

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
SECCIÓN DE COMPRA Y CONTRATACIONES
FICHA TECNICA

7 febrero, 2023

NO. SOLICITUD:	BAGRICOLA-CCC-LPN-2023-0001	OBJETO DE LA COMPRA:	CONTRATACION DE CONSULTORIA Y ADQUISICION DE UNA PLATAFORMA DE PREVENCIÓN DE FRAUDES, CUMPLIMIENTO Y RIESGO OPERACIONAL
RUBRO:	80101507 - Servicios de asesoramiento sobre tecnologías de la información	PLANIFICADA:	Si

DETALLES, ESPECIFICACIONES Y CONDICIONES ESPECIALES DE LOS SERVICIOS A SER OFERTADOS
1. MÓDULO DE PREVENCIÓN DE FRAUDES CANALES DIGITALES

No.	REQUISITOS	CUMPLE / NO CUMPLE
1.1	El sistema deberá contar con un modelo de prevención del fraude que incluya controles integrados y multicapa que cubran las diferentes etapas de la transacción en canales digitales incluyendo los ambientes Web y Movil e incorporando la Canal Digital de Personas y Canal Digital de Empresas: <ul style="list-style-type: none"> • Controles Onboarding en canales digitales • Evaluación de riesgos de los dispositivos que utiliza el cliente para acceder al canal transaccional • Analisis del comportamiento y evaluación de riesgos durante la sesión • Monitoreo y alertamiento del comportamiento del cliente en los canales digitales y sus habitos transaccionales • Monitoreo, alertamiento y correlación de eventos del comportamiento del cliente en los diferentes productos y canales digitales. 	
1.2	El sistema de prevención de fraude debe incluir un sistema experto de detección en la industria de prevención y control de fraude, sobre los productos de: <ul style="list-style-type: none"> • Protección en operaciones financieras a través de la banca digital web y banca móvil 	
1.3	El sistema debe poder llevar a cabo la evaluación de las transacciones de 3 (tres) formas distintas y complementarias así: <ul style="list-style-type: none"> • En Tiempo Real, lo que significa que la evaluación de la transacción se lleva a cabo dentro del flujo de autorización, en el momento en que se realiza la transacción. • Cerca al tiempo real, lo que significa llevar a cabo la evaluación de la transacción en paralelo al flujo de autorización, con un retraso de pocos milisegundos desde la finalización de la transacción. • Batch o Lote, lo que significa realizar la evaluación de la transacción en paralelo al flujo de autorización y en lotes, o grupos de transacciones, que eventualmente se produce con un retraso que va de unos minutos a unas horas desde la finalización de la transacción. 	
1.4	El sistema debe tener la posibilidad de funcionar con soluciones On-Premises, Cloud as a Service o Híbridas.	
1.5	El sistema debe aplicar modelos de Machine Learning con la capacidad de ser exportados para analisis mediante diferentes algoritmos que permitan rastrear el perfil de comportamiento de transacciones, teniendo en cuenta también el comportamiento del cliente / titular de la cuenta y los terminales, para generar una puntuación de fraude en ellos.	
1.6	El sistema debe poder recibir datos de múltiples procesos comerciales y múltiples canales, cubriendo todas las transacciones, y con la posibilidad de correlacionar eventos entre los procesos comerciales y canales.	
1.7	El sistema debe tener funcionalidad de listas del tipo: listas de bloqueo (listas negras), listas de excepciones (listas blancas), listas de terminales comprometidas, listas de direcciones IP comprometidas, entre otras, configurables en línea a través de la interfaz del sistema y permitiendo su creación, alteración y eliminación.	
1.8	El sistema debe ser altamente paramétrico, fácil y comprensible de utilizar, la entidad debe poder generar o modificar los controles por su cuenta sin depender del proveedor.	
1.9	El sistema debe tener la capacidad de construir un perfil transaccional integral de los cliente para cumplir con las normativas del regulador y ofrecer la capacidad de correlacionar eventos en tiempo real para ser más asertivos en la detección de fraude.	
1.10	El sistema deberá tener un grupo de reglas pre construidas que permitan evitar los principales casos conocidos de fraude por banca digital por medio de trasferencias de cuentas, ya sea de una a una o de una cuenta a múltiples cuentas, igualmente debe contar con condiciones de alertamiento y de identificación de cuentas mula.	

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
SECCIÓN DE COMPRA Y CONTRATACIONES
FICHA TECNICA
7 febrero, 2023

1.11	El sistema deberá llevar el perfil transaccional del cliente: qué operaciones hace usualmente, en qué fechas, por qué montos usuales, y usualmente a qué cuentas hace acreditamientos, y alertar cuando se den variaciones significativas contra el comportamiento transaccional.	
1.12	El sistema deberá controlar las operaciones administrativas que hace el personal interno de la entidad con la configuración del producto de Banca digital (Fraude Interno). Debe tener pre configurados controles de alertamiento en caso de operaciones administrativas sospechosas por sí mismas, o por la combinación entre operación administrativa sospechosa y posteriores operaciones financieras fuera del patrón normal de comportamiento.	
1.13	El sistema debe llevar un perfil navegacional del cliente, para registrar sus hábitos de opciones que utiliza. Para poder emitir alertas cuando hay variaciones sospechosas.	
1.14	El sistema pre configurado deberá ser capaz de integrar un scoring de riesgo total tomando en cuenta diferentes aspectos, que incluyan como mínimo: operaciones administrativas sobre la cuenta, operaciones financieras, hábito navegacional y desde dónde se conecta. Ese scoring de riesgo debe poderse utilizar para establecer prioridades de atención de alertas, o tomar acciones de alertamiento o no en función del índice de riesgo.	
1.15	El sistema deberá poder interactuar con el sistema autorizador de la entidad totalmente en línea para denegar la realización de transferencias u operaciones financieras bajo circunstancias de alta probabilidad de fraude.	
1.16	El sistema deberá realizar un monitoreo del comportamiento del cliente en sus dispositivos ej: velocidad de tecleo, movimiento del mouse, presión a la pantalla táctil del móvil etc, y generar alertas por variaciones significativas que pueden indicar que es otra persona o un sistema automatizado el que está registrando datos o utilizando los dispositivos.	
1.17	El sistema deberá incorporar una herramienta que obtenga información de los dispositivos que utiliza el cliente (Tablet, PC escritorio, Laptop, Móvil, etc.) y mediante esta información crear un perfil del dispositivo tipo "Device Finger Print", mediante el cual se realice una valoración de riesgo y se realicen los procesos de monitoreo y alertamiento de condiciones anómalas y fraudulentas y sus respectivas acciones de mitigación y contención.	
1.18	El sistema debe incluir mecanismos de alertamiento y contención de transacciones cuando se identifique que dado el comportamiento del dispositivo móvil se pueda inferir que este tiene un código malicioso tipo malware o troyanos, inclusive si no hay conexión en línea hacia los servidores de prevención de fraude, es decir el control de mitigación y seguridad de código malicioso debe estar incorporado en el SDK que se integra con el APP de la entidad.	
1.19	Los componentes de software provistos por el proveedor de la solución (Java Script/SDK) deben ser livianos y no generar impacto en el rendimiento de los entornos web y móviles.	
1.20	El sistema debe incorporar mecanismos de validación para identificar y alertar si los accesos vía internet desde los clientes corresponden a redes anonimadas tipo red TOR y/o provienen de Proxys catalogados de alto riesgo e incluidos en listas negras.	
1.21	La solución debe contar con un modelo de autenticación multifactor basada en procesos de autenticación fuerte que permita configurar el sistema para autorizar / denegar operaciones financieras en tiempo real y realizar validaciones por medio alterno con el cliente para operaciones de alto riesgo a partir de una variada gama de métodos de validación y confirmación de operaciones, el sistema de autenticación multifactor debe contar como mínimo con: <ul style="list-style-type: none"> - Generación de retos dinámicos - Los factores de autenticación pueden ser seleccionados de un grupo de retos disponibles para la entidad - Deben contener autenticación robusta - Deben tener inteligencia en los retos - Deben tener variedad en los retos - Deben tener facilidad de integración a la solución digital de la entidad 	
1.22	El sistema debe incorporar mecanismos de detección y alertamiento cuando el website de la entidad haya sido clonado y activado en servidores externos para campañas de Phishing hacia los clientes de la entidad.	
1.23	El proveedor debe presentar dentro del alcance de su propuesta un proceso de transferencia de conocimiento y capacitación certificada de este módulo de la solución.	
1.24	Este módulo del sistema deberá tener una licencia de suscripción por 3 AÑOS con mantenimiento y servicio incluido.	
1.25	El nivel de servicios (SLA) de mantenimiento y soporte para este módulo del sistema, deberá ser de 24*7*365	




BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
7 febrero, 2023
SECCIÓN DE COMPRA Y CONTRATACIONES
FICHA TECNICA
CAPACIDADES DE CONFIGURACIÓN Y COMPATIBILIDAD

1.26	Interfases de alimentación transaccional: La solución debe permitir el monitoreo de múltiples eventos transaccionales, proporcionar capacidades de configuración para que la institución pueda ir incorporando gradualmente nuevos controles a los eventos contratados, o poder crear nuevos eventos transaccionales y sus controles para la protección de los canales contratados, y poder establecer el método de comunicación para el envío de las transacciones a la herramienta de monitoreo. El sistema debe ajustarse por parametrización al orden y tamaño de los diferentes campos que contenga la trama. Todo esto para realizarlo de forma autónoma y sin que participe el proveedor.	
1.27	Interfases de alimentación transaccional: El sistema, al momento de recibir las transacciones, debe ser capaz de enriquecer la trama con información complementaria que no viene en el registro transaccional, que pueda ser necesario para el monitoreo. Ejemplo: traer el código del cliente e información adicional del mismo.	FA
1.28	Interfases de alimentación transaccional: El sistema debe permitir crear reglas de calidad de datos para alertar al área responsable de los registros que están llegando con errores. Las reglas de calidad de datos son configurables para que puedan ser creadas y modificadas por el personal de la institución de forma autónoma.	
1.29	Motor de Análisis: La solución debe ser parametrizable en cuanto a las reglas de monitoreo que podrán crearse o modificarse para cada evento transaccional, y la institución pueda crear sus propias reglas de forma independiente para la protección de los productos contratados.	FS
1.30	Motor de análisis: la solución debe poder correlacionar relaciones entre diferentes eventos transaccionales en la creación de reglas. Por ejemplo: relacionar transacciones monetarias anormales con modificación previa de información sensible relacionada de un evento administrativo.	
1.31	Motor de Análisis: La solución debe poder funcionar en Tiempo Real Sincrónico o Asincrónico con la capacidad de detener desde la primera transacción atípica o fraudulenta.	
1.32	Modelos Operativos pre constuidos: La solución debe incluir sistemas pre parametrizados para prevención de fraude sobre el motor de análisis principal, que incorpore conocimiento experto del sector financiero y mejores prácticas en controles antifraude, para permitir obtener resultados desde el primer día en producción, para las siguientes áreas: • Web Banking • Banca Móvil	
1.33	Los modelos de prevención deben incluir prevención de fraude interno y fraude externo.	
1.34	Los modelos de detección con conocimiento experto deben ser totalmente administrables y modificables por la institución después de la recepción de los mismos, sin dependencia del proveedor.	
1.35	El sistema debe permitir que cada área tenga y tipifique sus propios controles, alertas y reportes, de acuerdo a la perspectiva y responsabilidad de cada área en lo que refiere a la detección, prevención e investigación de fraudes.	
1.36	La solución debe proveer consultas y reportes de apoyo para evaluación de desempeño de los controles, ajustando el modelo en los momentos que sea requerido por la institución.	
1.38	La solución que soporta este modulo debiera ser compatible e integrarse con el Core Bancario EasyBank y Base de Datos Informix y SQL	
CAPACIDADES DE SEGURIDAD		
1.39	La solución debe contar con un sistema completo de administración de seguridad basados en perfiles de acceso. Los diferentes usuarios de la aplicación se deberan poder asociar a perfiles de acceso específicos.	
1.40	Los perfiles de acceso deberan controlar, además de las opciones de menú, los tipos de información o productos que pueden consultar y modificar, dependiendo del área o producto bajo su responsabilidad.	
1.41	El sistema de seguridad debe permitir configurar un control de validación para que modificaciones especificas puedan requerir de un doble ingreso de contraseña, o de ingreso de contraseña de un supervisor.	
1.42	El sistema debe generar bitácoras de auditoria de todos los cambios que se realicen en el mismo, e incluir consultas dinámicas sobre esa información.	
1.43	Se debe garantizar que los componentes de la solución no puedan ser modificados o alterados por personal no autorizado.	
1.44	El sistema debe garantizar la desconexión del usuario por tiempo de espera. Esta función debe ser configurable.	

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
SECCIÓN DE COMPRA Y CONTRATACIONES
FICHA TECNICA
7 febrero, 2023

1.45	El sistema debe permitir la desactivación y activación manual de los usuarios.	
1.46	El sistema debe garantizar que el mismo usuario no pueda estar activo, simultáneamente, en diferentes computadoras / conexiones.	
1.47	El sistema debe auditar las acciones a través de logs que registran todas las actividades de consulta y los cambios realizados por los usuarios del sistema	
CAPACIDADES DE DETECCIÓN		
1.48	<p>La solución debe utilizar un modelo combinado de detección de múltiples tecnologías para aumentar la eficiencia y eficacia, que incluya como mínimo los siguientes modelos de detección:</p> <ul style="list-style-type: none"> • Reglas expertas de negocio • Score Dinámico (puntuación y calificación de riesgos). • Patrones (secuencias y tiempos de operaciones entre distintas transacciones, tanto financieras como no financieras). • Factores de riesgo • Data mining on line • Redes Neuronales • Machine learning con herramientas que permitan exportar los dataset para entrenamiento en otras tecnologías de Machine Learning tipo ONNX. 	
1.49	La solución debe incluir perfil Transaccional por Cliente, Dispositivo, empleado, lugar de realización de la operación, y permite configurar perfiles estadísticos adicionales de forma paramétrica	
1.50	La solución debe incluir un sistema experto pre configurado para detectar patrones de fraude conocidos, así como detectar variaciones sospechosas fuera del comportamiento habitual del cliente y/o del empleado.	ER
1.51	El sistema debe permitir crear de forma paramétrica múltiples archivos de información estadística. Incluyendo diversos criterios de agrupación para saber el comportamiento de múltiples perfiles. Llevar contadores de transacciones, acumulados de montos, promedios para diferentes periodos de tiempo: diario, mensual, anual, y por periodos paramétricos de días. La información se debe calcular en línea con cada nueva transacción, para que el modelo de detección pueda detectar variaciones de comportamiento en real time sin tener que hacer esos cálculos con el histórico transaccional.	EJ
1.52	El sistema debe calcular un Score de riesgo de fraude a las transacciones analizadas para establecer una jerarquía de posibilidad de fraude, y permitir que en el proceso de investigación se pueda utilizar esa información para la prioridad de atención de las alertas.	
1.53	El sistema debe incluir criterios de velocidad de operaciones, y de georeferenciación.	
CAPACIDADES DE ALERTAMIENTO		
1.54	El sistema debe soportar que las alertas se puedan enviar de forma individual o combinada a: grupos de analistas-investigadores, a personas individuales, a gerentes, etc. Los criterios de distribución deben poder ser configurables por el destinatario final.	
1.55	<p>Envío de Alertas; el sistema de alertamiento debe tener la capacidad de enviar las alertas por los siguientes mecanismos:</p> <ul style="list-style-type: none"> • Consola de alertas que podrán ser atendidas por los analistas de fraude. • Vía Telefónica (canal de voz). • Mensajes SMS Bidireccional, es decir dar la capacidad al cliente responder un mensaje que alerte sobre un potencial fraude. • Por facebook messenger • Por Telegram, Whatsapp, Signal, otros. • A aplicaciones móviles tipo Push • E-mail. Enviar un texto con la descripción de una alerta individual • E-mail. Poder enviar reportes adjuntos que tengan el detalle de todas las alertas que cumplieron con ciertas características en un periodo de tiempo. 	
1.56	Para los envíos por vía telefónica, mensajes SMS, E-mail, se debe poder construir un texto de mensaje a enviar de forma paramétrica, que permita incluir tanto partes fijas como traer valores de diferentes campos de la transacción que se quieren alertar	
1.57	El sistema debe permitir la creación de alertas en línea (antes de autorizada la operación), y formar parte del proceso de autorización o negación de operaciones.	
1.58	Representación de alertas; el sistema debe indicar en las alertas mostradas las reglas que se cumplieron para generar la alerta.	

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
SECCIÓN DE COMPRA Y CONTRATACIONES
7 febrero, 2023
FICHA TECNICA

1.59	Agrupación de alertas; el sistema debe permitir a los analistas de fraude la agrupación de alertas por múltiples criterios de forma paramétrica. También deberá poder cambiarse el criterio de agrupación en vivo en caso que se necesite hacer algún análisis inmediato.	
1.60	El sistema debe permitir ejecutar acciones de defensa como: bloqueos, inactivaciones de terminales o usuarios, etc. Cuando se cumplan reglas que hagan necesario alguna acción de defensa, el sistema deberá poder ir a ejecutar rutinas específicas en los distintos aplicativos de la institución, previa asignación de permisos necesarios.	
1.61	El sistema debe contar con una consola de visualización de alertas que permita la administración de las mismas por parte de los grupos de analistas. Diferentes grupos deberán poder recibir información diferente dependiendo del área de responsabilidad a la que pertenezcan.	
1.62	La consola visualizadora de alertas debe permitir revisar el movimiento histórico de la cuenta que se esté analizando.	
1.63	La consola visualizadora de alertas deberá permitir seleccionar grupos de alertas o transacciones que cumplan con ciertos criterios.	
1.64	Entre las herramientas de apoyo a los investigadores de alertas deberá existir la funcionalidad de consulta al perfil del cliente, perfil de la cuenta, perfil del comercio, etc. Los perfiles deberán poder incluir tanto información transaccional resumida como información general. Los elementos que se muestren deberán poderse configurar de manera paramétrica.	
1.65	Los analistas deberán poder reordenar las columnas del visor de alertas en el proceso de gestión de alertas, según su conveniencia.	
1.66	Los analistas deberán, mediante el visor de alertas poder hacer filtros selectivos por cualquier criterio sobre la información presentada.	
1.67	El sistema tiene que permitir la corrección de casos ya previamente calificados, ejemplos: en vez de descartada ponerla como fraude, o en vez de fraude ponerla como buena y confirmada por el cliente.	
1.68	El sistema de alertas debe poder escalar alertas automáticamente según criterios previamente establecidos (ej. Tiempo transcurrido, riesgo, etc.).	
1.69	Los analistas de fraude deben poder calificar desde la consola de alertas el resultado del proceso de investigación, para retroalimentación del sistema: si la transacción efectivamente fue fraude, si el cliente confirmó que era una transacción válida, o si se descartó por criterio personal del analista.	
1.70	Los analistas de fraude deberán poder realizar un descarte de alertas de manera: Individual (una alerta) o Grupal (varias alertas).	
1.71	Listas de inclusión ó exclusión: el sistema deberá permitir incorporar información de listados especiales de inclusión ó exclusión para complementar reglas de forma paramétrica (listas negras, blancas o grises). Deben poderse cargar de forma automática de fuentes externas, o poderse grabar directamente en el sistema de forma manual.	
1.72	Consultas y modificaciones de cuentas e información de los clientes y funcionarios; el sistema debe permitir la incorporación de información de realización de consultas y modificaciones de información sensible de los clientes por parte de los empleados internos de la institución.	

CAPACIDADES DE REPORTES Y ESTADISTICAS

1.73	El sistema deberá contar con herramientas para generar reportes gerenciales y estadísticos, con los cuales se debe poder realizar el análisis de efectividad de las reglas creadas en la herramienta además de un análisis del comportamiento de los eventos, que permita a su vez depurar los procesos creados para la detección del fraude.	
1.74	La solución debe permitir el acceso inmediato y/o programado por medio de consultas y reportes, a todas aquellas transacciones que sean registradas en la misma y que por alguna necesidad del área operativa, se requiere tener acceso a la información.	
1.75	El acceso a la información de las transacciones debe contar con medidas de control de acceso para que solamente los perfiles indicados por la entidad puedan visualizar dicha información.	
1.76	Reportes automatizados; el administrador del sistema deberá poder configurar reportes.	
1.77	Reportes de transacciones; los analistas de fraude deberán poder generar reportes estadísticos de las transacciones alertadas.	

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
SECCIÓN DE COMPRA Y CONTRATACIONES
FICHA TECNICA

7 febrero, 2023

2. MÓDULO DE PREVENCIÓN DE FRAUDES PRODUCTOS Y SERVICIOS DE CARA AL CLIENTE Y EMISOR

No.	REQUISITOS	CUMPLE / NO CUMPLE
2.1	Este modulo prevención de fraude debe incluir un sistema experto de detección en la industria de prevención y control de fraude, sobre los productos de: <ul style="list-style-type: none"> • Tarjeta Crédito y Débito tanto en operaciones presentes como no presentes • Protección desde el punto de vista del emisor 	
2.2	El modelo de detección debe monitorear múltiples canales tales como: <ul style="list-style-type: none"> • ATMs • Puntos de venta físicos y electrónicos 	
2.3	El sistema debe poder llevar a cabo la evaluación de las transacciones de 3 (tres) formas distintas y complementarias: <ul style="list-style-type: none"> • en Tiempo real, dentro del flujo de autorización. • Cercano a tiempo real, con un retraso de pocos milisegundos desde la finalización de la transacción • Batch o lotes, en trupos de transacciones. 	
2.4	El sistema debe permitir la creación y gestión, por parte del usuario, de negocios multiples o procesos multi-negocio, cuyo análisis se realiza de forma segregada, pero que, por otro lado, puede ser operado y administrado en una sola plataforma.	
2.5	El sistema debe permitir la creación y gestión por parte del usuario, de vistas múltiples y flexibles sobre transacciones, tales como: evaluar una transacción desde el punto de vista del cliente / titular de la cuenta, evaluar una transacción bajo el punto vista del canal de acceso, evaluar desde el punto de vista de la transacción que esta realizando el cliente (Transferencia, inscripción de cuentas nuevas, pago de servicios, pago de tarjetas, pagos de creditos, recarga de moviles, etc.).	
2.6	El sistema debe permitir marcar el resultado de la investigación por parte del usuario, de cada transacción: Fraude, no fraude, descartado, pendiente.	
2.7	La solución debe permitir crear reglas de forma autónoma. Al construir estas reglas, se podrán evaluar: campos de las tramas transaccionales, información enriquecida de dichas tramas transaccionales (por ejemplo: datos del titular del producto, datos del dispositivo desde donde se está originando una transacción, riesgo del dispositivo, etc), valores estadísticos históricos por múltiples perfiles: contadores y acumuladores para distintos periodos de tiempo, valor más alto, valor más bajo, campos calculados por fórmula, comparaciones contra listas negras/blancas/grises o de inclusión/explusión, y tablas de riesgo dinámicas.	
2.8	La investigación de fraude y fraude sospechoso en la historia de las transacciones.	
2.9	El sistema debe permitir la generación de informes, incluidos, entre otros, informes operativos, informes de gestión, sintéticos y analíticos, que presentan los índices de rendimiento del modelo, las reglas y los usuarios del sistema, así como los niveles de fraude de los diferentes canales.	
2.10	El sistema debe permitir la gestión de la configuración para reglas, alertas, casos, flujos, perfiles de acceso y usuarios, en línea y accesibles para los usuarios del sistema sin requerir cambios o lanzamientos sistémicos por parte del equipo de desarrollo.	
2.11	El sistema debe implementar todos los procesos necesarios para adherirse a las buenas prácticas de la industria para monitorear transacciones.	
2.12	El sistema debe tener una interfaz gráfica amigable (GUI), disponible a través del navegador, que muestre toda la información (pantallas, formularios, informes, mensajes de error y todas las demás formas de interacción con el usuario).	
2.13	El sistema debe tener un único repositorio para almacenar toda la evidencia recopilada durante el proceso de investigación de un caso, y esa evidencia debe ser accesible solo para usuarios autorizados o grupos de usuarios desde la pantalla de ese caso.	
2.14	El sistema debe aplicar modelos de Machine Learning y redes Neurales para rastrear el perfil de comportamiento de transacciones, teniendo en cuenta también el comportamiento del cliente / titular de la cuenta y los terminales, para generar una puntuación de fraude en ellos.	
2.15	El sistema debe poder recibir datos de múltiples procesos comerciales y múltiples canales, cubriendo todas las transacciones, y con la posibilidad de correlacionar eventos entre los procesos comerciales y canales.	




BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
SECCIÓN DE COMPRA Y CONTRATACIONES
FICHA TECNICA

7 febrero, 2023

2.16	El sistema debe permitir la reevaluación de sus modelos para mantener su nivel de desempeño, a intervalos que serán definidos por la empresa contratante o al menos, cuando los niveles de desempeño del modelo (s) se vuelvan insatisfactorios.	
2.17	Cada modelo del sistema debe poder recibir, información externa, de otras entidades en el mercado financiero, y entregada por la empresa.	
2.18	El sistema debe tener funcionalidad de listas del tipo: listas de bloqueo (listas negras), listas de excepciones (listas blancas), listas de terminales comprometidas, listas de direcciones IP comprometidas, entre otras, configurables en línea a través de la interfaz del sistema y permitiendo su creación, alteración y eliminación	
2.19	El sistema debe implementar la funcionalidad (Workflow) de flujo de trabajo para manejar alertas entre diferentes grupos, en base a estados previamente configurados en línea.	
2.20	El sistema debe ser altamente paramétrico, fácil y comprensible de utilizar, la entidad debe poder generar o modificar los controles por su cuenta sin depender del proveedor	
2.21	El sistema debe tener la capacidad de construir un perfil transaccional integral de los cliente para cumplir con las normativas del regulador y ofrecer la capacidad de correlacionar eventos en tiempo real para ser más asertivos en la detección de fraude	
2.22	El proponente debe presentar dentro del alcance de su propuesta un proceso de transferencia de conocimiento y capacitación certificada de la solución	
2.23	Este modulo del sistema debera tener una licencia de suscripción por 3 AÑOS con mantenimiento y servicio incluido.	
2.24	El nivel de servicios (SLA) de mantenimiento y soporte para este modulo del sistema, debera ser de 24*7*365	
CAPACIDADES DE CONFIGURACIÓN Y COMPATIBILIDAD		
2.25	Multiproducto: La solución debe ser multiproducto, es decir, tiene que permitir el mantenimiento y monitoreo de los diferentes tipos de productos que posee la institución, considerando la operación identificada en ventanilla, back office y medios de pago.	
2.26	Interfaces de alimentación transaccional: La solución debe permitir el monitoreo de múltiples eventos transaccionales, proporcionar capacidades de configuración para que la institución pueda ir incorporando gradualmente nuevos controles a los eventos contratados, o poder crear nuevos eventos transaccionales y sus controles para la protección de los canales contratados, y poder establecer el método de comunicación para el envío de las transacciones a la herramienta de monitoreo. El sistema debe ajustarse por parametrización al orden y tamaño de los diferentes campos que contenga la trama. Todo esto para realizarlo de forma autónoma y sin que participe el proveedor.	
2.27	Interfaces de alimentación transaccional: El sistema, al momento de recibir las transacciones, debe ser capaz de enriquecer la trama con información complementaria que no viene en el registro transaccional, que pueda ser necesario para el monitoreo. Ejemplo: traer el código del cliente e información adicional del mismo.	
2.28	Interfaces de alimentación transaccional: El sistema, al momento de recibir las transacciones, debe ser capaz de enriquecer la trama con información complementaria que no viene en el registro transaccional, que pueda ser necesario para el monitoreo. Ejemplo: traer el código del cliente e información adicional del mismo.	
2.29	Interfaces de alimentación transaccional: El sistema, al momento de recibir las transacciones, debe ser capaz de enriquecer la trama con información complementaria que no viene en el registro transaccional, que pueda ser necesario para el monitoreo. Ejemplo: traer el código del cliente e información adicional del mismo.	
2.30	Interfaces de alimentación transaccional: El sistema, al momento de recibir las transacciones, debe ser capaz de enriquecer la trama con información complementaria que no viene en el registro transaccional, que pueda ser necesario para el monitoreo. Ejemplo: traer el código del cliente e información adicional del mismo.	
2.31	Interfaces de alimentación transaccional: El sistema, al momento de recibir las transacciones, debe ser capaz de enriquecer la trama con información complementaria que no viene en el registro transaccional, que pueda ser necesario para el monitoreo. Ejemplo: traer el código del cliente e información adicional del mismo.	
2.32	Interfaces de alimentación transaccional: El sistema, al momento de recibir las transacciones, debe ser capaz de enriquecer la trama con información complementaria que no viene en el registro transaccional, que pueda ser necesario para el monitoreo. Ejemplo: traer el código del cliente e información adicional del mismo.	

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
SECCIÓN DE COMPRA Y CONTRATACIONES
FICHA TECNICA

7 febrero, 2023

2.33	Los modelos de prevención deben incluir prevención de fraude interno y fraude externo.	
2.34	Los modelos de detección con conocimiento experto deben ser totalmente administrables y modificables por la institución después de la recepción de los mismos, sin dependencia del proveedor.	
2.35	El sistema debe permitir que cada área tenga y tipifique sus propios controles, alertas y reportes, de acuerdo a la perspectiva y responsabilidad de cada área en lo que refiere a la detección, prevención e investigación de fraudes.	
2.36	La solución debe proveer consultas y reportes de apoyo para evaluación de desempeño de los controles, ajustando el modelo en los momentos que sea requerido por la institución.	
2.37	La solución que soporta este modulo debera ser compatible e integrarse con el Core Bancario EasyBank y Base de Datos Informix y SQL.	
CAPACIDADES DE SEGURIDAD		
2.38	La solución debe contar con un sistema completo de administración de seguridad basados en perfiles de acceso. Los diferentes usuarios de la aplicación se deberán poder asociar a perfiles de acceso específicos.	
2.39	El control de acceso de usuarios al sistema debe soportar integración con un directorio activo de Microsoft.	
2.40	Los perfiles de acceso deberán controlar, además de las opciones de menú, los tipos de información o productos que pueden consultar y modificar, dependiendo del área o producto bajo su responsabilidad.	
2.41	El sistema de seguridad debe permitir configurar un control de validación para que modificaciones específicas puedan requerir de un doble ingreso de contraseña, o de ingreso de contraseña de un supervisor.	
2.42	El sistema debe generar bitácoras de auditoría de todos los cambios que se realicen en el mismo, e incluir consultas dinámicas sobre esa información.	
2.43	Se debe garantizar que los componentes de la solución no puedan ser modificados o alterados por personal no autorizado.	
2.44	El sistema debe garantizar la desconexión del usuario por tiempo de espera. Esta función debe ser configurable.	
2.45	El sistema debe permitir la desactivación y activación manual de los usuarios.	
2.46	El sistema debe garantizar que el mismo usuario no pueda estar activo, simultáneamente, en diferentes computadoras / conexiones.	
2.47	El sistema debe auditar las acciones a través de logs que registran todas las actividades de consulta y los cambios realizados por los usuarios del sistema	
CAPACIDADES DE DETECCIÓN		
2.47	La solución debe utilizar un modelo combinado de detección de múltiples tecnologías para aumentar la eficiencia y eficacia, que incluya como mínimo los siguientes modelos de detección: <ul style="list-style-type: none"> • Reglas expertas de negocio • Score Dinámico (puntuación y calificación de riesgos) • Patrones (secuencias y tiempos de operaciones entre distintas transacciones, tanto financieras como no financieras). • Factores de riesgo • Data mining on line • Redes Neuronales Nativas • Soportar protocolo ONNX para intercambio con los mejores modelos de machine learning del mercado 	
2.48	La solución debe incluir perfil Transaccional por Cliente, Dispositivo, empleados, lugar de realización de la operación, y permite configurar perfiles estadísticos adicionales de forma paramétrica	
2.49	La solución debe incluir un sistema experto pre configurado para detectar patrones de fraude conocidos, así como detectar variaciones sospechosas fuera del comportamiento habitual del cliente.	
2.50	La solución debe incluir un datamart estadístico que se pueda ir actualizando totalmente en línea y que pueda realizar validaciones de perfilamiento estadístico del cliente, cuenta, canal, etc, sin tener que buscar en los transaccionales históricos. Esto para permitir hacer estas evaluaciones en fracciones de segundo, lo que es requisito para ambientes en real time, donde se interactúa con el movimiento transaccional.	

En
 GS

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
SECCIÓN DE COMPRA Y CONTRATACIONES
FICHA TECNICA

7 febrero, 2023

2.51	El sistema debe permitir crear de forma paramétrica múltiples archivos de información estadística. Incluyendo diversos criterios de agrupación para saber el comportamiento de múltiples perfiles. Llevar contadores de transacciones, acumulados de montos, promedios para diferentes períodos de tiempo: diario, mensual, anual, y por períodos paramétricos de días. La información se debe calcular en línea con cada nueva transacción, para que el modelo de detección pueda detectar variaciones de comportamiento en real time sin tener que hacer esos cálculos con el histórico transaccional.	
2.52	Los modelos de machine learning se deben alimentar con información enriquecida incluyendo, como mínimo, lo siguiente: los campos de la transacción, los campos del cliente dueño del producto que realiza la transacción, información estadística actualizada del comportamiento del producto y del cliente	
2.53	El sistema debe calcular un Score de riesgo de fraude a las transacciones analizadas para establecer una jerarquía de posibilidad de fraude, y permitir que en el proceso de investigación se pueda utilizar esa información para la prioridad de atención de las alertas.	
2.54	El sistema debe incluir criterios de velocidad de operaciones, y de georeferenciación.	
2.55	El sistema debe permitir crear reglas mediante análisis de experto y basados en los datos de una transacción específica, o por un acumulado de transacciones.	
2.56	El sistema debe permitir el acople de diferentes reglas para formar nuevas reglas entre sí.	
2.57	El sistema debe permitir crear y modificar tablas paramétricas (listas blancas, negras, de inclusión, de exclusión, etc.). Las listas se deben poder alimentar: por aprendizaje automático, de forma manual, o importándolas de fuentes externas. Los elementos de la lista deben poder establecer un fecha límite de permanencia en la misma.	
2.58	Se pueden crear todas las listas que se requiera, sin limitaciones	
2.59	Las listas no tienen límite en la cantidad de elementos que la conforman	
2.60	El sistema debe permitir crear y modificar tablas paramétricas por múltiples campos: por ejemplo: límites por transacción, por día, y por mes para cierto tipo de operación, para cada producto. Se deben poder utilizar los elementos de esas listas al crear reglas de experto.	
2.61	El sistema debe mantener históricos del detalle transaccional para cada evento que se analice. La cantidad de meses de historia de cada evento que se deben mantener, deben ser configurables. Se debe poder hacer consultas a ese historial, filtrar por criterio, agrupar por algún criterio, o hacer gráficas estadísticas dinámicas para posteriores análisis.	
2.62	El sistema debe poder encontrar y alertar totalmente en línea y de forma automática de los posibles puntos de compromiso (coincidencias históricas en casos de fraude). El análisis de puntos de compromiso deberá poder hacerse por: coincidencia de terminales, coincidencia de empleados que participaron en operaciones administrativas sensibles relacionadas etc.	
2.63	El sistema debe poder identificar un lote de cuentas o transacciones posiblemente comprometidas que pasaron por posibles puntos de compromiso en las ventanas de riesgo, para poder tomar acciones con ellas.	
2.64	El sistema debe soportar que las alertas se puedan enviar de forma individual o combinada a: grupos de analistas-investigadores, a personas individuales, a gerentes, etc. Los criterios de distribución deben poder ser configurables por el destinatario final.	
2.65	Envío de Alertas; el sistema de alertamiento debe tener la capacidad de enviar las alertas por los siguientes mecanismos: <ul style="list-style-type: none"> • Consola de alertas que podrán ser atendidas por los analistas de fraude. • Vía Telefónica (canal de voz). • A aplicaciones móviles tipo Push • E-mail. Enviar un texto con la descripción de una alerta individual • E-mail. Poder enviar reportes adjuntos que tengan el detalle de todas las alertas que cumplieron con ciertas características en un período de tiempo. 	
2.66	Para los envíos por vía telefónica, mensajes SMS, E-mail, se debe poder construir un texto de mensaje a enviar de forma paramétrica, que permita incluir tanto partes fijas como traer valores de diferentes campos de la transacción que se quieren alertar.	
2.67	El sistema debe permitir la creación de alertas en línea (antes de autorizada la operación), y formar parte del proceso de autorización o negación de operaciones.	
2.68	Representación de alertas; el sistema debe indicar en las alertas mostradas las reglas que se cumplieron para generar la alerta.	
2.69	Agrupación de alertas; el sistema debe permitir a los analistas de fraude la agrupación de alertas por múltiples criterios de forma paramétrica. También deberá poder cambiarse el criterio de agrupación en vivo en caso que se necesite hacer algún análisis inmediato.	

Handwritten marks: a stylized signature and the number 6.

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
7 febrero, 2023
SECCIÓN DE COMPRA Y CONTRATACIONES
FICHA TECNICA

2.70	El sistema debe permitir ejecutar acciones de defensa como: bloqueos, inactivaciones de terminales o usuarios, etc. Cuando se cumplan reglas que hagan necesario alguna acción de defensa, el sistema deberá poder ir a ejecutar rutinas específicas en los distintos aplicativos de la institución, previa asignación de permisos necesarios.	
2.71	El sistema debe contar con una consola de visualización de alertas que permita la administración de las mismas por parte de los grupos de analistas. Diferentes grupos deberán poder recibir información diferente dependiendo del área de responsabilidad a la que pertenezcan.	
2.72	La consola visualizadora de alertas debe permitir revisar el movimiento histórico de la cuenta que se esté analizando.	
2.73	La consola visualizadora de alertas deberá permitir seleccionar grupos de alertas o transacciones que cumplan con ciertos criterios.	
2.74	Entre las herramientas de apoyo a los investigadores de alertas deberá existir la funcionalidad de consulta al perfil del cliente, perfil de la cuenta, perfil del comercio, etc. Los perfiles deberán poder incluir tanto información transaccional resumida como información general. Los elementos que se muestren deberán poderse configurar de manera paramétrica.	
2.75	Los analistas deberán poder reordenar las columnas del visor de alertas en el proceso de gestión de alertas, según su conveniencia.	
2.76	Los analistas deberán, mediante el visor de alertas poder hacer filtros selectivos por cualquier criterio sobre la información presentada.	
2.77	El sistema tiene que permitir la corrección de casos ya previamente calificados, ejemplos: en vez de descartada ponerla como fraude, o en vez de fraude ponerla como buena y confirmada por el cliente.	
2.78	El sistema de alertas debe poder escalar alertas automáticamente según criterios previamente establecidos (ej. Tiempo transcurrido, riesgo, etc.).	
2.79	Los analistas de fraude deben poder calificar desde la consola de alertas el resultado del proceso de investigación, para retroalimentación del sistema: si la transacción efectivamente fue fraude, si el cliente confirmó que era una transacción válida, o si se descartó por criterio personal del analista.	
2.80	Los analistas de fraude deberán poder realizar un descarte de alertas de manera: Individual (una alerta) o Grupal (varias alertas).	
2.81	Listas de inclusión ó exclusión: el sistema deberá permitir incorporar información de listados especiales de inclusión ó exclusión para complementar reglas de forma paramétrica (listas negras, blancas o grises). Deben poderse cargar de forma automática de fuentes externas, o poderse grabar directamente en el sistema de forma manual.	
2.82	Consultas y modificaciones de cuentas e información de los clientes y funcionarios; el sistema debe permitir la incorporación de información de realización de consultas y modificaciones de información sensible de los clientes por parte de los empleados internos de la institución.	
CAPACIDADES DE REPORTES Y ESTADISTICAS		
2.83	El sistema deberá contar con herramientas para generar reportes estadísticos, con los cuales se debe poder realizar el análisis de efectividad de las reglas creadas en la herramienta además de un análisis del comportamiento de los eventos, que permita a su vez depurar los procesos creados para la detección del fraude.	
2.84	El sistema debe soportar la generación de perfiles bajo criterios múltiples según la información disponible que se haga llegar a la aplicación, y dichos perfiles deberán poder ser consultados por los analistas de prevención de fraude. Ejemplo: perfil del cliente, perfil del empleado, perfil de la sucursal, perfil del comercio, etc.	
2.85	Reportes automatizados; el administrador del sistema deberá poder configurar el envío automatizado de reportes a cuentas de correo electrónico.	
2.86	Reportes de transacciones; los analistas de fraude deberán poder generar reportes estadísticos de las transacciones alertadas, con al menos los siguientes criterios: <ul style="list-style-type: none"> • Reglas que generaron la alerta. • Monto económico relacionado. • Reportes de reglas. 	

ER
GJ

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
SECCIÓN DE COMPRA Y CONTRATACIONES
7 febrero, 2023
FICHA TECNICA

2.87	<p>El administrador del sistema deberá poder configurar reportes estadísticos del uso de las reglas creadas, con al menos los siguientes criterios:</p> <ul style="list-style-type: none"> • Reglas más efectivas. • Reglas con mayor relación económica. • Reportes históricos de transacciones. 	
2.88	<p>El usuario del sistema deberá poder generar consultas y/o reportes detallados de los históricos de transacciones.</p>	
2.89	<p>Tableros de Control Gerencial. El sistema deberá tener la capacidad de presentar Tableros de Control Gerencial, considerando al menos:</p> <ul style="list-style-type: none"> • Gráficos de Análisis de fraude por región. • Gráficos de Canales de fraude con mayor frecuencia. • Gráficos de Tipos de Comercio con mayor frecuencia de fraude. • Gráficos de Alertas ingresadas con relación a fraudes confirmados. • Gráficos de Alertas gestionadas por analista. • Gráficos de Alertas pendientes por gestionar. • Gráficos de tipo de fraude con mayor frecuencia. • Gráficos de incidencia de fraude mensual y anual. 	
2.90	<p>Información de Clientes y Empleados; el sistema debe tener la capacidad de registrar la información del cliente y empleado así como visualizar en pantalla el perfil del cliente considerando al menos:</p> <ul style="list-style-type: none"> • Tipo de cliente. • Nombre completo. • Número de identificación. • Persona natural o jurídica. • Números de teléfono (al menos 3 registros). • Correo electrónico (al menos 3 registros). • Direcciones físicas (al menos 3 registros). • Declaración de movimientos transaccionales del cliente. 	
CAPACIDADES DE PREVENCIÓN DE FRAUDE EN TARJETA DE CRÉDITO Y DÉBITO DESDE EL PUNTO DEL VISTA DEL EMISOR		
2.91	<p>Modelos Operativos pre constuidos: La solución debe incluir un sistema experto pre configurado que incorpore conocimiento del sector financiero y mejores prácticas en controles antifraude, que permita a la entidad obtener resultados desde el primer día de puesta en marcha del sistema de prevención de fraude en Tarjeta de crédito y débito, desde el punto de vista de emisor, tanto para transacciones financieras con tarjeta presente como no presente.</p>	
2.92	<p>El sistema experto debe detectar fraude tanto en operaciones financieras como no financieras, fraude externo y fraude con complicidad interna.</p>	
2.93	<p>El sistema debe calcular un scoring de riesgo de fraude para cada alerta. Se debe poder trabajar las alertas ordenadas por ese scoring de riesgo, también se debe poder cambiar el criterio de ordenamiento</p>	
2.94	<p>El sistema debe poder funcionar 100% en tiempo real, con tiempos de respuesta exigidos por las marcas, informando al autorizador qué operaciones no se deben autorizar.</p>	
2.95	<p>En casos de rechazos en real time, el sistema debe poder iniciar un proceso de validación por medio alterno con el cliente para que él pueda confirmar si es él quien está haciendo la operación o no, para poderla autorizar o confirmar el rechazo. chat, contraseña escrita, contraseña enviada por medio audible, y que pueda acoplarse a medios alternos de validación que incorpore la institución en el futuro, como confirmación por huella u otros medios biométricos.</p>	
2.96	<p>El sistema debe permitir incorporar scorings de riesgo que vengan de otras plataformas o de las marcas, y utilizar ese indicador para generar su propio indicador de riesgo consolidado.</p>	
2.97	<p>Para compras en ambiente no presente, el sistema en real time deberá tener la posibilidad de brindar la funcionalidad al cliente final para que mediante el APP de la entidad pueda generar un código de seguridad dinámico para confirmar su compra (CVV Dinamico), en lugar del número que trae preimpreso la tarjeta, incluyendo también la validación del mismo en el momento de la autorización/rechazo de la operación.</p>	

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
SECCIÓN DE COMPRA Y CONTRATACIONES
FICHA TECNICA

7 febrero, 2023

2.98	<p>El sistema deberá contar con herramientas que permitan la autogestión del cliente en sus medios de pago mediante opciones en el APP de la entidad como:</p> <ul style="list-style-type: none"> • Apagado y encendido de sus tarjetas • Activar o desactivar el uso de las tarjetas en POS • Activar o desactivar el uso de las tarjetas en ATM's • Activar o desactivar el uso de las tarjetas en Internet • Activar o desactivar el uso de las tarjetas en el extranjero y por países. • Generar limites de uso por transacción, día o mes. 	
2.99	<p>La solución deberá llevar el control por cliente y guardar el perfil de comportamiento del mismo, para todas sus tarjetas, tanto para cuando tenga tarjetas secundarias como en el caso que tuvo cambio de tarjetas. El perfil histórico no deberá perderse cuando haga cambio de tarjeta.</p>	
2.100	<p>La solución debe ser PA-DSS Validated (Payment Application Data Security Standard) para estar alineada y validada con la normativa PCI, que incluye normas para encriptación de la información y visualización del número de la tarjeta.</p>	
2.101	<p>La solución debe ser capaz de analizar la secuencia de varias transacciones, para detectar comportamientos riesgosos de fraude. El usuario final debe poder incorporar nuevas secuencias de riesgo.</p>	
2.102	<p>El sistema debe poder analizar factores de riesgo e incorporarlos en el scoring completo del riesgo: control de velocidad, ubicación (geo referenciación), canal por el que se realiza la operación, horario, rango de monto, frecuencia, y variaciones con respecto al perfil del cliente, del comercio, del MCC.</p>	
2.103	<p>El sistema debe proveer reglas de conocimiento experto por patrones conocidos de fraude. El administrador de la solución deberá poder modificar esas reglas y crear adicionales. Deben poderse crear fórmulas con funciones estadísticas para detectar variaciones contra el perfil del comportamiento del cliente, de la tarjeta, del comercio, de la terminal o ATM.</p>	
2.104	<p>La eficiencia de cada una de las reglas debe poderse medir de manera independiente para cada una de ellas, para poder definir las mejores reglas, y las reglas que necesitan un afinamiento.</p>	
2.105	<p>El sistema deberá llevar un registro de las transacciones fraudulentas que no fueron detectadas, e incorporar un ambiente donde puedan incorporarse y probar reglas nuevas para detectar esas transacciones no detectadas y aumentar la eficiencia del modelo.</p>	
2.106	<p>El sistema deberá contar con controles para tarjetas con chip.</p>	
2.107	<p>El sistema deberá incluir un módulo de administración eficiente de alertas que pueda configurarse su apariencia de forma paramétrica. Deberá permitir consultar la forma de integración del scoring, permitir la consulta del estado de cuenta del cliente con criterios de selección, hacer búsquedas y agrupamientos de información.</p>	
2.108	<p>El módulo de administración de alertas debe permitir hacer búsqueda del perfil del cliente, del perfil del comercio, y otros tipos de perfil. Deberá permitir ver tanto datos generales del cliente o comercio, notificaciones de viaje, y otros campos, los cuales se puedan definir de forma paramétrica. Deberá permitir revisar también el resumen de comportamiento del cliente.</p>	
2.110	<p>El módulo de administración de alertas deberá poderse integrar con sistemas de video vigilancia para poder ver la imagen de las personas que realizaron operaciones sospechosas.</p>	
2.111	<p>El sistema deberá incluir la funcionalidad de bloqueos de tarjeta, de perfil de cliente, de empleado, de manera automática para operaciones de alto riesgo.</p>	
2.112	<p>El sistema deberá brindar consultas y reporteria orientada a diferentes tipos de usuario: para el supervisor de investigadores, para el gerente de riesgos o tarjeta, y para el responsable de optimización del sistema de reglas, etc.</p>	
2.113	<p>La solución deberá contar con un sistema de aprendizaje automático que mejore la eficiencia de las reglas en el tiempo, en función de los casos fraude que se detecten.</p>	
2.114	<p>El sistema deberá encontrar y alertar totalmente en línea y de forma automática los posibles puntos de compromiso en base al historial de las tarjetas que sufran fraude. El análisis de puntos de compromiso deberá hacerse por comercios, terminales comunes de consumo, usuarios que participaron en operaciones administrativas sensibles sobre esas tarjetas, permitiendo a la institución identificar potenciales fraudes en el compromiso de información.</p>	

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
SECCIÓN DE COMPRA Y CONTRATACIONES
FICHA TECNICA
7 febrero, 2023

2.115	El sistema deberá identificar lotes de tarjetas posiblemente comprometidas que pasaron por posibles puntos de compromiso en las ventanas de riesgo, para poder tomar acciones automáticas con ellas.	
2.116	Detección de puntos comunes de fraude; el sistema debe incorporar la capacidad de identificar puntos comunes de fraude en tiempo real, como comercios, regiones, países, mcc y proporcionar información sobre los mismos. Esos puntos comunes de fraude también deben actualizar el modelo de manera automática e inmediata como parte del proceso de auto ajuste del modelo.	
3. MÓDULO DE PREVENCIÓN DE FRAUDES DE OPERACIONES INTERNAS		
No.	REQUISITOS	CUMPLE / NO CUMPLE
3.1	El modelo de detección debe monitorear múltiples canales tales como: <ul style="list-style-type: none"> • Unidades, Secciones y Departamentos Internos • Localidad Sucursales • Localidad Oficinas de Servicios • Localidad Stands 	
3.2	El sistema debe poder llevar a cabo la evaluación de las transacciones de 3 (tres) formas distintas y complementarias: <ul style="list-style-type: none"> • en Tiempo real, dentro del flujo de autorización. • Cercano a tiempo real, con un retraso de pocos milisegundos desde la finalización de la transacción • Batch o lotes, en trupos de transacciones. 	
3.3	El sistema debe permitir la creación y gestión, por parte del usuario, de negocios multiples o procesos multi-negocio, cuyo análisis se realiza de forma segregada, pero que, por otro lado, puede ser operado y administrado en una sola plataforma.	
3.4	El sistema debe permitir la creación y gestión por parte del usuario, de vistas múltiples y flexibles sobre transacciones, tales como: evaluar una transacción desde el punto de vista del cliente / titular de la cuenta, evaluar una transacción bajo el punto vista del canal de acceso, evaluar desde el punto de vista de la transacción que esta realizando el cliente (Transferencia, inscripción de cuentas nuevas, pago de servicios, pago de tarjetas, pagos de creditos, recarga de moviles, etc.).	
3.5	El sistema debe permitir marcar el resultado de la investigación por parte del usuario, de cada transacción: Fraude, no fraude, descartado, pendiente.	
3.6	La solución debe permitir crear reglas de forma autónoma. Al construir estas reglas, se podrán evaluar: campos de las tramas transaccionales, información enriquecida de dichas tramas transaccionales (por ejemplo: datos del titular del producto, datos del dispositivo desde donde se está originando una transacción, riesgo del dispositivo, etc), valores estadísticos históricos por múltiples perfiles: contadores y acumuladores para distintos periodos de tiempo, valor más alto, valor más bajo, campos calculados por fórmula, comparaciones contra listas negras/blancas/grises o de inclusión/exclusión, y tablas de riesgo dinámicas.	
3.7	La investigación de fraude y fraude sospechoso en la historia de las transacciones.	
3.8	El sistema debe permitir la generación de informes, incluidos, entre otros, informes operativos, informes de gestión, sintéticos y analíticos, que presentan los índices de rendimiento del modelo, las reglas y los usuarios del sistema, así como los niveles de fraude de los diferentes canales.	
3.9	El sistema debe permitir la gestión de la configuración para reglas, alertas, casos, flujos, perfiles de acceso y usuarios, en línea y accesibles para los usuarios del sistema sin requerir cambios o lanzamientos sistémicos por parte del equipo de desarrollo.	
#####	El sistema debe implementar todos los procesos necesarios para adherirse a las buenas prácticas de la industria para monitorear transacciones.	
3.11	El sistema debe tener una interfaz gráfica amigable (GUI), disponible a través del navegador, que muestre toda la información (pantallas, formularios, informes, mensajes de error y todas las demás formas de interacción con el usuario).	
3.12	El sistema debe tener un único repositorio para almacenar toda la evidencia recopilada durante el proceso de investigación de un caso, y esa evidencia debe ser accesible solo para usuarios autorizados o grupos de usuarios desde la pantalla de ese caso.	
3.13	El sistema debe aplicar modelos de Machine Learning y redes Neuronales para rastrear el perfil de comportamiento de transacciones, teniendo en cuenta también el comportamiento del empleado, para generar una puntuación de fraude en ellos.	

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA

7 febrero, 2023

SECCIÓN DE COMPRA Y CONTRATACIONES
FICHA TECNICA

3.14	El sistema debe permitir la reevaluación de sus modelos para mantener su nivel de desempeño, a intervalos que serán definidos por la empresa contratante o al menos, cuando los niveles de desempeño del modelo (s) se vuelvan insatisfactorios.	
3.15	El sistema debe tener funcionalidad de listas del tipo: listas de bloqueo (listas negras), listas de excepciones (listas blancas), listas de terminales comprometidas, listas de direcciones IP comprometidas, entre otras, configurables en línea a través de la interfaz del sistema y permitiendo su creación, alteración y eliminación	
3.16	El sistema debe implementar la funcionalidad (Workflow) de flujo de trabajo para manejar alertas entre diferentes grupos, en base a estados previamente configurados en línea.	
3.17	El sistema debe ser altamente paramétrico, fácil y comprensible de utilizar, la entidad debe poder generar o modificar los controles por su cuenta sin depender del proveedor	
3.18	El sistema debe tener la capacidad de construir un perfil transaccional integral de los cliente para cumplir con las normativas del regulador y ofrecer la capacidad de correlacionar eventos en tiempo real para ser más asertivos en la detección de fraude	
3.19	El proponente debe presentar dentro del alcance de su propuesta un proceso de transferencia de conocimiento y capacitación certificada de la solución	
CAPACIDADES DE CONFIGURACIÓN		
3.20	Multiproducto: La solución debe ser multiproducto, es decir, tiene que permitir el mantenimiento y monitoreo de los diferentes tipos de productos que posee la institución, considerando la operación identificada en ventanilla, back office y medios de pago.	
3.21	Interfases de alimentación transaccional: La solución debe permitir el monitoreo de múltiples eventos transaccionales, proporcionar capacidades de configuración para que la institución pueda ir incorporando gradualmente nuevos controles a los eventos contratados, o poder crear nuevos eventos transaccionales y sus controles para la protección de los canales contratados, y poder establecer el método de comunicación para el envío de las transacciones a la herramienta de monitoreo. El sistema debe ajustarse por parametrización al orden y tamaño de los diferentes campos que contenga la trama. Todo esto para realizarlo de forma autónoma y sin que participe el proveedor.	E/A
3.22	Interfases de alimentación transaccional: El sistema, al momento de recibir las transacciones, debe ser capaz de enriquecer la trama con información complementaria que no viene en el registro transaccional, que pueda ser necesario para el monitoreo. Ejemplo: traer el código del cliente e información adicional del mismo.	G
3.23	Interfases de alimentación transaccional: El sistema debe permitir crear reglas de calidad de datos para alertar al área responsable de los registros que están llegando con errores. Las reglas de calidad de datos son configurables para que puedan ser creadas y modificadas por el personal de la institución de forma autónoma.	
3.24	Motor de Análisis: La solución debe ser parametrizable en cuanto a las reglas de monitoreo que podrán crearse o modificarse para cada evento transaccional, y la institución pueda crear sus propias reglas de forma independiente para la protección de los productos contratados.	
3.25	Motor de análisis: la solución debe poder correlacionar relaciones entre diferentes eventos transaccionales en la creación de reglas. Por ejemplo: relacionar transacciones monetarias anormales con modificación previa de información sensible relacionada de un evento administrativo	
3.26	Motor de Análisis: La solución debe poder funcionar en Tiempo Real Sincrónico o Asincrónico con la capacidad de detener desde la primera transacción atípica o fraudulenta.	
3.27	Modelos Operativos pre constuidos: La solución debe incluir sistemas pre parametrizados para prevención de fraude sobre el motor de análisis principal, que incorpore conocimiento experto del sector financiero y mejores prácticas en controles antifraude, para permitir obtener resultados desde el primer día en producción, para las siguientes áreas: • Cuentas de depósito (ahorros, cheques y plazos fijos) • El sistema debe contener los escenarios más importantes en cuanto a tipologías de fraude tanto interno como externo enfocado en cuentas de depósito y múltiples canales.	
3.28	Los modelos de prevención deben incluir prevención de fraude interno y fraude externo.	

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
SECCIÓN DE COMPRA Y CONTRATACIONES
FICHA TECNICA

7 febrero, 2023

3.29	Los modelos de detección con conocimiento experto deben ser totalmente administrables y modificables por la institución después de la recepción de los mismos, sin dependencia del proveedor.	
3.30	El sistema debe permitir que cada área tenga y tipifique sus propios controles, alertas y reportes, de acuerdo a la perspectiva y responsabilidad de cada área en lo que refiere a la detección, prevención e investigación de fraudes.	
3.31	La solución debe proveer consultas y reportes de apoyo para evaluación de desempeño de los controles, ajustando el modelo en los momentos que sea requerido por la institución.	
CAPACIDADES DE SEGURIDAD		
3.32	La solución debe contar con un sistema completo de administración de seguridad basados en perfiles de acceso. Los diferentes usuarios de la aplicación se deberán poder asociar a perfiles de acceso específicos.	
3.33	El control de acceso de usuarios al sistema debe soportar integración con un directorio activo de Microsoft.	
3.34	Los perfiles de acceso deberán controlar, además de las opciones de menú, los tipos de información o productos que pueden consultar y modificar, dependiendo del área o producto bajo su responsabilidad.	
3.35	El sistema de seguridad debe permitir configurar un control de validación para que modificaciones específicas puedan requerir de un doble ingreso de contraseña, o de ingreso de contraseña de un supervisor.	
3.36	El sistema debe generar bitácoras de auditoría de todos los cambios que se realicen en el mismo, e incluir consultas dinámicas sobre esa información.	
3.37	Se debe garantizar que los componentes de la solución no puedan ser modificados o alterados por personal no autorizado.	
3.38	El sistema debe garantizar la desconexión del usuario por tiempo de espera. Esta función debe ser configurable.	
3.39	El sistema debe permitir la desactivación y activación manual de los usuarios.	
3.40	El sistema debe garantizar que el mismo usuario no pueda estar activo, simultáneamente, en diferentes computadoras / conexiones.	
3.41	El sistema debe auditar las acciones a través de logs que registran todas las actividades de consulta y los cambios realizados por los usuarios del sistema	
CAPACIDADES DE DETECCIÓN		
3.42	La solución debe utilizar un modelo combinado de detección de múltiples tecnologías para aumentar la eficiencia y eficacia, que incluya como mínimo los siguientes modelos de detección: <ul style="list-style-type: none"> • Reglas expertas de negocio • Score Dinámico (puntuación y calificación de riesgos). • Patrones (secuencias y tiempos de operaciones entre distintas transacciones, tanto financieras como no financieras). • Factores de riesgo • Data mining on line • Redes Neuronales • Machine learning con herramientas que permitan exportar los dataset para entrenamiento en otras tecnologías de Machine Learning tipo ONNX. 	
3.43	La solución debe incluir perfil Transaccional por Cliente, Dispositivo, empleado, lugar de realización de la operación, y permite configurar perfiles estadísticos adicionales de forma paramétrica	
3.44	La solución debe incluir un sistema experto pre configurado para detectar patrones de fraude conocidos, así como detectar variaciones sospechosas fuera del comportamiento habitual del cliente y/o del empleado.	
3.45	El sistema debe permitir crear de forma paramétrica múltiples archivos de información estadística. Incluyendo diversos criterios de agrupación para saber el comportamiento de múltiples perfiles. Llevar contadores de transacciones, acumulados de montos, promedios para diferentes períodos de tiempo: diario, mensual, anual, y por períodos paramétricos de días. La información se debe calcular en línea con cada nueva transacción, para que el modelo de detección pueda detectar variaciones de comportamiento en real time sin tener que hacer esos cálculos con el histórico transaccional.	

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
SECCIÓN DE COMPRA Y CONTRATACIONES
FICHA TECNICA

7 febrero, 2023

3.46	El sistema debe calcular un Score de riesgo de fraude a las transacciones analizadas para establecer una jerarquía de posibilidad de fraude, y permitir que en el proceso de investigación se pueda utilizar esa información para la prioridad de atención de las alertas.	
3.47	El sistema debe incluir criterios de velocidad de operaciones, y de georeferenciación.	
CAPACIDADES DE ALERTAMIENTO		
3.48	El sistema debe soportar que las alertas se puedan enviar de forma individual o combinada a: grupos de analistas-investigadores, a personas individuales, a gerentes, etc. Los criterios de distribución deben poder ser configurables por el destinatario final.	
3.49	Envío de Alertas; el sistema de alertamiento debe tener la capacidad de enviar las alertas por los siguientes mecanismos: <ul style="list-style-type: none"> • Consola de alertas que podran ser atendidas por los analistas de fraude. • Vía Telefónica (canal de voz). • Mensajes SMS Bidireccional, es decir dar la capacidad al cliente responder un mensaje que alerte sobre un potencial fraude. • Por facebook messenger • Por Telegram, Whatsapp, Signal, otros. • - A aplicaciones móviles tipo Push • E-mail. Enviar un texto con la descripción de una alerta individual • E-mail. Poder enviar reportes adjuntos que tengan el detalle de todas las alertas que cumplieron con ciertas características en un periodo de tiempo. 	
3.50	Para los envíos por vía telefónica, mensajes SMS, E-mail, se debe poder construir un texto de mensaje a enviar de forma paramétrica, que permita incluir tanto partes fijas como traer valores de diferentes campos de la transacción que se quieren alertar	
3.51	El sistema debe permitir la creación de alertas en línea (antes de autorizada la operación), y formar parte del proceso de autorización o negación de operaciones.	
3.52	Representación de alertas; el sistema debe indicar en las alertas mostradas las reglas que se cumplieron para generar la alerta.	
3.53	Agrupación de alertas; el sistema debe permitir a los analistas de fraude la agrupación de alertas por múltiples criterios de forma paramétrica. También deberá poder cambiarse el criterio de agrupación en vivo en caso que se necesite hacer algún análisis inmediato.	
3.54	El sistema debe permitir ejecutar acciones de defensa como: bloqueos, inactivaciones de terminales o usuarios, etc. Cuando se cumplan reglas que hagan necesario alguna acción de defensa, el sistema deberá poder ir a ejecutar rutinas específicas en los distintos aplicativos de la institución, previa asignación de permisos necesarios.	
3.55	El sistema debe contar con una consola de visualización de alertas que permita la administración de las mismas por parte de los grupos de analistas. Diferentes grupos deberán poder recibir información diferente dependiendo del área de responsabilidad a la que pertenezcan.	
3.56	La consola visualizadora de alertas debe permitir revisar el movimiento histórico de la cuenta que se esté analizando.	
3.57	La consola visualizadora de alertas deberá permitir seleccionar grupos de alertas o transacciones que cumplan con ciertos criterios.	
3.58	Entre las herramientas de apoyo a los investigadores de alertas deberá existir la funcionalidad de consulta al perfil del cliente, perfil de la cuenta, perfil del comercio, etc. Los perfiles deberán poder incluir tanto información transaccional resumida como información general. Los elementos que se muestren deberán poderse configurar de manera paramétrica.	
3.59	Los analistas deberán poder reordenar las columnas del visor de alertas en el proceso de gestión de alertas, según su conveniencia.	
3.60	Los analistas deberán, mediante el visor de alertas poder hacer filtros selectivos por cualquier criterio sobre la información presentada.	
3.61	El sistema tiene que permitir la corrección de casos ya previamente calificados, ejemplos: en vez de descartada ponerla como fraude, o en vez de fraude ponerla como buena y confirmada por el cliente.	
3.62	El sistema de alertas debe poder escalar alertas automáticamente según criterios previamente establecidos (ej. Tiempo transcurrido, riesgo, etc.).	
3.63	Los analistas de fraude deben poder calificar desde la consola de alertas el resultado del proceso de investigación, para retroalimentación del sistema: si la transacción efectivamente fue fraude, si el cliente confirmó que era una transacción válida, o si se descartó por criterio personal del analista.	

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
SECCIÓN DE COMPRA Y CONTRATACIONES
FICHA TECNICA

7 febrero, 2023

3.64	Los analistas de fraude deberan poder realizar un descarte de alertas de manera: Individual (una alerta) o Grupal (varias alertas).	
3.65	Listas de inclusión ó exclusión: el sistema deberá permitir incorporar información de listados especiales de inclusión ó exclusión para complementar reglas de forma paramétrica (listas negras, blancas o grises). Deben poderse cargar de forma automática de fuentes externas, o poderse grabar directamente en el sistema de forma manual.	
3.66	Consultas y modificaciones de cuentas e información de los clientes y funcionarios; el sistema debe permitir la incorporación de información de realización de consultas y modificaciones de información sensible de los clientes por parte de los empleados internos de la institución.	

CAPACIDADES DE REPORTES Y ESTADISTICAS

3.67	El sistema deberá contar con herramientas para generar reportes gerenciales y estadísticos, con los cuales se debe poder realizar el análisis de efectividad de las reglas creadas en la herramienta además de un análisis del comportamiento de los eventos, que permita a su vez depurar los procesos creados para la detección del fraude.	
3.68	La solución debe permitir el acceso inmediato y/o programado por medio de consultas y reportes, a todas aquellas transacciones que sean registradas en la misma y que por alguna necesidad del área operativa, se requiere tener acceso a la información.	
3.69	El acceso a la información de las transacciones debe contar con medidas de control de acceso para que solamente los perfiles indicados por la entidad puedan visualizar dicha información.	
3.70	Reportes automatizados; el administrador del sistema deberá poder configurar reportes.	
3.71	Reportes de transacciones; los analistas de fraude deberan poder generar reportes estadísticos de las transacciones alertadas.	
3.72	Este módulo del sistema deberá tener una licencia de suscripción por 3 AÑOS con mantenimiento y servicio incluido.	

4. MODULO DE CUMPLIMIENTO Y PREVENCION DE LAVADO DE DINERO

No.	REQUISITOS	CUMPLE / NO CUMPLE
4.1	Cumple con marcos de referencia internacional como GAFI, Acta Patriota, BSA.	
4.2	El sistema tiene la capacidad de realizar una gestión cualitativa de evaluación de riesgos de lavado de dinero acorde al ISO 31000 (Identificar, Analizar, Evaluar y establecer medidas de mitigación del riesgo)	
4.3	En el caso de la evaluación de riesgo de la cartera de clientes, el sistema esta basado en el análisis de factores de riesgo considerando como mínimo: Personas, productos, canales, jurisdicciones y análisis de comportamiento transaccional.	
4.4	El sistema permite crear, modificar o eliminar factores y subfactores de riesgo de una forma paramétrica.	
4.5	El sistema puede manejar excepciones a través de un valor default para campos que no tengan correspondencia en una tabla. Por ejemplo actividad económica.	
4.6	En base a los factores definidos el sistema deberá asignar un nivel de riesgo por cliente en base a una escala determinada (como mínimo alto, mediano y bajo riesgo)	
4.7	El sistema puede interactuar con el proceso de apertura de cuentas para brindar el riesgo inherente de cliente y así mismo indicar si hay coincidencias con listas PEPs y las que se definan como parte del proceso.	
4.8	Durante la relación comercial con el cliente, el sistema permite aplicar medidas de control para mitigar el riesgo del cliente y obtener una calificación de riesgo residual.	
4.9	El sistema permite evaluar periódicamente el riesgo a nivel de cartera de clientes y compararlo con periodos anteriores.	
4.10	El sistema cuenta con una consulta de la valoración de riesgo del cliente de los últimos dos años y puede mostrar la calificación por cada factor de riesgo y bajar a detalle de la calificación de los subfactores de riesgo.	
4.11	El sistema permite segmentar a los clientes por nivel de riesgo inherente o residual.	

ER
65

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA

7 febrero, 2023

SECCIÓN DE COMPRA Y CONTRATACIONES
FICHA TECNICA

4.12	El sistema permite evaluar el riesgo de cliente en función de coincidencias con listas como OFAC, CIA, ONU, PEPs, y otras que la institución maneje como parte de sus bases de datos.	
4.13	El sistema permite barridos periódicos a la base de datos de clientes buscando nuevas coincidencias con listas.	
4.14	El sistema permite la gestión de riesgo empleados.	
4.15	El sistema permite al gestión de riesgo de proveedores y terceras partes.	
4.16	Permite la asignación de riesgo por jurisdicciones (países, regiones, paraísos fiscales, etc.)	
4.17	El sistema permite el manejo de riesgo por sucursales y región del país donde operen.	
4.18	El sistema permite asignar un nivel de riesgo a los canales y productos de la institución.	
4.19	El sistema permite afinar el modelo de factores de riesgo en base a modelos de reconocido valor técnico (modelos matemáticos, estadísticos o sistemas de inteligencia artificial)	
4.20	El sistema cuenta con un ambiente de simulación para poder evaluar escenarios derivados de cambios en la parametrización del sistema	
4.21	El sistema permite el afinamiento de los pesos asociados a los factores de riesgo sugiriendo modificaciones a los pesos en base al análisis de comportamiento histórico	
4.22	Permite considerar la información proporcionada por el cliente sobre proyecciones de volúmenes de operación y que se encuentren cargados en el Core Bancario. Esto con el objetivo de compararlos con la actividad registrada en el sistema de monitoreo. Además permite el manejo de umbrales de tolerancia definidos acorde a las políticas del banco.	
4.23	El sistema consolida la información del cliente y todos sus productos, teniendo un análisis de comportamiento integral del cliente.	
SEGMENTACIÓN DE CLIENTES		
4.24	El sistema permite crear segmentos de clientes por nivel de riesgo	
4.25	El sistema permite crear segmentos de clientes combinando variables como: nivel de riesgo, nivel de ingreso, jurisdicciones, actividad económica y cualquier combinación de campos que residan en el perfil del cliente	
4.26	El sistema permite segmentar clientes por técnicas de reconocido valor técnico, por ejemplo K-prototype	
OPERACION DEL SISTEMA Y GESTION DE CASOS DE INVESTIGACION (CASE MANAGEMENT)		
4.27	El sistema esta diseñado para trabajar en tiempo real y hacer análisis de riesgo al momento que se ejecuta una transacción.	
4.28	El sistema cuenta con una herramienta para el manejo de interacciones con el cliente	
4.29	El sistema alerta en línea por la detección de operaciones fuera del patrón de comportamiento del cliente.	
4.30	El sistema debe permitir la generación de alertas manuales.	
4.31	El sistema permite modificar parámetros o reglas de negocio para afinar la sensibilidad o ponderación de cada criterio de monitoreo.	
4.32	La parametrización de las alertas deberá ser de fácil manejo para reaccionar a las necesidades del negocio sin requerir de un desarrollo adicional por parte del proveedor.	
4.33	El sistema cuenta con una consola de alertas donde puede centralizarse la información del cliente para hacer más eficiente el análisis por parte de cumplimiento	
4.34	La consola de alertas tiene la funcionalidad de consultar el movimiento histórico del cliente y poder aplicar filtros de una forma dinámica y con gráficos asociados al los criterios seleccionados	
4.35	El sistema deberá permitir el ordenar las alertas por criterios como severidad de alerta (score), por cliente, por cuenta, por jurisdicción y otros campos de despliegue.	
4.36	El sistema tiene integrada la funcionalidad de administración de casos de investigación (Case Management) la cual puede personalizarse según los procedimientos de la institución	
4.37	Todo proceso de investigación deberá tener un monitoreo en cuanto a tiempos de vencimiento de tareas, es decir que en el sistema se pueda definir de forma paramétrica tiempos máximos de atención para cada etapa del proceso.	

ER

GS

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
SECCIÓN DE COMPRA Y CONTRATACIONES
FICHA TECNICA

7 febrero, 2023

4.38	Quando se genere un caso de investigación se deberá enviar un e-mail al funcionario receptor del mismo para asegurarse que esté enterado que tiene una tarea por resolver. Durante el proceso deberá poder recibir recordatorios de la fecha de vencimiento del mismo.	
4.39	El sistema deberá manejar un escalamiento de casos cuando se haya vencido un plazo determinado y deberá enviarlo a un funcionario superior	
4.40	El sistema permite la creación de un procedimiento (case management) para clientes de alto riesgo o PEPs y por otro lado también permite generar casos en forma manual	
4.41	El sistema genera reportes o bitácoras de volúmenes de transacciones referidas para monitoreo, sobre acciones tomadas por monitoreo, en base mensual, diaria y semanal	
CONOCIMIENTO DEL CLIENTE Y ANALISIS DE COMPORTAMIENTO CONTRA SEGMENTO		
4.42	El sistema genera un perfil transaccional de clientes (cumpliendo con prácticas de KYC, KYE, KY3) y comparándolo con la actividad del segmento al que esté asociado	
4.43	El sistema permite aplicar controles en el proceso de pre-vinculación	
4.44	El sistema genera un perfil transaccional del cliente en base a su comportamiento histórico pudiendo utilizar variables como promedios o desviaciones estándar.	
4.45	El sistema puede incorporar información de la geolocalización de la cual el cliente hace sus operaciones	
4.46	El sistema permite la creación de nuevos criterios y reglas	
4.47	El sistema permite la consulta en línea de históricos de transacciones de los últimos 12 meses (o el tiempo que la institución especifique)	
4.48	El sistema tiene la facilidad de filtrar por tipo de transacciones, fecha, monto, tipo de cuenta, país, etc.	
4.49	El sistema cuenta con la funcionalidad de agregar comentarios en los procesos de investigación.	
4.50	El análisis transaccional que se realice deberá ser a nivel del cliente consolidando todas las cuentas que este tenga; deberá considerar la actividad del cliente así como la transaccionalidad que realizará buscando que exista congruencia entre una y otra. Así mismo permitirá revisar el detalle de todas sus cuentas.	
4.51	El sistema deberá estar en capacidad de recibir transacciones de todos los canales y todos los productos de la institución.	
4.52	El sistema permite un análisis del cliente y sus relaciones directas con otras cuentas (beneficiario, firmante, etc.) o bien relaciones como mismo teléfono, mismo correo electrónico, transferencias de fondos desde o hacia otras cuentas, etc. Estas relaciones deberá mostrarlas de forma gráfica.	
VALIDACION CONTRA LAS LISTAS		
4.53	El sistema deberá sincronizar automáticamente y de forma programada listas como OFAC, CIA y ONU. Además deberá permitir cargar las listas que tenga a disposición la institución y hacer validaciones de forma paramétrica según políticas definidas.	
4.54	Las listas deberán validarse en línea cuando ocurren las transacciones y así mismo deberán programarse de forma paramétrica barridos a las bases de datos de la institución para establecer nuevas coincidencias en la cartera de clientes mientras sostengan una relación.	
4.55	Dentro de las listas a validar deberán considerarse acciones concretas de búsqueda para personas consideradas como PEPS o que figuren en listas de alto riesgo. Durante la relación comercial: deberá hacerse un barrido periódico de la cartera de clientes y luego el sistema deberá generar un reporte o bien alertas (según se defina) en base a las coincidencias encontradas.	
4.56	El sistema deberá contar con algoritmos de búsqueda en listas tales como comparación fonética y así mismo poder parametrizar porcentajes de coincidencias en base al peso de cada elemento en la búsqueda (por ejemplo: pesos asociados a nombres y apellidos).	
4.57	El sistema deberá tener la capacidad de validar listas positivas, negativas o también denominadas listas negras, PEPs y en general, aquellas listas que la institución tenga a su disposición en fuentes electrónicas de información.	
4.58	La carga de listas al sistema deberá poder ejecutarse en forma automática y por otros métodos como transferencia de archivos o digitación manual de información (usualmente derivado del monitoreo de medios)	

 ER
 GS

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA

7 febrero, 2023

SECCIÓN DE COMPRA Y CONTRATACIONES
FICHA TECNICA

4.59	Durante el proceso de análisis el sistema permita que se le asigne un nivel de riesgo a las alertas y deberá tenerse un estatus del estado de gestión de la alerta. Asimismo, permitirá clasificarlas con base al resultado del análisis final (descartada, reportada, no reportada), habrá ocasiones en que se determine no reportar, sin embargo este resultado deberá considerarse para futuros monitoreos.	
4.60	El sistema debe contar con una infraestructura que permita cubrir los requerimientos establecidos por el ente regulador en relación a la identificación y conocimiento del cliente, estableciendo los campos de captura requeridos para dicho fin.	
MONITOREO DE OPERACIONES		
4.61	El monitoreo deberá realizarse en línea (al momento en que se realiza la operación). El sistema deberá alertar por la detección de operaciones fuera del perfil transaccional de los clientes. En el caso de realizar transferencias deberá evaluar si hay operaciones a países de riesgo, o países de baja imposición fiscal. En general estos criterios deberán definirse de forma paramétrica.	
4.62	El sistema identifica transferencias de un cliente a un empleado.	
4.63	El sistema identifica depósitos, retiros y compra/venta de divisas fuera del patrón de comportamiento del cliente	
4.64	El sistema identifica transferencias realizadas con dinero en efectivo recién depositado. Esto se refiere a análisis de secuencias.	
4.65	El sistema identifica transacciones a una cuenta de reciente apertura (período definido de forma paramétrica).	
4.66	El sistema identifica transferencias a cuentas que no se hayan registrado previamente	
4.67	El sistema identifica transacciones por montos cuantiosos. El parámetro se establecerá de acuerdo al perfil transaccional del cliente, si es persona natural o jurídica.	
4.68	El sistema identifica múltiples transacciones por montos bajos a una misma cuenta en un período corto.	
4.69	El sistema identifica una o más transacciones de una cuenta a varias destino en un periodo de tiempo definido y que el monto sea cuantioso dependiendo del perfil transaccional del cliente	
4.70	El sistema identifica múltiples transacciones cerca del límite diario de compra o venta de divisas operadas en una misma cuenta.	
4.71	Se deberá identificar a los clientes cuyas operaciones en un mes de calendario superen el equivalente a 100,000 dólares. (este valor debe ser parametrico)	
4.72	El sistema identifica si varias cuentas de el Banco realizan transacciones a una misma cuenta destino en un periodo de tiempo definido.	
4.73	El sistema identifica transferencias desde varias cuentas origen a una cuenta.	
4.74	El sistema deberá presentar de forma gráfica los traslados de fondos entre cuentas.	
4.75	El sistema identifica el incremento en el monto transaccional contra históricos (semanas anteriores o un parámetro definido).	
4.76	El sistema identifica transacciones fuera de la zona geográfica acorde con el patrón de comportamiento del cliente. Incluyendo zonas geográficas de alto riesgo.	
4.77	El sistema identifica cuando un cliente registra múltiples cuentas en un periodo corto de tiempo.	
MONITOREO DE OPERACIONES INTERNACIONALES		
4.78	El sistema deberá tener la capacidad de interpretar operaciones en formato SWIFT o manejar los formatos definidos de mutuo acuerdo para el manejo de transferencias internacionales	
4.79	El sistema deberá tener la capacidad de detener en tiempo real una operación cuyo origen o destino sea un país de alto riesgo o que el Ordenante o Beneficiario tengan posibles coincidencias con la lista OFAC u otra condición definida por al institución	
4.80	Si una operación se detiene en tiempo real, el sistema deberá seguir un procedimiento para la validación de la operación y su final autorización o rechazo	
4.81	En cuanto al proceso de opeaciones salientes, el sistema tiene la capacidad de detener una operación si existe un posible duplicado (dos o mas transacciones con el mismo beneficiario y/o el mismo monto)	
4.82	El sistema deberá tener la capacidad de analizar si hay 3 o mas instituciones involucradas en la operación, es decir deberá poder evaluar la cadena de pago.	
4.83	El sistema deberá manejar estadísticas de comportamiento transaccional de transferencias por cliente	

 EN
 BS

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
SECCIÓN DE COMPRA Y CONTRATACIONES
7 febrero, 2023
FICHA TECNICA

AMBIENTE DE SIMULACION Y AFINAMIENTO	
4.84	El sistema deberá contar con una herramienta que permita afinar el modelo de detección basada en muestras de movimientos del ambiente de producción
4.85	El sistema deberá permitir evaluar escenarios si se modifican reglas para poder medir el impacto que tendrán tanto en cantidad de alertas generadas como en la eficiencia de detección
4.86	El sistema puede sugerir modificaciones a los pesos asignados para los factores de riesgo (personas, productos, canales, jurisdicciones)
REPORTES INTERNOS Y EXTERNOS	
4.87	Deberá incluir una herramienta que permita elaborar y explotar los diferentes informes que por normativa deben enviarse al ente regulador como por ejemplo: <ul style="list-style-type: none"> • Operaciones en efectivo que superen un valor umbral definido • Operaciones inusuales SAR por sus siglas en inglés • Transferencias internacionales que superen un valor umbral definido • Otros que requiera la normativa y que se definan en el documento de alcances del proyecto.
4.88	El sistema deberá contar con reportes gráficos tipo "tableros de control" que permitan analizar las tendencias o variables mas importantes relacionadas con los reportes al ente regulador
4.89	El sistema deberá tener la capacidad de generar reportes tipo "tableros de control" donde puede analizarse el desempeño de la unidad de cumplimiento
4.90	El sistema deberá presentar de forma gráfica la distribución de clientes por nivel de riesgo inherente y/o residual.
4.91	El sistema deberá generar un reporte conteniendo información del cliente, el valor obtenido por cada factor de riesgo, el riesgo inherente y el riesgo residual a una fecha determinada. Estas fechas podrán estar asociadas a periodos como evaluaciones bimensuales, trimestrales o semestrales, según lo defina la institución.
4.92	El sistema puede exportar reportes a formatos de hoja electrónica como excel, PDF, HTML y XML.
4.93	Se deberá contar con la facilidad de generar reportes de información relativos a cualquier aspecto generado dentro del sistema, es decir y como ejemplo los siguientes: alertas generadas, alertas en seguimiento, alertas presentadas al comité, alertas reportadas a la autoridad, total de alertas detectadas por el sistema, etc.
BASE DE DATOS Y FUENTES DE INFORMACION	
4.94	El sistema guarda su información en una base de datos relacional como SQL server
4.95	El sistema tiene la capacidad de conectarse con múltiples fuentes de información de forma simultánea está orientado a comunicarse en tiempo real
4.96	El sistema cuenta con distintos métodos de comunicación como el uso de interfases, TCP/IP, Data Queues, Web Services, etc.
4.97	El sistema tiene la capacidad de cargar información en batch cuando sea requerido
4.98	El sistema puede cargar archivos tipo texto o CSV
CAPACIDADES DE SEGURIDAD	
4.99	El Sistema soporta el concepto de hacer / verificar (Maker-Checker) para transacciones sensitivas (un individuo hace y otro verifica).
4.100	El Sistema cuenta con bitácoras que permitan el registro de eventos realizados por el administrador de seguridad.
4.101	El Sistema registra pistas de auditoría en una bitácora en relación a todas las acciones que realiza un usuario.
4.102	El sistema puede restringir el acceso de un usuario por dirección IP, MAC address, horarios y días de la semana
4.103	La bitácora está protegida contra accesos no autorizados.
4.104	El Sistema cuenta con parámetros de default de eventos auditables.
4.105	El sistema registra las actividades realizadas por el administrador de seguridad: Creación, borrado y modificación de objetos en el sistema - cuentas de usuario, grupos, perfiles, reinicialización de contraseñas, bloqueos, desbloqueos, entre otros-.
4.106	Cuando la bitácora de auditoría esta por saturarse, el Sistema automáticamente lo notifica por medio de mensajes o alarmas.

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
SECCIÓN DE COMPRA Y CONTRATACIONES
FICHA TECNICA

7 febrero, 2023

4.107	El Sistema puede proveer información de todos los intentos de acceso inválidos por User ID; incluyendo intentos por contraseña incorrecta, bloqueo de User ID, intentos de acceso a cuenta bloqueada, intento de acceso desde una terminal no permitida.	
4.108	Existen reportes predefinidos de la bitácora de auditoría.	
4.109	Los reportes de la bitácora de seguridad pueden ser definidos por el usuario.	
4.110	El Sistema (o sistema de seguridad, en caso de existir) puede listar la identidad de todos los usuarios activos del Sistema y su perfil asociado.	
4.111	El Sistema genera una alarma después de un número específico de intentos fallidos consecutivos de acceso.	
4.112	El Sistema permite cambiar las contraseñas por el usuario en cualquier momento (password o número PIN).	
4.113	El Sistema obliga periódicamente a los usuarios el cambio de password en un período determinado, por ejemplo cada 30 días.	
4.114	El Sistema requiere una re-autenticación del usuario cuando intenta cambiar su password.	
4.115	El sistema cumple con las políticas de contraseña: Restringir a una longitud mínima (ejemplo 8 caracteres) las contraseñas de acceso Las contraseñas deben ser alfanuméricas - letras y números.	
4.116	El Sistema tiene la capacidad de restringir el establecimiento de una sesión basado en: <ul style="list-style-type: none"> • Hora y Fecha • Día de la Semana • Fecha calendario de entrada • Fuente de la conexión 	
4.117	Se pueden crear en el Sistema perfiles de usuarios (roles o grupos).	
4.118	El Sistema registra los cambios realizados a las facultades de los usuarios en la bitácora de auditoría.	
4.119	El Sistema cumple con las siguientes reglas para la construcción de passwords: <ul style="list-style-type: none"> • El password es de un mínimo de ocho (8) caracteres alfa-numéricos. • El password es diferente al User ID. • Los passwords son seleccionados por el usuario, a menos que sea generado aleatoriamente "random" y requiera ser cambiado en su siguiente acceso. 	
4.120	Pueden generarse reportes y consultas de los perfiles de usuario.	
4.121	Este módulo del sistema deberá tener una licencia de suscripción por 3 AÑOS con mantenimiento y servicio incluido.	

5. MÓDULO DE GESTIÓN Y CONTROL DE RIESGOS OPERACIONALES

No.	REQUISITOS	CUMPLE / NO CUMPLE
5.1	La solución debe ser totalmente parametrizable, y de facil manejo para el usuario final (amigable e intuitiva)	
5.2	La solución debe permitir integraciones nativas con otros sistemas de gestión de riesgos, incidentes y gestión documental.	
5.3	La solución debe emitir notificaciones o alertas en tiempo real soportada en las parametrizaciones técnicas realizadas por el administrador de la solución.	
5.3	La solución debe permitir configurar notificaciones o alertas cuando el usuario final registre los eventos o incidentes, cuando se superan umbrales de tolerancia y cuando hay atrasos en planes de acción programados de cualquier área.	
5.4	La solución debe tener capacidad de conectarse de manera gráfica y amigable a diferentes fuentes de información parametrizadas previamente por el administrador	
5.5	La solución debe permitir adjuntar archivos en formato pdf, word, excel a cualquier registro (proceso, normativa, política, riesgo, control, plan de acción, etc.). Cuál es el número máximo de archivos que se pueden adjuntar y cual es su peso máximo (MB)?	
5.6	La solución debe poseer una suite de soluciones que pueden gestionar riesgos en tiempo real como por ejemplo prevención de fraude en: cuentas activas/pasivas, tarjetas de débito o crédito, prevención de lavado de activos, entre otros.	
5.7	La solución ofertada debe cumplir con las especificaciones de la norma aplicable.	
5.8	La solución ofertada debe permitir definir de forma paramétrica diferentes dimensiones de riesgo y estas a su vez pueden estar vinculadas con una o varias estructuras de análisis.	

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
SECCIÓN DE COMPRA Y CONTRATACIONES
FICHA TECNICA

5.9	La solución debe contar con mecanismos para apoyar el proceso de documentación, diseño de flujos de trabajo, evaluación y análisis en términos de impacto de negocio, presentación de informes, visualización y remediación de riesgos	
5.10	La solución ofertada debe permitir definir de forma paramétrica las estructuras de análisis para cada dimensión (Procesos, Normativas, Activos de Información, Políticas, Clientes, Proveedores, entre otros) y que cada estructura se le puedan definir los campos donde se ingresará la información.	
5.11	La solución ofertada debe permitir generar un plan de acción asociado riesgos, fallas o controles	
5.12	La solución ofertada debe permitir dentro de los ciclos de análisis de gestión identificar el desplazamiento de los riesgos (evolución)	
5.13	La solución ofertada debe administrar un enfoque cualitativo y cuantitativo de gestión de riesgos.	
5.14	La solución ofertada debe tener capacidad de integrar enfoques cualitativo y cuantitativo de gestión de riesgos	
5.15	La solución ofertada debe contar con un Workflow de evaluaciones o autorizaciones para los planes de acción	
5.16	La solución ofertada debe administrar procesos de evaluación y de auto-evaluación de riesgos	
5.17	La solución ofertada debe administrar procesos de evaluación de riesgos y controles por Departamentos	
5.18	La solución ofertada debe poseer encuestas de autoevaluación predefinidas (mejores prácticas)	
5.19	La solución ofertada debe permitir identificar riesgos, fallas, controles por procesos	
5.20	La solución ofertada debe permitir valorar el nivel de impacto y frecuencia de un riesgo a través de varios criterios, pudiendo parametrizar diferentes cuestionarios para la evaluación de los mismos.	
5.21	La solución ofertada debe permitir parametrizar la calificación de los controles	
5.22	La solución ofertada debe permitir definir cuestionarios para calificar las pruebas de eficiencia de los controles y que las respuestas afecten la calificación de la solidez de los mismos	
5.23	La solución ofertada debe permitir la administración de planes de acción para implementar medidas de mitigación o darle seguimiento a un evento de pérdida, incluyendo: planificación de fechas límite para realizar actividades, control de cumplimiento, emisión de alertas en caso de atrasos	
5.24	La solución ofertada debe permitir la definición, registro, captura (manual y automática) y administración de indicadores claves de riesgos KRI y que se generen alertas cuando se sobrepasen los umbrales	
5.25	La solución ofertada debe contar con un módulo de captura de eventos de pérdidas, multas, sanciones, tanto manuales como automáticas, para la creación de base de datos histórica.	
5.26	La solución ofertada debe permitir parametrizar los responsables del tratamiento de riesgo por Rol o Usuario	
5.27	La solución ofertada debe permitir calcular el nivel de riesgo para cada dimensión de análisis del riesgo que se defina (riesgo operacional, riesgo tecnológico, riesgo de incumplimiento de normas, entre otros) y permite mostrar en forma integrada los resultados de las distintas dimensiones de análisis.	
5.28	La solución ofertada debe tener la capacidad de administrar un sistema de gestión de las obligaciones para el cumplimiento de normativas y políticas de la organización	
5.29	La solución ofertada debe permitir detallar las políticas, adjuntar el documento electrónico y publicarlo a las personas involucradas, así como definir de forma paramétrica un cuestionario para evaluar quiénes leyeron la política, quiénes la comprendieron y luego generar estadísticas con el resultado de las respuestas a los cuestionarios.	
5.30	La solución ofertada debe permitir definir los compromisos que se tienen por Normativa o Política, detallando cada una de las actividades, fechas, responsables, recurrencia; y que el sistema dé un seguimiento automático a cada uno de los compromisos notificando el correo electrónico el cumplimiento o incumplimiento de los mismos	
5.31	La solución ofertada debe permitir registrar las consecuencias financieras o no financieras por el incumplimiento a las normativas.	
5.32	La solución ofertada debe permitir visualizar en calendario todas las actividades y compromisos vigentes, el responsable de los mismos y porcentaje de avance asociado.	
5.33	La solución ofertada debe estar basada en ambiente web y poseer estándares de seguridad.	
5.34	El proveedor debe presentar dentro del alcance de su propuesta un proceso de transferencia de conocimiento y capacitación certificada de este modulo de la solución.	

FS

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
SECCIÓN DE COMPRA Y CONTRATACIONES

7 febrero, 2023

FICHA TECNICA

5.35	Este modulo del sistema debera tener una licencia de suscripción por 3 AÑOS con mantenimiento y servicio incluido.	
5.36	El nivel de servicios (SLA) de mantenimiento y soporte para este modulo del sistema, debera ser de 24*7*365	
REPORTES INTERNOS Y EXTERNOS		
5.37	La solución ofertada debe contar con informes gerenciales parametrizables (gráficos de barras, de líneas, de pie, histogramas, entre otros) que puedan exportarse a diferentes formatos	
5.38	La solución ofertada debe permitir configurar tableros de comando gerenciales (proceso de gestión, riesgo, indicadores, eventos de pérdida, incidentes, entre otros)	
5.39	La solución ofertada debe permitir generar reporte de matriz de riesgos y controles por país, empresa, regional, ciudad, oficina, sucursal o agencia, unidad de negocio, sistema de riesgo, entre otros.	
5.40	La solución ofertada debe permitir generar reporte de estatus de planes de acción (planes definidos, por iniciar, estatus de avance del proceso, concluidos)	
5.41	La solución ofertada debe permitir generar gráficos de mapas de calor por riesgo inherente y residual con filtros de información para obtener resultados específicos	
5.42	La solución ofertada debe permitir generar gráficos de mapas de calor consolidados por país, empresa, regional, ciudad, agencia, unidad de negocio, entre otros) detallando la valoración del riesgo (inherente, residual)	
5.43	La solución ofertada debe permitir generar gráficos de mapas de calor por riesgo residual con desplazamiento (comparativo entre dos periodos distintos midiendo cambios en evaluación del riesgo)	
5.44	La solución ofertada debe permitir generar reportes de fallas identificadas por factor de riesgo.	
5.45	La solución ofertada debe permitir generar mapa de riesgo organizacional por país, empresa, ciudad, agencia, unidad de negocio, entre otros.	
5.46	La solución ofertada debe permitir generar un reporte de registros de eventos de pérdidas en forma histórica para analizar su comportamiento	
5.47	La solución ofertada debe permitir perfilar reportes para distintos niveles de la organización	
5.48	La solución ofertada debe permitir enviar alertas via e-mail a los usuarios para acceder a los reportes consolidados de alertas	
5.49	La solución ofertada debe permitir visualizar el calendario con el detalle de las actividades o compromisos por día, responsable, fecha de inicio y fin y el porcentaje de avance.	
5.50	La solución ofertada debe permitir generar reportes en tiempo real y tableros específicos del usuario para conocer los esfuerzos de evaluación y el cumplimiento de normas y políticas de la organización.	
5.51	La solución ofertada debe permitir relacionar Evaluaciones de Riesgo, Indicadores, Eventos, Controles, Planes de Acción, entre otros, para poder realizar reportes e información de gestión consolidada.	
5.52	La solución ofertada debe permitir generar reportes con mapas de riesgo historicos y realizar análisis comparativos en los periodos de tiempo establecidos	
5.53	La solución ofertada debe permitir personalizar los reportes a la imagen corporativo (colores, logotipo, entre otros).	
5.54	La solución ofertada debe permitir generar mapas de calor de riesgo inherente y residual por factores de riesgo	
RIESGO OPERATIVO		
5.55	La solución debe permitir realizar parametrización del mapa de riesgo (asignación de pesos diferentes a cada cuadrante y configuración de la severidad)	
5.56	La solución debe permitir establecer ponderación de manera paramétrica por negocio (empresa), proceso u área de la cadena de valor de la entidad. Para ser considerada en la valoración y mapeo de los riesgos.	
5.57	La solución debe permitir administrar la estructura organizacional de la compañía (incluir, inactivar, copiar y/o cortar sucursales, líneas de negocio, dependencias o áreas de la compañía) asegurando la integridad y trazabilidad de los cambios y sus impactos en los mapas de riesgos.	
5.58	La solución debe permitir administrar la lista de empleados de la institución.	

 ER
 JS

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA
SECCIÓN DE COMPRA Y CONTRATACIONES

7 febrero, 2023

FICHA TECNICA

5.59	La solución debe permitir administrar la gestión de Registros de Eventos y Pérdidas (configurando y parametizando de acuerdo a las necesidades de la institución, las líneas de negocio, productos, clasificación de los tipos de pérdidas y el diseño de las pantallas de captura de los registros de eventos de pérdida)	
5.60	La solución debe permitir en su modelo de análisis recibir información en tiempo real	
5.61	La solución debe permitir administrar alertas en tiempo real cuando: se superan umbrales de tolerancia y cuando hay atrasos en planes de acción programados de cualquier área	
5.62	La solución debe permitir conectarse con múltiples fuentes electrónicas de información para recibir o entregar información	
5.63	La solución debe permitir definir de forma paramétrica "Entidades", definiendo los campos necesarios para cada entidad y que luego dichas entidades se puedan asociar a las estructuras de análisis, por ejemplo: que a la estructura de Proveedores se asocie la entidad "Contactos" donde se grabarán todos los contactos por cada proveedor o que a la estructura de Clientes se le asocie la entidad "Estado de Resultados" para ingresar la información correspondiente a cada cliente.	
5.64	La solución debe permitir integrar enfoques cualitativo y cuantitativo de gestión de riesgos	
5.65	La solución debe permitir poseer un workflow de evaluaciones	
5.66	La solución debe permitir un proceso continuo de autoevaluación de riesgos y controles	
5.67	La solución debe permitir establecer las actividades significativas del negocio	
5.68	La solución debe permitir la consolidación del nivel de riesgo de la entidad mediante métodos ponderados y determinando las direcciones de la evolución del riesgo (tendencia).	
CÁLCULO DEL VAR		
5.69	La solución debe utilizarse para calcular el capital regulatorio con base en el método avanzado.	
5.70	La solución debe permitir generar gráficas de comportamiento del VAR con base en datos históricos	
5.71	La solución debe permitir generar gráficas de comportamiento del VAR con base en escenarios (ingreso manual de datos)	
5.72	La solución debe tener la capacidad de generar reportes de riesgo por línea de negocio	
5.73	La solución debe tener la capacidad de generar reportes o gráficas por riesgo inherente o residual de forma parametrizable	
5.74	La solución debe tener la capacidad de generar el VAR por categoría de riesgo y línea de negocio	
CAPACIDADES DE SEGURIDAD		
5.75	La solución debe contar con un sistema completo de administración de seguridad basados en perfiles de acceso. Los diferentes usuarios de la aplicación se deberán poder asociar a perfiles de acceso específicos.	
5.76	Los perfiles de acceso deberán controlar, además de las opciones de menú, los tipos de información o productos que pueden consultar y modificar, dependiendo del área o producto bajo su responsabilidad.	
5.77	El sistema de seguridad debe permitir configurar un control de validación para que modificaciones específicas puedan requerir de un doble ingreso de contraseña, o de ingreso de contraseña de un supervisor.	
5.78	El sistema debe generar bitácoras de auditoría de todos los cambios que se realicen en el mismo, e incluir consultas dinámicas sobre esa información.	
5.79	Se debe garantizar que los componentes de la solución no puedan ser modificados o alterados por personal no autorizado.	
5.80	El sistema debe garantizar la desconexión del usuario por tiempo de espera. Esta función debe ser configurable.	
5.81	El sistema debe permitir la desactivación y activación manual de los usuarios.	
5.82	El sistema debe garantizar que el mismo usuario no pueda estar activo, simultáneamente, en diferentes computadoras / conexiones.	
5.83	El sistema debe auditar las acciones a través de logs que registran todas las actividades de consulta y los cambios realizados por los usuarios del sistema	
5.84	Este módulo del sistema deberá tener una licencia de suscripción por 3 AÑOS con mantenimiento y servicio incluido.	

ER

65

6. CAPACITACIONES Y ENTRENAMIENTOS (TODOS LOS MÓDULOS DE LA PLATAFORMA)

No.	REQUISITOS	CUMPLE / NO CUMPLE
6.1	La metodología de implementación deberá considerar la capacitación a usuarios finales que gestionaran y administraran los modulos de la plataforma.	
6.2	La metodología de implementación deberá considerar la capacitación a administradores del sistema que puedan adquirir un grado de especialización que les permita administrar y modificar condiciones o parámetros en el sistema sin que intervenga el proveedor del software.	
6.3	La capacitación administradores deberá dejar en capacidad a los administradores de modificar los workflows de investigación en el sistema, sin que tenga que intervenga necesariamente el proveedor del software.	
6.4	La capacitación deberá brindar a la institución un alto grado de autonomía en cuanto a la administración del sistema.	
6.5	Debe contarse con la posibilidad de obtener un curso ejecutivo no mayor a dos días para que funcionarios de alto nivel puedan conocer el alcance del sistema.	
6.6	La solución ofertada debe ofrecer capacitación técnica media y avanzada (certificación) de cada modulo de la plataforma a 2 usuarios finales por modulo. Un total de 10 capacitaciones.	

7. TIEMPO Y ORDEN DE IMPLEMENTACIÓN

No.	REQUISITOS	CUMPLE / NO CUMPLE
7.1	Los siguientes módulos deberán implementarse en los primeros seis (6) meses del proyecto: Módulo Prevención de Fraude en la Banca Digital Módulo Prevención de Fraudes Internos (sucursales y empleados) Módulo Prevención de lavado de dinero y Cumplimiento	
7.2	Los siguientes módulos deberán implementarse en los siguientes cinco (5) meses del proyecto: Módulo Prevención de Fraude Productos (TC, TD, Otros). Módulo Gestión de Riesgo Operacional	
7.3	Para la ejecución entrega de documentación, capacitaciones y cierre del proyecto , se dispondra de un (1) mes de tiempo luego de implementados todos los módulos antes mencionados.	
7.4	La duración total de la implementación, prueba, pase a producción, documentación, capacitaciones y cierre del proyecto es de doce (12) meses .	

CONDICIONES TECNICAS ESPECIALES DEL OFERENTE

COMPETENCIAS DE LA EMPRESA OFERENTE		PUNTAJACIÓN
1	El suplidor de la solución debe presentar certificación de la solución, indicando que el mismo, está autorizado a ser representante directo de la marca ofertada en República Dominicana. (Se validará directamante con el fabricante). No Subsanable.	10
2	El suplidor de la solución debe presentar una certificación por parte del fabricante indicando que está certificado para vender e instalar los componentes propuestos a el Banco Agrícola. (Se validará directamante con el fabricante). No Subsanable.	10

3	<p>El suplidor debe poseer años de experiencia demostrada ofreciendo consultoria e implementando este tipo de proyectos. El puntaje se determina de la siguiente manera, presentando carta o certificaciones que abalen sus años de experiencia en consultoria e implementando proyectos de prevencion de fraudes.</p> <ul style="list-style-type: none"> - 10 años o mas de experiencia. Valor 15 Puntos. - Entre 5 a 9 años de experiencia. Valor 8 Puntos. - Entre 2 a 4 años de experiencia. Valor 4 Puntos. 	15
4	<p>El suplidor debe incluir evidencia de proyectos en los cuales haya implementado solución de los modulos requeridos en esta ficha técnica, de manera local en República Dominicana. El puntaje se determina de la siguiente manera:</p> <ul style="list-style-type: none"> - 5 o mas cartas de clientes donde hayan implementado y este en funcionamiento actual al menos 4 módulos de la solución requerida. Valor 20 Puntos. - 3 cartas de clientes donde hayan implementado y este en funcionamiento actual al menos 3 módulos de la solución requerida. Valor 15 Puntos. - Minimo requerido de 2 cartas de clientes donde hayan implementado y este en funcionamiento actual al menos 2 módulos de la solución requerida. Valor 10 Puntos. 	20

COMPETENCIAS PROFESIONALES DEL PERSONAL

DADO EL AMPLIO ALCANCE DE LA PLATAFORMA Y SUS DIFERENTES MÓDULOS REQUERIDOS, SE SOLICITA UN PERSONAL PROFESIONAL REQUERIDO, EL CUAL, DEBE CUMPLIR CON LAS SIGUIENTES COMPETENCIAS:

5	<p>Rol: Gerente de Proyecto (Project Manager).</p> <p>Se requiere asignar un gerente de proyecto, el cual se encargue de llevar la gestión del proyecto de acuerdo con una metodología de manejo de proyectos avalada por el Project Management Institute.</p> <ul style="list-style-type: none"> - Debe contar con la certificación PMP vigente para el manejo del proyecto. - Preparar y entregar informes diarios de seguimiento del proyecto. - Debe estar dedicado 100% onsite a este proyecto. <p>NOTA: En caso de no enviar el perfil con todos los requerimientos, la puntuación sera cero (0).</p>	5
6	<p>Rol: Consultor Técnico General del Proyecto</p> <p>Se requiere un personal como lider tecnico del proyecto, el mismo, debe cumplir con el siguiente perfil de competencias: Esta persona se encargara de garantizar en el proyecto que los diferentes módulos de la solución, puedan operar como un unico sistema integrado.</p> <p>Ingeniero o Licenciado de carreras afines, como: Informatica, Sistemas, Industrial, Finanzas, otros.</p> <p>Poseer al menos 3 certificaciones o capacitación oficial de al menos 3 de los 5 módulos de la solución ofertada:</p> <ul style="list-style-type: none"> - Módulo Canales Digitales - Módulo Prevención de Fraudes de Productos TC-TD, otros. - Módulo Fraude Interno - Módulo Cumplimiento y prevención Lavado de Activos - Módulo Gestión y Control Riesgos Operacionales <p>NOTA: En caso de no enviar el perfil con todos los requerimientos, la puntuación sera cero (0).</p>	10
7	<p>Rol: Consultor Prevención de Fraudes</p> <p>Se requiere un personal como Consultor Prevención de Fraudes, el mismo, debe cumplir con el siguiente perfil de competencias:</p> <p>Esta persona se encargara de asesorar e implementar los módulos de prevención de fraudes de la solución ofertada.</p> <p>Ingeniero o Licenciado de carreras afines, como: Informatica, Sistemas, Industrial, Finanzas, otros.</p> <p>Poseer certificaciones o capacitación oficial de los siguientes módulos de la solución ofertada:</p> <ul style="list-style-type: none"> - Módulo Canales Digitales - Módulo Prevención de Fraudes de Productos TC-TD, otros. - Módulo Fraude Interno <p>NOTA: En caso de no enviar el perfil con todos los requerimientos, la puntuación sera cero (0).</p>	10

BANCO AGRÍCOLA DE LA REPUBLICA DOMINICANA

7 febrero, 2023

SECCIÓN DE COMPRA Y CONTRATACIONES
FICHA TECNICA

8	<p>Rol: Consultor Cumplimiento y Lavado de Activos</p> <p>Se requiere un personal como Consultor Cumplimiento y Lavado de Activos, el mismo, debe cumplir con el siguiente perfil de competencias:</p> <p>Esta persona se encargara de asesorar e implementar el módulo de Cumplimiento y Lavado de Activos de la solución ofertada. Ingeniero o Licenciado de carreras afines, como: Informatica, Sistemas, Industrial, Finanzas, otros.</p> <p>Poseer la certificación o capacitación oficial de los siguientes módulos de la solución ofertada:</p> <p>- Módulo Cumplimiento y prevención Lavado de Activos</p> <p>NOTA: En caso de no enviar el perfil con todos los requerimientos, la puntuación sera cero (0).</p>	10
9	<p>Rol: Consultor Gestión y Control Riesgos Operacionales</p> <p>Se requiere un personal como Consultor Cumplimiento y Lavado de Activos, el mismo, debe cumplir con el siguiente perfil de competencias:</p> <p>Esta persona se encargara de asesorar e implementar el módulo de Gestión y Control Riesgos Operacionales de la solución ofertada. Ingeniero o Licenciado de carreras afines, como: Informatica, Sistemas, Industrial, Finanzas, otros.</p> <p>Poseer la certificación o capacitación oficial de los siguientes módulos de la solución ofertada:</p> <p>- Módulo Gestión y Control Riesgos Operacionales</p> <p>NOTA: En caso de no enviar el perfil con todos los requerimientos, la puntuación sera cero (0).</p>	10
TOTAL PUNTUACION:		100

