ADENDA 1

TÉRMINOS DE REFERENCIA 535

OBJETO: “La Fiduciaria Colombiana de Comercio Exterior S.A. FIDUCOLDEX, está interesada en contratar la prestación de servicios de una plataforma tecnológica, modalidad SaaS, que soporte la adecuada gestión del Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo- SARLAFT.

FIDUCOLDEX, actuando en nombre propio**,** conforme lo establecido en el numeral 1.7. de los Términos de Referencia, se permite Adendar en lo siguiente:

PRIMERO. - Se modifica el numeral 2.2 de los Términos de Referencia, con el fin de modificar un numeral de las Condiciones Específicas de la prestación del servicio de la plataforma tecnológica la el referido numeral será del siguiente tenor:

2.2 CONDICIONES TÉCNICAS Y ALCANCE DEL OBJETO

Condiciones Específicas de la prestación del servicio de la plataforma tecnológica.

La herramienta debe contar con dos (2) módulos: un (1) módulo de monitoreo transaccional de clientes y usuarios y un (1) módulo de consulta en listas restrictivas y medios relacionados, que se integren a los sistemas de información SIFI y SISA.

El módulo de monitoreo transaccional de clientes y usuarios debe:

- Ser un sistema paramétrico que permita identificar, gestionar y documentar en tiempo real y de forma centralizada señales de alerta, operaciones inusuales y/o sospechosas mediante el análisis automático realizado a las transacciones ejecutadas al interior de la Fiduciaria a través de la parametrización de reglas lógicas y fórmulas matemáticas.
- Integrarse con los core Fiduciarios (SIFI y SISA) permitiendo obtener la información básica y financiera de los terceros creados en los sistemas, así como las operaciones ejecutadas al interior de la Fiduciaria.
- Flujo de trabajo parametrizable que integre los diferentes actores que participan en la atención de las señales de alerta, permitiendo el análisis y documentación a varios niveles jerárquicos, así como la centralización de los soportes requeridos para la atención de los casos. Definición de reglas lógicas y construcción de fórmulas matemáticas a través de las cuales se analizan cada una de las operaciones ejecutadas al interior de la Fiduciaria con el fin de identificar operaciones inusuales.
- Envío de correos electrónicos a los responsables de atender las coincidencias generadas, así como a los jefes o superiores al momento de presentarse un vencimiento.
- Generación de alertas producto del monitoreo transaccional, las cuales pueden ser exportables en formato Word o Excel.
- El software debe procesar las alertas producto del proceso de segmentación de factores de riesgos SARLAFT

El módulo de listas debe tener listas restrictivas, listas asociadas a LA/FT, listas informativas, PEPS, listas propias, entre otras, y debe:

- Realizar la validación de terceros en listas restrictivas y de medios relacionados para detectar posibles asociaciones de individuos vinculados con actividades de LA/FT.
- Parametrizar los algoritmos de búsqueda requeridos de acuerdo a las necesidades, así como los porcentajes de coincidencia deseados en los resultados arrojados por la plataforma una vez ejecutadas las búsquedas manuales y/o cruces automáticos.
- Realizar el cruce automático con las bases de terceros de los core fiduciarios cada vez que las listas de control sean actualizadas, generando resultados coincidentes de los registros propios de la compañía con los registros en listas de control.
- Permitir la consulta de registros de manera individual y cargue masivo con tiempos de respuesta que estén acordes a la operatividad de la Fiduciaria.
- Actualización del software por lo menos una vez al año sin costo adicional

Condiciones Específicas de la prestación del servicio de la plataforma tecnológica.

- Capacitación técnica al área de tecnología relacionada con la conectividad, desarrollos realizados, integración de los sistemas existentes y demás temas concernientes con el uso de la herramienta.
- Capacitación funcional de la herramienta al personal responsable del manejo de la aplicación de los módulos operativos.
- Especificar los acuerdos de niveles de servicio (ANS) que ofrece y describir las condiciones que ofrece en atención al cliente para los aspectos del software ofrecido como soporte técnico 24x7, atención remota o por teléfono, etc.
- Certificar que los datos de Fiducoldex sean separados y no sean accesibles por otros clientes en la nube.
- Certificar que disponen de medidas de continuidad de negocio, en caso de incidente o de desastre.
- Garantizar la capacidad de escalamiento del servicio respecto a las necesidades de Fiducoldex.
- Garantizar la entrega de los datos pertenecientes a Fiducoldex, los cuales reposan en la infraestructura del proveedor, en el caso de finalización del contrato, asegurando la confidencialidad e integridad de la información y la posterior, destrucción de la mismos en las instalaciones del proveedor.
- Garantizar la trazabilidad de los registros (logs) que se generan sobre la plataforma y que hacen referencia al uso del software.
- Notificar cualquier incidente de seguridad de la información que afecte a Fiducoldex.
- Garantizar que el proveedor dispone de una política de tratamiento de datos personales aplicable, según la normatividad de Colombia.
- Presentar reportes históricos sobre fallas en los servicios suministrados por el proveedor y/o si han presentados incidentes de fuga de información, cada vez que se requiera por FIDUCOLDEX.
- Garantizar que cuenta con procedimientos definidos para la identificación, control y monitoreo de los riesgos de seguridad de la información.
- Garantizar que el proveedor dispone de políticas de copia de seguridad y de respaldo de información (Backup de datos).
- Garantizar que el software cuenta con las mejoras prácticas de desarrollo en materia de seguridad de la información y calidad del software.

- Garantizar que el software y su infraestructura cuenta con las últimas actualizaciones de seguridad (tales como parches, actualizaciones de antivirus, actualizaciones del sistema) que mitiguen vulnerabilidades conocidas.
- Garantizar el balanceo de carga para cuando se presente exceso de tráfico de información.
- Garantizar que todo intercambio de información con FIDUCOLDEX se intercambie de forma cifrada.
- Capacidad de respuesta en soporte técnico. El proveedor debe proporcionar documentado los niveles de servicio especificando tiempos de respuesta y solución del incidente que explique las características de atención según el nivel de criticidad.
- Certificar que el aplicativo soporta IPV6 nativo en coexistencia con IPV4, de acuerdo con lo establecido en la Resolución 2710 de 2017.

De igual manera, el proveedor que resulte seleccionado debe estar en la capacidad de suministrar la siguiente información:

- Entregar documentación del procedimiento de cómo se mitiga la fuga y pérdida de datos, fallos en el control de accesos, vulnerabilidad de los sistemas, secuestro de cuentas, empleados maliciosos.
- Certificar las medidas de seguridad de la información adoptadas para conservar los datos de Fiducoldex como actualizaciones, backups, auditoria, etc.
- Entregar documentación en donde se indiquen cuáles son las medidas de seguridad que aplican en las transferencias de datos.
- Certificar que el proveedor dispone de una política de seguridad de la información para el control de su infraestructura (firewalls, detección de antivirus, autenticación multifactor para el panel de control) y que se efectúan auditorías periódicamente por un ente externo.
- Certificar que el proveedor cuenta con políticas y acuerdos de confidencialidad para el manejo de la información bajo su responsabilidad.
- Certificar que el software y su infraestructura cumple con la normatividad colombiana aplicable para efectos de auditoria.

El proveedor debe ***certificar*** que cumple con la matriz CSA_CCM referente al cumplimiento de los controles de seguridad de la información en ambientes Cloud. ***Una vez seleccionado el proveedor, este debe documentar los controles implementados para el cumplimiento de la matriz CSA_CCM.***

Así mismo debe:

- Certificar el cumplimiento de la Ley de protección de datos personales -Ley 1581 de 2012
- Certificar que tiene implementados procedimientos para atención de: consultas, reclamos y gestión de incidentes.
- El proveedor sería nombrado como Encargado de la base de datos y cumpliría con sus deberes aplicados en materia de la ley de protección de datos personales. Adicionalmente, debe especificar una descripción de temas relacionados con:
- Soporte para la gestión de datos sensibles en el aplicativo (cifrado de información y otros controles soportados)
- Marcación y bloqueo de información de acuerdo con la ley.
- Soporte de borrado de información, dependiendo de las tablas de retención documental (TRD)
- Al ser un servicio en la nube, garantizar cumplimiento de la matriz de Controles de Seguridad en la Nube (CCM).

Con relación a Continuidad del Negocio:

Entregar documentación del procedimiento y/o certificaciones para el cumplimiento de la estrategia de continuidad provista, RTO ofrecidos y la estrategia para garantizar continuidad en caso de presentarse un incidente de seguridad

SEGUNDO. - Se modifica el numeral 2.2 de los Términos de Referencia, el cual quedará así:

2.9. ENTREGA Y PRESENTACIÓN DE LA PROPUESTA

La propuesta deberá estar firmada por el representante legal de la persona jurídica o su apoderado debidamente facultado, y ser presentada en i) Original; ii) Una copia en CD, con todos los documentos que la componen junto con su propuesta técnica y económica, incluyendo todos los archivos y anexos. De igual manera deberá entregarse el (Anexo 3) FTGAD15 (FORMATO INSCRIPCIÓN DE PROVEEDOR) teniendo especial cuidado de incluir todos los anexos que indica el formulario.

Los demás requerimientos contenidos en los Términos de Referencia, se mantienen en las mismas Condiciones.

TERCERO. - Se modifica el numeral VI de los Términos de Referencia, con el fin de modificar el nombre de los anexos, el cual será:

VI. FORMATOS Y ANEXOS

- Anexo No. 1. Carta de presentación de la propuesta
- Anexo No. 2. MATRIZ CLOUD CONTROLS MATRIX VERSION 3.0.
- Anexo No. 3. FTGAD15 (formato inscripción de proveedor).