

## Anexo Técnico No. 2.

### *"Gestor Contractual - Requerimientos Funcionales - RFI"*

A continuación, se describen las necesidades de la Fiduciaria para el proceso implementación de una solución informática eficaz, amigable y ágil, para la automatización, seguimiento, control y monitoreo en tiempo real, así como la generación de informes de los procesos contractuales, durante las etapas precontractual, contractual y postcontractual de los contratos administrativos, contratos fiduciarios y contratación derivada, en sus diferentes modalidades. Sin perjuicio alguno de requerir determinar con mayor detalle cada uno de los requerimientos aquí descritos de forma conjunta con el proveedor seleccionado.

#### I. Requerimientos Funcionales:

##### 1. Implementación:

- La modalidad en la que se requiere la implementación de la herramienta es SaaS u On-premise
- Para la modalidad On-premise es necesario que se indiquen las características de la infraestructura requerida.
- La herramienta debe permitir la conexión Vía internet/intranet en todos los navegadores.
- Solución rápida e intuitiva
- Flexibilidad en la parametrización
- Módulo ayuda en línea
- Visualización en computadores, tabletas y smarthphone.
- Debe poseer mecanismos para evitar la inyección de código malicioso en formularios
- Permitir almacenar y clasificar la documentación y/o información en pública, privada y secreta, para lo cual se debe permitir que el usuario que determine la clasificación de la información como privada o secreta asigne una clave, o en su defecto, parametrizar la herramienta para que la documentación y/o información privada y secreta pueda ser consultada y visualizada únicamente por el usuario que así la clasifique.
- Permitir la integración con los diferentes servidores de correo electrónico de acuerdo con las necesidades o políticas de la entidad.
- Una vez finalizado el trámite, la herramienta debe incorporar opciones para el cierre del expediente. (manual o automático).
- La herramienta debe hacer accesible el contenido de los expedientes de acuerdo con los roles y permisos.
- No debe permitir la eliminación de un expediente electrónico o de su contenido.
- Proporcionar herramientas para la generación de informes y reportes.
- Generar informes que incluyan como mínimo gráficos y tablas.
- Proporcionar a los usuarios herramientas para informes estadísticos de la Gestión Contractual dentro de un rango específico de tiempo, sin limitación del lapso requerido para el informe.
- Permitir que los informes referidos en precedencia puedan ser impresos o exportados por los usuarios

en cualquier tipo de formato electrónico (txt, pdf, xls, excel, csv, entre otros)

- Todas las acciones efectuadas sobre el trámite contractual deben ser registradas en un historial de eventos que puede ser consultado por los usuarios de consulta y administradores.
- Garantizar que los documentos electrónicos de archivo que se capturen se asocien a una TRD configurada en el sistema.
- Establecer niveles de seguridad del expediente de acuerdo con los niveles de seguridad establecidos por la entidad.
- Otorgar un número único de identificación al trámite al momento de creación del mismo.
- permitir almacenar contenidos como: videos, audio, imagen, entre otros, de la misma forma que los documentos electrónicos de texto
- Permitir la gestión de notificaciones y avisos por medio de correo electrónico.
- Activación o desactivación de las cuentas de correo que serán gestionadas de manera automatizada.
- El sistema debe permitir al usuario buscar y recuperar información que se encuentre dentro de documentos, listas de documentos y metadatos, de acuerdo con el perfil de acceso.
- Proporcionar una función de búsqueda que permita utilizar combinaciones de criterios de búsqueda:
  - Operadores booleanos (y, o, exclusivo, o, no);
  - Coincidencias aproximadas;
  - Intervalos de tiempo;
  - Permitir búsqueda con comodines (\*, ?, \$, =, +, -);
  - Por agrupaciones (Código, Serie, subseries, asunto, usuario, área responsable, palabras clave...);
  - Tipos de formatos
  - Cualquier combinación valida con un número limitado de criterios de búsqueda, utilizando cualquier combinación de contenido textual o de metadatos.
  - Opción de autocompletar.
- El sistema debe permitir:
  - Ver la lista de resultados de una búsqueda,
  - Listar documentos que componen un resultado de la búsqueda,
  - Ver la lista de todos los expedientes y documentos relacionados a cualquier serie determinada, con su respectivo contenido.
- Proporcionar al usuario maneras flexibles de imprimir los documentos correspondientes a cada trámite contractual.
- En los resultados de búsqueda se presenten únicamente las carpetas y documentos a los que el usuario tiene acceso de acuerdo con los niveles de permisos definidos.
- Permitir la delegación de tareas dependiendo del rol designado a los funcionarios.
- Cargar archivos en diferentes formatos
- Herramienta de edición / diseño de plantillas de Word
- Permitir la búsqueda indexada de información.
- Generación en PDF o XLSX listado de contratación según criterios de búsqueda.
- Generación en PDF o XLSX los informes de seguimiento o supervisión.

- El historial de eventos del expediente electrónico o contrato pueda ser exportado en PDF o XLSX.
  - Indicadores
2. ANS: El proponente deberá adjuntar el Anexo No. 4 "Aceptación de ANS", debidamente suscrito por su representante legal en señal de conocimiento y aceptación de los ANS y la penalización contemplada por el incumplimiento a estos.

Adicionalmente, el proponente deberá cumplir con los siguientes ANS según la etapa:

- Durante la etapa de implementación:  
Atención de requerimientos funcionales y técnicos:
    - Reuniones virtuales de 2 horas semanales, de acuerdo con las solicitudes que presente la Fiduciaria.
    - Respuesta a correos electrónicos sobre aspectos de la implementación con avances en 1 día hábil,
  - En la etapa licenciamiento:
    - Atención de peticiones dentro del día hábil siguiente de la solicitud que se presente
    - Soporte y mantenimiento debe ser 7\*24\*365
    - Ofrecerá una disponibilidad de al menos el noventa y nueve punto noventa y cinco por ciento (99.95%) en su servicio de cómputo en la nube
3. Control y Seguridad:

- Permitir la creación y administración de usuarios, roles y permisos
- Permitir revocar privilegios de un grupo o usuarios seleccionados
- La cantidad de usuarios que usaran la herramienta será de 200, estimando 150 con acceso full.
- Ofrecer opciones de configuración para asignar o eliminar roles después de un período predefinido automáticamente
- Permitir configurar controles y restringir el acceso de acuerdo con los perfiles configurados por el administrador del sistema.
- Soportar diferentes mecanismos de autenticación y debe permitir la integración con el Directorio Activo de la Fiduciaria.
- Debe permitir a un usuario autorizado parametrizar el número de intentos fallidos de ingreso a la sesión.
- Bloquear al usuario una vez se hayan completado el número de intentos fallidos configurados por el usuario autorizado para el inicio de sesión y notificar mediante un mensaje de alerta.
- Programar rutinas de copia de seguridad (backup) y su recuperación cuando sea necesario
- Notificar al usuario encargado, fallas críticas en los servicios del sistema en el instante en que se presentan
- Permitir la creación, gestión y configuración de niveles de clasificación de información a que haya lugar (Clasificada, reservada, confidencial, de acuerdo a la normatividad existente) y permitir acceso a esta dependiendo el rol de usuario.
- Contar con mecanismos de recuperación de credenciales de acceso obedeciendo las políticas de ingreso

seguro

- Permitir configurar y ejercer controles sobre tiempos de inactividad y bloqueo.
- La aplicación debe cumplir con las mejores prácticas de desarrollo de software definidas en el estándar OWASP (Open Web Application Security Project).
- Mecanismos de autenticación y seguridad
- Controles para definir perfiles o grupos de usuarios.
- Garantizar que las transacciones u operaciones que realice el sistema las cuales presenten fallos en su ejecución deben reversarse al estado inicial en la ejecución del proceso. (rollback) (evita envío de información incompleta y pérdida de la misma).
- Aplicar técnicas criptográficas en las operaciones y/o transacciones críticas o sensibles para la organización.
- Los procesos de importación o exportación de información, deberá realizarse a través de interfaces seguras y aplicar protocolos y mecanismos de seguridad
- No debe limitar el número de roles o grupos que se puedan configurar
- Permitir marcar un usuario individual como inactivo, sin eliminarlo del sistema
- Generación de registros de control o hashes que permitan validar la integridad de los registros de seguridad generados.
- Inclusión en los reportes generados de un rótulo que permita identificar su nivel de clasificación (clasificado, reservado, restringido, entre otros), de acuerdo con la clasificación asignada mediante parámetro al momento de su creación
- Permitir la definición por parámetro y controlar la longitud mínima y máxima de las contraseñas
- Permitir la definición por parámetro y controlar el número de contraseñas a recordar (Histórico de contraseñas).
- Permitir la definición de un diccionario de contraseñas no válidas y controlar que las contraseñas no coincidan con las existentes en dicho diccionario
- Controlar mediante parámetro la complejidad de la contraseña.
- La contraseña debe tener una combinación de caracteres numéricos, alfabéticos (Mayúsculas y Minúsculas) y signos o caracteres especiales
- Las contraseñas nunca pueden ser almacenadas en formato texto. Deben ser almacenadas por medio de un algoritmo de encriptación de una sola vía reconocido por la industria como versión 2 (PBKDF2) o SHA-256.
- Desconectar los usuarios que hayan permanecido inactivos en el sistema durante un tiempo definido mediante un parámetro que especifique este tiempo
- Permitir definir por parámetro y controlar la vigencia mínima, vigencia máxima y tiempo de aviso de vencimiento, de las contraseñas
- Gestionar estados para las cuentas de usuario: Habilitado, deshabilitado, bloqueado, suspendido
- Contar con procedimientos automáticos para copias de seguridad y restauración encaminados a realizar copias periódicas de seguridad de todos elementos dentro del sistema (carpetas, documentos, metadatos, usuarios, roles, permisos, configuraciones específicas).

- Al presentarse fallas durante la restauración de las copias de seguridad debe permitir notificar sobre el fallo y los detalles de este, para que el administrador tome las decisiones necesarias para subsanar los errores
- Contar con una Política definida, aprobada, sensibilizada e implementada de Protección de datos, especialmente teniendo la Protección de datos personales de la Ley 1581 de 2012.
- Tener implementado un manual de procesos de tratamiento de los datos, para todos sus proyectos y clientes
- Tener un inventario de bases de datos, realiza registro y actualización anual nacional de base de datos ante la SIC
- Contar con una política que contenga los principios, procedimientos y lineamientos para la gestión de la seguridad de la información y riesgo de ciberseguridad en la entidad
- Tener establecido un proceso que gestione los riesgos de seguridad de la información y la ciberseguridad
- Contar con indicadores para medir la eficacia y eficiencia de la gestión de la seguridad de la información y la ciberseguridad
- Realizar pruebas de análisis de vulnerabilidades, ethical hacking y análisis de código (según aplique el proyecto), y cerrar las brechas, antes de salida a producción.
- Contar con un procedimiento definido, aprobado e implementado de gestión de incidentes de seguridad de la información y ciberseguridad
- Contar con mecanismos de control para la fuga de información de la organización
- Se debe tener implementado un procedimiento formal para la gestión de los incidentes de Seguridad de la Información dentro de la organización.
- Deben tener implementados procedimientos para el reporte de Incidentes relacionados con terceras partes (clientes - proveedores), entendiéndose como incidente a cualquier situación que afecte la confidencialidad, integridad o disponibilidad de la información o que involucre datos personales que se encuentre en la solución propuesta
- Para la adquisición o desarrollo de aplicaciones se deben contemplar mecanismos de desarrollo seguro
- Se debe contar con una política de ciclo de vida de desarrollo seguro
- Se deben tener definidos procedimientos de Control de Cambios para aplicaciones y sistemas operativos
- Tener procedimientos para el reporte de controles de cambios relacionadas con Terceras partes. (Clientes – Proveedores)
- Se deben efectuar periódicamente pruebas de seguridad (análisis de vulnerabilidades y Ethical Hacking), así como la ejecución del plan de mitigación, con el fin de identificar y corregir vulnerabilidades, a su desarrollo y desarrollo con terceros, y ser entregados dichos informes y mitigación a FIDUCOLDEX

#### EN NUBE:

- Contar con la certificación ISO 27001, y de observancia a los estándares o buenas prácticas, tales como ISO 27017 y 27018
- Contar con la certificación ISO 27001, y de observancia a los estándares o buenas prácticas, tales como ISO 27017 y 27018

- El proponente podrá demostrar que cuenta con certificaciones con estándares o mejores prácticas que reemplacen, sustituyan o modifiquen las anteriores
- Disponer de informes de controles de organización de servicios (SOC1, SOC2, SOC3)
- Asegurar una disponibilidad mínima del 99.95% en la prestación del servicio en la nube en la modalidad IaaS y PaaS o de 99,95 para la modalidad SaaS, de acuerdo con lo establecido en la propuesta e informar bajo que modalidad de nube ofrece los servicios (IaaS, PaaS y SaaS) y la respectiva disponibilidad del servicio
- Informar las amenazas, vulnerabilidades y riesgos de las API o Servicios Web suministrados en la nube, así como los controles para mitigar los riesgos
- El procesamiento de la información debe cumplir con normas equivalentes o superiores a las aplicables en Colombia, relacionadas con la protección de datos personales y penalización de actos que atenten contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos
- Debe informar a la Fiduciaria cuales son los mecanismos que permitan contar con respaldo de la información que se procesa en la nube y está a disposición de la Fiduciaria cuando así lo requiera
- Garantizar una independencia de la información de la Fiduciaria y sus backups con respecto a la información de otros clientes que utilice el software y procesen en la nube, esta independencia se puede hacer a nivel lógico o físico.
- El acceso a la información y los respaldos debe estar habilitado exclusivamente para la Fiduciaria"
- Garantizar que la información de las operaciones en tránsito o reposo esté cifrada, la inscripción debe estar basada en estándares y algoritmos reconocidos internacionalmente que brinden al menos la seguridad ofrecida por AES, RSA o 3DES.
- Así mismo, se debe contar con canales de comunicación con el proveedor de servicios en la nube cifrados de extremo a extremo y que en lo posible usen rutas diferentes"
- Permitir la administración de usuarios y de privilegios para el acceso a los servicios ofrecidos, así como a las plataformas, aplicaciones y bases de datos que operen en la nube
- Monitorear los servicios contratados para detectar operaciones o cambios no deseados y/o adelantar las acciones preventivas o correctivas cuando se requiera
- Presentar un informe periódico según se acuerde a la Fiduciaria para verificar los ANS establecidos
- Así mismo deberá indicar si el servicio lo presta con el apoyo de subcontratistas o partners caso en el cual deberá informar cuales son los procedimientos para verificar el cumplimiento de los ANS.
- Garantizar que, en el evento de toma de posesión, la SFC, Fogafín, Fogacoop, o quienes éstas designen, puedan acceder a la información y a la administración de los sistemas de información que operan en la nube
- Informar, en cuanto le sea posible, a la Fiduciaria sobre cualquier evento o situación que pudiera afectar significativamente la prestación del servicio
- Cumplir y certificar el borrado seguro de los datos existentes en los medios de almacenamiento cuando finalice el contrato, cuando lo solicite la Fiduciaria o cuando EL contratista elimine y/o reemplace dichos medios
- Realizar el análisis de vulnerabilidades a necesidad de la Fiduciaria y asegurar la corrección oportuna y

eficaz de las vulnerabilidades informáticas detectadas

- Contar con múltiple factor de autenticación para el acceso a la(s) consola(s) de administración por parte de la Fiduciaria
- Asegurar que todo el licenciamiento dispuesto en la plataforma tecnológica y/o software utilizado en la prestación del servicio cumple con la ley de Derechos de Autor del país donde se encuentre la nube que aloja la información
- Contar con planes de contingencia y continuidad de negocio y estos se encuentran documentados probados para el servicio ofrecido
- Establecer un Gobierno, Roles y responsabilidades para la gestión de la continuidad del negocio
- Establecer un sistema básico de gestión de continuidad del negocio
- Tener los RTO Y RPO de procesos críticos definidos
- El servicio ofrecido debe estar definido en catalogo si es o no proceso critico
- Capacitar a sus colaboradores en términos de continuidad, indique resultados y última fecha de realización
- Ejecutar formación específica a personal que participa directamente en la continuidad del negocio en la entidad

#### 4. Flujos de Trabajo:

- Creación, administración y ejecución de flujos de trabajo.
- Diagramar y modelar flujos de trabajo.
- Diagramar tareas que componen un proceso y/o procedimiento
- Parametrizar los tiempos de ejecución y respuesta de los procesos ejecutados
- Incorporar un mecanismo de validación para analizar los flujos de trabajo modelados
- Permitir la parametrización de Reglas para la configuración y gestión de:
  - Estados del Flujo de Proceso
  - Validación de Actividades
  - Definición y asignación de usuarios
- Parametrizar los accesos, creación, modificación o control total para usuarios o grupos de usuarios de los flujos de trabajo
- Permitir al usuario del flujo de trabajo:
  - Visualizar las actividades que tiene pendientes por realizar
  - Priorizar por diferentes criterios
  - Visualizar información en tiempo real sobre el desempeño de sus procesos
  - Visualizar de manera gráfica el estado de cada flujo de trabajo
  - No debe limitar el ingreso de acciones que componen cada flujo de trabajo
- Generar los flujos de trabajo en un formato estándar.
- Generar un identificador único para cada flujo de trabajo
- Generar una trazabilidad de las acciones de los flujos de trabajo
- Permitir solo a un rol administrador autorizado a crear, parametrizar, administrar y poner en ejecución

flujos de trabajo

- Permite definir los flujos de trabajo basado en plantillas.
- Permitir detener un flujo de trabajo.
- Definir los tiempos límite de ejecución de los flujos y de cada una de sus actividades enviando notificaciones de incumplimiento
- Contar con semáforos o cualquier mecanismo que permita visualizar de una manera ágil el cumplimiento de tiempos en cada una de las actividades de un flujo.
- Actualización de estados de contrato (precontractual, contractual o postcontractual)

## 5. Firmas electrónicas:

- Interoperabilidad con el operador de facturación electrónica de la entidad para la firma de sus representantes legales y demás funcionarios del flujo de trabajo, al respecto se podrá contar con una herramienta ofrecida por el proponente, o que exista interoperabilidad con las herramientas Signio y AdobeSign contratadas por la Fiduciaria.
- Funcionalidades: - Estampado cronológico fecha y Hora- Firma electrónica Componente automatizado para firmar a través del sistema documentos salientes
- Verificación de firma electrónica: Se debe contar con mecanismos para verificación (validez, archivos, entre otros)
- Funcionalidad para incorporar una imagen con la firma del firmante.
- Cantidad de documentos a firmar ilimitados
- Uso de MFA Multiple factor de autenticación, para la ejecución de la firma electronica

## 6. Trazabilidad:

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

## 7. Interoperabilidad:

- Servidores de correo
- Gestor Documental
- Repositorio en la nube
- Debe permitir involucrar diferentes usuarios internos y externos a los flujos contractuales por unidades de negocio, con diferentes responsabilidades dentro del proceso.

- Debe permitir integrarse a aplicativos CORE de la Fiduciaria, a través de servicios WEB o cualquier tecnología de integración en tiempo real.

## 8. Migración:

- La documentación que se cargue a la herramienta a implementar debe migrar al Gestor Documental de Fiducoldex, de modo que la totalidad de documentación generada por la Fiduciaria se conserve en un único repositorio.
- Debe permitir extracción y descargue
- Entrega de la Información en medios con Cintas, DVD o HD extraíbles

## II. Requerimientos tecnológicos y soporte:

- La solución debe estar soportada con un tipo de arquitectura reconocida, mencionar el tipo y detalle de esta.
- La solución debe implementarse en modalidad SaaS u On-premise
- Entregar Manuales de usuario y Manuales técnicos
- Debe tener implementado un diseño adaptativo responsive
- Soportar IPV6
- La plataforma debe tener implementado mecanismos adecuados para interoperar con otros sistemas de interés de su dominio
- Altamente parametrizable
- La plataforma debe ser compatible con diferentes navegadores web (Explorer, Mozilla, Chrome, Safari) y con los S.O. licenciados e implementados en la Fiduciaria.
- Disponer de frameworks que permiten implementar Las funcionalidades requeridas sin codificación
- Contener herramientas de desarrollo low-code para implementar las funcionalidades requeridas.
- Gestionar errores y excepciones de La plataforma.
- Mantenimiento Correctivo: Atención inmediata.
- Mantenimiento Preventivo: Cuando aplique
- Reportes de Servicio: Informe mensual de los soportes técnicos prestados.
- Permitir la atención y recepción de los incidentes
- Reporte sobre las vulnerabilidades que afecten la plataforma o herramienta implementada
- La plataforma que soporta la solución debe ser HA y redundante
- La plataforma debe ser intuitiva y fácil de usar por parte del usuario final.
- Disponer de documentación en línea y herramientas para facilitar el soporte del sistema
- Debe contar con un alto grado de Personalización que brinde mayores posibilidades de configuración de cada aplicación y que den valor agregado en soluciones de la empresa y de sus clientes
- Tener implementado servicios de integración
- Manejo de ETL's para el procesamiento de datos, especificar tecnología utilizada

- Debe tener entornos de prueba, desarrollo y producción, mediante los cuales se realicen actividades de prueba, actualizaciones, capacitaciones y desarrollo de funcionalidades manera aislada e independiente, cumpliendo con medidas de seguridad para no comprometer ni divulgar la información crítica y/o sensible.
- La solución debe proporcionar un mínimo de almacenamiento de 1.7 TB, estimado a utilizar durante los 12 meses proyectados de la ejecución del contrato. Se estima aproximadamente 70 usuarios durante la vigencia del año
- Capacitación funcional y técnica
- Pruebas de carga y estrés.
- Actualización de Nuevos Releases y nuevas versiones
- Gestión de Mejora de Producto (Arquitectura de Producto).

### III. Requerimientos Seguridad de la información:

- Posibilidad de autenticación contra el LDAP/Directorio Activo de la compañía y MFA Multiple factor de autenticación
- Generar informes de vulnerabilidades
- El proveedor de la solución debe garantizar durante la vigencia del contrato que la aplicación y la infraestructura sobre la cual se ejecuta cuenten con las últimas actualizaciones y versiones disponibles
- Cuenta con logs de auditoría, sobre cambios funcionales o cambios directamente en bases de datos y que puedan ser integrados a nuestro SIEM Splunk.
- Permitir transacciones especiales con rastro de auditoría sin que afecte el rendimiento operativo del aplicativo y demás procesos
- logs de auditoría, sobre cambios funcionales o cambios directamente en bases de datos y que sean integrados al SIEM Splunk
- Cuenta con Informe de Vulnerabilidades (OWASP), con evidencias
- Cuenta con logs de auditoría, sobre cambios funcionales o cambios directamente en bases de datos que sean integrados al SIEM Splunk
- Permite definir estructuras de datos y columnas a auditar sin afectar el rendimiento de la aplicación.
- El sistema no debe permitir realizar el guardado automático de contraseña.
- Administrar y controlar las sesiones.
- La función de logout del sistema debe terminar completamente con la sesión o conexión asociada.
- El sistema no debe permitir logeos concurrentes con el mismo usuario.
- Los controles de acceso en caso de falla del sistema deben actuar en forma segura.
- El aplicativo debe administrar y gestionar Logs
- El sistema debe almacenar en un registro de auditoría cada cambio de parámetro con la información de fecha, hora, valor anterior, valor nuevo, usuario del sistema e IP, actividad (ingreso/borrado/modificación)
- El sistema debe permitir el acceso a los logs, solo a personal autorizado
- El sistema deberá utilizar una rutina centralizada para todas las operaciones de login.

- El sistema deberá registrar en un log todas las funciones administrativas, incluyendo cambios en la configuración de seguridad, intentos fallidos, excepciones del sistema.
- El sistema deberá utilizar una función de hash para validar la integridad de los logs
- El sistema debe contar con conexiones TLS para todo el contenido que requiera acceso autenticado y para todo otro tipo de información sensible
- El sistema proporcionara una herramienta que haga parte del módulo de Seguridad y Auditoria que facilite el análisis de datos de acceso a las aplicaciones
- Los componentes del sistema propuesto deben correr sobre protocolos seguros https
- El proveedor debe entregar el detalle de los roles y funciones asociadas a cada rol, describiendo detalladamente el alcance de cada función para así poder identificar internamente el rol que se debe asignar a cada funcionario de acuerdo con sus funciones
- El sistema generará informes que permitan visualizar los roles por aplicación, usuarios del sistema, privilegios de cada rol por opción, opciones con permisos por rol.
- 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
- Debe poderse 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.
- El sistema debe permitir configurar el tiempo de inactividad por sesión de usuario
- 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).
- El sistema debe contar con un módulo para la administración de la seguridad del sistema.
- El sistema debe ser sometido a pruebas de código seguro
- Dentro del soporte de la solución debe incluirse la corrección de vulnerabilidades de nivel alto y medio que se encuentren al aplicativo sin costo adicional.
- La solución debe permitir integrarse con otras aplicaciones de manera segura, cumpliendo estándares como Web Services seguros para mensajería SOAP, tal como:
- Mecanismos: ciframiento de la información del mensaje, Manejo del Timestamp, Identificación y autenticación del servicio: con certificados y firma digitales del body del mensaje, No repudio: firma digital del mensaje request y responds
- 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 del sistema ante una interrupción de la operación de su infraestructura tecnológica.
- Adoptará las medidas de índole técnica y organizativas necesarias para garantizar la confidencialidad, integridad y disponibilidad de la información y evitar su alteración, pérdida, tratamiento o acceso no

autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o de fenómenos físicos o naturales. A estos efectos el proveedor deberá aplicar los aspectos establecidos en la Norma ISO 27001:2013, de acuerdo con la naturaleza de los datos que trate. La información revelada será dirigida al proveedor y los contenidos serán sólo para el uso de quienes haya sido dirigida, y no deberá divulgarse a terceras personas. El proveedor se hará responsable ante terceros a quienes se haya divulgado esta información sin previo consentimiento.

- Asegurará que, como producto de la prestación del servicio, entregará a la Fiduciaria una solución que garantice confidencialidad, integridad y disponibilidad de la información relacionada con el objeto de este.
- Tramitará de manera previa la autorización de FIDUCOLDEX para cualquier conexión e interacción con la red de la fiduciaria y su información.
- Aceptará el monitoreo de cualquier conexión e interacción con la red de la fiduciaria y su información cuando FIDUCOLDEX lo considere oportuno.
- Garantizará que cualquier interrupción programada de la solución o servicio con fines de actualización y mejoras debe ser administrada bajo un acuerdo de nivel de servicios previamente acordada con FIDUCOLDEX, principalmente con el fin de mantener informados a sus clientes y usuarios en los términos que establece la ley.
- Utilizará los recursos tecnológicos que le entregue FIDUCOLDEX, en forma exclusiva para el desarrollo de la labor para la prestación del servicio.
- Cumplirá con especial cuidado, el principio de buen uso y confidencialidad de los medios de acceso que ha entregado FIDUCOLDEX.
- Garantizará a FIDUCOLDEX que el personal asignado para la atención del contrato conoce y cumple las políticas contenidas en este contrato y responde por cualquier inobservancia de estas.
- Dará cumplimiento a lo estipulado en la política de Seguridad de la información para las relaciones con proveedores, relacionado con:
  - Se autoriza a FIDUCOLDEX a evaluar y auditar los controles de seguridad implementados por el proveedor, en forma periódica o cuando se presenten cambios significativos en los controles o en la relación contractual entre ambas partes.
  - Se obliga a informar a FIDUCOLDEX sobre cualquier violación a la seguridad de la información que afecte sus operaciones o sus negocios.
  - Comunicará a FIDUCOLDEX los planes de tratamiento que contempla ante posibles violaciones de la seguridad y los tiempos en que tendrán efecto esas acciones.
  - Informará a FIDUCOLDEX, todos los cambios en su entorno que afecten el negocio o la operación de su cliente, en forma oportuna.
  - Comunicará a FIDUCOLDEX los cambios o modificaciones programados de los servicios prestados, los cuales serán previamente autorizados por la Fiduciaria.
  - Los recursos que FIDUCOLDEX pone a disposición del personal externo, independientemente del tipo

- que sean (informáticos, datos (físicos o lógicos), software, redes, sistemas de comunicación, etc.), están disponibles exclusivamente para el cumplimiento de las obligaciones.
- Si la información de propiedad de FIDUCOLDEX es administrada por un tercero, se requiere contar con procedimientos y compromisos que garanticen un manejo seguro de la información.
  - No revelará a terceros la información a la que tenga acceso.
- Implementar el protocolo HSTS o Http Strict Transport Security, para reducir las posibilidades de que un atacante pueda interceptar las comunicaciones y recopilar cookies y datos similares intercambiados durante la sesión. Previo a salir en producción, debe cumplir con los requerimientos y precargar en la lista HSTS.
  - Contará y mantendrá los estándares o buenas prácticas, tales como ISO 27017 (controles de seguridad para servicios en la nube) y 27018 (Protección Información Personal en la nube). El proveedor puede certificarse con estándares o mejores prácticas que reemplacen, sustituyan o modifiquen las anteriores. Entregará a FIDUCOLDEX las certificaciones que demuestren la vigencia de estas.
  - Disponer de informes de auditores externos según el marco de informes SOC - controles de organización de servicios (SOC1, SOC2, SOC3).
  - Ofrecerá una disponibilidad de al menos el noventa y nueve punto noventa y cinco por ciento (99.95%) en su servicio de cómputo en la nube.
  - Gestionar que las API o Servicios Web suministrados por el proveedor de servicios en la nube no exponen a FIDUCOLDEX a riesgos de seguridad de la información o de ciberseguridad.
  - Realizar la corrección oportuna y eficaz de las vulnerabilidades informáticas detectadas.
  - Documentar las jurisdicciones donde se procesará la información y certificará que las mismas cuentan con normas similares o más exigentes que las aplicables en Colombia, relacionadas con la protección de datos personales y penalización de actos que atenten contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos.
  - Garantizar la independencia de la información de FIDUCOLDEX y de sus copias de respaldo de la información de las otras entidades que procesen en la nube. La independencia se puede dar a nivel lógico o físico.
  - Mantener cifrada la información clasificada como confidencial en tránsito, usando estándares y algoritmos reconocidos por AES, o 3DES internacionalmente que brinden al menos la seguridad ofrecida
  - Brindar al FIDUCOLDEX la posibilidad de tener bajo su control la administración de usuarios y de privilegios para el acceso a los servicios ofrecidos,
  - Utilizar técnicas de múltiple factor de autenticación para el acceso a las consolas de administración por parte de FIDUCOLDEX.
  - Informar al FIDUCOLDEX en cuanto le sea posible, sobre cualquier evento o situación que pudiera llegar a afectar la prestación del servicio y, por ende, el cumplimiento por parte de la vigilada de sus obligaciones frente a los clientes y a otras entidades
  - Monitorear los servicios y su infraestructura para detectar operaciones o cambios no deseados y/o adelantar las acciones preventivas o correctivas cuando se requiera.
  - Garantizar que la comunicación con FIDUCOLDEX se realice utilizando mecanismos que permitan cifrados

de extremo a extremo y que en lo posible usen rutas diferentes.

- Utilizar los recursos tecnológicos asignados en el servicio en la nube, de forma exclusiva para el desarrollo de la gestión, garantizando la separación lógica de la información de FIDUCOLDEX.
- Garantizar y certificar que todo licenciamiento dispuesto en la plataforma tecnológica y/o software utilizado en la prestación del servicio cumple con la Ley de Derechos de Autor del país donde se encuentre la Nube que aloja la información.
- Documentará el tipo de nube y los sitios de procesamiento.
- Establecerá mecanismos que permitan contar con respaldo de la información que se procesa en la nube, la cual debe estar a disposición de FIDUCOLDEX cuando así lo requiera.
- Aceptará el monitoreo de cualquier conexión e interacción con la red de FIDUCOLDEX y su información cuando FIDUCOLDEX lo considere oportuno.
- Garantizará que, en el evento de toma de posesión, la SFC, Fogafin, Fogacoop, o quienes éstas designen, puedan acceder a la información y a la administración de los sistemas de información que operan en la nube.
- Aceptará que FIDUCOLDEX pueda verificar el cumplimiento de los acuerdos y niveles de servicio establecidos con el proveedor de servicios y los subcontratistas de éstos, cuando sean estos quienes prestan el servicio.
- Dispondrá de un monitoreo sobre la infraestructura y el aplicativo que permita detectar y contener oportunamente un incidente de seguridad, así como retornar el aplicativo en operación, de acuerdo con los niveles de servicio que se acuerden.
- Entregará la siguiente información a FIDUCOLDEX:
  - Documento con el tipo de nube y los sitios de procesamiento contratados
  - Nombre del subcontratista(s) o partner(s) que le prestarán servicios asociados al objeto del contrato.
  - La ubicación física o región donde se procesarán y almacenarán los datos.
  - Las certificaciones otorgadas al proveedor del servicio y/o sitio de procesamiento.
  - La relación de auditorías a las que se somete el proveedor de servicios contratado.
  - El diagrama con la plataforma tecnológica que soportará los servicios contratados.
  - Los reportes generales de auditorías, pruebas de vulnerabilidades.
- Garantizará que el aplicativo y la infraestructura donde se aloja, deben cumplir con la normativa y mejores prácticas de Ciberseguridad tanto de Colombia como del país donde se aloja la información.
- Garantizará que el aplicativo cuente con la trazabilidad transaccional en la operación.
- Garantizará que el aplicativo se encuentre actualizado en la legislación y normatividad colombiana
- Implementará las recomendaciones de seguridad informática emitidas por Open Web Application Security Project –OWASP–, cumpliendo con el OWASP Top 10, documento de alto nivel que se centra sobre las vulnerabilidades más críticas en la web. El proveedor debe realizar periódicamente o a solicitud de la Fiduciaria, un escaneo del software y revisará que todas las vulnerabilidades incluidas se encuentren resueltas. Estos informes deberán ser presentados trimestralmente o de acuerdo con la periodicidad definida por la Fiduciaria al Supervisor y con copia a la Dirección de Seguridad de la Información.
- El proveedor garantizará que el Centro de Datos donde se presta el servicio Hosting, este certificado en

modalidad TIER III o superior. Aportará la certificación de sismo resistencia del sitio.

- Las demás obligaciones que contribuyan a garantizar el cabal cumplimiento, ejecución y finalización del presente contrato, que sean propias de este tipo de contratos de acuerdo con la ley o que aparezcan consignadas en otras cláusulas de este documento o sus anexos.
- El proveedor garantizará que los bienes y servicios relacionados con las TIC soportan el protocolo IPV6 nativo en coexistencia con el protocolo IPV4, en cumplimiento de la Resolución 0002710 de 2017, expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones.

#### IV. Protección De Datos Personales:

El proveedor es encargado del tratamiento, tratará por cuenta de FIDUCOLDEX, responsable del tratamiento, los datos de carácter personal necesarios para el suministro de medios y plataforma para el procesamiento y control de los datos personales proporcionados como parte de los servicios en la nube y demás servicios anexos objeto del presente contrato.

El proveedor como encargado del Tratamiento deberá cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la Ley 1581 de 2012 y en otras que rijan su actividad:

- Cumplirá la Política de Protección de datos de FIDUCOLDEX, publicada en la página <http://www.FIDUCOLDEX.com.co/seccion/politica-de-tratamiento-de-datos-personales>
- Realizará el tratamiento de la información conforme a los requisitos definidos, a las Políticas de Protección de Datos Personales desarrolladas por FIDUCOLDEX y a las finalidades del tratamiento autorizadas por el Titular.
- Garantizará al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- Adoptar e implementar medidas de seguridad, necesarias y eficientes, que permitan mantener la información resguardada bajo un ambiente de control físico y lógico que asegure que sólo podrá tener acceso a dicha información el personal autorizado. Se deberán tomar medidas necesarias y razonables de seguridad sobre la información que repose en soportes físicos, así como de la información electrónica.
- Conservará la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Realizará oportunamente la actualización, rectificación o supresión de los datos en los términos de la mencionada ley.
- Actualizará la información reportada por FIDUCOLDEX como responsable del tratamiento dentro de los cinco (5) días hábiles siguientes contados a partir de su recibo.
- Garantizará la existencia de políticas sobre Tratamiento de la información de conformidad con lo previsto en el Art. 18 de la Ley 1581 de 2012.
- Adoptará un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares, de manera que garantice la oportunidad y la calidad de las respuestas de acuerdo con lo establecido en la Ley 1581 de

2012.

- En el caso que resulte aplicable, registrará en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la mencionada Ley.
- En el caso que resulte aplicable, insertará en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
- Se abstendrá de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
- Permitirá el acceso a la información únicamente a las personas que en desarrollo de sus funciones y responsabilidades del cargo lo requieran.
- Garantizará que el personal que tenga acceso a la Información de FIDUCOLDEX se encuentre informado de:
  - Su calidad de Encargado de la información de FIDUCOLDEX.
  - Los requisitos de seguridad de la información del presente Contrato.
  - Las políticas de protección de datos personales de FIDUCOLDEX, las cuales se encuentran publicadas en la página web <http://www.FIDUCOLDEX.com.co/seccion/politica-de-tratamiento-de-datos-personales>.
  - Las medidas de seguridad físicas y electrónicas que se adoptarán sobre la información suministrada por FIDUCOLDEX.
- Garantizará que todos los empleados y colaboradores que se encuentren involucrados en el Tratamiento de la información tengan conocimiento de las obligaciones que en materia de protección deben asumir. En consecuencia, sus empleados y colaboradores deben suscribir cláusulas de confidencialidad y Tratamiento adecuado de la información
- Se abstendrá de revelar la información de la entidad, de clientes o de personas naturales que le haya sido entregada para el cumplimiento de este contrato a terceros no autorizados.
- Se abstendrá de utilizar la información para una finalidad distinta a las autorizadas por FIDUCOLDEX
  - Informará de forma oportuna a la Superintendencia de Industria y Comercio y a FIDUCOLDEX como responsable del tratamiento cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares que puedan presentar y que afecten o amenacen la integridad, disponibilidad y confidencialidad de la información
- Cumplirá las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.
- En el evento en que el proveedor sea requerido por una autoridad, para el suministro de información de FIDUCOLDEX, incluyendo la información de personas naturales suministrada por la entidad, deberá informar inmediatamente a FIDUCOLDEX a fin de que este pueda adoptar o establecer las medidas necesarias para garantizar la confidencialidad de la información ante el requerimiento de las autoridades.
- El proveedor como encargado del tratamiento entiende y acepta que el uso indebido de la información suministrada por FIDUCOLDEX puede llegar a tener implicaciones penales, acarrear sanciones administrativas por parte de la Superintendencia de Industria y Comercio, en su calidad de Autoridad en materia de protección de datos personales y en materia de reserva bancaria por parte de la Superintendencia Financiera de Colombia; será responsable por cualquier perjuicio que cause a los



titulares como consecuencia directa o indirecta del incumplimiento de cualquiera de las obligaciones que se desprenden de lo aquí establecido.

- El proveedor deberá tomar las medidas de custodia adecuadas que permitan conservar el carácter confidencial de la información y evitar que ésta sea visualizada, modificada o sustraída por personal no autorizado.
- La información de la que el proveedor tenga conocimiento no podrá ser compartida con terceros, salvo que medie autorización expresa de FIDUCOLDEX o que deba hacerlo con ocasión de la prestación del servicio.

Calle 28 N. 13A – 24, Edificio Museo del Parque, Torre B, pisos 6 – Bogotá D.C. PBX: (601) 327 55 00 o Línea Gratuita  
Nacional 01 8000 124211 fiducoldex@fiducoldex.com.co

[www.fiducoldex.com.co](http://www.fiducoldex.com.co)

“Defensor del Consumidor Financiero de la FIDUCIARIA COLOMBIANA DE COMERCIO EXTERIOR S.A. -FIDUCOLDEX- Dra. Liliana Otero Álvarez (Principal) y Dra. Lina Rocío Gutiérrez (Suplente) ubicadas en la Carrera 13 # 73 - 34 Oficina 202 Edificio Catania de la ciudad de Bogotá D.C. PBX: (601) 8088017 y celular: 313 7993800. E-mail: [defensorfiducoldex@umobogados.com](mailto:defensorfiducoldex@umobogados.com); Horario de atención: de 8:00 a.m. a 5:00 p.m. de lunes a viernes en jornada continua. Si Usted requiere información adicional acerca de la Defensoría del Consumidor Financiero de FIDUCOLDEX S.A., consúltenos de forma telefónica al teléfono 3275500, diríjase directamente a nuestras oficinas ubicadas en la Calle 28 No. 13A- 24 Piso 6, en la ciudad de Bogotá D.C., o al correo electrónico [fiducoldex@fiducoldex.com.co](mailto:fiducoldex@fiducoldex.com.co). Las funciones del Defensor del Consumidor son las que corresponden al artículo 13 de la Ley 1328 de 2009, y demás normas que la reglamentan y que se relacionan a continuación: 1.-Atender de manera oportuna y efectiva a los consumidores financieros de las entidades correspondientes.2.-Conocer y resolver en forma objetiva y gratuita para los consumidores, las quejas que éstos le presenten; 3.-Actuar como conciliador entre los consumidores financieros y la respectiva entidad vigilada en los términos indicados en la Ley 640 de 2001, su reglamentación, o en las normas que la modifiquen o sustituyan;4.-Ser vocero de los consumidores financieros ante la respectiva entidad vigilada.5.-Efectuar recomendaciones a la entidad vigilada relacionadas con los servicios y la atención al consumidor financiero, y en general en materias enmarcadas en el ámbito de su actividad;6.- Proponer a las autoridades competentes las modificaciones normativas que resulten convenientes para la mejor protección de los derechos de los consumidores financieros; y,7.- Las demás que le asigne el Gobierno Nacional y que tengan como propósito el adecuado, desarrollo del SAC.”