BANCO VisionFund ECUADOR

TÉRMINOS DE REFERENCIA

Solución Integral de Prevención y Detección de Fraude en Canales Electrónicos

1. Antecedentes y justificación

Banco VisionFund Ecuador es una entidad financiera privada regulada por la Superintendencia de Bancos del Ecuador, con operaciones en canales digitales que incluyen banca web, banca móvil, transferencias interbancarias, tarjetas de débito y APIs transaccionales.

El panorama actual de amenazas cibernéticas representa un riesgo creciente para las instituciones financieras ecuatorianas. En 2026, Ecuador registró más de 12 millones de ciberataques, un incremento del 30% respecto al año anterior, posicionándose como el tercer país más afectado de América Latina. La filtración del Registro Civil en mayo de 2026 expuso más de 10 millones de fotografías biométricas en la dark web, incrementando significativamente el riesgo de fraude por suplantación de identidad mediante deepfake.

2. Objeto

El presente documento establece los términos de referencia para la contratación de una Solución Integral de Prevención y Detección de Fraude en Canales Electrónicos para el Banco VisionFund Ecuador, que permita identificar, prevenir, alertar y mitigar actividades fraudulentas en tiempo real sobre los canales digitales y transaccionales de la institución.

Nota: Este documento no constituye un compromiso de contratación. El Banco se reserva el derecho de rechazar cualquier propuesta, solicitar información adicional, modificar los criterios de evaluación, o declarar desierto el proceso en cualquier etapa.

3. Objetivos

3.1 Objetivo general

Contratar una plataforma tecnológica especializada que permita al Banco detectar, prevenir y gestionar el fraude en tiempo real en todos sus canales electrónicos, reduciendo pérdidas económicas, protegiendo a los clientes y cumpliendo con las obligaciones regulatorias vigentes.

3.2 Objetivos específicos

- Reducir pérdidas económicas ocasionadas por fraude electrónico en los canales digitales del Banco.
- Detectar actividades sospechosas en tiempo real mediante analítica avanzada e inteligencia artificial.
- Proteger a clientes y usuarios de ataques de ingeniería social, phishing, deepfake y robo de credenciales.
- Cumplir los requisitos regulatorios de la Superintendencia de Bancos relacionados con gestión de fraude y riesgo tecnológico.
- Fortalecer la confianza en los servicios digitales del Banco mediante controles efectivos y visibles.
- Disminuir la tasa de falsos positivos para mejorar la experiencia del cliente legítimo.

- Proporcionar capacidades de investigación y gestión de casos para el equipo de seguridad.

4. Alcance de la solución – Canales protegidos

La solución deberá cubrir de forma integral y simultánea los siguientes canales:

N°	Canal	Descripción del alcance
1	Banca Web	Monitoreo de sesiones, autenticación, navegación y transacciones en el portal web del Banco.
2	Banca Móvil	Monitoreo de sesiones, autenticación y transacciones realizadas desde la aplicación móvil.
3	Transferencias interbancarias	Evaluación de riesgo para transferencias electrónicas de acuerdo con reglas configurables definidas por el Banco.
4	Tarjetas de débito	Monitoreo de transacciones con tarjeta, detección de patrones anómalos y bloqueo automático. **Opcional – puede añadirse en una segunda fase**
5	APIs transaccionales	Monitoreo de llamadas a APIs expuestas, detección de abuso, scraping y automatización maliciosa. **Opcional – puede añadirse en una segunda fase**

5. Requerimientos funcionales

Nota: Para cada requerimiento, el proveedor que presente la propuesta deberá indicar: **C** = Cumple nativamente | **CP** = Cumple parcialmente | **NC** = No cumple.

5.1 Monitoreo transaccional en tiempo real

N°	Requerimiento	Tipo	Respuesta
5.1.1	Evaluación en línea de todas las transacciones antes de su autorización, con decisión en tiempo real.	Obligatorio	
5.1.2	Cálculo de puntaje de riesgo (score) por transacción con umbral configurable por la institución.	Obligatorio	
5.1.3	Bloqueo automático de transacciones que superen el umbral de riesgo definido.	Obligatorio	
5.1.4	Aprobación automática de transacciones de bajo riesgo sin fricción adicional para el cliente.	Obligatorio	
5.1.5	Escalamiento configurable para revisión manual de transacciones en zona de riesgo medio.	Obligatorio	
5.1.6	Generación automática de alertas para los analistas responsables del monitoreo antifraude.	Obligatorio	
5.1.7	Tiempo de respuesta menor o igual a 1 segundo.	Obligatorio	
5.1.8	La solución deberá soportar al menos un crecimiento del 25% sobre el volumen transaccional promedio actual.	Obligatorio	

5.2 Motor de reglas antifraude

N°	Requerimiento	Tipo	Respuesta
5.2.1	Motor de reglas configurable por la institución sin dependencia del proveedor para ajustes operativos.	Obligatorio	
5.2.2	Detección de transferencias que superen montos umbral configurables por tipo de usuario y canal.	Obligatorio	
5.2.3	Detección de transacciones fuera del horario habitual del cliente.	Obligatorio	

5.2.4	Detección de operaciones realizadas desde ubicaciones geográficas inusuales para el cliente.	Obligatorio	
5.2.5	Detección de múltiples intentos fallidos de autenticación en ventana de tiempo configurable.	Obligatorio	
5.2.6	Detección de incrementos atípicos en la actividad financiera del cliente.	Obligatorio	
5.2.7	Detección de cambios de dispositivo o navegador en sesión activa.	Deseable	
5.2.8	Versionamiento de reglas con historial de cambios y opción de rollback.	Deseable	
5.2.9	Simulación de impacto de nuevas reglas antes de activarlas en producción.	Opcional	

5.3 Análisis de comportamiento (Behavioral Analytics)

N°	Requerimiento	Tipo	Respuesta
5.3.1	Construcción automática de perfiles de comportamiento por cliente y actualización continua.	Obligatorio	
5.3.2	Análisis de frecuencia transaccional, horarios habituales y patrones de uso por canal.	Obligatorio	
5.3.3	Análisis de geolocalización y correlación con historial de accesos previos.	Deseable	
5.3.4	Biometría conductual: velocidad de digitación, presión táctil, ángulo del dispositivo, patrones de scroll.	Opcional	
5.3.5	Análisis de navegación dentro de la aplicación para detectar comportamiento asistido por terceros.	Opcional	
5.3.6	Identificación de sesiones donde el cliente está siendo guiado (ingeniería social en tiempo real).	Opcional	
5.3.7	Análisis de múltiples dispositivos por cliente para detectar uso no autorizado.	Opcional	

5.4 Inteligencia artificial y machine learning

N°	Requerimiento	Tipo	Respuesta
5.4.1	Modelos de ML supervisado y no supervisado para detección de anomalías transaccionales.	Deseable	
5.4.2	Capacidad de incorporar nuevas reglas de detección de fraude sin requerir desarrollos complejos.	Deseable	
5.4.3	Reducción activa de falsos positivos mediante retroalimentación de casos resueltos.	Deseable	
5.4.4	Predicción de comportamientos fraudulentos antes de que se materialicen.	Deseable	
5.4.5	Clasificación automática de riesgos con explicabilidad de la decisión (explainable AI).	Deseable	
5.4.6	Modelos adaptativos que evolucionan con nuevas tácticas de fraude sin intervención manual.	Deseable	
5.4.7	IA generativa para análisis y síntesis de campañas de fraude y anillos delictivos.	Deseable	
5.4.8	Simulador de ataques para probar la resiliencia del sistema ante nuevos vectores.	Deseable	

5.5 Gestión de casos e investigación

N°	Requerimiento	Tipo	Respuesta

5.5.1	Apertura automática de casos de investigación ante alertas de fraude con priorización automática.	Obligatorio	
5.5.2	Asignación y reasignación de casos a analistas con seguimiento de estado.	Obligatorio	
5.5.3	Consulta centralizada de información relevante para el análisis de alertas de fraude.	Obligatorio	
5.5.4	Registro y almacenamiento de evidencias asociadas a los casos con trazabilidad de las acciones realizadas.	Obligatorio	
5.5.5	Escalamiento configurable con notificaciones automáticas a niveles superiores.	Deseable	
5.5.6	Auditoría completa de todas las acciones realizadas por los analistas.	Obligatorio	
5.5.7	Identificación de anillos de fraude: correlación de casos relacionados por patrones comunes.	Opcional	
5.5.8	Capacidad de integración mediante API con herramientas de gestión de incidentes o requerimientos existentes en la institución.	Opcional	

6. Capacidades de ciberseguridad requeridas

6.1 Device Fingerprinting e inteligencia de dispositivos

N°	Requerimiento	Tipo	Respuesta
6.1.1	Identificación única de dispositivos mediante sistema operativo, navegador, IP, configuración y huella digital.	Obligatorio	
6.1.2	Detección de cambios en el dispositivo registrado durante sesión activa.	Obligatorio	
6.1.3	Generación de alertas ante accesos desde dispositivos no reconocidos o no previamente utilizados por el cliente.	Obligatorio	
6.1.4	Correlación de dispositivo con historial de fraude en base de datos global.	Opcional	
6.1.5	Detección de VPN, proxies y redes Tor usadas para enmascarar ubicación.	Deseable	

6.2 Detección de malware y acceso remoto

N°	Requerimiento	Tipo	Respuesta
6.2.1	Detección de troyanos bancarios, malware móvil, keyloggers y RAT basada en comportamiento y contexto.	Opcional	
6.2.2	Detección en tiempo real de herramientas de acceso remoto activas: AnyDesk, TeamViewer, Supremo, UltraViewer.	Opcional	
6.2.3	Evaluación del riesgo del dispositivo en tiempo real con capacidad de bloqueo preventivo de la sesión.	Obligatorio	
6.2.4	Detección de aplicaciones maliciosas instaladas en dispositivos móviles.	Opcional	
6.2.5	Alertas al analista ante detección de software de acceso remoto durante sesión bancaria.	Deseable	

6.3 Detección de emuladores y dispositivos comprometidos

N°	Requerimiento	Tipo	Respuesta
6.3.1	Identificación de dispositivos rooteados o con jailbreak con bloqueo configurable.	Deseable	

6.3.2	Identificación de entornos de ejecución que pudieran representar un riesgo para la operación.	Deseable	
6.3.3	Detección de técnicas de inyección digital para evasión biométrica (deepfake).	Opcional	
6.3.4	Liveness detection: verificación de que el usuario es una persona viva y presente al momento de la autenticación.	Opcional	
6.3.5	Anti-spoofing: detección de fotos, videos o deepfakes presentados en el proceso de verificación facial.	Opcional	

7. Tipos de fraude que la solución debe detectar

N°	Tipo de fraude	Descripción	Tipo	Respuesta
7.1	**Phishing / Smishing / Vishing**	Comunicaciones fraudulentas que suplantan al Banco para robar credenciales.	Deseable	
7.2	**Robo de credenciales**	Uso de credenciales obtenidas por filtraciones o ataques para acceder a cuentas.	Obligatorio	
7.3	**Account Takeover (ATO)**	Toma no autorizada de control de cuentas de clientes legítimos.	Obligatorio	
7.4	**SIM Swapping**	Duplicación fraudulenta de SIM para interceptar OTP y autenticaciones.	Deseable	
7.5	**Ingeniería social avanzada**	Manipulación psicológica potenciada por IA (voz clonada, deepfake de video).	Deseable	
7.6	**Fraude por deepfake**	Suplantación mediante identidades sintéticas en procesos biométricos.	Deseable	
7.7	**Fraude mediante bots**	Ataques automatizados de credential stuffing y brute force.	Obligatorio	
7.8	**Fraude transaccional**	Transferencias no autorizadas, pagos fraudulentos y desvío de fondos.	Obligatorio	
7.9	**Fraude con tarjetas**	Uso no autorizado de tarjetas de débito en canales presenciales y digitales.	Deseable	
7.10	**Fraude en pagos instantáneos**	Manipulación de transferencias ACH y pagos QR.	Deseable	
7.11	**Fraude interno**	Operaciones irregulares ejecutadas por personal del Banco.	Obligatorio	
7.12	**New Account Fraud**	Apertura de cuentas con identidades sintéticas o robadas.	Deseable	
7.13	**Mule Account Detection**	Identificación de cuentas utilizadas como destino de fondos fraudulentos.	Obligatorio	
7.14	**Fraude mediante IA generativa**	Ataques que utilizan IA para crear contenido fraudulento personalizado.	Deseable	

8. Requerimientos técnicos y de arquitectura

8.1 Integración y arquitectura

N°	Requerimiento	Tipo	Respuesta
8.1.1	APIs REST o SOAP documentadas para integración con core bancario FBS Financial 2.5.	Obligatorio	

8.1.2	Integración con switch transaccional para monitoreo de transacciones en tiempo real.	Obligatorio	
8.1.3	Integración con los mecanismos de autenticación y autorización utilizados por el Banco (MFA y otros controles de acceso).	Obligatorio	
8.1.4	Integración con SIEM institucional para correlación de eventos de seguridad.	Deseable	
8.1.5	Integración con DLP para detección de fuga de información vinculada a fraude.	Opcional	
8.1.6	Soporte para modalidad on-premise, cloud privado o híbrido.	Opcional	
8.1.7	Disponibilidad garantizada mínima del 99.9% con SLA documentado y penalidades.	Obligatorio	
8.1.8	La solución deberá permitir el crecimiento de capacidad conforme aumenten las necesidades operativas del Banco.	Obligatorio	
8.1.9	Plan de recuperación ante desastres (DRP) con RTO máximo de 4 horas y RPO de 1 hora.	Obligatorio	
8.1.10	Entornos separados de desarrollo, QA y producción.	Deseable	

8.2 Seguridad de la plataforma

N°	Requerimiento	Tipo	Respuesta
8.2.1	Cifrado TLS 1.2 mínimo (preferible TLS 1.3) en tránsito y AES-256 en reposo.	Obligatorio	
8.2.2	Acceso a la plataforma con MFA para todos los roles de administración y análisis.	Obligatorio	
8.2.3	Logs de auditoría completos e inmutables de todas las acciones en la plataforma.	Obligatorio	
8.2.4	El proveedor deberá contar con certificación ISO 27001, SOC 2 Type II o demostrar la adopción formal de controles equivalentes de seguridad de la información.	Deseable	
8.2.5	Política de gestión de vulnerabilidades del proveedor con SLA de remediación por criticidad CVSS.	Obligatorio	
8.2.6	Derecho contractual del Banco a realizar auditorías de seguridad sobre la plataforma.	Obligatorio	
8.2.7	Separación lógica de datos si la arquitectura es multi-tenant.	Obligatorio	

8.3 Protección de datos y privacidad

N°	Requerimiento	Tipo	Respuesta
8.3.1	Los datos deberán almacenarse en jurisdicciones que garanticen niveles adecuados de protección de datos y sean aceptadas por el Banco, conforme a la normativa aplicable.	Obligatorio	
8.3.2	Firma de Acuerdo de Encargo de Tratamiento conforme a la LOPDP ecuatoriana.	Obligatorio	
8.3.3	Mecanismo de devolución o eliminación certificada de datos al término del contrato.	Obligatorio	
8.3.4	Notificación al Banco de incidentes de seguridad o privacidad que involucren información institucional, dentro de los plazos acordados contractualmente y conforme a la normativa aplicable.	Obligatorio	
8.3.5	Política de retención de datos configurable conforme a requisitos regulatorios ecuatorianos.	Obligatorio	

9. Dashboards, reportería y KPIs

La plataforma deberá proporcionar los siguientes módulos de visibilidad y análisis:

N°	Dashboard / Reporte	Indicadores principales	Frecuencia
9.1	**Postura ejecutiva de fraude**	Monto de fraude evitado, tasa por canal, top-5 riesgos, tendencia 12 meses.	**Mensual / On-demand**
9.2	**Monitoreo operativo en tiempo real**	Alertas activas, transacciones bloqueadas, queue de revisión manual, MTTD/MTTR.	**Continuo**
9.3	**Efectividad de las reglas y controles antifraude**	Tasa de detección, falsos positivos, falsos negativos, precisión del scoring.	**Semanal**
9.4	**Gestión de casos**	Casos abiertos/cerrados, tiempo promedio de investigación, casos por analista.	**Diario**
9.5	**Análisis de fraude por canal**	Estadísticas por canal, tipo de fraude, segmento de cliente, horario.	**Mensual**
9.6	**Reportes regulatorios**	Exportación de información y reportes para atender requerimientos regulatorios y de control interno.	**A demanda**
9.7	**KPIs de ciberseguridad**	Disponibilidad de la plataforma, alertas generadas, eventos de riesgo identificados y tendencias de fraude.	**Continuo**

Los KPIs definidos por el Banco que la plataforma debe alimentar de forma automática son:

N°	KPI	Descripción
9.8	**Monto de fraude evitado**	Valor monetario de transacciones fraudulentas bloqueadas.
9.9	**Tasa de fraude por canal**	% de transacciones fraudulentas sobre el total por canal.
9.10	**Tiempo promedio de detección (MTTD)**	Tiempo desde la transacción hasta la generación de la alerta.
9.11	**Tiempo promedio de respuesta (MTTR)**	Tiempo desde la alerta hasta la acción de contención.
9.12	**Porcentaje de falsos positivos**	% de alertas que resultaron ser transacciones legítimas.
9.13	**Porcentaje de falsos negativos**	% de fraudes materializados no detectados por la plataforma.
9.14	**Número de cuentas comprometidas**	Cuentas con compromiso confirmado en el período.
9.15	**Disponibilidad de la plataforma**	% de uptime efectivo vs SLA comprometido.
9.16	**Efectividad de controles antifraude**	% de eventos o transacciones fraudulentas identificadas por los mecanismos de detección de la solución respecto al total de fraudes confirmados.

10. Marco normativo y estándares de cumplimiento

La solución deberá contribuir al cumplimiento de las siguientes normativas y estándares, cuyo cumplimiento será verificado durante la evaluación:

Normativa / Estándar	Aspecto relevante	Criticidad
Resolución SB-2021-2126	Gestión de riesgo operativo, seguridad de canales electrónicos, monitoreo, auditoría externa.	**Alta**
Ley Orgánica de Ciberseguridad (mayo 2026)	Notificación de incidentes en 72h, punto de contacto 24/7, coordinación con CSIRT Nacional.	**Alta**

LOPDP y su Reglamento	Protección de datos personales, notificación de brechas en 5 días, encargos de tratamiento.	**Alta**
UAFE — Prevención AML	Monitoreo de operaciones inusuales, detección de mulas, reportes ROII.	**Alta**
Código Orgánico Monetario y Financiero	Marco prudencial, secreto bancario, deberes fiduciarios.	**Alta**
ISO/IEC 27001:2022	Controles del SGSI, gestión de riesgos, mejora continua.	**Media**
NIST CSF 2.0	Funciones Detectar y Responder del marco de ciberseguridad.	**Media**
PCI DSS v4.0	Protección de datos de tarjetahabientes en transacciones electrónicas.	**Baja**
OWASP ASVS / MASVS	Seguridad de aplicaciones web y móviles.	**Baja**
MITRE ATT&CK	Cobertura de técnicas y tácticas de ataque para casos de uso del sistema.	**Baja**

11. Implementación, soporte y continuidad del servicio

N°	Requerimiento	Tipo	Respuesta
11.1	Plan de implementación detallado con fases, hitos, responsables y plazos hasta go-live.	**Obligatorio**	
11.2	Tiempo máximo estimado de implementación hasta go-live: especificar en semanas.	**Obligatorio**	
11.3	Soporte en español para incidentes críticos conforme SLA acordado.	**Obligatorio**	
11.4	Capacitación inicial incluida para administradores, analistas y personal técnico del Banco.	**Obligatorio**	
11.5	Experiencia demostrable en instituciones financieras o sectores regulados.	**Obligatorio**	
11.6	Plan de continuidad del servicio del proveedor ante eventos que afecten su operación.	**Obligatorio**	
11.7	Proceso formal de gestión de cambios y actualizaciones con aviso previo al Banco.	**Obligatorio**	
11.8	Cláusula de salida: portabilidad de datos, documentación técnica y soporte en transición.	**Obligatorio**	

12. Información comercial requerida

El proveedor deberá presentar su propuesta comercial en documento separado, incluyendo de forma desglosada y clara:

N°	Componente	Detalle requerido
12.1	**Modelo de licenciamiento**	Especificar de forma independiente el costo del licenciamiento base de la solución y el costo de cada módulo adicional ofertado. Indicar modalidad de cobro (por transacción, usuario, canal, suscripción anual u otra) y proyección de costos para al menos un año. Señalar claramente pagos únicos y pagos recurrentes.
12.2	**Costo de implementación**	Desglosar los costos asociados a análisis, parametrización, integración, pruebas, capacitación, acompañamiento en puesta en producción y gestión del proyecto. Incluir gastos de viaje o servicios adicionales en caso de aplicar.
12.3	**Costo anual de mantenimiento y soporte**	Especificar detalladamente los servicios incluidos en el mantenimiento anual, soporte funcional, soporte técnico, actualizaciones, parches y nuevas versiones. Identificar claramente cualquier actividad que genere costos adicionales.
12.4	**Costo de capacitación**	Desglosar los costos de capacitación inicial y capacitaciones posteriores. Indicar modalidad presencial, virtual o mixta, cantidad de participantes y horas incluidas.

12.5	**Costos de integración**	Presentar de forma independiente los costos de integración con el core bancario, canales electrónicos, sistemas de autenticación, SIEM u otras plataformas requeridas. Especificar horas estimadas o costo fijo por cada integración.
12.6	**Módulos opcionales y sus costos**	Threat intelligence, dark web monitoring, simulador de ataques, etc.
12.7	**Penalidades por incumplimiento de SLA**	Presentar el esquema de penalizaciones aplicables por incumplimiento de disponibilidad, tiempos de atención, tiempos de respuesta y tiempos de solución comprometidos contractualmente.
12.8	**Condiciones de renovación**	Detallar las condiciones de renovación, incrementos anuales aplicables, vigencia de precios, mecanismos de actualización de tarifas y condiciones para terminación o no renovación del contrato.
12.9	**Propuesta de valor y ROI estimado**	Presentar de forma independiente los beneficios esperados de la solución, reducción estimada de fraude, mejoras operativas y retorno de inversión proyectado, considerando el volumen transaccional actual del Banco.

13. Criterios de evaluación y ponderación

Las propuestas serán evaluadas conforme a los siguientes criterios. Puntaje máximo por criterio: 5 puntos. Puntaje final = puntaje obtenido × peso.

#	Criterio de evaluación	Peso	Puntaje (0-5)	Ponderado
1	Capacidades de detección y prevención en tiempo real (sección 5.1 y 5.2)	25%		
2	Análisis de comportamiento e IA/ML (sección 5.3 y 5.4)	15%		
3	Capacidades de ciberseguridad: device intelligence, malware, deepfake (sección 6)	15%		
4	Cobertura de tipos de fraude (sección 7)	10%		
5	Arquitectura, integración y rendimiento técnico (sección 8)	10%		
6	Gestión de casos, dashboards y reportería (secciones 5.5 y 9)	5%		
7	Cumplimiento normativo y seguridad de la plataforma (secciones 8.2, 8.3 y 10)	5%		
8	Implementación, soporte y continuidad (sección 11)	5%		
9	Propuesta comercial y modelo de costo-beneficio (sección 12)	8%		
10	Experiencia en sector financiero latinoamericano y referencias verificables	2%		
TOTAL		100%		

Puntaje mínimo para ser considerada: 3/5 en los criterios de Detección y Prevención de Fraude, Gestión de Casos, Cobertura de Tipos de Fraude, Arquitectura e Integración, y Seguridad de la Plataforma. Las funcionalidades avanzadas o de valor agregado no serán causales de descalificación.

14. Causales de descalificación automática

Una propuesta será descalificada automáticamente si el proveedor:

- No acepta firmar el Acuerdo de Encargo de Tratamiento de Datos Personales conforme a la LOPDP.
- No acepta el derecho del Banco a realizar auditorías de seguridad sobre la plataforma.
- No puede garantizar contractualmente los niveles de disponibilidad comprometidos en su propuesta.
- No acepta los requisitos de protección de datos y confidencialidad establecidos por el Banco.

- No cumple con los niveles de desempeño y tiempos de respuesta comprometidos en su propuesta técnica.
- No cuenta con experiencia comprobable en instituciones financieras o sectores regulados.
- No cumple con los requisitos de residencia, protección y tratamiento de datos definidos por el Banco y la normativa aplicable.

Nota: Las funcionalidades avanzadas consideradas como **deseables** u **opcionales** dentro del presente TDR, tales como capacidades avanzadas de inteligencia artificial, biometría conductual, detección de deepfakes, inteligencia global de dispositivos u otras similares, no constituirán causales de descalificación automática.

15. Proceso de evaluación y condiciones

15.1 Formato de respuesta

- El proveedor deberá responder cada requerimiento con las calificaciones C / CP / NC
- Deberá adjuntarse evidencia técnica para los requerimientos marcados como Obligatorio.
- La propuesta comercial deberá presentarse en documento separado del técnico.

15.2 Proceso

- **Recepción de propuestas:** fecha a definir por el Banco.
- **Evaluación técnica documental**: 5 días hábiles tras recepción.
- **Demo técnica obligatoria para proveedores preseleccionados:** sesión mínima de 3 horas en ambiente de pruebas con casos de uso reales del sector financiero.
- **Verificación de referencias:** el Banco contactará directamente a los clientes referenciados.
- Decisión final comunicada por escrito a todos los participantes.

15.3 Condiciones generales

- Los valores de la propuesta deben expresarse en dólares de los Estados Unidos (USD) sin IVA.
- **Validez de la oferta:** 60 días calendario desde la fecha de presentación.
- Banco VisionFund Ecuador se reserva el derecho de modificar los términos, ampliar plazos, declarar desierto el proceso o dividir la adjudicación entre varios proveedores.
- Toda comunicación durante el proceso deberá realizarse por escrito a través del canal oficial definido por el Banco.
- La presentación de una propuesta implica la aceptación de todas las condiciones establecidas en el presente TDR.

15.4 Consulta, ampliación de detalles y aclaración de dudas (técnicas)

- Msc. Gonzalo Ñauta B. – **Oficial de Seguridad de la Información** – rigoberto_nauta@visionfund.org – 0985777483
- Msc. Jessica Báez – **Analista de Ciberseguridad** – jessica_baez@visionfund.org – 0984059719