gestión de PQSD.
4. Arquitectura tecnológica (Gerencia de Tecnología e Información).
5. Privacidad de la Información– Ley 1581 de 2012 - Decretos Reglamentarios (Gerencia de Riesgos).
6. Seguridad de la Información y Ciberseguridad (Gerencia de Riesgos).
7. Servicios digitales - Gobierno Digital – Min Tic (Todas las áreas).
8. Norma ISO 27001:2013 y 27001:2022.

3. ESPECIFICACIONES FUNCIONALES, NO FUNCIONALES Y TÉCNICAS DEL PROYECTO

3.1. ESPECIFICACIONES FUNCIONALES

a. Tablas de Retención Documental:

1. El SGDEA debe garantizar que los documentos electrónicos de archivo que se capturen o generen, se asocien a una TRD configurada en el sistema para cada dependencia Los documentos pueden ser producidos por el SGDEA u otro sistema de información de la Fiduprevisora que este integrado con el SGDEA.

2. El SGDEA debe permitir configurar Tablas de Retención Documental de acuerdo con la necesidad de la entidad, sin restricción.

3. El SGDEA debe permitir actualizar las Tablas de Retención Documental por una o varias dependencias, que guarde el histórico de cambios realizados.

4. El SGDEA debe permitir ajustar la plantilla del formato de TRD de acuerdo con las necesidades de la entidad (añadir o quitar campos).

5. 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.

6. 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.

7. EL SGDEA debe permitir la importación y exportación total o parcial de la Tabla de Retención Documental, en un formato abierto y editable, teniendo en cuenta:

   Para la importación:

   • Permitir la importación de los metadatos asociados a archivos CSV, Excel o Xml y/o formato común y conocido.

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

   Para la Exportación:

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

   • Los procesos de importación y exportación deben generar reportes y estas acciones deben quedar registradas en las pistas de auditoría.

8. 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.

9. 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.

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

11. El SGDEA debe permitir la transferencia de la estructura de la TRD mediante un archivo XML.

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

13. 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.

b. Roles y permisos

1. 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.

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

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

4. 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 auditoría.

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

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

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

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

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

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

11. 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 teniendo en cuenta la clasificación de la información en la Tabla de control de acceso, los cuales pueden ser totales, parciales por tipos documentales.

12. El SGDEA debe permitir un directorio activo en donde se administre todo lo relacionado con la gestión de usuarios y contraseñas.

13. El SGDEA no debe permitir inactivar usuarios que tenga tareas pendientes y debe permitir la reasignación masiva e individual de las tareas pendientes de estos usuarios.

14. El SGDEA debe proveer información de contexto e información del estado del usuario en todo momento.

c. Otros

1. La solución debe permitir que cada usuario pueda consultar sus tareas y radicados por diferentes estados como gestionados, pendientes, por vencer, etc.

2. La solución debe permitirle al usuario organizar y filtrar tareas por diferentes criterios (número de identificación, nombre, fecha de radicado, número de radicado, entre otros), así mismo personalizar los campos (columnas) que requiera visualizar.

3. Debe permitir elaborar tableros de control (dashboard) analíticos, dinámicos y parametrizables por diferentes criterios según las necesidades de cada área. Los tableros deben permitir utilizar diferentes tipos de gráficos, deben ser exportables en formatos conocidos como Excel junto con el detallado del reporte, es decir, con cada uno de los registros.

4. Debe contar con una interfaz intuitiva, fácil de usar y navegar.

5. La solución debe contar con formularios de consulta de información configurables por el Usuario mediante la Herramienta de Consulta.

6. La solución debe contar con herramienta de Búsqueda en cada uno de sus módulos.

7. La solución debe contar con mapas de navegación en los módulos de la aplicación que ofrezcan una visión gráfica del ciclo de vida de los diferentes procesos funcionales.

8. El SGDEA debe permitir consultar y descargar la relación de roles que hay en el sistema, junto con los permisos que tienen cada uno y los usuarios que lo tienen asignado.

9. El SGDEA debe manejar matriz de tipificación en los procesos de gestión y trámite, con control de tiempo por etapa.

10. El SGDEA debe ser una herramienta intuitiva para mejorar la experiencia del usuario y minimizar los clics para la ejecución de procesos.

3.1.1. Módulo de Ventanilla Única Virtual / Física:

Diseño

- Diseño Tablas de Retención Documental: Contiene el ciclo de vida de la información, parametriza el gestor documental.

- Diseño de la ventanilla única: Documentación física.

- Diseño de la ventanilla digital: Documentación electrónica, Seguridad y privacidad de la información.

- Personalización de formularios y plantillas de acuerdo con las necesidades de la Fiduciaria.

- Diseño de matriz de tipificación para la asignación, tramite y gestión de comunicaciones.

Requerimientos funcionales:

a. Radicación, distribución, Asignación y trámite:

1. 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.

2. 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.

3. Cada código debe contener un componente de secuencia numérica que el SGDEA debe reiniciar automáticamente cada 1ro. de enero (Acuerdo 01 de2024 – AGN).

4. El SGDEA no debe tener límite para la cantidad de radicados (Recibida, Enviada e Interna) que se generen, de acuerdo con las necesidades y volúmenes, por lo que se debe configurar la secuencia de radicados que soporte todos los canales de la Fiduprevisora y sistemas con los que se integre el SGDEA; manteniendo siempre la estructura de los radicados.

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

6. 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 con la normatividad existente) y permitir acceso a esta dependiendo el rol de usuario.

7. El SGDEA debe disponer de una función de integración con aplicaciones externas principalmente ekogui, lupa, legis, controleg, entre otros, para radicar comunicaciones oficiales enviadas por canales distintos al sistema (páginas web, correos electrónicos u otros sistemas de información de la entidad). Que permita importar directamente los radicados por correo electrónico al sistema con los metadatos disponibles en el correo. Que permita importar directamente los radicados por correo electrónico al sistema con los metadatos disponibles en el correo.

8. 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, para las comunicaciones en soporte físico se requiere que el proceso de digitalización y asignación del radicado se realice de forma masiva.

9. El SGDEA debe permitir que la radicación masiva se realice usando la funcionalidad de combinación de correspondencia.

10. 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.

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

12. El SGDEA debe permitir la configuración de múltiples plantillas por negocio de acuerdo con las necesidades de la entidad.

13. 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.

14. 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. El sistema debe tener capacidad OCR que permita la clasificación y/o indexación de la imagen.

15. 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.

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

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

18. El SGDEA debe permitir que el sticker del radicado, pueda ser ubicado en diferentes partes dentro del documento a selección del radicador.

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

20. Cuando se radique un correo electrónico, el SGDEA debe capturarlo en el formato

nativo (EML o MSG) en que se genera la comunicación.

21. La radicación del correo electrónico(web) o físico debe, a través del SGDEA, tenerlas siguientes funciones:

    i. Generar un número único y consecutivo 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. Debe generar acta de anulación con la firma del funcionario que realizo el proceso.
    vii. No debe permitir eliminar radicados.
    viii. Debe permitir reasignar, devolver, archivar o tramitar la respuesta física o electrónica de los radicados de forma unitaria y/o masiva y así dejar trazabilidad de estos cambios y log de auditoría.

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

23. 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 con las necesidades de las áreas de la entidad. Esto puede estar dado por medio de la integración a Microsoft Word como herramienta de gestión de las plantillas. Además, debe permitir que para elaborar las comunicaciones se puedan incorporar imágenes y cuadros, manteniendo siempre la consistencia y orden del documento que se genere, y permitiendo copiar y pegar.

24. El objetivo de la plantilla debe ser generar automáticamente documentos que se generen en las áreas como correspondencia interna, de salida o respuesta a un radicado.

25. 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.

26. El SGDEA debe permitir que el rol centralizador asigne una o varias comunicaciones que se deben gestionar y/o archive directamente las que son de carácter informativo,

27. 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, dependencias 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.

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

29. Debe permitir en cualquier momento la parametrización de los formularios de radicación debe ser intuitiva y simple, que no se requiera codificación para generar y modificar los formularios, que sean Point and click.

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

31. 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). El apoyo de esas tecnologías sea también para la clasificación de documentos, la indexación automática, búsqueda en el contenido y asignación para el área y/o usuario de acuerdo con el árbol de tipificación.

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

33. El SGDEA debe permitir que los registros almacenados temporalmente sean modificados y completados para continuar con su proceso.

34. 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.

35. El SGDEA debe permitir el registro de información básica de contexto (metadatos) automáticamente obteniéndola del encabezado del correo electrónico.

36. El SGDEA debe cumplir con el servicio de la Firma Digital/Electrónica: Servicios nativos y/o integración con terceros para firma digital/electrónica:

    - Se debe garantizar que la firma implementada sea única, no falsificable, verificable, no repudio (innegable) y viable (que sea fácil de generar porel

firmante).

- Que la solución esté disponible y sea parametrizable para implementaren cualquier proceso futuro o documento nuevo que se genere.

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

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

39. El SGDEA debe integrar la firma electrónica certificada en los procesos de gestión y tramite de comunicaciones de salida e internas, esta debe acogerse a lo establecido la ley 527 de 1999.

40. El SGDEA debe dejar registrada la trazabilidad del envió de comunicaciones por correo electrónico, fecha, hora, destinario y relación de documentos adjuntos.

41. El SGDEA 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 esta 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.

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

43. 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.

44. El SGDEA debe permitir la captura automática de metadatos pertenecientes a mensajes de correo electrónico y sus archivos adjuntos.

45. El SGDEA debe permitir al usuario capturar un mensaje de correo electrónico asignándolo dentro de una serie, subserie o expediente.

46. El SGDEA debe tener la opción de capturar en una sola operación, varios correos electrónicos seleccionados manualmente.

b. Expediente Electrónico:

1. 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).

2. El SGDEA debe generar el FUID de los expedientes creados por cada dependencia y el FUID consolidado de forma automática.

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

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

   - La eliminación de acuerdo con la disposición final establecida en las TRD.
   - Eliminación por un rol administrativo como parte de un procedimiento auditado.
   - Los procesos de eliminación deben quedar en el historial de eventos del expediente.

5. 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.

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

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

8. 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.

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

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

11. 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.

12. 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.

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

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

15. El SGDEA debe permitir la visualización de los documentos de forma fácil, sin necesidad de ingresar a todo el expediente o radicado.

16. El SGDEA debe garantizar que se descarguen copias controladas de los tipos documentales que conforman los expedientes

17. El SGDEA debe tener un sistema de validación que impida la creación de expedientes duplicados, la validación debe ser serie, subserie y nombre del expediente.

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

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

    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.

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

21. El SGDEA debe emitir una alerta al administrador en el caso en que un expediente electrónico esté listo para ser eliminado y alguno de sus documentos esté vinculados a otro expediente. El proceso de eliminación debe aplazarse para permitir una de las siguientes acciones correctivas:

    - Solicitar confirmación para continuar o cancelar el proceso;
    - Esta acción deberá quedar en las pistas de auditoria relacionando mínimo los siguientes datos: fecha de inicio; identidad del usuario autorizado; motivo de la acción.
    - Deberá permitir copiar el documento a un expediente determinado y actualizar las referencias correspondientes, con el fin de garantizar la integridad del expediente.

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

23. 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.

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

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

26. El SGDEA debe permitir que el historial de eventos del expediente se genere desde que se crea el expediente electrónico y que pueda ser exportado

27. 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.

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

29. El SGDEA debe permitir que al momento de la captura o en una etapa posterior de procesamiento, se puedan ingresar metadatos adicionales.

30. Los documentos dentro del SGDEA deberán heredar los metadatos de su serie o subserie.

31. El SGDEA debe permitir exportar el índice electrónico a formato XML, PDF, Excel.

32. El SGDEA debe permitir que un documento pueda estar ubicado en diferentes partes de la estructura de clasificación, sin que esto signifique la duplicación del documento.

33. Conservar 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.

34. 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.

35. El SGDEA no debe limitar la duración de los tiempos de retención.

36. El SGDEA debe permitir gestionar contenidos como: videos, audio, imagen, entre otros, de la misma forma que los documentos electrónicos de texto.

37. El SGDEA no debe limitar el número de documentos que pueden ser capturados en cualquier serie, subserie, expediente ni sobre el número de documentos que se pueden almacenar.

38. Para la captura de documentos que tienen anexos el SGDEA deberá gestionarlos como unidad, restringiendo el uso de formatos comprimidos.

39. Debe permitir el cargue masivo de expedientes y documentos electrónicos teniendo en cuenta estructura definida de metadatos y de acuerdo con TRD.

40. El SGDEA debe permitir la integración con los diferentes servidores de correo electrónico de acuerdo con las necesidades o políticas de cada organización.

41. Los documentos dentro del SGDEA deberán heredar los metadatos de su serie o subserie.

42. El SGDEA debe hacer accesible el contenido de los expedientes de acuerdo con los roles y permisos

43. El SGDEA debe generar el FUID de la totalidad de expedientes creados y cargados en el sistema por dependencia, serie y subserie.

44. La plantilla del FUID se debe poder modificar quitar o añadir columnas de acuerdo a las necesidades de la entidad.

45. El SGDEA debe permitir la asignación de un vocabulario controlado y normalizado compatible con las normas nacionales y estándares internacionales.

46. El SGDEA debe generar el FUID con los campos establecidos por la entidad de los expedientes creados y cargados al sistema.

47. El SGDEA debe permitir la incorporación de la firma electrónica para la generación del índice del expediente electrónico.

48. El SGDEA debe permitir la reubicación de una carpeta (o conjunto de carpetas) o documento, a un lugar distinto dentro de la estructura de clasificación, y garantizar que se mantengan los metadatos y demás atributos (permisos)

49. El SGDEA debe registrar en la pista de auditoría, cuando se realice la reubicación de una carpeta (o conjunto de carpetas) o documento.

50. El SGDEA debe permitir registrar las razones por las que se realiza la reubicación de cualquier elemento de la estructura de clasificación y almacenarlo como una propiedad o metadato

51. El SGDEA debe permitir que un documento pueda estar ubicado en diferentes partes de la estructura de clasificación, sin que esto signifique la duplicación del documento.

52. 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.

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

54. 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.

c. Otros:

1. 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). El apoyo de esas tecnologías sea también para la clasificación de documentos, la indexación automática, búsqueda en el contenido y asignación para el área y/o usuario de acuerdo con el árbol de tipificación.

2. Debe permitir parametrizar, crear, modificar y eliminar elementos dentro del árbol de tipificación.

3. Debe permitir revisar, aprobar y firmar comunicaciones de salida de manera masiva.

4. Debe permitir archivar comunicaciones masivamente.

5. Para los radicados de entrada debe permitir realizar asignación y reasignación individual y masiva de manera automática y manual.

6. Debe permitir realizar tipificación masiva a las comunicaciones de entrada.

7. Para los radicados de entrada debe permitir realizar Re-tipificación individual y masiva del tipo de PQRS a comunicación.

8. Debe permitir revisar, aprobar y firmar comunicaciones de salida de manera masiva.

9. El SGDEA debe permitir configurar firmas corporativas por dependencia.

10. Debe permitir archivar comunicaciones de entrada masivamente en un solo proceso.

3.1.2. Módulo PQRS:

Diseño

- Del portal funcionario: Modulo integrado de gestión.
- Personalización de formularios y plantillas, de acuerdo con las necesidades de la Fiduciaria.
- Diseño de matriz de tipificación para la asignación, tramite y gestión de comunicaciones.

a. **Requerimientos funcionales**:

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

2. Definir los tiempos límite de ejecución de los flujos y de cada una de sus actividades enviando notificaciones de incumplimiento.

3. El SGDEA debe generar los flujos de trabajo en un formato/ plantillas estándar.

4. El SGDEA debe generar un identificador único para cada flujo de trabajo.

5. El SGDEA debe generar una trazabilidad de las acciones de los flujos de trabajo e incluirla en las pistas de auditoría.

6. El SGDEA debe permitir al usuario del flujo de trabajo:

   - Visualizar las actividades que tiene pendientes por realizar.
   - Priorizar por diferentes criterios (fechas, vencimiento, semáforos, etc).
   - Visualizar información en tiempo real sobre el desempeño de sus procesos.

7. El SGDEA debe permitir detener o asignar un flujo de trabajo.

8. El SGDEA debe permitir diagramar tareas que componen un proceso y/o procedimiento.

9. El SGDEA debe permitir diagramar y modelar flujos de trabajo.

10. El SGDEA debe permitir incorporar un mecanismo de simulación para analizar los flujos de trabajo modelados.

11. Los flujos deben ser administrados dependiendo del nivel de complejidad de la siguiente manera:

    Flujos Complejos: Proveedor
    Flujos Sencillos: Fiduprevisora

    El SGDEA debe permitir la parametrización de Reglas para la configuración y gestión de:

    - Estados del Flujo de Proceso.
    - Validación de Actividades.
    - Definición y asignación de usuarios.

12. El SGDEA debe permitir parametrizar los accesos, creación, modificación o control total para usuarios o grupos de usuarios de los flujos de trabajo.

13. El SGDEA debe permitir guardar el proyecto o borrador de una comunicación, hasta que sea radicado.

14. El SGDEA debe permitir parametrizar los tiempos de ejecución y respuesta de los procesos ejecutados.

15. El SGDEA no debe limitar el ingreso de acciones que componen cada flujo de trabajo.

16. El SGDEA debe permitir contener múltiples versiones de un mismo proceso y/o procedimiento.

17. Debe permitir al administrador seleccionar la última versión.

18. 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.

19. El SGDEA debe registrar en cada documento los datos del usuario quien proyectó, revisó y aprobó.

20. El SGDEA debe permitir configurar flujos de trabajo que incluyan arboles de decisión, identificando que tipo de solicitud se va a radicar (Petición, queja, reclamo, o sugerencia)

21. El SGDEA debe permitir el uso de correo electrónico como medio de notificación de las acciones que se realizan en el flujo, así como el envío de respuesta física

22. Debe suministrar firma electrónica certificada, firma electrónica o digital dentro del flujo, según la necesidad del proceso.

23. 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.

24. El SGDEA debe permitir tipificar por diferentes criterios y de manera individual y masiva los radicados de entrada, así mismo generar respuestas masivas con diferentes proformas para cada tipología; y luego de contar con la evidencia de entrega de la comunicación de salida, se archive cada radicado de entrada con su respectivo radicado de respuesta, por lo que el número de cada radicado de respuesta debe ser diferente.

25. Debe permitir parametrizar, generar y enviar respuestas automáticas con plantillas a radicados de entrada según la necesidad, por ejemplo, que para un radicado que esté próximo a vencer genere y envíe un radicado de salida informando una prórroga. Asimismo, actualizar automáticamente el tiempo de vencimiento del radicado de entrada.

26. Debe permitir configurar reportes de acuerdo con las necesidades del área.

27. Para los radicados de entrada debe permitir realizar asignación y reasignación individual y masiva de manera automática y manual

28. Debe permitir realizar tipificación masiva a las comunicaciones de entrada

29. Para los radicados de entrada debe permitir realizar retipificación individual y masiva del tipo de comunicación y actualizar los parámetros de gestión a la nueva clasificación.

30. Debe permitir al usuario contar con la posibilidad de tener carpetas u otra forma de ordenar los radicados a gestionar según su necesidad

31. Debe permitir disponer de un formulario en la página web para recibir las PQRSD de acuerdo con los estándares de publicación y divulgación de información como se indica en el anexo 2 resolución MINTIC 1519 del 2020 y las demás que sean requeridas por la Fiduprevisora.

32. Debe permitir parametrizar, crear, modificar y eliminar elementos dentro del árbol de tipificación.

33. Debe disponer de una consulta para los clientes y usuarios que les permita saber el estado de su radicado.

34. Debe permitir revisar, aprobar y firmar comunicaciones de salida de manera masiva.

35. Debe permitir archivar comunicaciones masivamente.

36. Debe incluir un servicio de correo electrónico para el envío de comunicaciones de salida.

37. Debe incluir el envío de las comunicaciones por correo electrónico, además de correo electrónico certificado según la necesidad de las áreas.

38. Debe contar con la funcionalidad para que en las comunicaciones de salida que se envíen por correo electrónico, el correo enviado quede como un archivo adjunto al radicado de salida.

39. Debe permitir registrar el resultado del envío de las comunicaciones de salida y para las que se envíen por correo electrónico el estado se debe actualizar automáticamente y permitir descargar un reporte de esta información.

40. Debe permitir elaborar comunicaciones de salida a través de trabajo colaborativo entre distintas áreas y usuarios guardando el control de cambios, el usuario debe tener la opción de seleccionar si requiere o no trabajo colaborativo.

41. Debe permitir la remisión de respuestas o de comunicaciones internas a varios destinatarios, en una sola transacción.

42. Debe permitir la consulta del histórico de radicados de salida.

43. Transmisión de quejas y reclamos al sistema Smartsupervison de la Superintendencia Financiera de Colombia, de conformidad con las Circulares Externas 023 de 2021, 038 de 2022, 041 de 2022 y las demás normas que lo rijan y se llegaran a expedir.

44. Debe permitir parametrizar los horarios de transmisión para cada uno de los momentos, a smartsupervision, los cuales pueden ser sincrónicos y/o asincrónicos. Es de resaltar que las mencionadas transmisiones son automáticas.

45. Debe generar reportes de cada una de las transmisiones de smartsupervison.

46. Realizar la transmisión automática de la PQRS que regule la Superintendencia de Salud, entes de control y ramas del poder público, con las condiciones que soliciten las entidades. Las transmisiones deben ser parametrizables y permitir la generación de reportes.

b. Formularios de registro y parametrización:

1. El sistema debe contar con un módulo integrado y expuesto desde el portal Web de la entidad, para la radicación de PQRS.

2. El módulo de PQRS Web debe permitir formular PQRS de manera anónima.

3. El módulo de PQRS Web debe permitir registrar a ciudadanos que deseen ser identificados.

4. El sistema debe permitir la validación de la existencia del correo electrónico provisto por el ciudadano.

5. Validado el ciudadano, este puede formular PQRS desde la Web.

6. El ciudadano puede seleccionar el tipo de PQRS, Petición, queja etc.

7. El ciudadano puede seleccionar la temática general de que trata su PQRS.

8. Después de radicado por el ciudadano, el sistema debe presentar un numero de radicado único para posterior consulta.

9. 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. Debe enviársele una notificación vía correo electrónico con los datos del nuevo radicado que tiene en su bandeja de trabajo. Revisar la posible inclusión de una integración entre el sistema SGDEA con el servicio de correo que utilice la Fiduciaria, que le permita realizar algunas actividades referentes al trámite desde la interfaz de correo. El sistema debe enviarle la PQRS formulada desde la Web al correo electrónico registrado por el ciudadano.

10. El ciudadano debe contar con un módulo que permita consultar las respuestas emitidas por la entidad.

11. El módulo del ciudadano debe permitirle cambiar sus datos personales.

3.1.3. Módulo Administración Documental:

Diseño

- Del portal archivista: Parametrizar la normatividad vigente que aplica la entidad.
- Personalización de formularios y plantillas de acuerdo con las necesidades de la Fiduciaria

Requerimientos funcionales:

1. El SGDEA debe garantizar los permisos de acción sobre el expediente, respondiendo a las Tablas de Control de Acceso configuradas en el sistema.

2. El SGDEA debe permitir establecer niveles de seguridad del expediente de acuerdo con los niveles de seguridad establecidos por la entidad.

3. El SGDEA debe disponer de la búsqueda de información, parametrizado con base en la Tabla de Control de Acceso, instrumento archivístico en el cual se tiene definida la clasificación de acceso de cada serie documental (publica, confidencial y reservada) de acuerdo con lo establecido en la Ley 1712 de 2014 y aprobadas por el archivo general de la nación para que los usuarios autorizados y con permisos asignados, acceden a los documentos permitidos.

4. 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.

5. Todos los expedientes deberán contar con un índice electrónico, el cual debe ser firmado electrónicamente una vez se cierre el expediente.

6. Los SGDEA deben permitir como mínimo las siguientes acciones de disposición para cualquier regla de retención y disposición:

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

7. 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 auditoría.

8. 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.

9. 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:
    - Transferencias documentales primarias de acuerdo con lo establecido por el Archivo General de la Nación.

10. 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.

11. El SGDEA debe alertar y 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.

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

13. 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.

14. El SGDEA debe generar un acta de transferencia de forma automática, asignando un número de acta, fecha y lista expedientes transferidos.

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

16. 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.

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

18. 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).

19. 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.

20. 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.

21. El SGDEA debe permitir el cargue de los inventarios de archivo físico con código de carpeta, FUID y ubicación topográfica, este inventario se pueda actualizar mínimo una vez al mes y guardar el histórico.

22. El SGDEA debe permitir tener tableros de control de los inventarios cargados SGDEA no debe tener límite de peso para el cargue de inventario, y se debe poder cargar

uno o varios archivos

23. Debe permitir consultar, controlar y generar reportes de inventarios del archivo físico con ubicación topográfica del sitio de custodia.

24. El Sistema debe permitir a los usuarios autorizados realizar solicitudes de préstamos de carpeta o folios físicos que se encuentran en el archivo central, esta solicitud debe tener un # consecutivo, fecha de cumplimiento y estado de gestión. Si la información se requiere en imagen esta se podrá disponer en la misma solución para consulta del solicitante. Cuando la información solicitada se encuentra en préstamo se debe notificar al solicitante para que no deje crear solicitud.

25. Se debe generar notificación y/o alerta de devolución de préstamos de documentos físicos al usuario solicitante y al administrador del sistema, cuando se ha pasado los días autorizados de préstamo de documentos.

26. El SGDEA debe permitir al usuario solicitar la prórroga del préstamo sin crear una nueva solicitud.

27. Se debe poder consultar la trazabilidad de estas consultas y préstamos y generar reportes.

28. Permitir que los usuarios a través de la solución soliciten recolección de cajas de archivo para ser transferidas al archivo central y generar número de solicitud con fecha de cumplimiento.

Otros:

1. Debe permitir registrar el acuse de recibo de los envíos de las comunicaciones de salidas o respuestas a PQRS, en físico y electrónico, de manera manual y automática, utilizando servicios o consultas a bases de datos u otros sistemas.

2. Debe incluir un servicio de correo electrónico certificado para el envío de comunicaciones de salida.

3. Debe incluir el envío de las comunicaciones por correo electrónico, además de correo electrónico certificado según la necesidad de las áreas.

4. Debe contar con la funcionalidad para que en las comunicaciones de salida que se envíen por correo electrónico, el correo enviado quede como un archivo adjunto al radicado de salida.

5. Debe permitir registrar el resultado del envío de las comunicaciones de salida y para las que se envíen por correo electrónico el estado se debe actualizar automáticamente y permitir descargar un reporte de esta información.

3.2. ESPECIFICACIONES NO FUNCIONALES

a. El Oferente debe garantizar el detalle de recolección y/o levantamiento de requerimientos funcionales y no funcionales y una vez levantados bajo su entendimiento, contar con la aprobación de estos por las áreas usuarias y/ o funcionales de la Fiduprevisora.

3.3. ESPECIFICACIONES TÉCNICAS

3.3.1. Arquitectura

a. Es necesario que se cuente con una arquitectura basada en microservicios que permita facilitar las integraciones a través de servicios WEB REST full (APIs) a través del ESB Fuse de red hat APIs /WEB service REST o integraciones diferentes APIs propuestas por el proveedor o solicitadas por Fiduprevisora S.A.

b. Los artefactos que componen la solución deben estar claramente identificados.

c. Debe asegurar el cumplimiento de la normatividad vigente de seguridad y ciberseguridad y la que se llegue a expedir durante la implementación y prestación del servicio de la Superintendencia Financiera de Colombia - SFC.

d. Debe ser una solución SaaS (Software as a Service), el almacenamiento y usuarios debe ser ilimitado.

e. El proveedor debe mantener su solución actualizada y alineada con los cambios y necesidades del negocio en términos legales y normativos.

f. La arquitectura de la solución debe estar documentada.

g. La solución debe implementar mecanismos adecuados para interoperar con otros sistemas de interés de su dominio.

h. La solución debe ser autosuficiente para llevar a cabo las funciones y requisitos esperados de su dominio (Soporta IPv6 e IPv4, Es arquitectura operativa 64 bits.)

i. La solución debe implementar un diseño adaptativo – responsive.

j. La solución debe facilitar la operación y control del sistema por parte de los administradores y/o diseñadores.

k. La arquitectura de la solución debe estar basada en Web.

l. La solución debe tener flexibilidad en la ejecución de cambios e implementaciones, se debe adecuar a tiempos óptimos de implantación.

m. La solución debe ser compatible las últimas versiones de los diferentes navegadores web (Edge, Mozilla, Chrome, Safari).

n. La solución debe contar con representación en Colombia por cuenta propia o través de Partners y el soporte sobre la misma debe brindarse desde Colombia y ubicación en la cuidad de Bogotá.

o. Cuando se produzca un fallo del software o del Hardware, debe resultar posible devolver el sistema a un estado conocido (más reciente que la copia de seguridad del día anterior) en menos de 2 horas de trabajo con el hardware disponible.

3.3.2. Madurez de Software y de Hardware

a. La solución debe contar con herramientas de desarrollo low-code para implementar las funcionalidades requeridas.

b. La solución debe contar con componentes para agilizar el desarrollo y las integraciones del(os) producto(s).

c. La modalidad de distribución requerida Saas (Softwre as a Service), bajo suscripción por usuarios. Especificar el stack tecnológico de la solución (arquitectura referencia, arquitectura solución, patrones de diseño, lenguajes de programación por componentes y sus respectivas versiones).

d. Referir las herramientas para desarrollo de programas y software del sistema para controlar dispositivos, diagnóstico, corrección y optimización.

e. Se debe garantizar que se cuenta con el manejo de errores y excepciones de la solución.

f. Implementar mecanismos de validación de los contenidos gestionados para garantizar su fiabilidad.

g. La solución debe soportar la configuración de alta disponibilidad y redundancia con base en lo definido en la norma ISO 27031.

h. Permitir la administración de los parámetros y la integración con los aplicativos implementados en Fiduprevisora que se requieran para la generación y administración de los documentos

i. Permitir sin costo las actualizaciones de versión de la solución.

j. La solución debe ser intuitiva y fácil de usar por parte del usuario final.

k. La solución debe facilitar la operación y control del sistema por parte de los administradores.y/o diseñadores.

l. La solución debe favorecer la reutilización de componentes para aquellos requerimientos evolutivos dentro de las funcionalidades estándar.

m. La solución debe permitir el mantenimiento y evolución de las funcionalidades del sistema.

n. Implementar mecanismos para optimizar el rendimiento del sistema.

o. Implementar mecanismos para optimizar el uso de recursos.

p. Disponer de documentación en línea y herramientas para facilitar el soporte del sistema.

q. Debe garantizar validaciones y/o reglas de negocio para evitar fallas en data entries. La solución debe contar con un diseño o standard para user interfaces y accesibilidad.

r. Se debe contar con una metodología de desarrollo de Software conocida y avalada en el mercado, informar el nivel de madurez, tiempo de implementación y el proceso que permite garantizar la calidad de los desarrollos.

s. Se debe indicar cuál es el nivel de soporte, proceso, tiempos de respuesta. así mismo se debe presentar SLA's de soporte y mantenimiento.

t. Se debe contar con proceso para versionamiento del código fuente y la(s) herramienta(s) usadas para tal fin.

u. Se debe contar con manuales de usuario, técnicos y de arquitectura de la solución u otros de la aplicación.

v. Se debe garantizar que se cuente con diagramas de arquitectura de datos. Adicionalmente garantizar que se realiza gestión de metadatos para la indexación de la información.

w. Se deben especificar cuáles son las Bases de Datos y los motores de interacción habilitados para instalar la base de datos.

x. Se debe contar con estándares y protocolos REST bajo protocolo https para definir mensajería para el intercambio de información.

y. Se debe garantizar la alta disponibilidad de la plataforma con ANS de mínimo 99.97.

3.3.3. Interoperabilidad y Acoplamiento

a. Es necesario que se permitan diferentes tipos de integración.

b. Debe permitir la interoperabilidad a través de arquitectura orientada a servicios ofreciendo (Web Services) o consumiendo servicios web expuestos para generar y/o capturar, datos, documentos y otros mecanismos de interoperabilidad, gestionarlos de acuerdo con la necesidad de los procesos.

c. La solución debe contar con estándares de interoperabilidad que aseguren la debida función y aprovechamiento de esta.

d. Debe integrarse a los aplicativos implementados en la Entidad que se requiera.

e. Permitir y validar cambios de roles, responsabilidades y gobierno IT.

f. Debe ser flexible a nivel de conectividad, data integration, workflow, componentes arquitectónicos – Architect, en la solución se debe usar contenerización.

g. Debe contar con planes de implementación y migración estandarizados para cargar datos de otras plataformas.

h. Se debe contar con documentación de las APIs de integración tipo swagger.

i. Se debe contar con posibilidad de integración con bus de servicios.

j. Se debe permitir configuración de intercambio de información a través del manejo de SFTP - Protocolo de transferencia de archivos de forma segura, inclusive con servicios de encriptación de la información.

k. Se debe incluir una descripción detallada de los componentes y funciones de continuidad, recuperación ante desastres, alta disponibilidad, clustering, entre otros (DR y HA), Continuidad Infraestructura: Clustering para BD, "Farms" y balanceadores para servidores WEB, Enlaces redundantes para comunicaciones. Especificar la capacidad técnica de la contingencia (memoria, discos, redes, entre otros).

l. Se debe contar con esquema de Alta Disponibilidad y sistema de replicación en línea.

m. Se debe permitir ambientes físicos y lógicos independientes para prueba y desarrollo, preproducción y producción, mediante los cuales se realicen actividades de prueba, actualizaciones, capacitaciones y desarrollo de funcionalidades manera aislada e independiente, cumpliendo con medidas de seguridad para no comprometer ni divulgar la información crítica y/o sensible. Adicionalmente se debe contar con herramientas de montaje y/o replicación de estos ambientes.

n. El SGDEA debe implementar como mínimo la funcionalidad de los siguientes servicios:

- Servicio del sistema
- Servicio de usuarios y grupos
- Servicio de roles
- Servicio de radicación y registro
- Servicio de formatos y formularios
- Servicio de flujos de trabajo
- Servicios de trabajo colaborativo y gestión de documentos
- Servicios de Clasificación
- Servicios Documentos Archivo
- Servicio archivos físicos
- Servicios de Metadatos
- Servicios de retención y disposición documental
- Servicios para búsqueda y reportes
- Servicios de exportación.

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

p. 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

q. 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.

r. El SGDEA debe permitir integrarse con los sistemas de Gestión de contenido CMS (Content Management System) u otros análogos, haciendo uso del protocolo CMIS 1.1 (Content Management Interoperability Services") u otro protocolo estándar necesario.

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

t. El SGDEA debe permitir recibir la información de los parámetros de entrada y los datos de salida de los servicios de interoperabilidad que se realicen a través de SOAP.

u. (Para interoperabilidad con aplicaciones web legadas) y REST (para interoperabilidad con aplicaciones web actuales).

v. 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.

w. 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.

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

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

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

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

bb. 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.

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

dd. 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.

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

ff. 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

3.3.4. Escalabilidad

a. La solución debe permitir escalamiento de servicios o funcionalidades específicas de la plataforma.

b. Especificar modelo de escalabilidad para el front-end (Cloud). En caso de que el front-end llegue a su máxima capacidad, indicar adicionalmente cual es el proceso para aumentar esa capacidad o en caso de que este subutilizado como es el proceso para disminuir su capacidad y como se determina la afectación de costos.

c. Especificar modelo de escalabilidad de cache de datos en servidor de aplicación.

d. Uso de CDN (Distribución de contenido, manejo de archivos Excel, pdf, imágenes, Word).

e. Se debe indicar cuales proveedor(es) de tecnología (IBM, Google, AWS, Microsoft Azure, Oracle Cloud) pueden ser usados para la infraestructura. Detallar adicionalmente los servicios usados del proveedor.

f. Contar con el uso de clústeres, tanto en la capa de aplicación como en la capa de datos, para atender las peticiones.

g. Descomponer el sistema en microservicios desacoplados que puedan escalarse de manera independiente. Esto permite que las diferentes partes del sistema se adapten según la demanda sin afectar el conjunto.

h. El sistema debe tener escalabilidad horizontal y vertical para que pueda crecer en función de la demanda, tanto incrementando capacidad (vertical) como agregando más servidores (horizontal).

3.3.5. Seguridad de la Información y CoB

a. Se debe garantizar que se cuenta con autenticación contra el LDAP/Directorio Activo de la compañía.

b. Se debe contar con Informe de Vulnerabilidades y planes de remediación.

c. Se requiere contar con logs de auditoría, sobre cambios funcionales o cambios directamente en bases de datos.

d. El sistema debe tener la trazabilidad de todas las acciones que generen todos los usuarios en el sistema.

e. La solución debe permitir definir estructuras de datos y columnas a auditar sin afectar el rendimiento de la aplicación.

f. La solución debe permitir realizar activación o desactivación total o parcial de la auditoría.

g. La solución debe permitir la administración y control de las sesiones.

h. La solución no debe permitir realizar el guardado automático de contraseña.

i. La función de logout de la solución debe terminar completamente con la sesión o conexión asociada.

j. La función de logout de la solución debe estar disponible en todas las páginas protegidas por autenticación.

k. La solución 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.

l. Si una sesión fue establecida antes del login, la solución debe cerrar dicha sesión y establecer una nueva luego de un login exitoso.

m. La solución debe generar un nuevo identificador de sesión luego de cada re-autenticación.

n. La solución no debe permitir ingresos concurrentes con el mismo usuario.

o. Los controles de acceso en caso de falla de la solución deben actuar en forma segura.

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

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

r. La solución 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).

s. La solución debe permitir el acceso a los logs, solo a personal autorizado.

t. La solución deberá utilizar una rutina centralizada para todas las operaciones de login.

u. La solución no deberá guardar información sensible en logs, incluyendo detalles innecesarios del sistema.

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

w. La solución deberá registrar en un log todas las fallas de validación.

x. La solución deberá registrar en un log todos los intentos de autenticación, en particular los fallidos.

y. La solución deberá registrar en un log todas las fallas en los controles de acceso.

z. La solución deberá registrar en un log todos los intentos de conexión con tokens inválidos o vencidos.

aa. La solución deberá registrar en un log todas las excepciones del sistema.

bb. La solución deberá registrar en un log todas las funciones administrativas, incluyendo cambios en la configuración de seguridad.

cc. La solución deberá registrar en un log, todas las fallas de conexión.

dd. La solución deberá registrar en un log las fallas de los módulos criptográficos. (Si aplica).

ee. La solución deberá utilizar una función de hash para validar la integridad de los logs.

ff. La solución debe contar con un módulo para la administración de la seguridad del sistema.

gg. La solución debe contar con conexiones TLS para todo el contenido que requiera acceso autenticado y para todo otro tipo de información sensible.

hh. La solución debe proporcionar 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 de la solución propuesta deben correr sobre protocolos seguros https.

jj. La solución debe tener la funcionalidad que permita la administración centralizada de los sistemas de Seguridad y Auditoria.

kk. El proveedor debe suministrar la documentación que describa 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.

ll. La solución debe tener un mecanismo de control de acceso que permita asignación o denegación de privilegios solo al rol que cumple un usuario autorizado.

mm. La solución debe limitar las opciones de menú y submenú de cada uno de los usuarios que utilizan los sistemas de información de acuerdo al perfil.

nn. La solución debe generar informes que permitan visualizar los roles por aplicación, usuarios del sistema, privilegios de cada rol por opción, opciones con permisos por rol.

oo. Se debe garantizar que la aplicación está libre de vulnerabilidades de seguridad de la información, realizando pruebas de revisiones de código estático y dinámico, análisis de vulnerabilidades, ejercicios completos de Ethical Hacking e implementación de los planes de remediación, que mitiguen la materialización de las mismas. Debe ser como mínimo cada 6 meses, o con cada cambio significativo en la aplicación.

pp. Para los usuarios de la solución, se debe permitir trabajar en ambiente con single sign on y permitir la integración de manera nativa con las soluciones de manejo de identidad y

control de accesos., adicionalmente se debe facilitar el uso de conectores para la sincronización y aprovisionamiento automático de contraseñas, Identidad y accesos.

qq. El control de acceso a las diferentes funciones y operaciones de la solución debe estar basado en roles y perfiles de usuario.

rr. La solución debe permitir administrar el ciclo de vida de los perfiles (Creación, Modificación, y Eliminación), ofreciendo granularidad para definir los tipos de privilegios a conceder.

ss. Se deben crear distintos perfiles de administradores (ej.: creación de administradores de usuarios, administradores operativos, administrador de parámetros de seguridad, entre otros) y segregar sus funciones de manera independiente.

tt. La solución debe permitir configurar el tiempo de inactividad de una sesión de usuario.

uu. La función de logout de la solución debe terminar completamente con la sesión o conexión asociada.

vv. La solución debe sincronizar la fecha y hora sus rastros de auditoria con los del sistema operativo de la plataforma donde se ejecuta y permite la sincronización de los relojes con la Hora Colombiana (debe cumplir Superintendencia de industria y comercio)

ww. Se debe garantizar la integridad del log bloqueando la modificación de estos a través de las opciones de la aplicación.

xx. La solución debe permitir integración con sistema de correlación de Logs o Syslog Server (SIEM).

yy. La solución debe garantizar que no se almacena información confidencial de autenticación en los logs (Contraseñas, Hash o certificados).

zz. La solución debe soportar de manera nativa algoritmos de cifrамiento fuerte tales como: 3DES, AES-256, HASH (SHA-512), entre otros.

aaa. La solución no debe tener quemadas en su código las llaves o semillas usadas por los algoritmos de encriptación.

bbb. Dentro del soporte de la solución debe estar incluida la corrección de vulnerabilidades de nivel alto y medio que se encuentren al aplicativo sin costo adicional.

ccc. 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.

ddd. El oferente debe contar con planes de continuidad de negocio que aseguren la disponibilidad de la solución ante una interrupción de la operación de su infraestructura tecnológica.

eee. Permitir contar con procedimientos automáticos para copias de seguridad y restauración encaminados a realizar copias periódicas (diarias y mensuales) de seguridad de todos los elementos dentro del sistema (carpetas, documentos, metadatos, usuarios, roles, permisos, configuraciones específicas).

fff. Garantizar que las operaciones realizadas en la solución estén protegidas contra adulteración, supresión, ocultamiento y demás operaciones que atenten contra la autenticidad, integridad y disponibilidad de la información**.**

ggg. Se obliga a aceptar y a aplicar los lineamientos del sistema integrado de gestión para proveedores y contratistas (Matriz de requerimientos de seguridad de la información para la adquisición de bienes o servicios), publicados en el portal web del CONTRATANTE, en el enlace que se relaciona a continuación: https://www.fiduprevisora.com.co/contratacion-prov-2/ y darse a conocer por escrito o validación a solicitud del CONTRATANTE.

3.3.6. Autenticidad

a. 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.

b. Implementación de Firma electrónica que permita relacionar la identidad y/o autorización de un usuario para firmar documentos.

c. Implementación de Firma Digital bajo certificados seguros que garanticen la autenticidad e integridad, para la gestión y creación de documentos.

3.3.7. Fiabilidad

a. 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.

b. Cumple y presentará planes de contingencia y continuidad para garantizar la disponibilidad solicitada del 99.997 %.

c. 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. Se debe manejar una copia de seguridad de la solución en una ubicación geográfica distinta como plan de continuidad del negocio y como DRP

d. Debe Garantizar un plan de contingencia durante la vigencia del contrato que permita la continuidad de la prestación del Servicio en caso de presentarse anomalías y/o eventos disruptivos que afecten la operación.
e. Se debe mantener y evidenciar que se cuenta con controles y ejercicios de prueba de los planes de continuidad.

f. Contar con una evaluación de riesgos de eventos que afecten la continuidad del negocio.

g. 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).

h. Debe garantizar que el tiempo de inactividad no prevista del SGDEA, no debe superar las 10 horas al trimestre y 40 horas al año.

i. 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).

3.3.8. Usabilidad

a. Debe contar con manuales de usuario estructurados adecuadamente.

b. Debe integrar contenidos explicativos, ejemplos y todos aquellos elementos que ayuden al autoaprendizaje.

c. Debe presentar ayudas en línea para las funcionalidades del sistema, sistemas guiados de consulta y tooltips para campos descriptivos en los formularios.

d. Debe permitir atajos para las funcionalidades importantes.

e. 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.

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

g. 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.

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

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

j. 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.

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

l. 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

m. 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.

n. La solución debe tener herramientas de diseño, creación y lanzamiento de formularios sin realizar desarrollo de software.

3.3.9. Portabilidad

a. 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.

b. Las interfaces de usuarios deben 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.

c. 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

d. 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.

e. 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.

3.3.10. Administración de sesiones

a. El sistema no debe permitir realizar el guardado automático de contraseña.
b. La función de logout del sistema debe terminar completamente con la sesión o conexión asociada.

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

d. 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.

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

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

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

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

3.3.11. Administración de Logs

a. 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).

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

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

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

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

f. El sistema deberá registrar en un log todas las fallas de validación.

g. El sistema deberá registrar en un log todos los intentos de autenticación, en particular los fallidos.

h. El sistema deberá registrar en un log todos los intentos de conexión con tokens inválidos o vencidos.

i. El sistema deberá registrar en un log todas las excepciones del sistema.
j. El sistema deberá registrar en un log todas las funciones administrativas, incluyendo cambios en la configuración de seguridad.

k. El sistema deberá registrar en un log las fallas de los módulos criptográficos.

l. El sistema deberá utilizar una función de hash para validar la integridad de los logs.

m. Las copias de respaldo de los archivos LOGS, deben custodiarse en una estancia alterna.

3.3.12. Administración de Seguridad

a. contar con un módulo para la administración de la seguridad del sistema.

b. contar con conexiones TLS para todo el contenido que requiera acceso autenticado y para todo otro tipo de información sensible.

c. El sistema proporcionará una herramienta que haga parte del módulo de Seguridad y Auditoria que facilite el análisis de datos de acceso a las aplicaciones.

d. Los componentes del sistema propuesto deben correr sobre protocolos seguros https y se debe contar con certificado para el acceso HTTPS.

e. El sistema debe tener una administración centralizada de los sistemas de Seguridad y Auditoria.

f. 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 con sus funciones.

g. Autenticación contra el LDAP/Directorio Activo de la compañía con protocolos ADFS o SAML 2.0.

h. 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.

i. El sistema debe limitar las opciones de menú y submenú de cada uno de los usuarios que utilizan los sistemas de información de acuerdo con el perfil.

j. El sistema deberá generar informes que permitan visualizar los roles por aplicación, usuarios del sistema, privilegios de cada rol por opción, opciones con permisos por rol.

k. Asegurar el cumplimiento de la Circular Externa No. 005 de 2019 y Circular 029 de 2014 de la Superintendencia Financiera de Colombia y cumplimiento de la ley de protección

de datos personales (Ley 1581 de 2012, Decreto reglamentario 1377 de 2013 y demás normas que las adicionen, aclaren o modifiquen).

3.3.13. Continuidad de Servicio

a. El proveedor debe contar con los servidores alojados en un DATA CENTER con domicilio nacional o internacional que garantice alta disponibilidad 99.997%, confidencialidad y seguridad de la información.

b. 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.

c. El SGDEA debe permitir la parametrización de al menos una copia de seguridad en una data center geográficamente diferente del principal.

d. 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.

e. 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).

f. El SGDEA en caso de presentarse fallas durante la restauración de las copias de seguridad debe permitir notificar sobre el fallo y los detalles a través de un informe de este, para que el administrador tome las decisiones necesarias para subsanar los errores.

g. Posee y presentará junto a esta propuesta la arquitectura de la solución ofertada y la infraestructura que soporta la solución ofertada. La solución debe permitir generar los reportes y/o tableros de control de los procesos que se llevan a cabo en ella, de acuerdo con necesidades de la Entidad, para consulta o seguimiento.

3.3.14. Otros Tecnológicos

a. Cada vez que se realice una modificación o actualización de versiones, el sistema guardará una nueva versión sin eliminar las anteriores. Además, debe permitir que el administrador del sistema pueda seleccionar y trabajar con la versión más reciente.

b. Deben contar con un equipo de personas de prueba independiente del equipo de desarrollo.

c. Tenga las capacidades de un ECM y BPM sin requerir herramientas de terceros o integraciones.

d. Debe contar con plan de continuidad que permita retomar la operación en 3 horas y con una copia de seguridad reciente al día anterior.

e. Debe contar con plan de contingencia de preproducción, pruebas y desarrollo que permita retomar la operación en 3 horas y con una copia de seguridad reciente al día anterior.

f. El proveedor deberá incluir la suscripción de los usuarios requeridos por la entidad, estos usuarios deben corresponder a los activos y que se encuentre habilitados en el sistema, los usuarios que se encuentre inactivos no se deben contar como suscritos.

g. El sistema debe ofrecer tiempos de respuesta rápidos, optimizando tanto la base de datos como las consultas de servidor.

h. El oferente debe ser fabricante directo de la solución presentada para esta implementación o distribuidor autorizado, para lo cual debe presentar la certificación que lo acredite como tal, adjunta a la propuesta.

i. La solución debe permitir generar los reportes y/o tableros de control de los procesos que se llevan a cabo en ella, de acuerdo con necesidades de la Entidad, para consulta o seguimiento.

j. Implementar los módulos relacionales en este anexo en paralelo para lo cual, se revisará en la etapa de diseño con el oferente seleccionado.

k. Cumplir Anexo No. 15 de Niveles de Servicio.

3.4. OBLIGACIONES A CARGO DEL CONTRATISTA

1. Desarrollar todas las actividades necesarias para el cumplimiento del objeto del contrato.

2. Atender los requerimientos e instrucciones que realice el contratante sobre la solución ofrecida, a fin de cumplir con la implementación de los requerimientos funcionales de la fiduciaria

3. Brindar atención a los requerimientos bajo los parámetros establecidos.

4. Brindar soporte en reinstalaciones, capacitaciones y dudas puntuales de usuario sobre la herramienta, solución o aplicativo.

5. Cumplir con los acuerdos de niveles de servicio acordados con el contratante.

6. Mantener actualizada la Política de Seguridad de la Información y Ciberseguridad de conformidad con los marcos normativo en la gestión de seguridad de la información y ciberseguridad. Así mismo deberá compartir esta con Fiduprevisora cuando así lo requiera.

7. Mantener contractualmente con sus contratistas y/o trabajadores, obligaciones frente a la gestión de la seguridad de la información y ciberseguridad, y velar por su cumplimiento, garantizando verificaciones anuales.

8. Gestionar de una manera efectiva los riesgos asociados a la Seguridad de la Información y Ciberseguridad, usando marcos de referencia aceptados para la gestión de riesgos como ISO 27005 o ISO 31000.

9. Contar con sistema de gestión en seguridad de la información y Ciberseguridad o demostrar la implementación de buenas prácticas alineadas a marcos internacionales como la ISO 27001 y la ISO 27032.

10. Contar con procedimientos para la adecuada obtención, retención, procesamiento y disposición final de la información física y digital.

11. Contar con procedimientos para la gestión de incidentes en seguridad de la información y ciberseguridad, que permitan la detección oportuna, contención, tratamiento, cierre y apropiación de las lecciones aprendidas.

12. Implementar monitoreo permanente sobre su infraestructura, sistemas de información y procesos que permitan identificar posibles incidentes de seguridad de la información y ciberseguridad. (El Tercero debe monitorear su infraestructura)

13. Mantener revisión constante de sitios de fabricantes, proveedores y otras instituciones que puedan generar alertas tempranas sobre posibles incidentes de seguridad de la información y ciberseguridad para analizarlas e implementarlas en caso de ser necesario.

14. Diseñar indicadores de gestión que permitan observar la efectividad en la gestión de la seguridad de la información y la ciberseguridad.

15. Contar con roles y responsabilidades definidas en la gestión de la seguridad de la información y la Ciberseguridad, y hacer seguimiento constante de sus cumplimientos.

16. Contar con un diagrama de seguridad perimetral en el que se observen los diferentes dispositivos y su posición estratégica para asegurar la confidencialidad, integridad y disponibilidad de la información, en un modelo de defensa en profundidad.

17. Garantizar que todos los componentes de su infraestructura y sistemas de información dentro del alcance del presente contrato cuentan con protección contra malware y virus.

18. Contar con un procedimiento formal para gestionar parches y actualizaciones para todos los componentes de su infraestructura y sistemas de información dentro del alcance del presente contrato.

19. Gestionar vulnerabilidades técnicas sobre la infraestructura y los sistemas de información, con especial atención en los que se encuentran conectados a internet. Para esto deberá al menos una vez al año, realizar pruebas de hacking ético y deberá realizar análisis de vulnerabilidades al menos dos veces al año cuyos resultados deberán ser compartidos con Fiduprevisora.

20. Implementar un ciclo de desarrollo de software que contemple en todas sus etapas técnicas de desarrollo seguro para todos los módulos y sistemas de información del alcance del presente contrato.

21. Contar con un plan de capacitación y sensibilización para sus empleados, terceros y usuarios en temas relevantes sobre gestión de riesgos, seguridad de la información y ciberseguridad, y el manejo adecuado de eventos que puedan ser incidentes.

22. Contar con escenarios de materialización de ataques cibernéticos dentro de su plan de continuidad de negocio y recuperación ante desastres, y probarlos al menos una vez al año, cuya constancia deberá ser remitida a Fiduprevisora.

23. Analizar periódicamente la conveniencia de contar con pólizas de seguro para cubrir gastos derivados de incidentes de seguridad de la información y ciberseguridad

24. Realizar pruebas de recuperación de la información respaldada y al menos una vez por semestre realizar una prueba de recuperación total de las herramientas que administran la información del objeto del Contrato

25. Adoptar las recomendaciones efectuadas por el equipo de seguridad de la información con el propósito de mejorar las prácticas de seguridad adoptadas en desarrollo del objeto del Contrato suscrito con el mismo. En caso de que el proveedor no esté en capacidad de adoptar dichas recomendaciones, deberá indicar al Contratante esta situación.

26. Cumplir con los requisitos exigidos en la circular externa No 42 del 2012 de la Superintendencia Financiera de Colombia respecto a las políticas de tecnología, seguridad de la información, y las establecidas al interior de la Fiduciaria que le sean aplicables.

27. Permitir la práctica de auditorías que requiera realizar el CONTRATANTE sobre el grado de ejecución y cumplimiento del CONTRATO y de las obligaciones del CONTRATISTA, en cumplimento a la circular externa 042 de 2012 proferida por la Superintendencia Financiera y la norma ISO 27003.
28. Cumplir con el modelo de desarrollo de software de la Fiduprevisora o cualquier otro documento interno de la entidad que lo modifique, sustituya o adicione.

29. Mantener indemne al CONTRATANTE de cualquier daño o perjuicio originado durante la ejecución del CONTRATO y hasta su terminación.

30. Dar inmediato aviso al CONTRATANTE acerca de la ocurrencia de cualquier evento o circunstancia que altere el normal desarrollo y/o ejecución del CONTRATO o ponga en riesgo la confidencialidad, integridad o disponibilidad de la información.

31. Cumplir con las condiciones técnicas, jurídicas, económicas, financieras y comerciales exigidas para la solución exigida.

32. Presentar de manera oportuna la correspondiente factura para su respectivo pago.

33. Destinar el recurso humano ofertado en sitio, única y exclusivamente al desarrollo de los proyectos que surjan durante la ejecución del presente CONTRATO. En ningún momento el CONTRATISTA podrá destinarlos para adelantar labores propias de otros contratos suscritos por el proveedor.

34. Abstenerse de divulgar o hacer uso de la información que con ocasión de la ejecución del CONTRATO pueda conocer acerca de la gestión adelantada los negocios administrados o de cualquiera de los funcionarios del CONTRATANTE.

35. Las demás inherentes al contrato de conformidad con la Ley y al desarrollo del objeto contractual.

3.5. DURACIÓN ESTIMADA

El plazo estimado de ejecución es de 36 meses. Los cuales se componen de:

- Hasta 9 meses de implementación.
- Hasta 3 meses de estabilización.
- 24 meses de soporte y mantenimiento.

3.6. FORMA DE PAGO ESTIMADA

Fiduprevisora S.A. bajo ninguna circunstancia realizará pagos anticipados. El pago se estima que se realizará de la siguiente manera:

- Implementación: el pago se hará sobre el cumplimiento de cada hito que se defina.

- Soporte y mantenimiento realizará en mensualidades vencidas, de conformidad con los servicios efectivamente prestados, es decir, de los Módulos que se hayan pasado a producción y estén funcionando en su totalidad.

- Los pagos relacionados con la bolsa de horas, se realizará por demanda, previa aprobación de la supervisión del contrato.

Los pagos se realizarán previa certificación y aprobación por parte de los supervisores del contrato y la presentación de la factura o cuenta de cobro, acompañada del informe de actividades.

4. INFORMACIÓN ESPECÍFICA DE LA COTIZACIÓN

4.1. Forma de presentación de la Cotización

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.

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.

4.2. 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 2023.

4.3. 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.

5. 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.

En caso en que el servicio se encuentre exento o excluido del IVA, es pertinente informar las razones financieras, tributarias y/o jurídicas que así lo contemplen.

Costos de Implementación

Descripción	Valor Antes de IVA	IVA (En caso de aplicar)	Valor Total
Módulo de Ventanilla Única			
Módulo de Administración Documental			
Módulo de Servicio al Cliente y atención de PQRS			

Costos de Soporte y Mantenimiento:

Descripción	Unidad de Medida	Cantidad	Valor unitario Antes de IVA	IVA (En caso de aplicar)	Valor unitario IVA Incluido	Valor Total
Módulo de Ventanilla Única	Mes	24				
Módulo de Administración Documental	Mes	24				
Módulo de Servicio al Cliente y atención de PQRS	Mes	24				

Bolsa De Horas

Vigencia	Cantidad Horas Año	Valor unitario Antes de IVA	IVA (En caso de aplicar)	Valor unitario IVA Incluido	Valor Total
2026	500				
2027	700				
2028	500				

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.

FIDUPREVISORA S.A.

Elaboró: R. Álvarez - Profesional Inteligencia de Mercados.
Revisó: María José Barguil Borja - Directora de Contratos Empresa.
Revisó: Christian Ramiro Fandiño Riveros – Gerente de Adquisiciones & Contratos.
Aprobó: Angela María Forero Sánchez - Gerente de Gestión Documental