INVITACIÓN A COTIZAR No. 027 DE 2023

Objeto: Fiduprevisora S.A. está interesada en recibir cotizaciones para implementar una herramienta que permita automatizar la fase precontractual y contractual de los diferentes negocios que se gestionan en la Vicepresidencia de Contratación Derivada.

Apertura de la Invitación: 10 de octubre de 2023.

Fecha límite para presentar observaciones: 13 de octubre de 2023 hasta las 18:00 pm.

Respuesta a Observaciones: 18 de octubre de 2023.

Recepción de Cotizaciones: 24 de octubre de 2023 hasta las 18:00 pm.

Áreas Responsables: Vicepresidencia de Contratación Derivada.

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

1.6. ALCANCE

Contar con una solución que permita gestionar los trámites relacionados con la etapa pre contractual y contractual por parte del cliente y de la Fiduprevisora, buscando centralizar y automatizar los trámites de los diferentes negocios que se gestionan en la Vicepresidencia de Contratación Derivada.

1.7. ESPECIFICACIONES TÉCNICAS DEL BIEN O SERVICIO

ESPECIFICACIONES FUNCIONALES

El Sistema debe obedecer a una plataforma transaccional que permita a los clientes de la Fiduprevisora el cargue y diligenciamiento de la información necesaria para la contratación de las necesidades del cliente, a su vez, el Sistema debe permitir por parte de la Fiduprevisora, la gestión de dicha documentación para la elaboración de los procesos contractuales y de todos los documentos que se generan con ocasión de la actividad contractual.

El Sistema deberá desarrollar diversos módulos, cuyos servicios se diferencien por los usuarios que pretenden acceder al mismo, tal y como se explica a continuación:

Módulo del Cliente: Permitirá que el cliente desde su usuario pueda elegir y crear la tipología de la necesidad que pretende satisfacer, en ese sentido, una vez validado el ingreso del cliente a través del usuario y contraseña, se desplegarán los servicios que tiene disponibles (Ejemplo: Contrato de obra, contrato de interventoría, orden de prestación de servicios, convenio, ratificación). Para cada uno de ellos, se adjuntará un check list de la información que se requiere para crear la necesidad, identificando cuáles campos son de obligatorio diligenciamiento (Ejemplo: la Instrucción, el objeto, el plazo, el valor, las partes, lugar de ejecución, fondo del que se deriva la contratación, certificado de disponibilidad presupuestal - cdp). Parte de la información descrita, deberá ser diligenciada en campo de texto, y otro tanto, deberá ser cargado como documentos anexos.

Una vez diligenciada la totalidad de la información por parte del Cliente, el sistema creará el trámite, generando un numero de instrucción, y notificará a la Fiduprevisora sobre la existencia del trámite.

Módulo de Fiduprevisora: La Fiduprevisora, ingresará con el rol de asignación (perteneciente a la Vicepresidencia de Contratación Derivada, en adelante VCD). Dicho Rol encontrará en un tablero de control la totalidad de los trámites creados, identificando las tipologías por colores, y para cada trámite tendrá la opción de asignar el trámite, para lo cual, contará con un listado de usuarios de abogados de la VCD. Una vez asignado el trámite al abogado, cambiará de estado (asignado), lo cual será notificado al correo del abogado a quien le corresponderá continuar con el trámite.

Al ingresar al Sistema con el rol de abogado, dicho rol encontrará en su carpeta la totalidad de los trámites asignados, y al ingresar al número del trámite encontrará la documentación diligenciada por el cliente, efectuará una revisión jurídica de la información y tendrá habilitadas dos opciones: (i) elaboración de la minuta; (ii) devolución del trámite al cliente para subsanar o completar información.

Es importante advertir, que, para la elaboración de la minuta del contrato, debe permitirse que el Sistema migre información que previamente ha diligenciado el cliente.

El usuario abogado, firmará el documento, y para el efecto, se consignará en la firma, el nombre del abogado, la fecha y hora de firma.

Tras la firma por parte del rol de abogado, la minuta será enviada al rol revisor. Dicho rol, tendrá disponible la totalidad de los trámites que correspondan a su área, y en cada número de trámite tendrá disponible la totalidad de la información asociada al mismo. Dicho rol, tendrá disponible cinco opciones: (i) firmar, (ii) devolver al abogado para ajustes, (iii) devolver al abogado aprobado para firma de cliente derivado, (iv) reasignar a otro abogado, (v) subsanar. La firma del documento, consignará el nombre del revisor, la fecha y hora de firma. Al volver aprobado al abogado para remitir para firma al cliente derivado, el Sistema debe suministrar un mecanismo para compartir la minuta al cliente derivado para firma.

Tras la firma por parte del rol de revisor, el trámite será enviado rol Director. Dicho rol, tendrá disponible la totalidad de los trámites que remitan los revisores, y en cada número de trámite tendrá disponible la totalidad de la información asociada al mismo. Dicho rol, tendrá disponible tres opciones: (i) firmar, (ii) devolver al revisor, (iv) subsanar. La firma del documento consignará el nombre del director, la fecha y hora de firma.

Una vez aprobado el trámite por parte del Director, se asignará al rol VCD, quien tendrá disponible la totalidad de los trámites que remita el Director, y en cada número de trámite tendrá disponible la totalidad de la información asociada al mismo. Únicamente se habilitará la opción de firma del documento, en tanto el Sistema válide la existencia de certificación SARLAFT para dicho trámite. Dicho rol, tendrá disponible tres opciones: (i) firmar, (ii) devolver al Director, (iv) subsanar. La firma del documento consignará el nombre del VCD, la fecha y hora de firma. Con la firma del VCD, el estado del trámite pasará a identificarse como perfeccionado por las partes.

El documento firmado, deberá ser remitido al Rol Notificador, para que se remita el documento perfeccionado al correo del cliente derivado. En dicho correo se requerirá la expedición de garantías y se indicará el link para el cargue de la información correspondiente a la póliza.

El cliente derivado cargará la póliza, lo cual será notificado al rol de asignación, quien se encargará de asignar la revisión de garantías al rol abogado, y se surtirán los pasos descritos previamente. Sin embargo, en este trámite no se generará una minuta, sino un acta de aprobación de garantía; con lo cual, el trámite variará al estado “legalizado”; y será remitido al cliente para la correspondiente suscripción de acta de inicio del contrato.

El sistema debe permitir:

1. Contar con una ventanilla única en la cual se radicarán las instrucciones emitidas por parte de los fideicomitentes, dicha ventanilla debe contar con la autenticación de usuario y contraseña desde diferentes roles de los clientes.

2. El sistema debe contar con las siguientes opciones:

a. Cargue de información de forma individual o masiva.

b. El cargue de la información por parte del cliente, tendrá algunos campos de diligenciamiento obligatorio, y otros campos, que debe permitir la transcripción de texto.

c. Eliminación o actualización de documentos.

d. El sistema debe permitir el uso de correo electrónico o celular como medio de notificación de las acciones que se realizan en el flujo.

e. Tablero de control para verificar el estado de los trámites (debe permitir identificar los tiempos por tareas asignadas, el número de trámites por usuarios, y alertar por vencimiento de tareas).

f. El tablero de control debe contener colorimetría para las distintas tareas asignadas a los usuarios.

g. Contar con un super-usuario, el cual será único, para el seguimiento y detalle de todas las tareas, el cual estará a cargo de la Fiduprevisora.

h. Debe contar con usuarios de consulta para que los clientes puedan identificar en qué estado se encuentra su trámite.

i. El sistema debe permitir notificar de en tiempo real y de manera automática el estado de los trámites a los terceros interesados.

j. El sistema debe permitir la gestión de alertas relacionadas con los trámites.

k. El sistema debe permitir almacenar la información precontractual de cada uno de los trámites de manera independiente.

l. El sistema debe permitir la creación de diferentes tipologías de contratos, y cada uno de ellos tendrá un flujo de información obligatoria diferente.

m. El sistema debe permitir asignar responsables a los trámites (coordinador, abogado, oficial de cumplimiento, vicepresidente, cliente).

n. El sistema debe permitir, a partir de plantillas precargadas, la elaboración de minutas de contrato (incluyendo la data que se carga cuando se crea el trámite).

o. El sistema debe permitir un mecanismo de firma segura, a través de un mecanismo de autenticación de uno o más pasos vías de la minuta del contrato por parte del tercero y de la entidad. En esta firma se deben identificar todas las personas involucradas en el proceso de elaboración del contrato.

p. El sistema debe permitir la interoperabilidad con el sistema encargado de la validación SARLAFT del tercero. Una vez efectuada dicha validación, debe alertar a los usuarios.

q. La validación del SARLAFT, deberá ser un requisito para permitir la firma del contrato por parte del rol vicepresidente.

r. El sistema debe permitir a partir de plantillas la elaboración del acta de inicio del contrato.

s. El sistema debe permitirla transferencia de documentación precontractual y el expediente precontractual al sistema de gestión contractual.

t. El sistema debe permitir la creación de radicados en el sistema de Gestión Documental de la entidad a través de una integración.

u. El sistema debe permitir por lo menos 600 trámites mensuales.

v. El sistema debe permitir copiar y pegar en cualquier campo.

w. El sistema debe permitir la parametrización del número de caracteres de acuerdo con la necesidad del cliente.

ESPECIFICACIONES TÉCNICAS

i. Arquitectura

• Contar 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.

• Garantizar manejo de estándares internacionales de integración como Asobancaria aplicable para este tipo de desarrollos, para comunicación y/o interfaces con otros sistemas, bien sea internos y/o externos. Las integraciones que llegasen a construirse entre aplicativos para este objetivo deberán serán propiedad de Fiduprevisora una vez finalizado su desarrollo y/o contrato.

• Debe asegurar el cumplimiento de la circular 007 de 2018 de la Superintendencia Financiera de Colombia - SFC.

• Debe estar desarrollado en lenguajes de última generación y que tengan soporte con el fabricante.

• Debe ser una solución SaaS (Software as a Service).

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

• La arquitectura de la solución debe estar documentada.

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

• 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.)

• La solución debe implementar un diseño adaptativo – responsive.

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

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

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

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

• 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.

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

ii. Madurez de Software y de Hardware.

• Contar con componentes para agilizar el desarrollo y las integraciones del(os) producto(s).

• 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).

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

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

• Implementar mecanismos de validación de los contenidos gestionados para garantizar su fiabilidad

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

• Permitir las actualizaciones de versión de la solución.

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

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

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

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

• Implementar mecanismos para optimizar el rendimiento del sistema.

• Implementar mecanismos para optimizar el uso de recursos.

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

• 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.
• Se debe contar con una metodología clara de desarrollo de Sw.

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

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

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

• Es necesario que se especifique, cual es el módulo o esquema para cumplir los requerimientos regulatorios, así mismo se debe indicar si los ajustes normativos a la solución están a cargo del proveedor o del cliente.

• 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.

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

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

• Se debe garantizar la alta disponibilidad de la plataforma con ANS de mínimo 99.96.

iii. Interoperabilidad y Acoplamiento

• Es necesario que se permitan diferentes tipos de integración.

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

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

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

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

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

• 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.

• 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).

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

• 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).

• Se debe permitir entornos de prueba, desarrollo y preproducción, 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.

iv. Escalabilidad

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

• La solución debe permitir el particionado de los datos para optimizar la eficiencia del sistema.

• 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.

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

• Especificar modelo de escalabilidad de base de datos (SQL - NoSQL), Reutilización de conexiones a BD, compresión, paralelización de procesos, para mejorar el rendimiento de la transaccionalidad.

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

• 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.

• Se debe contar en la solución con algún proceso para realizar escalamiento horizontal de la infraestructura. Indicar el proceso para aumentar las maquinas que soportan el producto.

• Se debe contar en la solución con algún proceso para realizar escalamiento vertical de la infraestructura. Indicar el proceso para aumentar las capacidades de las maquinas en memoria, disco, ancho de banda, entre otros.

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

• Describir y/o incluir los límites de crecimiento con base en la capacidad de la infraestructura.

v. Seguridad de la Información y CoB

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

• Se debe contar con Informe de Vulnerabilidades.

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

• La solución debe permitir definir auditar las estructuras de tablas y columnas sin afectar el rendimiento de la aplicación.

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

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

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

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

• 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.

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

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

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

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

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

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

• 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).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

• 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.

• Los componentes de la solución propuesta deben correr sobre protocolos seguros https.

• La solución debe tener una administración centralizada de los sistemas de Seguridad y Auditoria.

• 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 a sus funciones.

• 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.

• 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.

• 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.

• Se debe garantizar que la aplicación está libre de vulnerabilidades de seguridad de la información, realizando pruebas de revisiones de código estático y dinámico y análisis de vulnerabilidades, realizando ejercicios completos de Ethical Hacking para validar la posibilidad de aprovechamiento de las mismas, en el caso que se identifiquen.

• 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.

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

• 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.

• 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.

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

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

• 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)

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

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

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

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

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

• 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.

• 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.

• 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.

• 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).

• 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.

1.8. ESPECIFICACIONES TÉCNICAS DEL BIEN O SERVICIO

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

b. 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.

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

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

e. Cumplir con los acuerdos de niveles de servicio que se determinen en los planes de trabajo acordados con el contratante.

f. 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.

g. 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. h. 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.

i. 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.

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

k. 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.

l. 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)

m. 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.

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

o. 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.

p. 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

q. 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.

r. 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.

s. 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.

t. 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.

u. 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.

v. 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.

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

x. 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

y. 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.

z. 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.

aa. 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.

bb. 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.

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

dd. 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.

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

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

gg. 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.

hh. 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.

1.9. DURACIÓN

La duración o plazo estimado para la prestación del servicio es de treinta y seis (36) meses.

1.10. FORMA DE PAGO ESTIMADA

Fiduprevisora S.A. bajo ninguna circunstancia realizará anticipos o pagos anticipados, los pagos se estima que se realizarán de la siguiente manera: Pago inicial por concepto de implementación, que se realizará en un único pago a satisfacción de la Fiduciaria, con autorización de la supervisión del contrato. Valor fee mensual vencido por un periodo de 34 meses, una vez implementada la solución.

2. INFORMACIÓN ESPECÍFICA DE LA COTIZACIÓN.

2.1. 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.

2.2. 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.

2.3. 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 DEL CONTRATO INCLUIDO IVA
1					
2					
3					

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

3. 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.

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

DESCRIPCIÓN	UNIDAD DE MEDIDA	CANTIDAD	VALORUNITARIO ANTES DE IVA	IVA (En caso de aplicar)	VALOR TOTAL
IMPLEMENTACIÓN	UNIDAD	1			
FEE MENSUAL	MES	36			

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: Christian Fandiño - Gerente de Adquisiciones & Contratos.
Aprobó: Daniela Andrade Valencia – Vicepresidencia de Contratación Derivada.