

**INVITACIÓN A COTIZAR No.014 DE 2023**

Objeto: Fiduprevisora S.A. está interesada en recibir cotizaciones para realizar la adopción e implementación de BPM (Business Process Management) y RPA (Robotic Process Automation) con un SAAS, que permita la optimización, automatización e integración de los procesos de la organización, interoperabilidad con los diferentes sistemas, canales de entrada y salida de información, para transformar la operación y los servicios de los clientes internos y externos en procesos más eficientes y eficaces que contribuyan con los objetivos estratégicos de la organización.

Apertura de la Invitación: 27 de abril de 2023.

Fecha límite para presentar observaciones: 4 de mayo de 2023 hasta las 17:00 pm.

Respuesta a Observaciones: 9 de mayo de 2023.

Recepción de Cotizaciones: 23 de mayo 2023 de 2023 hasta las 17:00 pm.

Área Responsable: Vicepresidencia de Transformación y Arquitectura Organizacional.

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/wp-content/uploads/2019/12/Protocolo-de-buenas-practicas-1.pdf>



1.5. Matriz Riesgos

N°	FUENTE	ETAPA	TIPO	DESCRIPCION	CONSECUENCIA DE LA OCURRENCIA DEL EVENTO	PROBABILIDAD	IMPACTO	VALORACION DEL RIESGO	CATEGORIA	A QUIEN SE LE ASIGNA
1	Interna	Planeación	Operacional	No contar con el presupuesto para la adquisición del bien y/o servicio	-No adquisición del bien y/o servicio -Demoras en el inicio 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. INFORMACIÓN PARA LA COTIZACIÓN.

2.1. ALCANCE

Realizar el diagnóstico y la planeación para la implementación de BPM y RPA en todos los procesos de Fiduprevisora S.A., además de la implementación de estas tecnologías en los procesos Planeación y Gestión Operativa, y Contabilidad e Impuestos que permitan su optimización, automatización e integración; orquestando los diferentes sistemas de información, las actividades que realizan los usuarios internos y externos, los canales de entrada y salida de información, ejecutar la extracción de datos y/o información a partir de documentos en diferentes formatos, fuentes de información y cualquier otro medio que se requiera en la implementación de BPM y RPA, de acuerdo a los elementos que intervienen en cada proceso; para eliminar actividades que no agregan valor, simplificando la ejecución de otras, reemplazando las tareas repetitivas con un robot, disminuyendo tiempo, costo y la probabilidad de cometer errores, mitigar el riesgo operativo, que facilite el control de los procesos, brinde la trazabilidad de las operaciones realizadas y suministre la información para la toma de decisiones basadas en datos.



Los procesos de Planeación y Gestión Operativa y Contabilidad e Impuestos se gestionan haciendo uso de los sistemas PeopleSoft, FLEXIFON, PORFIN, SGDEA (Sistema de Gestión Documental) Portales Bancarios, Páginas WEB, Correo electrónico, herramientas de escritorio y los que durante la ejecución del contrato el proveedor considere necesarias.

2.2. CONDICIONES PARA LA PRESTACIÓN DEL SERVICIO

La empresa interesada debe tener experiencia en la implementación de herramientas de BPM y RPA en el sector financiero colombiano o regional.

2.3. Diagnóstico y Planeación

- a. La empresa interesada debe entender el estado actual de los procesos, elaborar el diagnóstico y establecer una metodología y un plan de automatización para los 28 procesos de la Fiduprevisora.
- b. Debe presentar el presupuesto que se requiere para el plan propuesto, en el cual se indique cómo mínimo etapas, cronograma y descripción de actividades, entregables, volumetría y transaccionalidad, la infraestructura y demás recursos tecnológicos con sus especificaciones, equipo de trabajo, horas de desarrollo, licencias, sistemas, aplicaciones o tecnologías complementarias que sean necesarias para la automatización de los procesos, y demás componentes que se identifiquen a partir del diagnóstico realizado.
- c. Debe tener en cuenta todos los factores de los procesos: objetivos estratégicos, caracterización, entradas, salidas, requisitos de los clientes internos y externos, fuentes de información, sistemas propios y de externos, entregables, requisitos legales y demás elementos que hagan parte del proceso.
- d. Debe identificar y documentar los problemas y las oportunidades de mejora, presentar la propuesta de optimización y los beneficios que se tendrían en cada proceso con la automatización.
- e. Debe explicar para cada proceso en que partes se utilizaría BPM y RPA, además de proponer otras tecnologías que contribuyan a la automatización, optimización y efectividad del proceso.
- f. Debe elaborar y desarrollar un plan de gestión del cambio durante todo el proyecto que permita comunicar, sensibilizar y formar a la organización para adoptar una cultura de automatización, aceptar los nuevos procesos y el uso de robots.

2.4. Requerimientos Tecnológicos

2.4.1. 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. Debe garantizar manejo de estándares internacionales de integración para comunicación y/o interfaces con otros sistemas, bien sea internos y/o externos de la Fiduprevisora S.A.
- c. Los productos que componen la solución deben estar claramente identificados.
- d. Debe asegurar el cumplimiento de la circular 007 de 2018 de la Superintendencia Financiera de Colombia - SFC.
- e. Debe estar desarrollado en lenguajes recientes, estables y que tengan soporte con el fabricante.
- f. Debe ser una solución SaaS (Software as a Service) y con implementación en nube.
- g. El proveedor debe mantener su solución actualizada y alineada con los cambios y necesidades del negocio en términos legales y normativos.
- h. La arquitectura de la solución debe estar documentada.
- i. Debe ser compatible con protocolo IPV6 tanto en la configuración del software, hardware y dentro del funcionamiento del sistema. En caso de almacenar, referenciar enlaces o almacenamiento de direcciones físicas IP debe ser transparente la interacción para toda la plataforma y el sistema en general. El cambio de direccionamiento IPV4 a IPV6 no debe generar errores o mal funcionamiento del software y sus componentes y en caso de presentarse, los corregirá o solucionará inmediatamente.
- j. La solución debe implementar un diseño adaptativo – responsive.
- k. La solución debe facilitar la operación y control del sistema por parte de los administradores y/o diseñadores.
- l. La arquitectura de la solución debe estar basada en Web.
- m. La solución debe tener procesos de gestión de cambios debidamente documentados que permita realizar actualizaciones y mejoras.
- n. La solución debe ser compatible con los diferentes navegadores web (Edge, Mozilla, Chrome, Safari).
- o. La solución debe contar con representación y soporte técnico en Colombia por cuenta propia a través de Partners.



- p. 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.

2.4.2. Madurez de Software y de Hardware

- a. Se requiere contar con herramientas low-code para implementar las funcionalidades requeridas como crear flujos de trabajo (Workflow) coordinando interacciones entre personas, sistemas y datos, sin el uso de codificación.
- b. La solución SAAS debe incluir el costo de licenciamiento, infraestructura y actualizaciones por el tiempo que dure el contrato. (debe indicar como es el manejo del licenciamiento, derechos, vigencias, limitantes), indicar además las versiones de los lenguajes de programación usados en el producto; especificar las versiones de cada uno.
- c. Referir las herramientas para desarrollo de programas y software del sistema para controlar dispositivos, diagnóstico, corrección y optimización.
- d. Se debe garantizar que se cuenta con el manejo de errores y excepciones de la solución.
- e. La solución debe soportar la configuración de alta disponibilidad y redundancia con base en lo definido en la norma ISO 27031.
- f. El datacenter debe cumplir con certificación TIER III o superior, certificado por el Uptime Institute en construcción y operación o ICREA nivel IV o superior en construcción y operación, certificado por la International Computer Room Experts Association.
- g. Permitir las actualizaciones de versión de la solución.
- h. La solución debe favorecer la reutilización de componentes para aquellos requerimientos evolutivos dentro de las funcionalidades estándar.
- i. La solución debe permitir el mantenimiento y evolución de las funcionalidades del sistema.
- j. Implementar mecanismos para optimizar el rendimiento del sistema.
- k. Disponer de documentación en línea y herramientas para facilitar el soporte del sistema.
- l. El diseño de las interfases de usuario, portales y/o aplicaciones se debe personalizar de acuerdo con el manual de identidad corporativa vigente de la Fiduprevisora S.A; el cual se le entregará al contratista en el momento de inicio de la ejecución de las actividades.
- m. La disponibilidad de la infraestructura que soporta la solución debe ser 99.95% sin contar las ventanas de mantenimiento.



- n. Se debe contar con manuales de usuario, técnicos u otros de la aplicación.
- o. 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.
- p. Se deben especificar cuáles son las Bases de Datos y los motores de interacción habilitados para instalar la base de datos.
- q. Se debe contar con estándares y protocolos REST bajo protocolo https para definir mensajería.

2.4.3. Interoperabilidad y Acoplamiento

- a. 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.
- b. La solución debe contar con estándares de interoperabilidad que aseguren la debida función y aprovechamiento de la misma.
- c. Debe permitir utilizar HTTPS como protocolo de transporte de los mensajes generados y recibidos por los servicios.
- d. 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 (para interoperabilidad con aplicaciones web legadas) y REST (para interoperabilidad con aplicaciones web actuales).
- e. 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.
- f. Debe permitir que los servicios expuestos mediante el protocolo de mensajería SOAP, se utilizará el protocolo de descubrimiento estándar UDDI.
- g. Debe proveer el catálogo de los tipos de objetos, junto con sus atributos y tipos de dato de estos.
- h. Permitir y validar cambios de roles, responsabilidades y gobierno IT.
- i. Debe contar con planes de implementación y migración estandarizados para cargar datos de otras plataformas.
- j. Se debe contar con documentación de las APIs de integración.



- k. Se debe contar con posibilidad de integración con bus de servicios.
- l. 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.
- m. Se debe garantizar que se maneja integración con active directory (LDAP).
- n. Se debe contar con esquema de Alta Disponibilidad en la plataforma de servidores y bases de datos que soporta la solución y sistema de replicación en línea.
- o. 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).
- p. Se debe entregar las métricas de desempeño de la solución (Peticiones x segundo, conexiones concurrentes, conexiones simultaneas, sesiones activas simultaneas, mínimos y máximos de ancho de banda transaccional).
- q. Se debe disponer de entornos de desarrollo y pruebas, mediante los cuales se realicen actividades de prueba, actualizaciones, capacitaciones y desarrollo de funcionalidades de 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.
- r. 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 requieran.
- s. Las interfaces de usuario del sistema deben ser intuitivas, rápidas, ágiles, estéticas, autoajustable a las características de las pantallas en cuanto a tamaño y resolución.
- t. Debe soportar la concurrencia de usuarios y las peticiones a las diferentes funcionalidades sin sacrificar la disponibilidad del sistema en determinado momento.

2.4.4. Escalabilidad

- a. Debe ser escalable permitiendo aumentar la capacidad del sistema para ofrecer más servicios a un mayor número de usuarios sin degradar la calidad del servicio.
- b. La solución debe permitir escalamiento de servicios o funcionalidades específicas de la plataforma.
- c. Debe garantizar la alta disponibilidad mínimo un 99.95 estándar de los servicios SaaS.



- d. Se debe indicar cual es la capacidad de crecimiento anual y bajo que parámetros se define.
- e. Uso de CDN (Distribución de contenido, manejo de archivos Excel, pdf, imágenes, Word)
- f. 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.
- g. Describir y/o incluir los límites de crecimiento con base en la capacidad de la infraestructura.

2.4.5. Seguridad de la información y CoB

- a. Se debe garantizar que se cuenta con autenticación contra el LDAP/Directorio Activo de la compañía cuando los usuarios sean internos, cuando los usuarios sean externos se deben gestionar mediante el procedimiento establecido por la entidad.
- b. Se debe garantizar la ejecución de dos análisis de vulnerabilidades al año, así mismo gestionar la atención de vulnerabilidades detectadas antes del siguiente análisis.
- c. Se requiere contar con logs de auditoría, sobre cambios funcionales o cambios directamente en bases de datos e integrarlos con un servicio de SOC de Fiduprevisora.
- d. La solución debe permitir que se definan estructuras de datos y columnas a auditar sin afectar el rendimiento de la aplicación.
- e. La solución debe permitir realizar activación o desactivación total o parcial de la auditoría.
- f. La solución debe permitir la administración y control de las sesiones.
- g. La solución no debe permitir realizar el guardado automático de contraseñas.
- h. La función de logout de la solución debe terminar completamente con la sesión o conexión asociada.
- i. La función de logout de la solución debe estar disponible en todas las páginas protegidas por autenticación.
- j. 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, la cual debe ser parametrizable.
- k. Si una sesión fue establecida antes del login, la solución debe cerrar dicha sesión y establecer una nueva luego de un login exitoso.
- l. La solución debe generar un nuevo identificador de sesión luego de cada re-autenticación.



- m. La solución no debe permitir ingresos concurrentes con el mismo usuario.
- n. Denegar todos los accesos en caso de que la aplicación no pueda acceder a la información de configuración de seguridad.
- o. En la solución se debe restringir el acceso a información relevante de la configuración a usuarios no autorizados.
- p. 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)
- q. La solución debe permitir el acceso a los logs, solo a personal autorizado.
- r. Debe tener una interfaz centralizada para todas las operaciones de inicio de sesión.
- s. La solución no deberá guardar información sensible en logs, incluyendo detalles innecesarios del sistema.
- t. Asegurar que existen mecanismos para conducir un análisis de los logs.
- u. La solución deberá registrar en un log todas las fallas de validación, todos los intentos de autenticación, en particular los fallidos.
- v. La solución deberá registrar en un log todas las fallas en los controles de acceso y todos los intentos de conexión con tokens inválidos o vencidos.
- w. Para servicios expuestos fuera de la red de la entidad la solución debe permitir el uso de un segundo nivel de autenticación.
- x. La solución deberá registrar en un log todas las funciones administrativas, incluyendo cambios en la configuración de seguridad.
- y. La solución deberá registrar en un log, todas las fallas de conexión.
- z. La solución deberá registrar en un log las fallas de los módulos criptográficos. (Si aplica)
- aa. La solución deberá utilizar una función de hash para validar la integridad de los logs.
- bb. La solución debe contar con un módulo para la administración de la seguridad del sistema.
- cc. La solución debe contar con conexiones TLS para todo el contenido que requiera acceso autenticado y para todo otro tipo de información sensible.



- dd. Debe ser 100% web, es decir, accedido mediante protocolo de transferencia https y debe estar en la capacidad para operar con protocolo de comunicación SSL implementado.
- ee. 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.
- ff. El proveedor debe contar con 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.
- gg. 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.
- hh. La solución 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.
- ii. 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.
- jj. Se debe garantizar que la aplicación está libre de vulnerabilidades de seguridad de la información, análisis de vulnerabilidades, realizando ejercicios completos de Ethical Hacking para validar la posibilidad de aprovechamiento de estas, en el caso que se identifiquen.
- kk. 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.
- ll. El control de acceso a las diferentes funciones y operaciones de la solución debe estar basado en roles y perfiles de usuario.
- mm. 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.
- nn. 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.
- oo. 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).
- pp. Se debe garantizar la integridad del log bloqueando la modificación de estos a través de las opciones de la aplicación.



- qq. La solución debe permitir integración con sistema de correlación de Logs o Syslog Server (SIEM).
- rr. La solución debe garantizar que no se almacena información confidencial de autenticación en los logs (Contraseñas, Hash o certificados).
- ss. La solución debe soportar de manera nativa algoritmos de ciframiento fuerte tales como: 3DES, AES-256, HASH (SHA-512), entre otros.
- tt. La solución no debe tener quemadas en su código las claves o semillas usadas por los algoritmos de encriptación.
- uu. 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.
- vv. 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.
- ww. 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 (documentos, metadatos, usuarios, roles, permisos, configuraciones específicas).
- xx. 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.
- yy. Cuando se realicen procesos de importación o exportación de información, deberá realizarse a través de interfaces seguras y aplicar protocolos y mecanismos de seguridad.
- zz. El proveedor deberá estar en la capacidad de prestar soporte remoto para la herramienta por el tiempo de ejecución del contrato, este requisito no ocasionará costo adicional para la Entidad.
- aaa. Brindar un plan de soporte durante la ejecución del contrato que contemple el cumplimiento de los ANS, horario de servicio, cantidad de horas de soporte, cantidad de horas para la ejecución de desarrollos evolutivos o mejoras.
- bbb. Brindar soporte en reinstalaciones, capacitaciones de usuario sobre la herramienta para la Entidad (área funcional y área técnica) por el tiempo de ejecución del contrato.



2.5. Requerimientos No Funcionales

- a. Debe permitir la creación y administración de roles y permisos, además de parametrizar los accesos, permisos (consulta, modificación, control total, etc.), eliminación y suspensión que se requieran para los usuarios o grupos de usuarios de los flujos de trabajo.
- b. Debe permitir controlar los perfiles y roles de los usuarios que ejecutan o consultan los flujos, tareas, trazabilidad, parametrizar calendarios, tiempos de alertas y la generación de tareas o instancias.
- c. Debe registrar el log de cada actividad y contar con la disponibilidad para su consulta.
- d. No debe limitar el número de roles o grupos que se puedan configurar.
- e. Debe ofrecer opciones de configuración para asignar o eliminar roles a usuarios después de un período predefinido o programado automáticamente.
- f. Debe permitir a un rol administrador crear, parametrizar, administrar, actualizar y eliminar la ejecución de tareas y flujos de trabajo.
- g. Debe contar con roles diferentes a administrador que puedan ejecutar tareas y también reasignarlas, de acuerdo con las necesidades de los procesos
- h. Debe permitir la parametrización de reglas como generación de tareas a partir de instancias de espera, estados de tareas, flujo de proceso y validación de actividades.
- i. Debe permitir parametrizar la programación de tiempos para la ejecución de tareas de acuerdo con la necesidad del proceso
- j. Se requiere tener perfiles de consulta por roles de acuerdo con las necesidades de los procesos.
- k. Se debe contar con manuales de usuarios y administrador de los procesos construidos en BPM y tareas de RPA.
- l. Se debe contar con manuales técnicos del BPM y RPA.
- m. Se debe contar con videos tutoriales en los cuales se explique el manejo de estos sistemas y de la operación en la cual se implementaron.
- n. Debe presentar ayudas en línea para las funcionalidades del sistema, sistemas guiados de consulta y tooltips para campos descriptivos en los formularios.
- o. Debe tener contenidos explicativos, ejemplos y todos aquellos elementos que ayuden al



autoaprendizaje.

- p. 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 los diferentes módulos con los que cuente el BPM.
- q. Debe permitir atajos para las funcionalidades importantes.
- r. Debe proporcionar en todo momento al usuario final y al administrador funciones de uso fácil e intuitivo.
- s. 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.
- t. El sistema 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.
- u. Debe garantizar el uso de tipográfico y de colores basado en la imagen corporativa de la Fiduprevisora.
- v. Debe garantizar la flexibilidad a los cambios que se requieran hacer de manera ágil y que no impliquen cambios estructurales o de ajuste al código de la aplicación.
- w. Al finalizar el periodo de servicio de las herramientas el proveedor debe entregar a la entidad un repositorio con toda la información generada durante la ejecución del contrato.

2.6. Requerimientos Funcionales

Para atender la automatización e integración de los procesos Planeación y Gestión Operativa, y Contabilidad e Impuestos Cliente se tienen los siguientes requerimientos.

2.6.1. Transversales BPM y RPA

- a. El BPM y RPA debe contar con un cuadro de mando o tablero de control con gráficos y reportes del estado de la gestión por proceso, ANS, tareas, periodos de tiempo, roles o usuarios; los cuales se deben generar por roles que correspondan al proceso y deben ser parametrizables por rangos de fechas.
- b. Debe tener la funcionalidad de crear reglas de negocio y condiciones como parte del proceso de diseño y ejecución.
- c. Disponer de una función de integración con aplicaciones internas y externas, para recibir o enviar información por diferentes canales (páginas web, correos electrónicos u otros sistemas de información de la entidad etc.) y diferentes formatos.



- d. Debe permitir generar los reportes mínimo Excel y PDF.
- e. Debe generar alertas por proceso y por tareas según la necesidad de los procesos.
- f. Debe permitir detener un flujo de trabajo para cada proceso.

2.6.2. BPM

- a. Debe tener un entorno para modelar los procesos usando el estándar BPMN y un repositorio para almacenar los diagramas.
- b. Debe permitir diagramar y modelar flujos de trabajo y contar con un mecanismo de simulación para analizar los flujos de trabajo modelados; y que estas actividades puedan ser modelados por usuarios que no son técnicos, es decir, que no requiera programación.
- c. Debe tener herramientas de diseño y creación de formularios sin código.
- d. Las tareas deben permitir generar y/o cargar más de un documento, los cuales deben quedar asociados en el gestor documental con la TRD correspondiente, según la actividad del proceso al que pertenezca.
- e. Las tareas deben permitir generar documentos en herramientas de escritorio (Excel, Access, Word, PDF) utilizando plantillas y a partir de fuentes de información y/o información que se registre en las tareas, estos documentos deben quedar asociados en el gestor documental con la TRD correspondiente, según la actividad del proceso al que pertenezca.
- f. Las tareas deben mostrar información que se genera a través de los flujos, así como también la que reposa en bases de datos u otras fuentes y que es informativa para el usuario, de acuerdo con la necesidad cada tarea.
- g. Las tareas deben permitir que se registren datos los cuales debe quedar guardados en los sistemas de información que requiera el proceso; así como también, que la información que se va a registrar permita utilizar listas desplegables, varias opciones, casillas, abiertas con validación de datos, formatos, entre otros.
- h. Proporcionar una herramienta que permita la creación, edición / diseño de plantillas para generar documentos, de acuerdo con las necesidades que requieran los procesos automatizados.
- i. Debe contar con la lógica para hacer asignación masiva o individual de tareas de acuerdo con las reglas que requiere cada proceso (roles, balanceo de cargas, prioridad, fecha de vencimiento, en orden de llegada, complejidad, entre otros) de manera automática o manual.
- j. Debe generar un identificador único para cada flujo de trabajo y para cada tarea.
- k. Debe permitir crear flujo, tareas o formularios a partir de uno existente en la solución.



- l. Debe permitir a los usuarios realizar consultas y filtros de las tareas asignadas, por proceso, tipo de tarea, roles, fechas y estado (tareas y procesos), las cuales se deben poder exportar a Excel.
- m. Debe contar con la trazabilidad de las acciones realizadas para cada caso o flujo de trabajo (tareas realizadas, usuarios que las ejecutan, fechas de creación y terminación de las tareas, archivos cargados, información registrada etc), la cual se debe poder consultar.
- n. Debe contar con semáforos en cada una de las tareas de acuerdo con el vencimiento para que sean ejecutadas, así mismo, generar alertas en cada uno de los flujos de trabajo utilizando tiempos límite de ejecución que permitan realizar seguimiento y control.
- o. Debe permitir crear instancias a partir de servicios, tareas, formularios, páginas web, procesos programados y demás inputs que requieran los procesos.
- p. Debe convertir el formato de documentos de Word o Excel a PDF.
- q. Debe permitir la funcionalidad de firmas electrónicas o digitales y estampado cronológico dentro del flujo.
- r. Debe tener tareas en la que se generen comunicaciones u otras operaciones de manera masiva.

2.6.3. RPA

- a. El RPA debe poder realizar capturas de información y hacer el reconocimiento de caracteres ópticos (OCR) y reconocimiento inteligente de caracteres (ICR), código de barras y QR.
- b. Debe elaborar archivos y documentos de acuerdo con las especificaciones de cada tarea, los cuales deben tener la posibilidad de cargarse en una tarea del BPM, en el gestor documental u otro sistema interno o externo según el proceso, asociarse a uno o varios expedientes y/o generar un radicado en el gestor documental y/o ser enviados por correo electrónico.
- c. Debe elaborar archivos y documentos de acuerdo con las especificaciones de cada tarea, los cuales deben tener la posibilidad de realizar consultas y extraer información de sistemas internos, externos o páginas web.
- d. Debe tener la capacidad de transcribir información en formularios, bases de datos, plantillas y demás elementos que se requieran en los procesos.

2.7. ETAPAS

Para los dos (2) de los 28 procesos que se automatizarán (Planeación y Gestión Operativa, y Contabilidad e Impuestos), se deben desarrollar como mínimo las siguientes etapas y actividades:



2.7.1. ETAPA 1. ANÁLISIS Y DISEÑO:

- a. Analizar los procesos que se automatizarán, comprender el objetivo y alcance de los mismos; identificar y entender las entradas, salidas, actividades que se ejecutan, sistemas y/o documentos fuente información, proveedores y clientes (interno y externo), roles, resultado esperado y demás elementos que intervengan para cumplir con los objetivos.
- b. Establecer cuáles son los datos y documentos que requieren y se generan en cada una de las actividades de los procesos a intervenir, las fuentes de información, las estrategias o procedimientos para lograr la captura o exportación de estos.
- c. Capacitar a los usuarios de los procesos que se van a intervenir, para que comprendan los beneficios y alcance que tiene la implementación de las herramientas BPM y RPA.
- d. Levantar información, realizar entrevistas con los usuarios funcionales, construir épicas e historias de usuario, entender el paso a paso de cada actividad y recopilar los requerimientos funcionales y no funcionales de cada proceso.
- e. Modelar en la notación BPMN el TO-BE de los procesos.
- f. Diseñar el proceso para carga de datos.
- g. Elaborar el diseño de las pantallas y formularios que se utilizaran en el flujo de cada proceso.
- h. Establecer las fases que se requieren para el desarrollo e implementación, el plan de actividades, riesgos asociados, la metodología que se va a utilizar debe ser AGIL con entregas continuas y la hoja de ruta de los procesos a impactar, los factores críticos, la capacidad técnica y organizacional con la que se cuenta.
- i. Definir reglas de negocio, los roles y perfiles de los usuarios de acuerdo con el TO-BE de los procesos modelados.
- j. Diseñar los KPIs y los reportes requeridos para el seguimiento y control de los procesos de acuerdo con la información capturada durante la ejecución de los procesos.
- k. Establecer la arquitectura de la solución y el modelo de datos.
- l. Identificar y diseñar las integraciones y servicios que se requiera para la interoperabilidad y ejecución de procesos.
- m. Documento tipo informe con el análisis, metodología a utilizar y las recomendaciones de los procesos objeto de automatización. Además, debe contener las actividades realizadas, los diseños, la hoja de ruta para el desarrollo y la implementación y todos los diagramas en BPMN y workflow para RPA realizados.

**2.7.2. ETAPA 2 DESARROLLO:**

- a. Realizar el desarrollo del TO-BE de los procedimientos diseñados para implementar BPM junto con las pantallas, formularios, modelo de datos, parámetros y demás elementos establecidos para su correcto funcionamiento.
- b. Realizar el desarrollo de flujos, pantallas, formularios y demás elementos de cada uno de los procedimientos diseñados.
- c. Realizar los desarrollos que se requieran para la extracción de datos o información para las tareas del BPM y/o ejecución de RPA; a partir de archivos, documentos, fuentes de información, formularios, página web y cualquier otro medio.
- d. Realizar los desarrollos y pruebas de las tareas que se ejecutaran con RPA y que se integren con el BPM y/u otros sistemas.
- e. Desarrollar y probar los procesos de carga de datos.
- f. Desarrollar y probar los servicios que se requieran para el funcionamiento de BPM y RPA que permitan la interoperabilidad con los demás sistemas de la organización.
- g. Desarrollar y probar los procesos de la transferencia de documentos y datos con los sistemas que interactúa cada proceso.
- h. Desarrollar y probar los reportes de los KPIs definidos y los reportes para el seguimiento y control de la operación.
- i. Configurar los perfiles en cada herramienta, de acuerdo con los roles definidos para la ejecución y seguimiento de cada proceso, así como también los roles de administración.
- j. Realizar pruebas y ajustes necesarios a los desarrollos, de acuerdo con las especificaciones y entregables establecidos en cada proceso.
- k. Realizar pruebas de recorrido, de carga y stress.
- l. Realizar pruebas calidad, regresión e integrales que aseguren la ejecución end to end de los procesos automatizados.
- m. La ejecución de las pruebas integrales se debe realizar por parte del equipo del área funcional que designe la Fiduprevisora, con el acompañamiento del equipo que designe la empresa contratante, el cual deberá tener el conocimiento y dominio de la solución que se va a probar.

2.7.3. ETAPA 3 IMPLEMENTACIÓN:

- a. Implementar los desarrollos y servicios en ambientes de producción que se requieran para el correcto funcionamiento de los procesos en los cuales se haya definido utilizar BPM y/o RPA.



- b. Puesta en funcionamiento en ambientes de producción de los procesos a los cuales se les implementan las herramientas BPM y/o RPA, con los KPI, reportes y consultas para el seguimiento y control de los procesos.
- c. Implementar y ejecutar la carga de datos de acuerdo con las necesidades de los procesos y/o actividades implementadas.
- d. Realizar actividades y procesos de sensibilización y adopción de la herramienta BPM y/o RPA.
- e. Capacitaciones a los usuarios de los procesos en los cuales se implementó BPM y/o RPA.
- f. Ajustes o correcciones para la estabilización de los procesos en los cuales se implementó BPM y/o RPA.
- g. Realizar retroalimentación y elaboración del documento final que contenga de forma clara la descripción de los procesos o tareas realizadas y un resumen de la gestión e implementación realizada durante esta etapa.
- h. Brindar soporte durante la estabilización de cada proceso.

2.8. Equipo Mínimo de Trabajo y Certificaciones

Se requiere de un equipo de trabajo con experiencia preferiblemente en el sector financiero durante el desarrollo del proyecto con al menos los siguientes perfiles.

Un (1) Gerente de Proyecto debe tener como mínimo cuatro (4) años de experiencia como director y/o coordinador y/o gerente y/o roles similares de gerencia y/o dirección de proyectos, en temas relacionados con el objeto del contrato; así mismo deben contar con título profesional en áreas administrativas, económicas, Ingenierías o afines y título de postgrado mínimo en la modalidad de especialización relacionado con proyectos.

Un (1) Arquitecto de procesos BPM debe tener como mínimo cinco (5) años de experiencia liderando procesos de transformación digital y automatización de procesos; así mismo deben contar con título profesional en áreas administrativas, Ingenierías o afines y título de postgrado mínimo en la modalidad de especialización relacionado con arquitectura empresarial y procesos.

Dos (2) Analistas de Procesos y requerimientos deben tener como mínimo tres (3) años de experiencia en actividades de levantamiento, análisis, diseño, optimización y documentación de procesos y especificación con BPMN 2.0, construir los documentos de requerimientos, casos de uso o historias de usuario, elaboración de manuales; así mismo deben contar con título profesional en áreas administrativas, Ingenierías o afines y diplomado o certificación relacionada con ingeniería de procesos o BPM y RPA

Un (1) Experto en Gestión del Cambio debe tener como mínimo cinco (5) años de experiencia como consultor en temas relacionados con el cambio, gestión del conocimiento o roles similares para la implementación de procesos de transformación; así mismo deben contar con título profesional en



áreas administrativas, Ingenierías, ciencias sociales o afines y con mínimo un postgrado y/o especialización y/o certificación relacionada con modelos de gestión del cambio o desarrollo organizacional.

Un (1) Líder Técnico debe tener como mínimo cinco (5) años de experiencia en arquitectura de soluciones, liderando equipos de desarrollo y procesos de implementación de BPM y RPA; así mismo deben contar con título profesional en Ingeniería de Sistema o afines y título de postgrado mínimo en la modalidad de especialización y/o certificación relacionada con arquitectura y desarrollo de software.

Dos (2) Desarrolladores Fullstack deben tener como mínimo tres (3) años de experiencia en APIs, bases de datos, servicios, BPM y RPA, y lenguajes de programación relacionados con estos sistemas; así mismo deben contar con título profesional en Ingeniería de Sistema o afines y con mínimo un postgrado y/o especialización y/o certificación relacionada con desarrollo de sistemas de BPM y RPA.

La empresa interesada debe indicar las certificaciones vigentes con las que cuenta el equipo de trabajo y la empresa que estén relacionadas con el objeto a cotizar, junto con el ente certificador como se muestra en el siguiente ejemplo:

Certificación	Ente certificador	Perfil del equipo mínimo (si aplica)	Oferente)
Certified Business Process Professional (CBPP)	Association of Business Process Management Professionals International (ABPMP)		
BPM2 Business Advanced	Object Management Group (OMG)		
Certified RPA Specialist	Arcitura.	Un desarrollador	
Certified RPA Professional	Automation Anywhere University	Dos desarrolladores	
Certified SOA Professional	Arcitura		
Certified SOA Architect	Arcitura		
TOGAF 9.2	The Open Group	Un arquitecto de proceso	
Scrum Máster Certified	ScrumStudy	Un analista de proceso	
Product Owner Certified	ScrumStudy	Un analista de proceso	
ISO/IEC 9001	ICONTEC		Certificado vigente
ISO/IEC 27001	ICONTEC		Certificado vigente
ISO/IEC 27031	ICONTEC		
Otras (indicar cuales)			



Las certificaciones y entes certificadores que se relacionan son a manera de ejemplo, por lo que el oferente puede relacionar otras, siempre y cuando estén vigentes, se relacionen con el objeto a contratar y se demuestren en el momento que se requieran.

2.9. DURACIÓN ESTIMADA.

La empresa interesada debe cotizar el servicio para:

- Diagnóstico, planeación e Implementación hasta 6 meses.
- Estabilización hasta 3 meses.
- Garantía mínimo 3 meses luego de la fase de implementación y estabilización.
- Soporte 6, 12, 24 y 36 meses.
- Costos de desarrollos evolutivos por hora.

2.10. FORMA DE PAGO ESTIMADA.

Fiduprevisora S.A. bajo ninguna circunstancia realizará anticipos o pagos anticipados, el pago se estima que se realizará un primer pago del 50% contra la definición de requerimientos y otro 50% al finalizar la implementación.

3. INFORMACIÓN ESPECÍFICA DE LA COTIZACIÓN.

3.1. Forma de presentación de la Cotización

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

3.2. Documentos de carácter jurídico y financiero

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

- I. Certificado de Representación Legal con fecha de expedición no mayor a 30 días calendario.
- II. Registro Único Tributario – RUT.
- III. Estados Financieros con corte a diciembre de 2022.

3.3. Experiencia Específica

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



No	EMPRESA O ENTIDAD	OBJETO	FECHA INICIO	FECHA FIN	VALOR TOTAL EJECUTADO EN SMMLV INCLUIDO IVA
1					
2					
3					

Nota* se recomienda que preferiblemente la experiencia relacionada no sea superior a 5 años respecto de la actual vigencia y debe estar relacionada con el sector financiero.

4. VALOR DE LA COTIZACIÓN

El valor de la cotización debe estar en pesos colombianos, debe incluir vigencia, IVA y demás impuestos a los que haya lugar, así como costos directos e indirectos.

DIAGNÓSTICO, PLANEACIÓN E IMPLEMENTACIÓN

DESCRIPCIÓN	VALOR ANTES DE IVA	IVA (En caso de aplicar)	VALOR TOTAL
Diagnóstico y Planeación (28 Procesos)			
Implementación (2 procesos) (Debe incluir las licencias de Acceso)			

SOPORTE Y MANTENIMIENTO

Tenga en cuenta que el valor que aquí se registre debe considerar la prestación del servicio 7X24.

DESCRIPCIÓN	VALOR UNITARIO POR MES	IVA (En caso de aplicar)	VALOR TOTAL
Soporte para 6 meses			
Soporte para 12 meses			
Soporte para 24 meses			
Soporte para 36 meses			

DESARROLLOS EVOLUTIVOS

Para el caso de desarrollos evolutivos el oferente deberá presentar los valores hora, de acuerdo con el recurso en la siguiente tabla:



DESCRIPCIÓN	Valor Hora Antes de IVA	IVA En caso de aplicar	Valor Total Hora
Hora hombre (Como referencia para desarrollos Evolutivos)			

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: Vanessa Gallego Peláez – Gerente de Adquisiciones & Contratos.

Aprobó: Osvaldo Rafael Puello Flórez – Gerente de Innovación y Desarrollo.

Aprobó: Katty Eljach Martínez – Vicepresidencia de Transformación y Arquitectura Organizacional.

“Defensoría del Consumidor Financiero: Dr. JOSÉ FEDERICO USTÁRIZ GÓNZALEZ. Carrera 11 A No 96-51 - Oficina 203, Edificio Oficity en la ciudad de Bogotá D.C. PBX 6108161 / 6108164, Fax: Ext. 500. E-mail: defensoriafiduprevisora@ustarizabogados.com de 8:00 am - 6:00 pm, lunes a viernes en jornada continua”.

Las funciones del Defensor del Consumidor son: Dar trámite a las quejas contra las entidades vigiladas en forma objetiva y gratuita. Ser vocero de los consumidores financieros ante la institución. Usted puede formular sus quejas contra la entidad con destino al Defensor del Consumidor en cualquiera agencia, sucursal, oficina de corresponsalia u oficina de atención al público de la entidad, asimismo tiene la posibilidad de dirigirse al Defensor con el ánimo de que éste formule recomendaciones y propuestas en aquellos aspectos que puedan favorecer las buenas relaciones entre la Fiduciaria y sus Consumidores. Para la presentación de quejas ante el Defensor del Consumidor no se exige ninguna formalidad, se sugiere que la misma contenga como mínimo los siguientes datos del reclamante: 1. Nombres y apellidos completos 2. Identificación 3. Domicilio (dirección y ciudad) 4. Descripción de los hechos y/o derechos que considere que le han sido vulnerados. De igual forma puede hacer uso del App “Defensoría del Consumidor Financiero” disponible para su descarga desde cualquier smartphone, por Play Store o por App Store.