LICITACIÓN PÚBLICA 09/2024
PLIEGO DE ESPECIFICACIONES TÉCNICAS

Objeto: PROVISION DE UNA PLATAFORMA DE DETECCION DE FRAUDE.

Fecha de Apertura: **06/11/2024** – 10.00 horas

Lugar de Apertura: Salón de los Presidentes – IAPSER Seguros – Casa Central, San Martín 918, Paraná, ER.

Presupuesto Oficial: U$D 116.000 + IVA (dólares estadounidenses CIENTO DIECISEIS MIL MAS IVA)

PLIEGO DE ESPECIFICACIONES TECNICAS

1. OBJETO

El presente llamado a Licitación Pública tiene por objeto la adquisición de una plataforma que debe proporcionar una solución tecnológica integral para la detección y prevención de fraudes en el sector asegurador, con capacidades de análisis de datos, inteligencia artificial y automatización de procesos de investigación. A continuación, se detallan las especificaciones técnicas y funcionales requeridas:

2. Características Funcionales

2.1 Detección de Fraude Basada en Inteligencia Artificial:

- El sistema debe utilizar algoritmos avanzados de Machine Learning y procesamiento de lenguaje natural (NLP) para detectar patrones de fraude en los reclamos y denuncias.
- Capacidad de análisis predictivo para detectar anomalías en tiempo real y alertar a los usuarios de posibles fraudes.
- Integración de modelos de clasificación y clustering para segmentar reclamos sospechosos y categorizarlos según el nivel de riesgo.

2.2 Análisis Multicanal:

- El sistema debe ser capaz de analizar datos de diferentes canales de comunicación, tales como audios fotos y documentos electrónicos.
- Permitir compartir información entre otras aseguradoras y el mercado.

2.3 Gestión de Casos y Flujos de Trabajo:

- Debe contar con un módulo para la gestión de casos de fraude, que permita la creación, seguimiento y resolución de incidentes.
- Capacidad para definir flujos de trabajo personalizados que incluyan la asignación automática de tareas a los investigadores de fraude.
- El sistema debe permitir la colaboración entre diferentes departamentos, con la posibilidad de adjuntar documentos y comentarios a cada caso.

2.4 Dashboards e Informes en Tiempo Real:

- El sistema debe ofrecer dashboards personalizables que presenten métricas clave sobre la cantidad de fraudes detectados, casos en curso, y análisis de tendencias.
- Capacidad para generar informes automatizados y exportar datos en diferentes formatos (PDF, Excel) para auditorías y reportes internos.
- Indicadores clave de desempeño (KPIs) para monitorear la efectividad de las investigaciones y la reducción del fraude.

2.5 Integración con Sistemas Externos:

- El sistema debe permitir la integración con bases de datos externas, y otros sistemas de gestión utilizados por la aseguradora.
- Soporte para la integración vía APIs para facilitar la conexión con otras plataformas relevantes, como registros de siniestros y bases de datos gubernamentales.

2.6 Configuración de Roles y Permisos:

- Debe contar con un sistema de gestión de usuarios que permita la creación de roles personalizados, asignación de permisos y restricciones de acceso según el nivel jerárquico del usuario.
- Soporte para la auditoría de acceso, con capacidad para registrar y reportar cada interacción de los usuarios con el sistema.

2.7 Escalabilidad y Personalización:

- El sistema debe ser escalable para soportar una creciente carga de datos y usuarios, sin afectar el rendimiento.
- Capacidad de personalización para ajustar las reglas de detección de fraude según las necesidades específicas de la compañía aseguradora.
- Capacidad de ser autoadministrable y configurable por la aseguradora cliente

2.8 Soporte Multilingüe y Multidivisa:

- El sistema debe soportar múltiples idiomas para su uso en diferentes jurisdicciones.
- Capacidad de manejar transacciones en distintas divisas para aseguradoras que operen en varios países.

2.9 Notificaciones y Alertas Automatizadas:

- El sistema debe permitir la configuración de alertas automatizadas por correo electrónico, SMS, o a través de la plataforma, cuando se detecten actividades sospechosas.
- Posibilidad de configurar alertas por niveles de criticidad (bajo, medio, alto) y asignar los casos a los equipos correspondientes.

3. Requisitos de Infraestructura

3.1 Plataforma en la Nube:

- El sistema debe estar implementado en una plataforma de nube certificada (preferiblemente Microsoft Azure) con alta disponibilidad, escalabilidad automática, y recuperación ante desastres (DRP) en múltiples zonas/regiones.
- La infraestructura en la nube debe garantizar una disponibilidad mínima del 99.9%.
- Soporte para configuraciones de red seguras, incluyendo la posibilidad de implementar VPN y reglas de firewall para restringir el acceso por direcciones IP específicas.

4. Seguridad de la Información

4.1 Certificaciones de Seguridad:

- El sistema debe cumplir con estándares internacionales de seguridad como ISO 27001 (Gestión de Seguridad de la Información) y debe estar en proceso o haber obtenido la certificación ISO 9001 (Gestión de Calidad).
- Cifrado de datos en reposo y en tránsito con algoritmos robustos, como AES de 256 bits, y autenticación de usuarios mediante SSL y protocolos seguros de conexión.

5. Gestión de Datos

5.1 Estructuración y Enriquecimiento de Datos:

- Capacidad para estructurar datos provenientes de diferentes fuentes, incluyendo audios del call center, fotos, y documentos digitales, con el fin de realizar investigaciones de fraude.
- El sistema debe soportar el análisis de videos y audios mediante técnicas de análisis de sentimiento y patrones para la detección de fraudes.

6. Cumplimiento Normativo

6.1 Políticas de Cumplimiento:

- El sistema debe estar alineado con las normativas locales e internacionales del sector asegurador en cuanto a prevención de fraudes y protección de datos (incluyendo normativas como GDPR).
- Auditorías de cumplimiento regulares para garantizar que el sistema opera de acuerdo con las normativas vigentes.

7. Soporte y Mantenimiento

7.1 Soporte Técnico:

- Soporte técnico 24/7 para incidentes críticos, con tiempos de respuesta en un máximo de 2 horas para problemas graves de seguridad o accesibilidad.
- Actualizaciones automáticas de seguridad y mejoras de sistema, con previo aviso al licenciatario.

3- Notas.

El oferente deberá ajustarse a los requisitos exigidos en el presente pliego de especificaciones técnicas quedando a su entera disponibilidad cotizar una plataforma con mayores funcionalidades a la mínima solicitada.

El oferente deberá suministrar una memoria descriptiva de la plataforma ofrecida, que permita apreciar claramente las características generales y particulares de estos, a efectos de una mejor evaluación.

El oferente deberá presentar una nómina de Aseguradores en donde se hayan realizado implementaciones similares a las solicitadas, debiendo informar Asegurada, y referente de la misma con Teléfono y Correo Electrónico.