Ficha Difusión de Requerimiento

Fecha de publicación: 13/05/2026

Entidad Contratante: Fondo MIVIVIENDA S.A.

RUC: 20414671773

Ficha de difusión de requerimiento

Requerimiento

Información general del requerimiento

Nro. de Requerimiento	3845
Descripción	SERVICIO DE DESARROLLO E IMPLEMENTACIÓN DE UNA PLATAFORMA INTEGRAL PARA LA GESTIÓN DE CRÉDITOS
Objeto	Servicio
Fecha y hora de publicación del requerimiento.	13/05/2026 13:32:13

Información general de la entidad

Entidad Convocante	FONDO MIVIVIENDA S.A.
Dirección legal	AV. PASEO DE LA REPUBLICA Nº 3121 SAN ISIDRO LIMA
Página Web	
Teléfono de la Entidad	2117373

Cronograma

Etapa	Fecha Inicio	Fecha Fin
Publicación del Requerimiento	13/05/2026	13/05/2026
Formulación de consultas y/o comentarios técnicos	14/05/2026	20/05/2026
Absolución de consultas y/o comentarios y cronograma de reunión de confirmación y/o aclaración	21/05/2026	25/05/2026
Acta de la reunión	26/05/2026	28/05/2026

Listado de archivos del requerimiento

Nro.	Nombre de Archivo	Tipo Archivo	Tamaño (KB)	Archivo (KB)	Usuario de publicación
1	TDR PLATAFORMA DE CREDITOS.docx	docx	935.38		70902556

Regresar

REQUERIMIENTO

SERVICIO DE DESARROLLO E IMPLEMENTACIÓN DE UNA PLATAFORMA INTEGRAL PARA LA GESTIÓN DE CRÉDITOS

3.1. FINALIDAD PÚBLICA DE LA CONTRATACIÓN

a) La finalidad del presente servicio es que el FONDO MIVIVIENDA S.A., en adelante, el FONDO, cuente con una Plataforma Integral y Unificada para la Gestión de Créditos, desarrollada e implementada a medida de sus necesidades operativas, normativas, funcionales y tecnológicas, que permita centralizar los procesos relacionados con el otorgamiento, administración, seguimiento, control, cobranza, liquidación y registro de productos financieros especializados, tales como créditos hipotecarios, fideicomisos, garantías y otros servicios vinculados a la gestión crediticia institucional.

b) El objeto de la contratación no corresponde a la adquisición de una licencia de software comercial preexistente, sino a la contratación de un servicio especializado que comprende el análisis, diseño, desarrollo, implementación, migración de información, puesta en producción, operación, soporte y mantenimiento de una plataforma tecnológica construida conforme a los procesos, reglas de negocio, requerimientos regulatorios y particularidades operativas del FONDO. En ese sentido, la plataforma deberá responder a la naturaleza institucional del FONDO, considerando su rol como entidad especializada en el financiamiento de la vivienda, su interacción con las Instituciones Financieras Intermediarias IFI, así como sus obligaciones de control, trazabilidad, reporte y cumplimiento normativo.

c) La plataforma deberá permitir la integración ordenada, segura y trazable con las IFI y con otras entidades externas que intervienen en los procesos de originación, administración, seguimiento, cobranza y control de las operaciones crediticias. Para ello, deberá contar con interfaces estandarizadas, mecanismos de interoperabilidad y controles de seguridad que faciliten una comunicación fluida entre el FONDO y sus aliados estratégicos, fortaleciendo la eficiencia operativa, la transparencia de la información y la percepción institucional frente a las entidades participantes.

d) Asimismo, la solución deberá contribuir a la automatización integral de los procesos vinculados al ciclo de vida del crédito, permitiendo que la información se encuentre disponible en línea, de manera oportuna y bajo adecuados controles de integridad, seguridad, trazabilidad y consistencia. Con ello, se busca reducir los tiempos operativos, disminuir los riesgos asociados al manejo manual o disperso de información, fortalecer el cumplimiento normativo y facilitar el seguimiento de cada etapa de la gestión crediticia.

e) La disponibilidad de información consolidada, confiable y oportuna permitirá al FONDO fortalecer su capacidad de análisis, control y toma de decisiones, al contar con datos estructurados que faciliten la generación de reportes operativos, financieros, contables, regulatorios y de gestión. De esta manera, la plataforma contribuirá a mejorar la eficiencia institucional y a brindar soporte tecnológico a los procesos críticos vinculados al negocio del FONDO.

f) El servicio comprenderá, además, la provisión, gestión, administración y operación de la infraestructura tecnológica requerida para el funcionamiento de la plataforma, bajo un entorno que asegure disponibilidad, escalabilidad, seguridad, continuidad operativa y mecanismos de recuperación ante desastres, conforme a los niveles de servicio que se establezcan contractualmente.

g) En conjunto, la plataforma constituirá un activo institucional estratégico, desarrollado a medida y bajo control del FONDO, orientado a modernizar la gestión crediticia, reducir la fragmentación de los sistemas actuales, mejorar la eficiencia operativa, fortalecer la trazabilidad de las operaciones y dotar a la entidad de una solución flexible, escalable

y adaptable frente a los cambios normativos, operativos y tecnológicos que puedan presentarse en el tiempo.

h) Además, esta iniciativa se alinea con los instrumentos de planificación estratégica que orientan la gestión institucional del FONDO enfocada en resultados, destacando especialmente el Plan de Gobierno Digital 2023–2026, cuyo objetivo prioritario es “optimizar la gestión administrativa y de control”.

i) Asimismo, este servicio contribuye directamente al cumplimiento de los siguientes objetivos estratégicos:

   1. Plan Estratégico Corporativo de FONAFE 2022–2026
   2. Plan Estratégico del FONDO 2022–2026
   3. Plan Operativo Institucional (POI) del FONDO

j) A continuación, se detallan los ejes de alineamiento principales:

   1. Objetivo Estratégico Corporativo: Implementar procesos de transformación digital.
   2. Objetivo Estratégico FONDO: Implementar la transformación digital del FONDO.
   3. Objetivo Específico FONDO: Implementar la transformación digital en FONDO.
   4. Indicador: Nivel de ejecución de proyectos de transformación digital.

k) Finalmente, el proyecto contribuye al logro del objetivo estratégico OE6: "Asegurar la eficiencia de la organización a través de la implementación del modelo de transformación digital", sentando las bases para una gestión moderna, integrada y con trazabilidad institucional.

POI:

ACTIVIDAD: AEI22: Implementar el equipo, infraestructura y el portafolio de proyectos de digitalización (Modelo de Gobierno Digital)

OE6: Asegurar eficiencia de la organización a través de la implementación del modelo de transformación digital.

3.2. DESCRIPCIÓN GENERAL DEL REQUERIMIENTO

3.2.1 Antecedentes:

a) El Fondo MIVIVIENDA S.A. es una entidad adscrita al Ministerio de Vivienda, Construcción y Saneamiento, supervisada por la Superintendencia de Banca, Seguros y AFP (SBS), que tiene a su cargo la gestión de productos y servicios vinculados al financiamiento de vivienda, a través de mecanismos de canalización con entidades del sistema financiero y fideicomisos especializados.

b) Para la administración de sus distintos productos y carteras, el FMV ha venido utilizando diversas soluciones tecnológicas desarrolladas o implementadas en distintos momentos, tales como el sistema SAOC para la gestión de la cartera de créditos desembolsados con y sin recursos del Fondo y del Bono del Buen Pagador; el sistema PRECOSS para la administración de productos como el Fideicomiso de la Cobertura de Riesgo Crediticio y el Premio al Buen Pagador; así como el sistema NSCC para la gestión de determinadas carteras transferidas o provenientes de entidades en liquidación.

c) No obstante, la coexistencia de múltiples sistemas ha generado un esquema operativo fragmentado, con procesos dispersos, actividades manuales, dificultades de integración, limitaciones para la trazabilidad de la información y mayores esfuerzos para la atención de requerimientos operativos, contables, regulatorios y de control. Esta situación incrementa el riesgo operativo, dificulta

la obtención oportuna de información y eleva los costos de mantenimiento y sostenibilidad tecnológica.

d) En ese contexto, el FMV ha identificado la necesidad de contar con una solución tecnológica integral que permita centralizar y modernizar la gestión de sus productos y servicios crediticios, reduciendo la dependencia de sistemas heredados y fortaleciendo la eficiencia operativa, el control de la información y la capacidad de evolución futura de la plataforma tecnológica institucional.

3.2.1 Descripción del Servicio

a) El presente requerimiento corresponde a la contratación de un servicio especializado para el desarrollo e implementación de una Plataforma Integral para la Gestión de Créditos del Fondo MIVIVIENDA S.A., bajo un enfoque de desarrollo de software a medida, orientado a cubrir las necesidades funcionales, operativas, contables y de integración propias del negocio del FMV.

b) La solución deberá permitir la gestión integral de los productos y servicios crediticios del FMV a lo largo de todo su ciclo operativo, desde la originación, evaluación, aprobación, desembolso, administración, cobranza, conciliación y cierre operativo-contable, hasta la generación de reportes y consultas requeridas por las áreas usuarias y de control. Asimismo, deberá contemplar la migración de información histórica proveniente de los sistemas actualmente en uso, así como la integración con los sistemas internos del FMV y con entidades externas que intervienen en los procesos relacionados con la gestión crediticia.

c) El servicio no se limita al desarrollo del software. Comprende también la provisión de la infraestructura tecnológica necesaria para la operación de la solución, así como los servicios asociados de instalación, configuración, despliegue, soporte técnico y funcional, administración operativa y atención de incidencias. Del mismo modo, deberá considerar la disponibilidad de una bolsa de horas para la atención de requerimientos adicionales, ajustes, mejoras o adecuaciones funcionales y técnicas que resulten necesarias durante la vigencia contractual, en función de las necesidades del FMV y dentro de las condiciones que se establezcan en los presentes términos de referencia.

d) En ese sentido, se trata de una contratación integral que abarca tanto la construcción de una solución tecnológica a medida como su puesta en funcionamiento, sostenimiento operativo y capacidad de evolución controlada durante el periodo contractual.

3.2.1 Alcance del requerimiento

a) El detalle del alcance se presenta en los puntos siguientes:

Ítem	Descripción	Fases	Detalle	
1	**Prestación Principal: Desarrollo e implementación de una PLATAFORMA para la GESTIÓN DE CRÉDITOS**	**FASE 1**	**1.1**	Diseño e Implementación de arquitectura de la nube
			1.2	Desarrollo e Implementación de la Plataforma para la Gestión de créditos - Nuevos Productos y Migración de Carteras (Reemplazo del Sistema NSCC)
			1.3	*Marcha Blanca de FASE 1*
		FASE 2	**2.1**	Desarrollo e Implementación de la Plataforma para la Gestión de créditos - Fideicomiso, Garantías y Provisiones (Reemplazo de actual sistema SAOC y SIR)
			2.2	*Marcha Blanca de la FASE 2*
		FASE 3	**3.1**	Migración datos históricos (COFIDE)
2		**FASE 4**	**4.1**	Operación

	Prestación Principal: Operación	**FASE 5**	**5.1**	Transición de salida
3	**Prestación accesoria: Servicio de Bolsa de horas (900 horas)**	**FASE 6**	**6.1**	Soporte a demanda

b) El servicio incluirá el desarrollo de una solución a medida y la infraestructura donde esta se brindará el servicio, que contemple todas las fases del ciclo de vida del proyecto: levantamiento, rediseño y optimización de procesos, diseño funcional y técnico, desarrollo, pruebas, implementación, migración, puesta en producción y soporte técnico y funcional continuo. Este soporte deberá garantizar la continuidad operativa, la atención oportuna de incidencias y requerimientos, así como la incorporación de mejoras evolutivas durante toda la vigencia del contrato.

c) La plataforma deberá ser configurable y dinámica de tal manera que se adapte a los procesos actuales del FMV. A fin de que el FMV considerase optimizar o rediseñar algún proceso, la PLATAFORMA deberá adecuarse a este nuevo proceso de una manera flexible, de tal manera que permita configurar productos, sin necesidad de desarrollo interno.

d) Proponer y consensuar con el FMV la mejora, rediseño y optimización de dichos procesos, asegurando:

   1. La trazabilidad de cada etapa.
   2. La conformidad con los marcos normativos vigentes.

e) La alineación con las mejores prácticas del sector financiero y de tecnología aplicada a servicios crediticios.

f) Garantizar que la automatización que se implemente esté sustentada en procesos previamente optimizados, evitando replicar ineficiencias o estructuras operativas obsoletas. La plataforma deberá reflejar los procesos mejorados y documentados, asegurando su adecuada gestión en entornos digitales.

3.2.1.1 Prestación Principal

3.2.1.1.1 Desarrollo e Implementación de la Plataforma para la GESTIÓN DE CRÉDITOS:

La prestación principal comprende el diseño, desarrollo, implementación, provisión de infraestructura TI y migración de datos históricos y operación de una plataforma integral orientada a la gestión de créditos hipotecarios, fideicomisos y garantías. Esta solución será desarrollada a medida, y su arquitectura estará basada en un entorno de nube pública y/o privada y/o híbrida, priorizando la eficiencia operativa, la seguridad de la información, ciberseguridad, datos personales, la escalabilidad y el cumplimiento normativo.

A) Diseño e implementación de la arquitectura en la nube

Como fase inicial del servicio, el CONTRATISTA deberá diseñar e implementar una arquitectura tecnológica en la nube publica y/o privada y/o híbrida, la cual deberá brindarse como servicio a FMV y deberá estar alojada en una de las principales plataformas públicas o en un centro de datos certificado por UPTIME INSTITUTE o ANSI/IA-942-C en operación en un nivel de TIER III o RATED-3 como mínimo, asimismo debe contar con su propio Centro de Operaciones de Red (NOC – Network Operations Center) y su propio Centro de Operaciones de Seguridad (SOC – Security Operations Center), los cuales brindarán los servicios de monitoreo, gestión y

atención de incidentes requeridos, manteniendo comunicación directa con la entidad garantizando un entorno moderno, seguro y con alto rendimiento operativo.

Esta arquitectura en la nube deberá cumplir, como mínimo, con las siguientes características:

- Alta disponibilidad, con un nivel de servicio mínimo del 99.5%, respaldado por un plan de recuperación ante desastres (DRP) alineado a los SLA establecidos.
- Eficiencia económica en el uso de recursos, así como escalabilidad automática, que permita adaptar la infraestructura según las necesidades crecientes del FONDO.
- Seguridad avanzada, incluyendo la encriptación de los datos donde corresponda, aislamiento de ambientes y cumplimiento con las mejores prácticas internacionales de ciberseguridad.
- La plataforma debe incluir capacidades de despliegue y orquestación de contenedores mediante Kubernetes, configurado para entornos de microservicios.
- La plataforma debe permitir Autenticación multifactor (MFA) y control de accesos granulares para mitigar riesgos de seguridad
- Contar con un servicio de almacenamiento de bloques basado en arquitectura distribuida. Se deben operar estos servicios sin detener los servicios de la solución de nube. Puede utilizarse para sistemas de archivos, bases de datos, y otro software de sistema o aplicaciones que necesiten almacenamiento de bloques. Este servicio debe permitir configurar almacenamiento en discos SSD (cómputo y base de datos) desde el mismo portal de autoaprovisionamiento.
- La infraestructura deberá garantizar una latencia máxima de 20 milisegundos (RTT) entre la nube del CONTRATISTA y la sede del FONDO, medida mensualmente mediante el comando ping desde un equipo de la red del FONDO hacia el punto de presencia de la infraestructura del CONTRATISTA, en horario laboral y bajo condiciones normales de carga de producción. El ancho de banda deberá ser suficiente para soportar la operación concurrente de la plataforma sin degradación del servicio. El incumplimiento de estos parámetros estará sujeto a las penalidades establecidas en el contrato.
- Capacidad de integración, garantizando compatibilidad con los sistemas internos del FONDO, tales como plataformas de facturación electrónica y demás aplicativos corporativos.

  El CONTRATISTA será responsable de:

  - Diseñar e implementar toda la arquitectura que alojará la Plataforma para la Gestión de Créditos. Para lo cual deberá habilitar los siguientes componentes y/o servicios críticos en la nube pública y/o privada y/o hibrida, dichos componentes pueden ser desplegados en modalidad IaaS y/o PaaS y/o ser desplegados como contenedores con soporte directo del CONTRATISTA.

Componente	Descripción técnica mínima
Clúster de Kubernetes	Clúster de 3 nodos worker y 3 nodos master. Se debe integrar a un repositorio de imágenes de contenedores y servicio de balanceo de carga, así como la gestión de volúmenes persistentes para los contenedores.
Keycloak (IdP)	Servicio de Autenticación OIDC con SSO, control de roles y federación LDAP/AD.
Redis (Cache)	Clúster con 3 nodos maestros + 3 réplicas, replicación asíncrona y failover automático.
MongoDB (NoSQL)	Replica Set (3 nodos) para datos no estructurados con respaldo automático.
Componentes DevOps	Jenkins, SonarQube y Nexus Repository con pipelines para el despliegue automatizo de aplicaciones.
API Gateway (Kong)	Servicio de gestión de acceso, autenticación OIDC y políticas de rate-limiting.

Clúster de Kafka	Plataforma de mensajería distribuida basada en Apache Kafka para procesamiento y transmisión de eventos en tiempo real, con configuración de alta disponibilidad y replicación entre nodos.
Monitorización y Logging	Prometheus/Grafana y ELK o equivalente para observabilidad y logs.

Las tecnologías especificadas corresponden al stack estándar de la industria para plataformas financieras de alto volumen y misión crítica. Su especificación responde a criterios técnicos objetivos y no restringe la competencia, dado que todas son de código abierto, implementables por cualquier proveedor del mercado.

La arquitectura requerida integra componentes especializados para orquestación de contenedores, gestión de identidades, caché distribuida, almacenamiento no relacional, integración y entrega continua, gestión de APIs, mensajería de eventos en tiempo real, y observabilidad operativa. Esta combinación constituye el modelo arquitectónico consolidado a nivel internacional para sistemas financieros escalables, de alta disponibilidad y misión crítica, garantizando interoperabilidad, seguridad, trazabilidad y capacidad de supervisión técnica durante toda la vigencia del contrato.

- Implementar la replicación para recuperación ante desastres de los componentes y/o servicios críticos de infraestructura de nube publica y/o privada y/o híbrida. Para esta replicación el CONTRATISTA deberá considerar los productos y/o licencias y/o suscripciones y/o servicios necesarios para cumplir el objetivo de FMV.

- Gestionar de forma continua la infraestructura de nube publica y/o privada y/o híbrida durante toda la vigencia del servicio, lo que incluye: provisión y monitoreo de recursos, mantenimiento preventivo y correctivo, administración de accesos, seguridad, disponibilidad operativa y despliegue de actualizaciones evolutivas correspondientes a la arquitectura de nube conforme a los requerimientos del FONDO.

Esta infraestructura deberá estar preparada para soportar una operación segura, escalable, interoperable y alineada con las necesidades técnicas y funcionales del FONDO.

B) Desarrollo e implementación de la plataforma

Sobre la arquitectura previamente implementada, el CONTRATISTA será responsable del desarrollo integral, implementación, configuración, integración, pruebas y puesta en producción de la Plataforma para la Gestión de Créditos, conforme a las fases previstas en el presente documento.

La responsabilidad del CONTRATISTA comprende el desarrollo de todos los módulos, componentes funcionales, componentes técnicos, reglas de negocio, reportes, procesos automatizados, interfaces, servicios, APIs, procesos batch, mecanismos de interoperabilidad e integraciones con sistemas internos y externos que hayan sido identificados como necesarios para asegurar el funcionamiento completo, continuo, seguro y operativo de la plataforma.

En tal sentido, el CONTRATISTA deberá garantizar que la plataforma opere de manera integral y al 100% de las funcionalidades previstas en el alcance aprobado, incluyendo las integraciones necesarias para la originación, administración, seguimiento, cobranza, conciliación, liquidación, registro contable, generación de reportes, interoperabilidad con entidades externas y demás procesos vinculados a la gestión de créditos del FONDO.

La Plataforma para la Gestión de Créditos deberá cumplir, como mínimo, con los siguientes lineamientos:

- Cumplimiento normativo: adaptación al marco regulatorio peruano, generación automatizada de informes normativos, interoperabilidad para el cumplimiento de obligaciones vinculadas a PLAFT, seguridad de la información, ciberseguridad, continuidad de negocio y demás disposiciones aplicables al FONDO.

- Buenas prácticas tecnológicas: arquitectura orientada a servicios, integración mediante APIs y/o mecanismos equivalentes, procesos optimizados, transaccionalidad en tiempo real, contabilidad diaria, trazabilidad completa, mantenibilidad, escalabilidad y control de versiones.

- Capacidades técnicas y funcionales: gestión de productos financieros, soporte para canales digitales, administración de reglas de negocio, parametrización funcional, resiliencia, disponibilidad permanente, interoperabilidad y capacidad de adaptación a nuevas necesidades institucionales.

- Interfaz web y administración: acceso mediante navegadores estándar, portal de administración de usuarios, perfiles, roles, permisos, parámetros, monitoreo funcional y administración de la solución.

- Integraciones obligatorias para la operación: desarrollo e implementación de las interfaces necesarias con los sistemas internos del FONDO, entidades externas, IFI, servicios de autenticación, sistemas contables, plataformas de cobranza, servicios de interoperabilidad, repositorios de información, componentes de seguridad y demás sistemas identificados en la etapa de análisis como necesarios para el funcionamiento integral de la plataforma.

- Actualizaciones y seguridad: despliegue de versiones actualizadas, aplicación de parches, copias de seguridad diarias, restauración granular, cifrado de datos, control de accesos, gestión de vulnerabilidades y cumplimiento de estándares de seguridad del sector financiero y regulaciones aplicables.

- Documentación técnica y funcional: el CONTRATISTA deberá entregar toda la documentación técnica, funcional, operativa, de integración, despliegue, administración y soporte correspondiente, conforme a lo indicado en el numeral 3.4.11.1 de la Fase 1 del presente documento.

C) Migración de datos históricos

El CONTRATISTA deberá ejecutar la migración de los datos históricos actualmente almacenados en las plataformas existentes, aplicando metodologías de data cleansing, estandarización y normalización, asegurando la integridad, consistencia y trazabilidad de la información trasladada a la nueva plataforma

3.2.1.1.2 Prestación principal: Operación del servicio

Durante la etapa de operación, el CONTRATISTA será responsable de garantizar la continuidad del servicio, asegurar la disponibilidad de la infraestructura en nube publica y/o privada y/o hibrida, así como la parte funcional de la Plataforma para la Gestión de Créditos y atender de manera oportuna cualquier incidencia que afecte su desempeño. Esta operación deberá ejecutarse bajo un modelo de gestión alineado a las mejores prácticas de ITIL, asegurando trazabilidad, eficiencia, mejora continua y cumplimiento normativo.

Asimismo, el CONTRATISTA deberá gestionar de manera integral la infraestructura tecnológica en la nube implementada para alojar la plataforma, asegurando su correcta provisión, mantenimiento preventivo y correctivo, administración de accesos, disponibilidad de recursos, escalabilidad, respaldo y recuperación ante desastres. Esta gestión deberá garantizar el cumplimiento de los niveles de servicio acordados (SLA), especialmente en cuanto a disponibilidad mínima (99.5%), rendimiento y seguridad de la información.

Durante toda la vigencia del servicio, el CONTRATISTA deberá realizar el monitoreo proactivo de la plataforma y su infraestructura, implementar las mejoras evolutivas necesarias y garantizar que la operación de la plataforma sea estable, segura, eficiente y alineada con los objetivos estratégicos del FONDO.

3.2.1.2 Prestación Accesoria

Servicio de Bolsa de Horas

De manera adicional y bajo demanda, el FONDO contará con una bolsa de 900 horas durante la etapa de operación del servicio. Estas horas estarán destinadas exclusivamente a la atención de requerimientos nuevos, mejoras evolutivas, ampliaciones funcionales, optimizaciones o adaptaciones de la plataforma, que surjan a partir de necesidades institucionales no contempladas en el alcance original del servicio contratado.

La bolsa de horas no será utilizada para la atención de incidencias, errores o problemas derivados de funcionalidades ya implementadas dentro del alcance principal del servicio, las cuales deberán ser gestionadas en el marco del soporte técnico regular incluido en la prestación principal.

El uso de estas horas deberá ser solicitado formalmente por el Supervisor de Aplicaciones de la OTI del FONDO mediante correo electrónico institucional al Gestor del Servicio del CONTRATISTA, detallando el requerimiento a desarrollar, el estimado de horas y la prioridad.

El Gestor del Servicio es el responsable de atender la solicitud, asignando el personal necesario de su equipo para ejecutar el desarrollo requerido. En un plazo máximo de cinco (05) días calendarios desde recibida la solicitud, el Gestor del Servicio remitirá al Supervisor de Aplicaciones una estimación de horas y plazo de entrega para su aprobación. Sin dicha aprobación no podrá iniciarse la ejecución.

Para efectos de valorización, control y seguimiento, las horas ejecutadas se contabilizarán conforme a las tarifas unitarias ofertadas por el Contratista en su propuesta económica, las cuales deberán incluir todos los costos asociados a la prestación del servicio y permanecerán fijas durante toda la ejecución contractual.
Los niveles de servicio (SLA) aplicables a los requerimientos atendidos mediante la bolsa de horas serán medidos y contabilizados en días calendario. Los requerimientos serán clasificados según su nivel de prioridad:

Prioridad Tiempo máximo de atención inicial Tiempo máximo para presentación de estimación técnica:

Alta	1 día calendario	2 días calendario
Media	2 días calendario	3 días calendario
Baja	3 días calendario	5 días calendario

La atención efectiva de cada requerimiento se realizará conforme al cronograma previamente aprobado por la Entidad.

El uso de la bolsa de horas deberá ser solicitado formalmente por el Supervisor de Aplicaciones del FONDO MIVIVIENDA, mediante correo electrónico o documento interno equivalente, detallando como mínimo la descripción del requerimiento, prioridad, objetivo funcional y plazo requerido.
Recibida la solicitud, el Contratista deberá remitir una estimación técnica que incluya las actividades a ejecutar, perfiles requeridos, cantidad estimada de horas y cronograma de ejecución.
La aprobación para el uso de la bolsa de horas será otorgada expresamente por la Jefatura de Tecnología de la Información del FONDO MIVIVIENDA, o quien haga sus veces, previa evaluación de la pertinencia técnica y disponibilidad de horas. Ninguna actividad asociada a la bolsa de horas podrá ejecutarse sin la aprobación previa de la Entidad.
El Contratista deberá llevar un registro actualizado del consumo de horas ejecutadas, el cual deberá contener como mínimo el requerimiento atendido, fecha de solicitud, personal asignado, perfil profesional, horas consumidas, estado de ejecución y conformidad del servicio. Dicho registro deberá ser remitido mensualmente al Supervisor de Aplicaciones del FONDO MIVIVIENDA para fines de control y seguimiento contractual.
La Entidad podrá verificar en cualquier momento el consumo acumulado de horas y solicitar los sustentos correspondientes

El Gestor del Servicio remitirá mensualmente al Supervisor de Aplicaciones un reporte con las horas consumidas por solicitud y el saldo disponible. Cuando el saldo sea igual o inferior al 20% del total contratado (180 horas), el Gestor del Servicio alertará formalmente al Supervisor de Aplicaciones. El saldo no consumido al término de la Fase 4 no genera derecho de pago al CONTRATISTA.

PERSONAL DE PRESTACIÓN ACCESORIA

Cantidad de Especialistas: 01
El Contratista deberá asignar como mínimo un (01) especialista para la ejecución de la prestación accesoria, pudiendo proponer una cantidad mayor de profesionales de acuerdo con su criterio técnico y las necesidades del servicio.
Asimismo, los perfiles específicos del personal asignado deberán ser presentados a la Entidad para su revisión dentro de los cinco (05) días calendario previos a la suscripción del Acta de Inicio de la Fase 4. La Entidad contará con un plazo de hasta tres (03) días calendario de presentado el perfil para efectuar la revisión correspondiente y comunicar observaciones, de ser el caso.

En caso de observaciones, el Contratista deberá efectuar la subsanación o reemplazo del personal observado dentro de los dos (02) días calendario siguientes a la notificación realizada por la Entidad.
La revisión y eventual conformidad de los perfiles del personal asignado no enervará ni condicionará la suscripción del Acta de Inicio de la Fase 4, la cual podrá formalizarse conforme al cronograma y condiciones establecidas contractualmente.

Experiencia del especialista del Servicio

Requisitos:
El personal clave deberá tener experiencia mínima de dos (02) años como Analista Desarrollador o Programador o Especialista en desarrollo o soporte de sistemas de información.
La tarifa por hora de este perfil será declarada por el postor en el Anexo de Oferta Económica como precio unitario, siendo fija durante toda la vigencia de la prestación accesoria.

Acreditación:
El postor debe señalar la denominación del puesto, cargo y/o posición, y tiempo de experiencia del personal clave propuesto (años, meses y días) en el Anexo

establecido en las bases, adjuntando en su oferta copia simple de cualquiera de los siguientes documentos: (i) contratos y su respectiva conformidad; (ii) constancias; (iii) certificados; o (iv) cualquier otra documentación que, de manera fehaciente, demuestre la experiencia del personal propuesto.
Estos documentos deben señalar los nombres y apellidos del personal clave; el cargo desempeñado indicando el día, mes y año de inicio y culminación; el nombre de la entidad u organización que emite el documento; la fecha de emisión y nombres y apellidos de quien suscribe el documento.
En caso los documentos que acreditan la experiencia establezcan esta en meses sin especificar los días se debe considerar el mes completo. Se considera aquella experiencia que no tenga una antigüedad mayor a veinticinco años anteriores a la fecha de la presentación de ofertas. De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo de la misma solo se considera una vez el periodo traslapado. En ningún caso corresponde exigir que el mismo personal clave acredite experiencia en más de un cargo.

Formación académica

Requisito:
Técnico profesional o Bachiller Universitario en Ingeniería Informática o Ingeniería de Computación y Sistemas o Computación e Informática.
Acreditación:
Copia de grado o título.
En caso se acredite estudios en el extranjero del personal clave, debe presentarse, adicionalmente, copia simple de la revalidación o reconocimiento del grado o título ante la SUNEDU.

3.3. CONDICIONES DE CONTRATACIÓN

a. MODALIDAD DE PAGO

El contrato se rige por la modalidad de pago de ESQUEMA MIXTO DE SUMA ALZADA Y PRECIOS UNITARIOS, de conformidad con el artículo 130 del Reglamento.

b. SISTEMA DE ENTREGA

NO APLICA

c. PLAZO DE PRESTACIÓN DEL SERVICIO

Los servicios materia de la presente convocatoria se prestan en el plazo indicado en el siguiente detalle:

PRESTACIÓN PRINCIPAL
El plazo de ejecución del servicio será de 1095 días calendario, equivalentes a 36 meses. El periodo se iniciará el día siguiente a la suscripción del Acta de Inicio de la FASE 1.

FASE 1:

La Fase 1 se iniciará con la suscripción del Acta de Inicio, la cual deberá firmarse dentro de los cinco (05) días calendario posteriores a la suscripción del contrato.

Dentro de dicho plazo, el CONTRATISTA convocará a la reunión de inicio del proyecto (*kick-off*), la cual será condición indispensable para la emisión y suscripción del Acta de Inicio de la Fase 1. En dicha reunión deberán cumplirse obligatoriamente las siguientes condiciones:

- Participación presencial y obligatoria de todo el equipo clave propuesto por el contratista, incluyendo a los responsables funcionales y técnicos correspondientes.

- Presentación formal del jefe de Proyecto designado por el FMV.

- Presentación y validación del Plan de Trabajo General, el cual deberá incluir el cronograma integral, hitos, entregables y actividades correspondientes a todas las fases contempladas en el TDR.

Una vez verificados y aceptados dichos elementos por parte del FMV, se procederá a la suscripción del Acta de Inicio de la Fase 1, siempre dentro del plazo máximo de cinco (05) días calendario posteriores a la suscripción del contrato. A partir **de la firma del acta**, se iniciarán las actividades planificadas correspondientes a esta fase, conforme al alcance definido en el presente documento.

Fases	Detalle		Plazo de ejecución
FASE 1	Etapa 1	Diseño e Implementación de la Arquitectura de la Nube	Esta etapa tendrá una duración máxima de sesenta (60) días calendario, contados desde el día siguiente de la firma del Acta de Inicio de la Fase 1.
	Etapa 2	Desarrollo e Implementación de la Plataforma para la Gestión de Créditos – Nuevos Productos y Migración de Carteras (Reemplazo del NSCC)	Esta etapa comenzará también el día siguiente de la firma del Acta de Inicio de la Fase 1 y podrá ejecutarse en paralelo con la etapa anterior, teniendo un plazo máximo de trescientos sesenta y cinco (365) días calendario para su culminación. La etapa tendrá un plazo de aprobación de siete (07) días calendarios contabilizados a partir del día siguiente de la presentación de los entregables correspondientes a dicha Etapa. En casos de existir observaciones, estas deberán ser subsanadas en un plazo máximo de cinco (05) días calendario contados a partir de la notificación correspondiente.
	Etapa 3	Marcha Blanca de FASE 1	Esta etapa se iniciará al día siguiente de aprobado los entregables de la Etapa 2 (Implementación de la Plataforma para la Gestión de Créditos – Nuevos Productos y Migración de Carteras (Reemplazo del NSCC)), y tendrá una duración de noventa (90) días calendario. Durante esta etapa se realizará la operación supervisada de la plataforma en un entorno real controlado. En caso subsistan incidencias críticas no resueltas al cierre de la etapa, el contratista deberá subsanarlas en un plazo máximo de cinco (05) días calendario contados desde el día siguiente de la fecha de culminación de la marcha blanca. La subsanación de estas observaciones será condición indispensable para la aprobación del informe de cierre de la etapa 3.
	Cierre	Acta de Cierre	El Acta de Cierre de la Fase 1 será presentada por el contratista al día siguiente de culminada dicha fase y su firma estará sujeta a la conformidad total del FMV, la cual se acreditará mediante la firma de todos los integrantes del Equipo Estratégico de Gobierno del Proyecto del FMV (Nivel Directivo), en un plazo máximo de siete (07) días calendario contados desde el día siguiente de la recepción del informe. En caso se formulen observaciones, estas deberán ser subsanadas por el contratista en un plazo no mayor a cinco (05) días calendario contados a partir de la notificación correspondiente.

FASE 2:

La Fase 2 se iniciará a partir del día siguiente de suscrito el **Acta de Inicio de la Fase 2**, la cual deberá ser firmada el mismo día de inicio de la Etapa 3 (Marcha Blanca) de la Fase 1. En esta Fase 2 se desarrollarán las siguientes etapas:

Fases	Detalle		Plazo de ejecución
FASE 2	**Etapa 2.1**	Implementación de la Plataforma para la Gestión de créditos - Fideicomiso, Garantías y Provisiones (Reemplazo de actual de los sistemas SAOC y SIR)	Esta etapa se iniciará al día siguiente de la firma del Acta de Inicio de la Fase 2. Su plazo de ejecución será de hasta trescientos sesenta y cinco (365) días calendario. Etapa tendrá un plazo de aprobación de siete (07) días calendarios contabilizados a partir del día siguiente de la presentación de los entregables correspondientes a dicha Etapa. En casos de existir observaciones, estas deberán ser subsanadas en un plazo máximo de cinco (05) días calendarios.
	Etapa 2.2	***Marcha Blanca de la FASE 2***	Esta etapa se iniciará al día siguiente de culminada la etapa 2.1 (Implementación de la Plataforma para la Gestión de Créditos – Fideicomiso, Garantías y Provisiones), y tendrá una duración de noventa (90) días calendario. Durante esta etapa se validará el funcionamiento completo de la solución implementada en un entorno de operación supervisada. En caso subsistan incidencias críticas no resueltas al cierre de la etapa, el contratista deberá subsanarlas en un plazo máximo de cinco (05) días calendario contados desde la fecha de culminación de la marcha blanca. El último día de esta etapa se procederá con la suscripción del Acta de Cierre de la Fase 2, con el visto bueno del responsable de la Oficina de Tecnologías de la Información y la Gerencia de Operaciones.
	Etapa *Cierre*	*Acta de Cierre*	El Acta de Cierre será presentada el último día de la Fase 2 y su firma estará condicionada a la conformidad total del FMV, expresada mediante la firma de todos los integrantes del Equipo Estratégico de Gobierno del Proyecto del FMV (Nivel Directivo), la cual deberá emitirse en un plazo máximo de siete (07) días calendario contados desde el día siguiente de la recepción del informe. En caso se identifiquen observaciones, estas deberán ser subsanadas por el contratista en un plazo no mayor a cinco (05) días calendario contados a partir de la notificación correspondiente.

FASE 3: Migración datos históricos (COFIDE)

La Fase 3 se iniciará al día siguiente de la suscripción del **Acta de Inicio de la Fase 3**, la cual deberá se suscripta a los treinta (30) días calendario de iniciado la Etapa 2.2 (Marcha Blanca de la Fase 2).

Fases	Detalle	Plazo de ejecución

FASE 3	**Etapa** 3.1	Migración datos históricos (COFIDE)	Esta etapa tendrá una duración máxima de ciento cincuenta (150) días calendario, contados a partir del día siguiente de la suscripción del Acta de Inicio de la Fase 3.
	Etapa 3.2.	Acta de Cierre	El Acta de Cierre será presentada el último día de la Fase 3 y su firma estará condicionada a la conformidad total del FMV, expresada mediante la firma de todos los integrantes del Equipo Estratégico de Gobierno del Proyecto del FMV (Nivel Directivo), la cual deberá emitirse en un plazo máximo de siete (07) días calendario siguientes contados desde la recepción del informe. En caso se identifiquen observaciones, estas deberán ser subsanadas por el contratista en un plazo no mayor a cinco (05) días calendario contados a partir de la notificación correspondiente.

FASE 4: Operación

La Fase 4 corresponde a la operación continua del servicio implementado y se iniciará con la suscripción del **Acta de Inicio de la Fase 4**, la cual deberá firmarse el mismo día de la suscripción del **Acta de Cierre de la Fase 1**.

Fases	Detalle		Plazo de ejecución
FASE 4	**Etapa** 4.1	Soporte	A partir del día siguiente de la firma del Acta de Inicio de la Fase 4, se dará inicio al período de operación del servicio, el cual tendrá una duración de seiscientos treinta (630) días calendario. La culminación de esta etapa será formalizada mediante la suscripción del Acta de Cierre de la Fase 4, la cual deberá ser firmada a más tardar el último día de la Fase 4, con el visto bueno del responsable de la Oficina de Tecnologías de la Información.

FASE 5: Transición de salida

La Fase 5 corresponde al proceso de cierre y transición final del servicio implementado, el cual se desarrollará durante los últimos treinta (30) días calendario del período de operación (Fase 4). Esta fase será ejecutada de forma superpuesta a la etapa operativa con el objetivo de garantizar la entrega ordenada de la información, sin afectar la continuidad del servicio. Durante este periodo, el CONTRATISTA deberá entregar los respaldos de la información del FONDO y, posteriormente, eliminarla de su infraestructura. Esta etapa no genera costos adicionales para el FMV.

No forman parte del alcance de esta fase las actividades de migración de la información o de la solución hacia otro proveedor, ni el soporte o acompañamiento a un nuevo proveedor, así como tampoco la adaptación de la plataforma a arquitecturas, plataformas o servicios de terceros.

Fases	Detalle	Plazo de ejecución

FASE 5	5.1	Transición de salida	Se desarrollará durante los últimos treinta (30) días calendario del período de operación (FASE 4), de forma superpuesta a esta etapa. Durante esta fase, el CONTRATISTA deberá gestionar y coordinar la entrega de los Backups de la información, tanto estructurada como no estructurada, así como de los documentos digitales contenidos en la plataforma que estén relacionados con el FONDO. Finalizada esta etapa y con la conformidad del FMV, se instruirá formalmente al CONTRATISTA la eliminación definitiva de la información. Esta etapa no genera costos para el FMV.

PRESTACIÓN ACCESORIA
Esta iniciará en la etapa de la operación del servicio, la cual inicia desde la fecha de inicio indicada en el Acta de Inicio de la Fase 4 y tiene una duración de duración de seiscientos treinta (630) días calendario.

d. LUGAR DE PRESTACIÓN DEL SERVICIO

El lugar de la ejecución del servicio se realizará en las instalaciones del FONDO, ubicada en Calle Amador Merino Reina 285 – San Isidro, y podrá realizarse de forma híbrida (presencial / remoto) en las instalaciones del contratista.

En caso del PMP CONTRATISTA deberá efectuar sus actividades de forma presencial en las instalaciones del FONDO en el mismo horario que tiene el personal; es decir, de lunes a viernes, de 8:30 am a 5:30 pm

e. ADELANTO DIRECTO

No aplica

f. PENALIDADES

PENALIDAD POR MORA:

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable, de conformidad con el artículo 120 del Reglamento.

OTRAS PENALIDADES

Adicionalmente a la penalidad por mora, se aplican las siguientes penalidades:

Otras penalidades			
N°	**Supuestos de aplicación de penalidad**	**Forma de cálculo**	**Procedimiento de verificación**
1	**No suscripción del Acta de Inicio de la Fase 1.** Si por causas atribuibles al CONTRATISTA no se suscribiese el Acta de Inicio de la Fase 1 dentro del plazo y bajo las condiciones establecidas en el presente documento, se aplicará una penalidad por cada día calendario de retraso en la suscripción del Acta, contado a partir del vencimiento del plazo previsto para su firma.	0.5% del monto del contrato original por cada acta suscrita de forma tardía y por cada día de retraso	
2	**Presentación de la terna de PMP FMV** Si el CONTRATISTA no remite la terna de tres profesionales, referentes al PMP FMV en el proyecto dentro del plazo establecido en el presente documento, se aplicará una penalidad por cada día de retraso en la presentación de los perfiles.	0.5% del monto del contrato original por cada día de retraso	
3	**Incumplimiento por Cambio No Autorizado de Personal Clave** Si el contratista cambia el personal clave asignado sin autorización	0.5% del monto del contrato original por cada persona detectada y por cada día	

	previa de la OTI, conforme el procedimiento establecido para reemplazo de personal del presente documento, se genera un incumplimiento y se computará por persona que ejecute el servicio sin haber tenido autorización previa y por día que el contratista demore en efectuar la presentación de reemplazo bajo el perfil establecido por cada profesional en el presente documento.	que el contratista demore en efectuar la presentación del personal de reemplazo bajo el perfil establecido por cada profesional en el presente documento.	La OTI, GO, GF y GR realizarán el seguimiento y verificación de las obligaciones de acuerdo con los términos de referencia y ante algún incumplimiento trasladará comunicación mediante correo electrónico al contratista y/o carta, precisando el supuesto incurrido para que remita sus descargos hasta dos (02) días hábiles contabilizados a partir del día siguiente de enviado el supuesto de aplicación. La OTI tendrá dos (02) días hábiles para evaluar el descargo, contabilizado a partir de recepcionado por el área usuaria. La decisión tomada se hará de conocimiento al Departamento de Logística a fin de que este en el plazo de 01 día hábil, contabilizado a partir del día siguiente de recepcionado el memorando o Informe enviado por la OTI, para su posterior notificación al contratista la aplicación o no de la penalidad.
4	**Penalidad por incumplimiento en el cronograma del servicio** Si el contratista incurre en retrasos en la ejecución de cualquier fase, etapa o entregable establecidos en el cronograma del servicio, por causas que le sean atribuibles, se aplicará una penalidad por cada día calendario de incumplimiento, contado a partir del día siguiente al vencimiento del plazo máximo definido para la etapa o entregable correspondiente o, en su caso, al vencimiento del plazo de subsanación otorgado y hasta la fecha de la subsanación de cualquier fase, etapa o entregable.	0.5% del monto del contrato original por cada día de retraso y por la etapa correspondiente.	
5	**No Presentación de Información Solicitada** Si por causas atribuibles al contratista, este no presenta los entregables requeridos dentro de los plazos establecidos, se aplicará una penalidad por cada entregable y por cada día de retraso.	0.25% del monto del contrato original por cada entregable y por cada día de retraso	
6	Cuando el CONTRATISTA del servicio declare en los entregables contractuales, que una funcionalidad ha sido implementada, una actividad ha sido completada, o que se ha cumplido con algún requisito establecido, y durante la validación, revisión o pruebas por parte de la OTI, se evidencie que dicha información es inexacta, se aplicará una penalidad por cada documento evidenciado.	0.25% del monto del contrato original por cada documento en el que se evidencie la inexactitud.	
7	**Falta de Generación de Alertas para Evitar Contingencias** Si el contratista no genera las alertas necesarias según el numeral del 9.4.1. para evitar contingencias en los procesos de cierre que puedan afectar económicamente a la entidad, se aplicará una penalidad por cada proceso no alertado.	1% del monto del contrato original por cada alerta no generada.	
8	Si la disponibilidad cae por debajo del 99.6%. **Código: SLA-01** **Forma de medición:** Disponibilidad de la plataforma **SLA:** 99.6% de uptime Si la disponibilidad cae por debajo del 99.6%, Penalización aplicada si el uptime mensual es inferior al 99.6%. Penalización aplicada según el porcentaje de disponibilidad perdido.	(99.6% - Uptime real%) * (facturación mensual del servicio) * 5%.	
9	Si el tiempo de respuesta o resolución excede los valores establecidos. Incidencias Criticas: Estas son incidencias que afectan gravemente el funcionamiento de la plataforma, causando interrupciones totales en la plataforma o impidiendo el acceso a funciones clave. **Código: SLA-02** **Forma de medición:** Clasificación de incidentes – Crítico **SLA:** Respuesta < 2 horas desde la notificación de la incidencia por parte del FONDO.Resolución < 4 horas desde la notificación de la incidencia por parte del FONDO. Dicha notificación será vía correo o plataforma. Penalización aplicada si los tiempos de resolución exceden lo establecido. Penalización por cada incidente no resuelto en el tiempo establecido.	((Tiempo de resolución real - Tiempo de resolución comprometido) / Tiempo de resolución comprometido) * Facturación mensual * 3%.	
10	Si el tiempo de respuesta o resolución excede los valores establecidos. Incidencias Alto: Impactan el servicio de manera significativa, pero no provocan una interrupción total de la plataforma. Pueden incluir problemas con algunos módulos específicos de la plataforma o dificultades en la ejecución de ciertos procesos importantes **Código: SLA-03** **Forma de medición:** Clasificación de incidentes – Alto **SLA:** Respuesta < 4 horas desde la notificación de la incidencia por parte del FONDO.	((Tiempo de resolución real - Tiempo de resolución comprometido) / Tiempo de resolución	

	Resolución < 6 horas desde la notificación de la incidencia por parte del FONDO. Dicha notificación será vía correo o plataforma. Penalización por cada incidente no resuelto en el tiempo establecido.	comprometido) * Facturación mensual * 2.5%	
11	Si el tiempo de respuesta o resolución excede los valores establecidos. Incidencias Medio: o Son problemas que no afectan gravemente la operatividad de la plataforma y tienen un impacto limitado o parcial. Pueden incluir fallos menores, como errores en informes no críticos o problemas con funcionalidades secundarias de la plataforma. **Código: SLA-04** **Forma de medición:** Clasificación de incidentes - Medio **SLA:** Respuesta < 8 horas, desde la notificación de la incidencia por parte del FONDO. Resolución < 16 horas desde la notificación de la incidencia por parte del FONDO. Dicha notificación será vía correo o plataforma. Penalización por cada incidente no resuelto en el tiempo establecido.	((Tiempo de resolución real - Tiempo de resolución comprometido) / Tiempo de resolución comprometido) * Facturación mensual * 2%	
12	Si el tiempo de respuesta o resolución excede los valores establecidos Incidencias Bajo: Son incidencias menores que tienen un impacto limitado en la plataforma y no afectan la funcionalidad principal de la plataforma **Código: SLA-05** **Forma de medición:** Clasificación de incidentes - Bajo **SLA:** Respuesta < 12 horas desde la notificación de la incidencia por parte del FONDO. Resolución < 24 horas desde la notificación de la incidencia por parte del FONDO. Dicha notificación será vía correo o plataforma. Penalización por cada incidente no resuelto en el tiempo establecido	((Tiempo de resolución real - Tiempo de resolución comprometido) / Tiempo de resolución comprometido) * Facturación mensual * 1%	
13	Si el soporte no está disponible en momentos críticos los como cierres mensuales, cierres contables o generación de reportes regulatorios. **Código: SLA-06** **Forma de medición:** **SLA:** Garantizar soporte 24/7 Respuesta < 15 minutos desde la notificación de la incidencia por parte del FONDO. Resolución < 1 hora desde la notificación de la incidencia por parte del FONDO. En caso de indisponibilidad del soporte en algún momento crítico, se aplicará una penalización Penalización aplicada en caso de indisponibilidad del soporte en momentos críticos.	((Tiempo real de atención - Tiempo de atención comprometido) / Tiempo de atención comprometido) * Facturación mensual * 3%	
14	Si el tiempo de respuesta de la PLATAFORMA en todas las operaciones, salvo las operaciones que sean más complejas debidamente coordinadas entre ambas partes, excede los 3 segundos. **Código: SLA-07** **Forma de medición: Tiempo de respuesta de la PLATAFORMA:** **SLA:** Respuesta < 3 segundos desde iniciado la interacción. Penalización aplicada por cada medición que supere el tiempo establecido	(Tiempo de respuesta real - 3 segundos) / 3 segundos * Facturación mensual * 2%.	
15	Si el tiempo de procesamiento de operaciones diarias o mensuales excede lo establecido. **Código: SLA-08** **Forma de medición:** Tiempo de procesamiento de	((Tiempo real de procesamiento - Tiempo establecido) / Tiempo	

	transacciones **SLA:** Cierre de operaciones diarias < 3 horas desde iniciado el cierre del día. Cierre de operaciones mensuales < 5 horas desde iniciado el cierre mensual. Penalización por cada incumplimiento de tiempo en procesos de cierre.	establecido) * Facturación mensual * 3%.	
16	Si el tiempo de restauración de cualquier componente del servicio excede las 4 horas, y esto sea por causas atribuibles al Contratista. **Código: SLA-09** **Forma de medición:** RTO (Recovery Time Objective) **SLA:** Penalización por cada incidente que supere el tiempo establecido.	((Tiempo real de restauración - 4 horas) / 4 horas) * Facturación mensual * 5%.	
17	Si se registra una pérdida de datos, y esto sea por causas atribuibles al Contratista. **Código: SLA-10** **Forma de medición:** RPO (Recovery Point Objective) **SLA:**. Cantidad de datos perdidos. Penalización basada en el periodo de información no recuperada, medido en horas o minutos, por causas atribuibles al Contratista.	(Horas de información no recuperada / Horas del periodo afectado) × Facturación mensual × 5%	
18	Si no se realizan las pruebas de recuperación según la periodicidad establecida. **Código: SLA-11** **Forma de medición:** Pruebas de recuperación **SLA:** Realizar pruebas de recuperación de desastres al menos dos veces al año Penalización en caso de incumplimiento de pruebas de recuperación.	Fórmula: (Número de pruebas faltantes / 2) * Facturación mensual * 4%.	
19	En caso se produzca un evento de pérdida de información sensible derivado de accesos no autorizados o vulneración de la arquitectura/plataforma **Código: SLA-12** **Forma de medición:** Pérdidas de información por fallas o vulnerabilidades **SLA:** 0 incidentes de pérdida de información Penalización por cada incidente confirmado de pérdida de información sensible, incluyendo información de clientes, transacciones o estados financieros, ocasionado por accesos no autorizados o vulneración de la arquitectura/plataforma bajo responsabilidad del Contratista. La penalidad será equivalente al 15% de la facturación mensual por cada incidente confirmado.	Fórmula: (N° de incidentes confirmados) × (Facturación mensual) × 15%.	

La suma de la aplicación de las penalidades por mora y otras penalidades no debe exceder el 10% del monto vigente del contrato o, de ser el caso, del ítem correspondiente.

g. SUBCONTRATACIÓN

Se encuentra prohibida la subcontratación de las prestaciones objeto del contrato, de conformidad con lo dispuesto en el artículo 108 del Reglamento de la Ley N°32069, dado que el servicio comprende el desarrollo de software a medida de carácter crítico que gestiona información financiera sujeta a supervisión de la SBS, siendo indispensable que el contratista mantenga responsabilidad directa e íntegra sobre el desarrollo, la calidad del código fuente y la seguridad de la información institucional del FMV durante toda la vigencia del contrato.

h. FÓRMULAS DE REAJUSTES

No corresponde

i. SOLUCIÓN DE CONTROVERSIAS CONTRACTUALES

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación, cuando se haya pactado, y arbitraje.

Para el caso de arbitraje, el postor ganador de la buena pro selecciona una de las siguientes Instituciones Arbitrales para administrarlo:

N.º	INSTITUCIONES ARBITRALES	RUC
1	Camara de Comercio de Lima - Centro de Arbitraje de la Camara de Comercio de Lima	20101266819
2	MARC PERU – Asociación para la prevención y solución de Conflictos	20426255317
3	Pontificia Universidad Católica de Perú - Centro de Análisis y Resolución de Conflictos de la Pontificia Universidad Católica del Perú	20155945860

j. PLAZO PARA RESPUESTAS ENTRE LAS PARTES

Para los plazos de respuesta de las partes sobre aspectos vinculados con la ejecución contractual que no han sido específicamente previstos en el Reglamento, aplica el plazo máximo de respuesta del siguiente cuadro:

Plazo máximo de respuesta	:	Cinco (05) días calendario.

Antes del vencimiento de este plazo máximo, las partes pueden acordar su prórroga para cada situación específica considerando la cláusula de notificaciones del contrato.

3.4. TÉRMINOS DE REFERENCIA

3.4.1 Parámetros Generales

La Plataforma para la Gestión de Créditos deberá contar con una capa de parametrización general que permita configurar su funcionamiento de manera flexible, integral y alineada a las necesidades operativas del FONDO. Como mínimo, deberá soportar las siguientes características funcionales:

- ✓ Multiempresa: Capacidad para generar información financiera y contable diferenciada por cada entidad o unidad de negocio, incluyendo estados financieros y reportes específicos por empresa.
- ✓ Multimoneda: Soporte para operar en diferentes monedas, tales como soles, dólares estadounidenses, soles VAC, entre otras que puedan ser requeridas en el futuro.
- ✓ Configuraciones generales: Módulo que permita definir parámetros globales que afectan el comportamiento general de la plataforma en todas sus áreas funcionales.
- ✓ Parámetros operacionales: Posibilidad de establecer reglas de operación para procesos diarios, adaptadas a la lógica de negocio del FONDO, de forma flexible y modificable.
- ✓ Gestión de catálogos: Administración de catálogos personalizables para productos, servicios, bonos, atributos crediticios y demás componentes operativos, permitiendo su actualización sin necesidad de desarrollos adicionales.
- ✓ Estructura organizacional: Configuración de la red operativa del FONDO, incluyendo oficinas, áreas y sucursales, lo que permitirá segmentar y administrar la operación por ubicación geográfica o estructura interna.

- ✓ Gestión de productos: Funcionalidad para la creación, modificación y parametrización de nuevos productos financieros, asegurando su correcta integración y trazabilidad dentro de la PLATAFORMA.
- ✓ Dashboard de gestión: Herramientas de visualización y análisis para el monitoreo en tiempo real de indicadores financieros, operativos y de gestión, con capacidad para generar reportes detallados que apoyen la toma de decisiones estratégicas.

3.4.2 Requerimientos funcionales mínimos

3.4.2.1 Gestión contable

La PLATAFORMA deberá generar los Asientos Contables Automáticos en base al flujo transaccional diario, soportado en una capa transversal de parámetros que permita la Conciliación Automática Diaria a través de los Cierre operativo diarios.

La PLATAFORMA deberá contar con la siguiente estructura funcional y operativa-contable:

1. **Paramétrica**: La PLATAFORMA deberá tener una capa de gestión y administración de parámetros que permita la configuración y personalización de las dinámicas contables en todas las variantes:

   a. Productos. La PLATAFORMA permitirá la creación de nuevos productos en forma paramétrica por parte de los usuarios del FONDO.
   b. Tipo de monedas
   c. Tipo de transacciones
   d. Asientos Contables

2. **Transaccional:** La PLATAFORMA deberá tener una estructura contable transaccional que permita generar la contabilidad cada vez que se ejecute una transacción en cualquier proceso, sea financiero, administrativo o de orden.

3. **Tiempo Real**: La PLATAFORMA deberá generar los asientos contables en tiempo real, al momento de generar la transacción y según los parámetros configurados, de tal forma que se vayan construyendo todos los hilos necesarios para la elaboración del cierre Operativo-Contable Diario.

4. **Cierre operativos diarios**: La PLATAFORMA deberá generar el cierre operativo diario que permita realizar un cuadre operativo-contable bajo el concepto general de “Arrastre de Saldos Diarios” **Asientos Contables**: La **PLATAFORMA** deberá generar los asientos contables que se hayan configurado por cada transacción en forma resumida que se genere o desprenda de cualquier proceso o liquidación.

5. **Los Registros contables automáticos, deben de tener la siguiente consideración:** La contabilidad en el FMV es desconcentrada por lo que cada gerencia es responsable de los registros contables que se genera por operaciones con impacto financiero. Todas las operaciones registradas por el área operativa deben generar un asiento contable automático (inclusive cuando se realizan extornos o modificaciones). Los asientos contables deben tener un flujo de aprobación en el sistema antes que pasen a la contabilidad del FMV.

6. **Conciliación de saldos automática**: Los sados de los reportes operativos deben de cuadrar con los saldos contables antes de que los asientos contables automáticos sean migrados a la contabilidad del FMV.

7. **Reportes de control de asientos en custodia de otras gerencias:** La plataforma debe de generar un reporte donde liste los asientos contables

generados, con el número de ID del sistema contable, detalle de quien lo elaboró quien lo aprobó y breve resumen de la operación.

8. **Reportes contables sustento de asientos contables, notas y anexos a los estados financieros:** Se requiere reportes automáticos de saldos y movimientos, por moneda, producto, a nivel detalle y resumen. Estos deben de tener una validación previa con los reportes operativos. Los reportes operativos deben de contar con una aprobación y no pueden ser modificados luego del cierre del periodo. La PLATAFORMA deberá generar las notas y anexos a los estados financieros.

9. **Informes Tributarios:** La PLATAFORMA deberá generar los insumos para la elaboración de los informes y reportes tributarios exigidos por la SUNAT en forma automática.

   Estos reportes e informes que se deberán implementar son los siguientes:
   - Libro de Inventarios y Balances (Cuentas por Cobrar y Provisiones)
   - Generación de Comprobantes electrónicos a través de sistema facturados 07 generando FACTURA, BOLETA DE VENTA, NOTA DE CREDITO y NOTA DE DEBITO según se requiera.
   - Registro de Ventas (detalle de los comprobantes electrónicos generados en cada cartera), incluyendo facturas, boletas de venta, anulaciones y notas de créditos emitidas.
   - Registro de Ventas detalle cualquier PENALIDAD que se cobren a las IFI o entidades, generando Nota de Débitos en caso se requiera.
   - Reporte de las PROVISIONES en donde se detalle: Provisión Genérica, especifica y recuperación de reserva legal (genérica y especifica); por cada cartera.
   - Reportes de diferencia de capital cuando se aplica la cláusula 13, por cada cartera que se administra. (mostrando en ellos el saldo de las reversiones que se ejecuten por cada cartera)
   - Reporte de adelanto de PREPAGO de cuotas con su respectiva emisión de comprobantes de pago, para cada cartera.

10. Esta nueva plataforma deberá transferir al nuevo ERP, los cálculos de las provisiones, recuperaciones e intereses diferidos que tengan efectos tributarios de todas las carteras que administrará la nueva plataformaDebido a cambios normativos realizados por los supervisores (SBS y SUNAT) se podrá solicitar reportes y/o asientos contables adicionales que a la fecha del desarrollo no se hayan incluido como parte de éste.

11. La plataforma deberá emitir los insumos para la generación del Balance Sectorial Institucional para el BCRP.

3.4.2.2 Gestión de Riesgos

La gestión de Riesgos permite realizar la Evaluación de los Riesgos asociados al otorgamiento de líneas a las Entidades del Sistema Financiero, de los créditos hipotecarios, así como la visita de revisión a las IFIs, el seguimiento de la cartera y su comportamiento en el tiempo o ciclo de vida de esta.

La PLATAFORMA deberá estar alineada al marco normativo vigente que regula la gestión de riesgo de crédito en el Perú, incluyendo: la Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la SBS; el Reglamento de Gestión de Riesgo de Crédito (Res. SBS N°3780-2011 y sus modificatorias); el Reglamento para el Requerimiento de Patrimonio Efectivo por Riesgo de Crédito (Res. SBS N°14354-2009); el Reglamento para la Evaluación y Clasificación del Deudor y la Exigencia de Provisiones (Res. SBS N°11356-2008 y sus

modificatorias); el Reglamento de la Gestión Integral de Riesgos (Res. SBS N°037-2008 y sus modificatorias); así como las Políticas de Riesgo de Crédito, Manuales de Procedimiento y Metodologías internas del FMV S.A.

Principios transversales obligatorios del módulo de Riesgos

La PLATAFORMA deberá incorporar, de manera transversal a todos los submódulos descritos en este numeral, como mínimo:

- Parametrización total de reglas, variables, umbrales, criterios y excepciones definidos por el FMV S.A., incluyendo vigencias.

- Versionado y control de cambios: toda modificación, actualización, eliminación de parámetros, reglas y data deberá ser registrado y archivado contando con un back up histórico de cambios (qué cambió, cuándo, quién lo aprobó), con posibilidad de reconstruir cálculos históricos.

- Trazabilidad: registro auditable de datos de entrada, transformaciones, resultados, validaciones, observaciones y aprobaciones (usuario/fecha/rol).

- Workflow y autonomías: estados del proceso y transiciones controladas por perfiles y autonomías configurables (analista, especialista, jefatura, gerencia, comité de riesgos).

- Controles automáticos y bloqueos: impedir otorgamientos, ampliaciones, desembolsos, cierres o envíos a contabilidad cuando existan incumplimientos a reglas críticas o validaciones pendientes.

- Gestión de evidencias: repositorio de documentos, reportes, comunicaciones, actas y respaldos, vinculados a IFI y periodo.

- Interoperabilidad: interfaces para ingesta de información desde fuentes definidas por el FMV (SBS/RCC/COFIDE/GO/sistemas de cobranza/IFIs), en modalidad API y/o batch, con validaciones de calidad.

- Seguridad y segregación: control de accesos por perfil y ámbito, limitando la exposición de información sensible conforme a políticas FMV.

- Nota de confidencialidad: Las fórmulas, ponderadores, umbrales, matrices internas y parámetros críticos serán proporcionados por el FMV S.A. de manera reservada (anexo confidencial o durante la fase de implementación) y deberán ser implementados en la PLATAFORMA sin quedar expuestos a usuarios no autorizados.

a) Admisión y Seguimiento de Líneas a Entidades del Sistema Financiero (ESFs)

La PLATAFORMA deberá soportar la admisión y seguimiento de líneas, incluyendo al menos línea de crédito y línea de garantía, con límites integrados y reglas de control por exposición consolidada

1. Límite de Exposición Máxima

La PLATAFORMA deberá implementar un módulo de cálculo del límite máximo de exposición total que el FMV puede otorgar a cada ESFS, con las siguientes características:

- Motor parametrizable conforme a la metodología FMV vigente (variables, factores, reglas y excepciones).
- Cálculo con periodicidad configurable y resguardo histórico de resultados por IFI.

- Control automático de exposición consolidada y bloqueo de solicitudes que excedan el límite, generando evidencia del motivo de rechazo.
- Acceso restringido por perfiles del área de Riesgos.

2. Monitoreo Individual por Línea

La PLATAFORMA deberá soportar el monitoreo individual de cada tipo de línea otorgada, con las siguientes funcionalidades:

- Descarga automática de desembolsos y saldos vigentes por línea.
- Generación de alertas configurables por porcentaje de uso individual de cada línea.
- Visualización diferenciada para cada tipo de línea:
  - ✓ Línea de Crédito: saldos desembolsados, porcentaje de uso y monto disponible.
  - ✓ Línea de Garantía: cartas fianza emitidas, montos, estado (vigente, ejecutada, vencida), porcentaje de uso y monto disponible.
- Esta información estará disponible para las áreas según los perfiles de acceso configurados en la plataforma.
- Registro de acciones y seguimiento de alertas (responsables/estado/evidencias).

3. Rating Interno

La PLATAFORMA deberá implementar un motor de Rating Interno configurable que permita determinar el nivel de riesgo de cada ESFS, con las siguientes características:

- El motor deberá soportar la configuración de múltiples módulos de evaluación (cuantitativos, cualitativos y de diversificación u otros definidos por el FMV), con indicadores y ponderaciones parametrizables por el FMV.
- Configuración de niveles de riesgo, periodicidad y reglas de asignación.
- Registro de resultados, evidencia de insumos utilizados y trazabilidad histórica.
- Versión del modelo y capacidad de reproducir resultados de periodos anteriores.
- Los resultados del Rating Interno servirán como insumo para los demás módulos del proceso de gestión de riesgos.

4. Criterios Económicos Financieros — Grado de Vigilancia

La PLATAFORMA deberá implementar un motor de determinación del Grado de Vigilancia de cada ESFS, con las siguientes características:

- El motor deberá utilizar como insumo el Rating Interno y verificar el cumplimiento de indicadores críticos configurables por el FMV S.A., con umbrales parametrizables según el tipo de entidad (IFIs, Empresas de Seguros, COOPAC, entre otras).
- Deberá considerar variables adicionales de riesgo configurables, incluyendo indicadores cualitativos.
- Asignará automáticamente el Grado de Vigilancia según reglas configurables y habilitará las acciones correspondientes en la plataforma:
- Activación de acciones asociadas según grado (monitoreo, solicitud de plan de acción/proyecciones, reuniones, elevación a comité, etc.), con seguimiento y evidencias.
- Historial de cambios de grado y trazabilidad de los gatilladores que lo originan.

5. Clasificación Equivalente

La PLATAFORMA deberá implementar un módulo de Clasificación Equivalente para la asignación de la clasificación regulatoria de cada IFI conforme a la normativa SBS vigente, con las siguientes características:

- Las variables, indicadores y reglas de asignación serán parametrizables por el FMV S.A.

- Cálculo periódico configurable, con registro del resultado y trazabilidad de componentes utilizados.
- Los resultados se utilizarán para el cálculo de provisiones del FMV.
- El módulo deberá soportar la configuración de excepciones por tipo de entidad según las políticas internas del FMV S.A.

6. **Cumplimiento de Condiciones de CRC, CRCA**
   La PLATAFORMA deberá implementar un módulo de Evaluación de Cumplimiento de las Condiciones del CRC y CRCA para cada IFI según los parámetros establecidos en los reglamentos antiguos y vigentes, con las siguientes características:
   - Las variables, indicadores y reglas de asignación serán parametrizables por el FMV S.A.
   - Cálculo periódico configurable, con registro del resultado y trazabilidad de componentes utilizados.
   - Los resultados se utilizarán para seguimiento por tarte de la GR, para cumplimiento normativo de la GO y para el informe de los resultados a las IFI por parte del GC.
   - El módulo deberá soportar la configuración de excepciones por tipo de entidad según las políticas internas del FMV S.A.

b) Seguimiento del Portafolio Fideicomiso COFIDE — Gestión de Cartera MiVivienda

La PLATAFORMA deberá implementar un módulo de Gestión de Riesgo de Crédito de Cartera MiVivienda con las siguientes características:

- Las variables de evaluación y sus ponderaciones serán parametrizables por el FMV S.A.
- Deberá manejar niveles de gestión configurables, con acciones asociadas a cada nivel (solicitud de proyecciones, planes de acción u otras acciones asociadas al nivel de gestión correspondiente).
- La periodicidad de evaluación será mensual configurable histórico y trazabilidad.
- Los resultados de este módulo alimentarán el módulo de Gestión de Cartera MiVivienda descrito en la sección de Visitas.

c) Visitas de Revisión de Cartera MiVivienda a ESFS

La PLATAFORMA deberá soportar el proceso completo de visitas de revisión de cartera MiVivienda a ESFS con créditos vigentes dentro del Fideicomiso COFIDE – FMV S.A., incluyendo los siguientes subprocesos:

1. **Plan Anual de Visitas**
La PLATAFORMA deberá implementar un módulo de Plan Anual de Visitas de Cartera Hipotecaria MIVIVIENDA:

- El motor deberá utilizar como insumo el Reporte de Líneas, Evolutivo de indicadores (información de la SBS) y verificar los umbrales configurables por el FMV S.A., según el tipo de entidad (IFIs, CMAC, ES, COOPAC, entre otras).
- Las variables, indicadores y reglas de asignación serán parametrizables por el FMV S.A.

2. **Verificación de Expedientes e Integración con ESFS**
La PLATAFORMA deberá disponer de dos mecanismos de interoperabilidad con las ESFs:

- **API de carga digital de expedientes y requerimientos solicitados:** La plataforma deberá exponer una API que permita a las ESFs cargar de forma digital los expedientes de la muestra de créditos a revisar, incluyendo toda la

documentación crediticia asociada. Así como deberá permitir el cargado de todo requerimiento solicitado a la IFI (bases subpréstamos, garantías, reprogramaciones u otros requerimientos asociados a la revisión). El estándar de formato y los requisitos de documentación serán definidos por el FMV S.A.

- **Integración con sistemas de las IFIs:** La PLATAFORMA deberá permitir la conexión con los sistemas de las IFIs para que la información de sus créditos MiVivienda alimente automáticamente la plataforma FMV. Deberá soportar tanto integración en tiempo real como por lotes (batch), según la capacidad tecnológica de cada entidad.

3. **Conciliación de Bases COFIDE vs IFI**
   La PLATAFORMA deberá permitir el cruce automático entre la base de datos de COFIDE y la información proporcionada por la IFI, identificando, registrando y clasificando las discrepancias encontradas en saldos, cronogramas, clasificaciones y garantías.

4. **Indicador de Resultado de visita y Seguimiento de Observaciones**
   La PLATAFORMA deberá implementar un módulo de Resultado de Visita y Seguimiento de Observaciones para la asignación del resultado del indicador de visita y Seguimiento de Observaciones.
   - Las variables, indicadores y reglas de asignación serán parametrizables por el FMV S.A.
   - Cálculo periódico configurable, con registro del resultado y trazabilidad de componentes utilizados.
   - Los resultados se utilizarán para el cálculo del Indicador de Gestión MIVIVIENDA.

d) Originación, Evaluación, Refinanciación de Créditos y Reclasificación de estado Contable a los Créditos Refinanciados

La PLATAFORMA deberá tener un proceso de Originación, Evaluación y Refinanciación de Créditos que permita realizar el registro, la evaluación detallada la calificación de los créditos hipotecarios solicitados y, cuando corresponda, la refinanciación de créditos hipotecarios, de conformidad con la normativa vigente aplicable y con las políticas, manuales y procedimientos internos del FMV S.A.
La PLATAFORMA deberá contemplar mecanismos de interoperabilidad mediante API y/o procesos batch con los sistemas del tercero encargado de la cobranza, a fin de asegurar el intercambio oportuno y trazable de información vinculada al ciclo de vida del crédito, incluyendo como mínimo el estado de la operación, cronogramas, saldos, pagos, mora, gestiones de cobranza, refinanciaciones, regularizaciones y demás datos que el FMV S.A. defina.La “Originación de Créditos” deberá contener los siguientes subprocesos:

1. **Solicitud de Créditos:** La PLATAFORMA deberá tener un módulo que permita registrar todas las solicitudes de créditos hipotecarios presentadas a FONDO, donde se registren todos los datos concernientes al solicitante y a las características de crédito, la documentación de sustento y demás datos requeridos por la normativa y por las políticas internas del FMV S.A.
2. **Evaluación de Créditos:** La PLATAFORMA deberá contener un módulo que incorpore las reglas de negocio alineados a la normativa vigente del FONDO, las cuales deberán ser parametrizables y actualizables. Este módulo deberá permitir la evaluación integral de la solicitud, considerando criterios financieros, documentarios, operativos y de riesgo, así como validaciones automáticas y manuales según corresponda.
3. **Calificación de Créditos:** La PLATAFORMA deberá tener el módulo de calificación de créditos que permita aprobar, observar o rechazar una solicitud de crédito, de acuerdo con los niveles de autonomías y flujos de aprobación configurados. **Registro de Excepciones**: La PLATAFORMA

debe permitir el registro, sustento, evaluación, aprobación y trazabilidad de excepciones, conforme a autonomías configurables, , excepciones vinculadas a condiciones financieras, operativas o comerciales, como por ejemplo reducciones de tasas u otras que el FMV S.A. defina.**Refinanciación de Créditos:** La PLATAFORMA deberá permitir el registro, evaluación, aprobación, formalización y seguimiento de solicitudes de refinanciación de créditos, de acuerdo con la normativa vigente aplicable y con las disposiciones internas del FMV S.A. Para ello, deberá como mínimo:

- Identificar y vincular de manera obligatoria el crédito refinanciado con la operación original, manteniendo trazabilidad histórica de sus condiciones iniciales, modificaciones, cronogramas, saldos y estado de la operación.
- Permitir el registro del motivo de refinanciación, las condiciones financieras originales y las nuevas condiciones propuestas, así como la documentación de sustento correspondiente.
- Incorporar reglas de negocio parametrizables para la evaluación de refinanciaciones, considerando criterios de elegibilidad, capacidad de pago, comportamiento crediticio, clasificación del deudor, garantías, condiciones del crédito y demás criterios definidos por el FMV S.A.
- Permitir la aprobación, observación o rechazo de la refinanciación según los niveles de autonomía y flujos de aprobación configurados.
- Registrar la fecha de refinanciación, el estado de la operación, la versión del cronograma aplicable y las aprobaciones efectuadas, manteniendo bitácora completa del proceso.
- Permitir la diferenciación y consulta de créditos originales, vigentes, refinanciados, cancelados o sustituidos, según la clasificación operativa que defina el FMV S.A.
- Integrarse con los módulos de riesgo, provisiones, contabilidad y con los sistemas de cobranza tercerizada mediante API y/o procesos batch, a fin de asegurar que la refinanciación tenga el tratamiento operativo, de seguimiento, cobranza y reporte que corresponda.

La PLATAFORMA deberá garantizar que toda operación de refinanciación mantenga evidencia digital, trazabilidad integral, control de versiones, carga documentaria y resguardo histórico, de manera que pueda identificarse claramente la secuencia de cambios, las condiciones aplicadas, las aprobaciones realizadas y la información intercambiada con los sistemas internos y/o de terceros vinculados al proceso de cobranza.

e) Cálculo, Validación y Seguimiento de Provisiones (FMV)

La PLATAFORMA deberá implementar un módulo integral para el cálculo, validación, seguimiento, control, análisis de variación y reporte mensual de provisiones del FMV, alineado al marco normativo SBS aplicable y a las metodologías internas vigentes, garantizando la auditabilidad, trazabilidad, reproducibilidad y resguardo histórico de cada proceso de cierre mensual.

El proceso de provisiones deberá ejecutarse con periodicidad mensual, permitiendo identificar de manera diferenciada cada cierre, sus insumos, reglas aplicadas, resultados obtenidos, validaciones efectuadas, observaciones formuladas y aprobaciones emitidas.

La PLATAFORMA deberá conservar el histórico de cada cierre mensual y permitir su consulta, reconstrucción y comparación posterior con fines de control, seguimiento, auditoría interna, supervisión y sustento ante terceros autorizados.

La PLATAFORMA deberá gestionar como mínimo los insumos necesarios para el cálculo mensual de provisiones, incluyendo: saldos de cierre por cartera, información de garantías y su estado, información de CRC rechazados cuando corresponda, información proveniente de RCC y/o fuentes SBS para clasificación, morosidad y demás variables requeridas, clasificación de la IFI y del subprestatario COOPAC cuando aplique, resultados de Clasificación Equivalente, y resultados o condiciones de CRC/CRCA en el ámbito del Fideicomiso COFIDE, así como sus

respectivas vigencias. La carga de estos insumos deberá poder realizarse mediante interfaces automáticas y/o procesos batch, incorporando controles de completitud, consistencia, duplicidad, vigencia y trazabilidad del origen, usuario, fecha y versión de la información cargada.
La PLATAFORMA deberá contar con un motor de cálculo de provisiones parametrizable, que permita configurar reglas, criterios, excepciones, vigencias y demás condiciones definidas por el FMV S.A., sin exponer a usuarios no autorizados fórmulas, matrices, tasas, factores ni parámetros sensibles. Dicho motor deberá soportar la generación de una base mensual de provisiones auditable, con detalle por operación y consolidado por cartera, así como la conservación de instantáneas, registros o versiones de los insumos y parámetros utilizados en cada cierre mensual, a fin de asegurar la reproducibilidad de los resultados y la trazabilidad completa del proceso.
La PLATAFORMA deberá implementar un flujo operativo con segregación de funciones, que contemple como mínimo: i) a GO (Cierre Operativo) como responsable de la carga de saldos, garantías y remisión de información de CRC rechazados, parámetros CRC y CRCA; ii) a GR como responsable de la validación del cálculo mensual, la generación de la base de provisiones, la validación de resultados, el análisis de variación y la elaboración de reportes; y iii) a Contabilidad como responsable de la recepción de reportes, la revisión del análisis de variación y la habilitación de la integración contable en el sistema que corresponda. La plataforma deberá registrar la intervención de cada rol, las fechas de atención, las observaciones formuladas y el estado de aprobación del proceso mensual.
La PLATAFORMA deberá incorporar validaciones obligatorias previas al cierre mensual, incluyendo como mínimo: la conciliación de saldos operativos frente a saldos contables y/o fuentes maestras; controles de consistencia respecto a vigencias, clasificaciones, garantías, condiciones CRC/CRCA y duplicidad de registros; la posibilidad de recalcular provisiones a efectos de verificar la reproducibilidad de los resultados; y el registro formal de evidencias, observaciones, regularizaciones y aprobaciones. Como regla de control, la PLATAFORMA no deberá permitir el cierre del proceso mensual ni la transferencia de información a Contabilidad mientras no exista conciliación y validación aprobada conforme a los perfiles autorizados.
La PLATAFORMA deberá permitir el análisis mensual de variación de provisiones, comparando resultados respecto del cierre mensual anterior y/o frente a otros cierres de referencia definidos por el FMV S.A., identificando de manera trazable los principales factores explicativos de la variación, tales como cambios en saldos, migración de clasificaciones, cambios en garantías, aplicación de condiciones CRC/CRCA, cambios en información de entrada u otros criterios establecidos por el FMV S.A. la PLATAFORMA permitir registrar el sustento de dichas variaciones, incorporar comentarios de análisis y adjuntar la documentación de respaldo correspondiente.
Adicionalmente, la PLATAFORMA deberá contemplar particularidades mínimas por cartera o esquema operativo. Para el Fideicomiso COFIDE, deberá soportar la gestión de condiciones CRC/CRCA, incluyendo sus vigencias, retiros, actualizaciones derivadas de evaluaciones anuales y, cuando corresponda, el tratamiento de saldos congelados con trazabilidad del saldo base utilizado. Para la Cartera Hipotecaria, deberá permitir el cálculo conforme al sistema de cobranza o esquema operativo definido por el FMV S.A., así como la validación de las variaciones resultantes. Para la Cartera Transferida al Fondo de Inversión, deberá soportar el cálculo y validación comparativa respecto del cierre mensual anterior u otra referencia definida por el FMV S.A. Para el Servicio CRC, deberá permitir el cálculo con insumos consolidados remitidos por la Gerencia de Operaciones y la validación de la variación obtenida.En el caso de las IFIs, la PLATAFORMA deberá utilizar la Clasificación Equivalente vigente en

cada período mensual como uno de los insumos determinantes para la asignación del tratamiento de provisiones que corresponda, de conformidad con la normativa aplicable y las metodologías internas vigentes del FMV S.A.

Como resultado del proceso, la PLATAFORMA deberá generar, como mínimo, la base mensual detallada de provisiones, los reportes mensuales consolidados por cartera, producto, IFIS, los reportes mensuales de conciliación y validación, los reportes comparativos mensuales de variación, y la bitácora completa del proceso, incluyendo usuarios intervinientes, fechas, observaciones, aprobaciones, versiones de insumos y reglas aplicadas. Todos estos productos deberán ser auditables, exportables en los formatos que defina el FMV S.A. y estar disponibles para consulta según los perfiles autorizados.

Asimismo, la PLATAFORMA deberá permitir la emisión de reportes mensuales auditables, con capacidad de consulta histórica, comparación entre cierres, identificación de ajustes, regularizaciones y reclasificaciones, así como la trazabilidad completa entre los datos fuente, el cálculo efectuado, el resultado final obtenido y la información remitida para el proceso contable.

La PLATAFORMA deberá contar con un módulo para la generación de reportes, los cuales deberán poder descargarse en distintos formatos, tales como PDF, Word, Excel y/o visualizarse mediante dashboards en Power BI, según sea necesario.

Asimismo, deberá incluir los anexos normativos correspondientes, los cuales deben mantenerse actualizados conforme a las disposiciones vigentes de las entidades reguladoras del Perú. Siempre y cuando la estimación de esfuerzo no exceda la bolsa de horas contratadas pare el soporte y mantenimiento.

También, la plataforma debe de relacionar todos los activos y pasivos a las cuentas contables según el marco normativo contable vigente de su momento y permita su actualización.

Los informes y anexos que debe generar en forma automática se encuentran descritos en el punto – Informes Normativos.

La plataforma, no permitirá el cierre operativo de ninguno de los módulos sin que haya pasado previamente la validación y conciliación de saldos operativos versus saldos contables, generándose un reporte. Luego de la validación cada área operativa podrá realizar la migración de la data al sistema de contabilidad (SIGA).

La plataforma debe generar los siguientes reportes operativos:

1. Reporte de conciliación de saldos de saldos operativos versus saldos contables. Este reporte, sirve adicionalmente como un validador y debe generarse antes del envío de la información operativa al sistema de contabilidad.
2. Detalle y consolidado por programas del comparativo de los saldos de las provisiones del fideicomiso COFIDE.
3. Detalle y consolidado por programas del comparativo de los saldos de las provisiones del fondo de inversión
4. Detalle y consolidado por programas del comparativo de los saldos de las provisiones del servicio CRC.
5. Reporte de Rating Interno por IFI con evolución histórica.
6. Reporte de requerimientos de visita cargados por las IFIs
7. Reporte Evolutivo de Indicadores
8. Reporte de conciliaciones de visita de cartera.
9. Reporte del Plan Anual

10. Reporte del Indicador de Resultado de Visita de Cartara Hipotecaria MIVIVIENDA
11. Reporte de Grado de Vigilancia por IFI con historial de cambios.
12. Reporte de Clasificación Equivalente por IFI.
13. Reporte de Gestión de Cartera MiVivienda por IFI con nivel de gestión asignado.
14. Reporte de exposición individual por línea (crédito y garantía) por IFI.
15. Reporte de refinanciaciones, con trazabilidad de operación original, condiciones modificadas, aprobaciones y estado de integración con cobranza.
16. Base y reportes mensuales auditables de provisiones por cartera Fideicomiso COFIDE, cartera directa, Cartera Fondos de inversión, productos, FI, Servicios CRA, CRCA.
17. Reporte de cumplimiento o no de las condiciones del CRC y CRCA por IFI.

3.4.2.3 Gestión BackOffice

3.4.2.3.1 Desembolsos diarios

a. La PLATAFORMA deberá permitir la generación de cartas de instrucción para los desembolsos diarios. La Plataforma deberá permitir la configuración de plantillas para que puedan ser utilizadas, cada plantilla deberá tener una versión que permita identificar con cual plantilla se generaron las cartas.
b. La PLATAFORMA deberá permitir la carga de la información del desembolso:
    - Datos de la IFI (Institución Financiera Intermediaria), nombre de la IFI y código de la IFI
    - Datos del producto, código del producto y nombre del producto
    - Datos del cliente, apellido paterno del cliente, apellido materno del cliente, nombres del cliente, documento de identidad, dirección del cliente, nombres del cónyuge
    - Datos del desembolso, fecha de desembolso, código de préstamo, valor de la vivienda, monto del préstamo, bonos, tasa
    - Datos del proyecto, nombre del proyecto, dirección del proyecto.
c. La PLATAFORMA deberá permitir generar las cartas de instrucción del subsidio enviadas al Banco de la Nación. Estas cartas deben permitir la configuración mediante plantillas y tener una identificación de la versión de la plantilla utilizada. Estas cartas deberán tener un flujo de firmas de diferentes niveles para su aprobación.
d. La PLATAFORMA deberá tener un control que permita alertar cuando se generen cartas de instrucción del subsidio fuera del horario de recepción del Banco de la Nación. El Banco de la Nación recibe las cartas de instrucción hasta las 10 am.
e. La PLATAFORMA deberá permitir generar las cartas de instrucción del préstamo enviadas al BCR (Banco Central de Reserva). Estas cartas deben permitir la configuración mediante plantillas y tener una identificación de la versión de la plantilla utilizada. Estas cartas deberán tener un flujo de firmas de diferentes niveles para su aprobación.
f. La PLATAFORMA deberá tener un control que permita alertar cuando se generen cartas de instrucción del préstamo fuera del horario de recepción del BCR. El BCR recibe las cartas de instrucción hasta las 4 pm.
g. La PLATAFORMA deberá permitir la conexión con el sistema LBTR de propiedad del BCR, para ejecutar las transferencias y solicitudes de cobro a las IFIS
h. La PLATAFORMA deberá generar el registro operativo y el registro contable de los desembolsos diarios.
i. La PLATAFORMA deberá soportar la administración de los desembolsos de los subsidios otorgados con recursos del MVCS (BBP) y los recursos del FMV (PBP-CI, BMS, etc).

j. La PLATAFORMA deberá soportar las recuperaciones de los subsidios mencionados en el punto anterior, bajo el mismo flujo operativo de los créditos.

3.4.2.3.2 Fondeo de la cuenta del FONDO para desembolsos (Fideicomiso COFIDE)

a. La PLATAFORMA deberá permitir generar las cartas de instrucción para la transferencia entre cuentas del **FONDO.** Estas cartas deben permitir la configuración mediante plantillas y tener una identificación de la versión de la plantilla utilizada. Estas cartas deberán tener un flujo de firmas de diferentes niveles para su aprobación.
b. Estas cartas de instrucción serán generadas con la información proporcionada por el área de Tesorería indicando las cuentas de origen y destino.
c. La PLATAFORMA deberá soportar para las cartas un flujo de firmas de diferentes niveles para su aprobación.
d. La PLATAFORMA deberá permitir la impresión de las cartas en formato tipo Word y PDF
e. La PLATAFORMA deberá permitir la integración con el correo para enviar las cartas de instrucción.
f. La PLATAFORMA deberá permitir la integración con las plataformas de los bancos en caso la transferencia se realice por ese medio y no por carta, según corresponda la instrucción de cuentas por parte de Tesorería.

3.4.2.3.3 Cobranza CRC-PBP (Fideicomiso Cobertura de riesgo crediticio – Premio del buen pagador en soles y dólares estado unidenses)

a. La cobranza se realiza los 21 de cada mes. En caso el día 21 no sea un día útil, se realiza el siguiente día útil.
b. La PLATAFORMA deberá permitir realizar los cálculos de los montos a cobrar del servicio CRC-PBP en la moneda del crédito, los cálculos a realizar son
    - Cálculo del IGV
    - Cálculo de la detracción
    - Cálculo total del servicio CRC
c. La PLATAFORMA deberá permitir la interconexión con el Sistema O7 para la generación de los comprobantes electrónicos. El sistema O7 tiene la conexión con SUNAT y genera los los comprobantes electrónicos proporcionando los XML y los PDF de cada comprobante electrónico. Así mismo deberá tener registrado según corresponda, el usuario asignado por la IFI para la recepción del comprobante electrónico momento de generarla.
d. La PLATAFORMA deberá soportar la emisión de boletas y poder enviarlo a los clientes.
e. La PLATAFORMA deberá tener un registro de los los comprobantes electrónicos generadas y permitir adjuntar los archivos XML y PDF generados por el Sistema O7 asociada a cada comprobante electrónico.
f. Los comprobantes electrónicos junto con sus respectivos archivos XML y PDF, son enviados a cada IFI.
g. La PLATAFORMA deberá permitir generar las cartas de instrucción por el Fidecomiso CRC/PBP para realizar el cargo en las cuentas de las IFI hacia la cuenta FONDO. Estas cartas deben permitir la configuración mediante plantillas y tener una identificación de la versión de la plantilla utilizada. Estas cartas deberán tener un flujo de firmas de diferentes niveles para su aprobación.
h. La PLATAFORMA deberá soportar para las cartas un flujo de firmas de diferentes niveles para su aprobación.
i. La PLATAFORMA deberá permitir la impresión de las cartas en formato tipo Word y PDF.
j. La PLATAFORMA deberá permitir la integración con el correo para enviar las cartas de instrucción.

k. La PLATAFORMA deberá permitir la integración con el sistema LBTR de propiedad del BCR, para ejecutar las solicitudes de cobro a las IFIS. Así mismo deberá permitir la aprobación de los apoderados según corresponda para el envío de la operación para aprobación de la IFI.
l. En el caso de La Empresa de Crédito Vívela, que no tiene una cuenta en el BCR. La PLATAFORMA debe generar una carta con los montos en soles y dólares, para que la entidad realice el abono en las cuentas del FONDO. La carta también debe tener una plantilla configurable con su respectivo versiona miento. Esta carta también debe permitir la impresión y envió por correo.
m. La PLATAFORMA deberá permitir la integración con el correo remitido por el buzón "Aplicaciones" para dar respuesta y enviar el correo a la IFI informando la solicitud de cobro generada en la plataforma LBTR, mostrando a su vez el detalle de la operación generada. Así mismo deberá tener la lista de con el detalle de los aprobadores de cada IFI, quienes deberán también recibir el correo ya que son los encargados de la aprobación de la solicitud de cobro generada en la plataforma LBTR.

3.4.2.3.4 Pagos PBP (Premio del buen pagador)

a. El pago de este premio se realiza los 22 de cada mes. En caso el día 22 no sea un día útil, se realiza el siguiente día útil.
b. La PLATAFORMA deberá permitir generar las cartas de instrucción para el pago PBP. Estas cartas deben permitir la configuración mediante plantillas y tener una identificación de la versión de la plantilla utilizada.
c. La PLATAFORMA deberá soportar para las cartas un flujo de firmas de diferentes niveles para su aprobación.
d. La PLATAFORMA deberá permitir la impresión de las cartas en formatos tipo Word y PDF.
e. La PLATAFORMA deberá permitir la integración con el correo para enviar las cartas de instrucción a la IFI.

3.4.2.3.5 Liquidación CRC-PBP

a. La PLATAFORMA deberá permitir realizar el cálculo del importe final de la liquidación, mediante la información generada de la cobranza CRC-PBP y el importe del ITF cuya información es calculada y remitida por el BCR.
b. La PLATAFORMA deberá permitir interactuar con la plataforma LBTR para realizar la transferencia de fondos a las cuentas soles y dólares del fideicomiso según el banco que corresponda.
c. La PLATAFORMA deberá permitir generar las cartas mediante plantillas configuradas, correspondientes a los avisos de abono para los bancos en donde se encuentran las cuentas del fideicomiso y el envío de las mismas a la entidad

3.4.2.3.6 Liquidación Servicio CRC (Cobertura de riesgos crediticio)

a. La PLATAFORMA deberá permitir generar las cartas de instrucción para la liquidación del servicio CRC. Estas cartas deben permitir la configuración mediante plantillas y tener una identificación de la versión de la plantilla utilizada.
b. La liquidación debe contener como mínimo los siguientes campos
    - Comisión CRC sin IGV
    - Cobro en cuentas del Fidecomiso
    - Comisión cobrada en el BCR
    - ITF cargada en la cuenta del BCR
    - Portes BCR
    - IGV
    - Detracción

c. LA PLATAFORMA deberá soportar para las cartas un flujo de firmas de diferentes niveles para su aprobación.
d. La PLATAFORMA deberá permitir la impresión de las cartas en formato tipo Word y PDF.
e. LA PLATAFORMA deberá permitir la integración con el correo para enviar las cartas de instrucción a las entidades.
f. La PLATAFORMA permitir la integración con el sistema LBTR de propiedad del BCR, para ejecutar transferencias las solicitudes de cobro a las IFIS. Así mismo deberá permitir la aprobación de los apoderados según corresponda para el envío de la operación para aprobación de la IFI.
g. La PLATAFORMA deberá permitir la interconexión con el Sistema O7 para la generación de los comprobantes electrónicos. El sistema O7 tiene la conexión con SUNAT y genera las facturas electrónicas proporcionando los XML y los PDF de cada comprobante electrónico. Así mismo deberá tener registrado según corresponda, el usuario asignado por la IFI para la recepción del comprobante electrónico al momento de generarla.
h. La PLATAFORMA deberá permitir la integración con el correo remitido por el buzón “Aplicaciones” para dar respuesta y enviar el correo a la IFI informando la solicitud de cobro generada en la plataforma LBTR, mostrando a su vez el detalle de la operación generada. Así mismo deberá tener la lista de con el detalle de los aprobadores de cada IFI, quienes deberán también recibir el correo ya que son los encargados de la aprobación de la solicitud de cobro generada en la plataforma LBTR.
i. La PLATAFORMA permitir la integración con el sistema LBTR de propiedad del BCR, para ejecutar transferencias correspondientes a la liquidación de del SERVICIO CRC a la entidad correspondiente para abono en la cuenta del FMV, permitiendo la aprobación de los apoderados según corresponda
j. La PLATAFORMA deberá permitir el registro del asiento por la transferencia recibida por la solicitud de cobro y por la transferencia realizada por la liquidación a la destinada del FMV, para lo cual se debe tener las plantillas correspondientes.

1. La PLATAFORMA deberá soportar la emisión de boletas y poder enviarlo a los clientes.
2. La PLATAFORMA deberá tener un registro de los comprobantes electrónicos generadas y permitir adjuntar los archivos XML y PDF generados por el Sistema O7 asociada con cada comprobante electrónico.
3. Los comprobantes electrónicos junto con sus respectivos archivos XML y PDF, son enviados a cada IFI.
4. Reporte de conciliación de saldos de saldos operativos versus saldos contables. Este reporte, sirve adicionalmente como un validador y debe generarse antes del envío de la información operativa al sistema de contabilidad.

La plataforma, no permitirá el cierre operativo de ninguno de los módulos sin que haya pasado previamente la validación y conciliación de saldos operativos versus saldos contables, generándose un reporte. Luego de la validación cada área operativa podrá realizar la migración de la data al sistema de contabilidad

3.4.2.4 Gestión Comercial

La PLATAFORMA deberá permitir la generación y administración de los reportes comerciales del FONDO. Los reportes comerciales podrán ser mensuales o diarios. La PLATAFORMA deberá permitir la generación y descarga de, por lo menos, los siguientes reportes comerciales:

1. **Reporte de perfil del cliente - FONDO**

a. Cantidad de créditos
b. Por género
c. Por rango de edad
d. Tasa ponderada mensual
e. Valor de la vivienda promedio
f. Créditos por IFI – Por zona geográfica y por producto

2. Reporte comercial
a. Informe de créditos por IFI.
b. Cantidad de créditos - por IFI, por zona geográfica, por producto y por descripción del destino.

3. Reporte por promotor
a. Ranking por promotor.
b. Por proyecto inmobiliario y por zona geográfica.
c. Información de estados financieros (Promotor y ET) relacionada a proyectos, garantías, sub prestatarios

La PLATAFORMA deberá permitir la integración y descarga de la información comercial requerida desde la plataforma de COFIDE.

La PLATAFORMA deberá tener la opción de un **Dashboard** que permita gestionar, administrar, configurar y visualizar los indicadores de la gestión comercial

3.4.2.5 Gestión de Tesorería

El área de Tesorería realiza el fondeo para los desembolsos, para lo cual valida el correo que le envían a diario con los montos a desembolsar. El área de Tesorería verifica en la cuenta del BCR el saldo disponible para el desembolso. En caso el saldo disponible en su cuenta del BCR sea menor al monto a desembolsar, realiza la transferencia entre sus cuentas corrientes en los Bancos locales hacia la cuenta en el BCR. La PLATAFORMA deberá soportar:

1. La PLATAFORMA deberá enviar por correo y permitir consultar los montos a desembolsar en forma diaria para que el área de Tesorería pueda validar contra el saldo disponible en la cuenta del BCR.
2. La PLATAFORMA permitirá el registro de la transferencia y conectarse con la plataforma que usa el área de Tesorería (por ahora el TraderLive) para la operación de transferencia desde las cuentas de los Bancos locales hacia la cuenta en el BCR.
3. La PLATAFORMA deberá enviar la notificación de la transferencia al área de BackOffice. Debe ser configurable para incluir en la notificación a otros usuarios.

3.4.2.6 Gestión de garantías

1. La PLATAFORMA deberá permitir la administración de las garantías (Hipotecarias y Cartas Fianzas) que son reportadas al **FONDO**, debido a los créditos reportados.

Parametrización de la garantía:
- La PLATAFORMA debe permitir la parametrización por tipos, subtipos de garantía, permitiendo configurar los datos en forma opcional u obligatoria por cada tipo y subtipo de garantía. Debe cumplir con la normativa de la SBS según corresponda.
- La PLATAFORMA debe permitir configurar tablas particulares, como mínimo: peritos, monedas, tipo de cobertura, estado de la garantía, estructura geográfica por región y departamento.

- La PLATAFORMA debe permitir configurar el envío de las notificaciones, en variables como: frecuencia y tiempo de envío, contenido a enviar, destinatarios a ser enviado.

2. El alcance de la administración de las garantías es:
   a. Niveles de Validación (registro y aprobador)
   b. Registro de la garantía
   c. Parametrización de la garantía
   d. Reportes de la garantía
   e. Otras operaciones de administración de la garantía

3. Niveles de validación – Administración de Garantías:
   La PLATAFORMA soportará 2 niveles para el proceso de Administración de Garantías:
   a. Nivel de Registro: este perfil permitirá el registro de la garantía, y
   b. Nivel Aprobador: este perfil permitirá la aprobación de la garantía (previamente registrada)

4. Sobre el registro de la garantía: la Plataforma deberá soportar:
   a. El registro de la Garantía (Nivel de Registro):
      - La carga masiva de la garantía sea a través de servicios transaccionales, funcionalidad que sea nativa de La PLATAFORMA propuesta.
      - La PLATAFORMA debe permitir el registro y control de la garantía por cliente, por operación y/o por la línea de crédito
      - La PLATAFORMA también deberá dar la opción de registro “uno a uno” de la garantía.
      - La PLATAFORMA podrá soportar la subida de sustento (archivos) como parte del registro.

   b. **La Aprobación de la Garantía (Nivel Aprobador):**
      - La PLATAFORMA debe permitir la revisión del registro previo realizado de la garantía, para la evaluación.
      - La PLATAFORMA debe permitir la **Aprobación u Observación** de la garantía, registrando el detalle de la observación (de manera descriptiva y/o adjuntando un archivo de sustento)

   c. **Notificación:**
      - La PLATAFORMA deberá notificar la conclusión del registro de la garantía hacia el Nivel Aprobador de la garantía.
      - La PLATAFORMA debe incluir el indicador de contabilización del tiempo estipulado para el envío de la notificación.

   d. **Parametrización de la garantía:**
      - La PLATAFORMA debe permitir la parametrización por tipos, subtipos de garantía, permitiendo configurar los datos en forma opcional u obligatoria por cada tipo y subtipo de garantía. Debe cumplir con la normativa de la SBS según corresponda.
      - La PLATAFORMA debe permitir configurar tablas particulares, como mínimo: peritos, monedas, tipo de cobertura, estado de la garantía, estructura geográfica por región y departamento.
      - La PLATAFORMA debe permitir configurar el envío de las notificaciones, en variables como: frecuencia y tiempo de envío, contenido a enviar, destinatarios a ser enviado.

   e. **Reportes:** La PLATAFORMA deberá incluir, por lo menos, los reportes siguientes sobre Administración de Garantías:
      - Por estatus
      - Por tipo de garantía

- Por historial de la garantía primigenia y sus renovaciones (de ser el caso).
- Por IFI
- Por Entidades técnicas o Promotores
- Por situación
- Por rangos de días por vencer 30 días, 60 días y 90 días (parametrizables). Alertas semanales antes del vencimiento.
- Alertas semanales de garantías vencidas que no se hayan ejecutado, honrado, renovado ni devuelto.

f. **Otras operaciones en la administración de la garantía:**
La PLATAFORMA debe permitir las operaciones siguientes:
- Cancelación de la garantía
- Anulación de la garantía
- Relación de garantías con operaciones y líneas de crédito
- La PLATAFORMA deberá permitir la integración operativa-contable.

3.4.2.7 Gestión de Fideicomiso (COFIDE)

3.4.2.7.1 Originación de los desembolsos

A) Fuente de información:

La PLATAFORMA deberá permitir la gestión de los productos Crediticios hipotecarios administrado por COFIDE (Fiduciario) La fuente para la carga del Archivo en formato Excel, el cual contenga las Solicitudes de los Créditos generados por la plataforma del Fiduciario. La PLATAFORMA deberá permitir la creación

a. Los diferentes productos crediticios actuales y los productos futuros que puedan ser creados, y
b. Los diferentes bonos actuales y los bonos futuros que puedan ser creados.
c. La PLATAFORMA deberá permitir la carga de archivos a través de **servicios transaccionales,** funcionalidad que deberá ser nativa de la PLATAFORMA propuesto.

Asimismo, LA PLATAFORMA deberá tener la capacidad de carga de archivos y procesamiento del mismo para la evaluación de los expedientes (postulantes a los créditos con BBP y sin BBP) en caso no exista Fiduciario

B) Niveles de validación - Proceso de originación

La PLATAFORMA soportará 2 niveles para el proceso de Originación:

a. Perfil de Registro: este perfil permitirá la subida del Archivo Excel al PLATAFORMA, para que pueda ser evaluado en línea por las Validaciones definidas.
   - Validación de formato
   - Validación de líneas
   - Validación de FCTP

b. Nivel Aprobador: este perfil permitirá la aprobación de las Solicitudes que previamente han pasado con éxito las Validaciones definidas.

C) Sobre las validaciones - Proceso de originación

La PLATAFORMA deberá cumplir con las validaciones adjuntas, así como detectar las aprobaciones y observaciones de cada una de las validaciones.
La PLATAFORMA deberá permitir la aprobación como excepción de las Solicitudes que no aprueban las validaciones indicadas (Observadas)
Las validaciones definidas para el presente proceso de Originación, son:

a. Validación 1: Consistencia del Excel
b. Validación 2: Reglas de Negocio de cada producto
c. Validación 3: Apoyo previo habitacional del estado, y
d. Validación 4: Titular cuenta con vivienda su nombre.

Es necesario realizar el cruce con las bases:

a. Nuevo Sistema Techo Propio
b. Sistema Integral de Procesos de Techo Propio
c. Base del estado de Postulación Techo Propio

Si en esta opción aparece una observación, deberá mostrarse un botón de quitar a ese postulante.

D) Validación de consistencia del Excel

La PLATAFORMA deberá realizar, como mínimo, las siguientes validaciones:

a. La consistencia de los campos en el Excel (campos numéricos, fecha, alfanuméricos, etc.)
b. La identificación de solicitudes duplicadas
c. Los casos de homonimia entre las solicitudes
d. No debe presentar inconvenientes con lectura de caracteres especiales (apostrofes, tildes, etc.)
e. Los apellidos y nombres del titular de la solicitud deben ser comparado contra la base PIDE.
f. Luego de las Validaciones de consistencia, la Plataforma deberá colocar el ESTADO a la solicitud, para esta primera validación:
    - **APROBADA la consistencia:** es decir, la solicitud ha pasado las validaciones de consistencia indicadas.
    - **OBSERVADA la consistencia:** es decir, que por lo menos hay 1 tipo de observación que presenta la solicitud (pueden haber más de 1 observación para la misma solicitud)
    - **RECHAZADA la consistencia:** es decir, la solicitud NO ha pasado las validaciones de consistencia indicadas.

La PLATAFORMA pueda permitir la subida de los escaneos de las solicitudes y los anexos (expedientes) y una vez validada verá mostrar una ventana donde se visualice cada observación por cliente por IFI.

- **Validar por reglas de Negocio de cada producto**

  Deberán evaluarse las solicitudes que aprobaron la consistencia de los datos de las solicitudes de créditos (Validación N° 1)

  La PLATAFORMA realizará las siguientes validaciones, según el documento de Regla de Negocio vigente para los Productos Crediticios y los Bonos:

    - Validaciones para productos crediticios:
        - Productos vigentes (código y nombre del producto)
        - Préstamos vigentes (código, nombre y tipo del préstamo)
    - Validaciones para bonos:
        - Valor de la vivienda (monto mínimo y máximo)
        - Valor del bono (según rango de valor de la vivienda)
        - Monto de los bonos según fecha de vigencia
    - Validaciones con grado de sostenibilidad y proyecto inmobiliario
        - Cruce con la base de proyectos sostenibles en el SAOC , debe coincidir con el archivo a validar.
    - Validaciones de IFI's
        - Cruce con la base en el SAOC de la IFI's registradas, debe coincidir con el archivo a validar. (mismo formato)

Luego de las Validaciones de las “Reglas de Negocio”, la PLATAFORMA deberá colocar el ESTADO de la Solicitud, para esta segunda validación:

- APROBADA la Regla de Negocio: es decir, la solicitud ha pasado las validaciones de las reglas de negocio vigentes.
- OBSERVADO por Regla de Negocio: es decir, que por lo menos hay 1 regla de negocio que no es cumplida en la solicitud (pueden haber más de 1 regla de negocio que no se cumpla, para la misma solicitud)
- RECHAZADA la Regla de Negocio: es decir, la solicitud NO ha pasado las validaciones de las reglas de negocio vigentes

- **Validar por Apoyo Habitacional Previo (AHP) del estado:**

  Deberán evaluarse las Solicitudes que aprobaron la Validación de Reglas de Negocio (Validación N° 2)

  La PLATAFORMA realizará las siguientes validaciones, según el documento de Reglas de Negocio vigente para el Apoyo Habitacional Previo (AHP) del estado:

  - La PLATAFORMA deberá validar que el Solicitante no tenga un subsidio vigente del Estado o del FONDO.

  Luego de las Validaciones de “Apoyo previo Habitacional” (AHP), la PLATAFORMA deberá colocar el ESTADO de la Solicitud, para esta tercera validación:

  - APROBADA por Apoyo Previo: es decir, que la Solicitud no presenta el Apoyo Habitacional Previo.
  - OBSERVADO por Apoyo Previo: es decir, que la Solicitud si presenta el Apoyo Habitacional Previo del estado.

  Esta validación es para los postulantes que hayan tenido un desembolso anterior con algún tipo de subsidio, se negará la operación. Esta información deberá realizar una validación con el Sistema Integral de Procesos de Techo Propio.

- **Validar la propiedad de una vivienda:**

  Deberán evaluarse las Solicitudes que aprobaron la Validación de Apoyo Habitacional Previo (AHP) del Estado (Validación N° 3)

  LA PLATAFORMA realizará las siguientes validaciones, según el documento de Reglas de Negocio vigente sobre la titularidad de una vivienda por parte del solicitante del crédito:

  - La PLATAFORMA deberá validar que el Solicitante del crédito no sea propietario de una vivienda (con base de RRPP)

  Luego de las Validaciones de “propiedad de una vivienda”, la PLATAFORMA deberá colocar el ESTADO de la Solicitud, para esta cuarta validación:

  - APROBADA la no propiedad de vivienda: es decir, que el titular de la Solicitud no es propietario de una vivienda.
  - OBSERVADO por propiedad de vivienda: es decir, que el titular de la Solicitud si presenta una vivienda.

  Para las validaciones 1, 2, 3 y 4 la Plataforma deberá permitir que solo las que tengan estado “Aprobado” en todas las validaciones continúe con la fase de Desembolso y para los estados “Observado” o “Rechazado” deberá mostrar una ventana detallado por cliente con el fin de enviar esa información a COFIDE en automático (en un botón).

Esta información deberá realizar una validación con SUNARP.

- **Sobre las Excepciones**

  La PLATAFORMA deberá permitir la aprobación de una solicitud observada a través de una excepción.
  Para tal efecto, La PLATAFORMA deberá permitir el registro del sustento (archivos o explicación textual) de dicha excepción.
  La PLATAFORMA deberá requerir un nivel aprobador de la solicitud de excepción, para dar por concluido el proceso de excepción.
  Las Solicitudes que hayan aprobado las validaciones indicadas en el proceso de Originación, continuarán el proceso y pasarán a la siguiente etapa (Desembolso)

  Esta excepción deberá aparecer antes de grabar los desembolsos, y deberá ser aprobado por un usuario APROBADOR.

- **Configuración**

  La PLATAFORMA debe presentar la opción de parametrizar las diferentes variables de los Productos Crediticios, Bonos, garantías, IFI:
  Las variables parametrizadas, como mínimo, son:

  Configuración de Productos:
  - Productos vigentes (código y nombre del producto)
  - Préstamos vigentes (código, nombre y tipo de préstamo)

  Configuración de los Valores del Bono:
  - Datos del Bono (código, nombre, tipo de bono)
  - Decreto asociado
  - UIT (valor y fecha de vigencia inicio y fin)
  - Valor del Bono será en porcentaje al valor de la vivienda
  - Valor de la vivienda (monto mínimo y máximo)
  - Valor del bono (según rango de valor de la vivienda)
  - Cantidad de rangos para cada tipo de bono
  - Monto de los bonos según fecha de vigencia

  Configuración del código y atributos de las IFI:
  - Código IFI
  - Descripción de la IFI
  - Cuenta BCRP
  - Correos de contacto
  - Dirección de domicilio
  - Persona de contacto para cartas y correos electrónicos

  Cabe señalar que la PLATAFORMA:
  - La Plataforma deberá permitir extraer información por periodos, en formato Excel, para cada una de las configuraciones descritas
  - Deberá soportar los cambios en los parámetros, según las Reglas de Negocio de cada producto.
  - Deberá soportar la vigencia de los bonos y productos crediticios (vigentes o no vigentes)

E) Sobre las consultas de gestión:

Se presenta el mínimo de consultas que debe presentar la plataforma, para facilidad e información a los usuarios:

- Por DNI del titular del crédito
- Por código de crédito
- Por tipo de producto

- Por estado: Aprobado, observado

Las Consultas definidas deben presentar la opción de exportar la información hacia Excel.

3.4.2.7.2 DESEMBOLSO DE PRESTAMO Y BBP

A) Fuente de información

La PLATAFORMA deberá presentar las solicitudes que hayan aprobado las validaciones indicadas en el proceso de Originación.

B) Niveles de validación

La PLATAFORMA soportará 2 niveles:

- **Nivel de Registro:** este perfil la **generación de los documentos de desembolso**, para que puedan ser aprobados por el siguiente nivel
- **Nivel Aprobador:** este perfil permitirá la aprobación de las Solicitudes que previamente han pasado con éxito las Validaciones de Desembolso.

C) Sobre las validaciones en el proceso de desembolso:

a) La PLATAFORMA deberá realizar las validaciones adjuntas, así como detectar las aprobaciones y observaciones de cada una de las validaciones planteadas.
b) Las Solicitudes que aprueben las validaciones indicadas, estarán disponibles para la **ejecución del desembolso.**
c) Las Solicitudes que no aprueben las validaciones indicadas (Observadas), podrán ser regularizadas en la PLATAFORMA como una **excepción.**
d) Las validaciones definidas para el presente proceso de Desembolso son:
    a. **Validación 1:** Línea de Crédito está disponible
    b. **Validación 2:** Reglas de Negocio para el desembolso
    c. **Validación 3:** Aprobación por control dual, en cuanto se valide las observaciones por apoyo previo por parte del EVALUADOR y el APROBADOR lo valide.

Una vez realizada todas las validaciones deberá grabarse la información solo a los que tienen estado “Aprobado”.

D) Validación de reglas de Negocio para desembolso:

La PLATAFORMA realizará las siguientes validaciones, según el documento de Regla de Negocio vigente para los Productos Crediticios y los Bonos:

a) Acceso al Nuevo Sistema Techo Propio (NSTP) y Sistema Integral de Procesos de Techo Propio.
b) Valida las cuentas bancarias de la IFI y/o BCP, así como la información requerida por el Back Office para realizar la transferencia.

Luego de las Validaciones, la plataforma deberá colocar el ESTADO a la solicitud, para esta primera validación:

a) **APROBADA la Regla de Negocio:** es decir, la solicitud ha pasado las validaciones de reglas de negocio vigentes, o
b) **OBSERVADA por Regla de Negocio:** es decir, que por lo menos hay 1 regla de negocio que presenta una observación en la solicitud (pueden haber más de 1 observación para la misma solicitud).

Para esta validación se debe tener en cuenta lo siguiente:

Si un cliente postulante al NCMV con BBP tuvo un crédito anterior inscrito como carga familiar (no como titular ni cónyuge), puede aplicar al BBP siempre y cuando el crédito anterior, tenga antigüedad mayor a 5 años; de no cumplir ambas condiciones en simultáneo, se rechaza.

E) Validación de la Línea de crédito:

La PLATAFORMA valida que la Línea de crédito tenga el estado "disponible".

Luego de la validación, la plataforma deberá colocar el ESTADO del desembolso de la Solicitud:

a) **APROBADO por LC:** es decir, la Solicitud **no** presenta una línea de crédito disponible.
b) **OBSERVADO por LC:** es decir, la Solicitud **si** presenta una línea de crédito disponible.

Una vez realizada todas las validaciones deberá grabarse la información solo a los que tienen estado "Aprobado".

F) Aprobación por control dual:

- La PLATAFORMA deberá permitir al **"Nivel de Registro"** la generación de los siguientes documentos de desembolso:
  - Orden de Desembolso por cada IFI
  - Solicitud de Transferencia a cada IFI

- La PLATAFORMA deberá permitir al "Nivel Aprobador" la opción de aprobación (o no) de las Solicitudes que han cumplido las validaciones definidas para desembolso

  a. **De ser aprobada:** La PLATAFORMA deberá permitir un campo para el llenado de observaciones por el nivel aprobador. La aprobación de la solicitud implica que la persona responsable está de acuerdo con la "Solicitud de Desembolso por cada IFI" y "Solicitud de transferencia a cada IFI" (que fueron generadas)
  b. **De ser desaprobada:** La PLATAFORMA deberá permitir el registro de un motivo de desaprobación, así como le llenado de observaciones por el nivel aprobador.

- Una vez realizada la aprobación, el **Nivel Aprobador:**
  - Debe permitir generar el cronograma de préstamos por cada IFI, una vez aprobada y contabilizada las operaciones la plataforma debe permitir enviar los cronogramas por los prestamos generados, y
  - Enviar notificación al perfil asignado de "Back Office" para que proceda a realizar la transferencia de fondos. Continúa la sección de "Back Office" del presente documento.

La PLATAFORMA deberá permitir generar el registro de información de los préstamos por cada IFI y notificar a Back office para que realice el voucher contable y se enviará la información al SIGA CONTABILIDAD

La PLATAFORMA deberá permitir la integración operativa-contable. (SIGA TESORERÍA)

I) Gestión operativa del BBP asociada al desembolso

LA PLATAFORMA debe almacenar todos los registros que se cargan de la plantilla remitida por el proveedor o cliente previa validación de reglas de negocio establecida en el punto de originación.

Adicional al grabado de la data debe registrarse en 2 momentos o fases del proceso

1. Fecha de asignación: que es la fecha de evaluación y cumple con las condiciones
2. Fecha de desembolso: que es la fecha que se ejecuta la transferencia del BBP

LA PLATAFORMA de manera automática enviará correos electrónicos al Dpto. Tesorería y Back Office indicando los montos que se transferirá a las IFI.

Luego y una vez ejecutado el proceso de carga y registro LA PLATAFORMA almacenará en una base de datos todas las operaciones ejecutadas con las variables cargadas.

LA PLATAFORMA, deberá hacer una interfase con la plataforma del MEF de nombre SIAF para que registre de manera automática todas las asignaciones y desembolsos en sus 03 fases (compromiso, devengado y girado), una vez registrados. Se informará mediante correo electrónico automático a los representantes autorizados para que apruebe las transferencias a ejecutar.

Al día siguiente de aprobado por los representantes en el SIAF, LA PLATAFORMA de manera automática, enviará una solicitud de desembolso de BBP (con visto del operador y/o firma de la Jefatura a cargo) al módulo del Gestor de Back Office para inicie el proceso de gestión de firmas y envió de carta al Banco de la Nación

LA PLATAFORMA tendrá una opción de mantenimiento de registro de correos electrónicos y programación de horario para su envío automático las comunicaciones que realice corresponden a los desembolsos ejecutados hacia las IFI y adjuntará un reporte con el detalle de los clientes finales beneficiados del BBP.

a. Proceso de saldo de BBP:

LA PLATAFORMA deberá tener una opción donde se registre todos los convenios que se suscribe con el MVCS, diferenciando los estados de convenios cerrados y convenios vigentes. Asimismo, se registrará el monto de recursos asignados con el cual inicia cada convenio, a fin de que se descuente de manera diaria los desembolsos que se ejecuten, sumando los BBP recuperados que se mostrará mediante reportes el saldo disponible por convenio, que permitirá sustentar al MVCS.
Todos los formatos serán proporcionados por el usuario

b. Proceso de recuperación de BBP:

Corresponde a todos aquellos BBP que fueron recuperados a solicitud de las IFI o por alguno de los incumplimientos establecidos en el Reglamento de BBP, LA PLATAFORMA, deberá validar que todos los atributos que se recuperen sean los mismos montos que fueron desembolsados y a su vez se le sume los intereses legales calculados (en base a la fórmula que se establezca y usando el factor del interés de la página web de la SBS) correctamente, de encontrar diferencias deberá emitir alertas para comunicarlo a la IFI. LA PLATAFORMA una

vez calcula el interés legal emitirá correos electrónicos automáticos informando a la IFI el monto que se le carga a su cuenta BCRP. LA PLATAFORMA deberá almacenar en su base de datos las recuperaciones realizadas que permita identificar por tipo de convenio para que luego de identificar todos los montos recuperados dentro del mes de ejecución emitir reportes según formato establecido para realizar las gestiones de devolución de dichos recursos al MVCS, LA PLATAFORMA de manera automática se generé una solicitud de instrucción mediante interfase con la plataforma que usa el Dpto. Tesorería y pueda dar atención a dicha transferencia a cuenta específica del BBP en el IBK.

Todos los formatos serán proporcionados por el usuario

c. Proceso de devolución de BBP:

LA PLATAFORMA deberá alertar luego de 02 meses posterior a la recuperación del BBP que se debe iniciar el proceso de devolución de recursos al MVCS, para ello deberá generar un reporte de todas las operaciones (BBP e intereses legales) por convenio suscrito y de manera automática mediante interfase al SIGA dar la instrucción al Dpto de Tesorería para su ejecución respectiva y transferencia de lo recuperado a la cuenta del Tesoro Público. Una vez atendido el pedido LA PLATAFORMA enviará un correo automático a los contactos del MVCS (estarán previamente registrado en opción) donde adjunte la evidencia o constancias de la transferencia y el reporte en PDF por la ejecución de la devolución que serán cargados en opción del sistema y que tendrá acceso Back Office para que cuelguen la evidencia.
Posteriormente LA PLATAFORMA deberá emitir una carta dirigida según formato establecido al MVCS formalizando la comunicación previamente mencionada.

Todos los formatos serán proporcionados por el usuario

d. Reportes por cierre Diario y Mensual de los BBP (actualmente emite el SAOC).

- **Reporte Diario de Desembolsos, Saldos y Recuperaciones de los BBP:**
  Este reporte debe reflejar las operaciones realizadas durante el día, desembolsos del BBP, el saldo según cada convenio suscrito y las recuperaciones de BBP por convenio y los intereses legales que corresponda.

- **Reporte Mensual de Desembolsos, Saldos y Recuperaciones de los BBP:**
  Similar al reporte diario, pero este debe compilar la información correspondiente a todo el mes.

3.4.2.7.3 RECAUDACIÓN

A) Recaudación diaria:

a. La PLATAFORMA deberá procesar en forma diaria la información compartida por **COFIDE** en archivos Excel compartidos en un SFTP y cargarlos en La PLATAFORMA de manera automática.
b. La PLATAFORMA deberá validar la información a cargar y mostrar los registros que tengan observaciones y el motivo de las observaciones.
c. La información es la lista de los clientes que han realizado prepagos parciales y prepagos totales. La PLATAFORMA deberá contar códigos de transacción que permitan identificar a cada tipo de transacción.

d. La PLATAFORMA deberá evaluar el tiempo que ha pasado desde el desembolso. Si el tiempo es mayor a 5 años, se deberá calcular el monto de recuperación de los atributos.
e. En los atributos están considerados los bonos: BBP, PBP, BMS por convenio
f. En caso de que La PLATAFORMA valide que el tiempo que ha pasado desde el desembolso es mayor a 5 años, no se requiere de la recuperación de atributos.
g. La PLATAFORMA deberá generar el registro operativo y registro contable diario de las recuperaciones diarias.

Condiciones lógicas que deberá tener en consideración la plataforma:

1. Archivo diario es enviado junto con el cortado y la carta orden integradas en columnas y en archivos para validar por correo.
2. Se colocan los archivos Excel en carpeta de días especial para recuperaciones, junto con los archivos.
3. Se cargan los archivos de la carpeta a la plataforma
4. La PLATAFORMA emite Msgbox preguntando si los valores de carta orden y cortado BCR coinciden con lo que se ha cargado en la PLATAFORMA para el día respectivo
5. Si la información es correcta, se continua con el proceso. Si no, se solicita verificar el archivo (problema de formato).
6. Se suben los archivos con botones especiales como "Cargar Cobranza", "Cargar Gastos de Extorno", "Cargar CartaOrden" y "Cargar CortadoBCR" que estos dos últimos tendrán las sub opciones "soles" o "dólares".
7. La PLATAFORMA crea una tabla interna (que cumple las mismas condiciones del archivo "RECUPER. DIARIAS") y que se puede descargar a modo de reporte para verificarlo manualmente. Pero también puede ser visualizada desde la plataforma sin descargar.
8. La PLATAFORMA puede interactuar con la BaseBBP y la BasePBP (aunquhe sea cuando están abiertas) y, en el caso de los atributos, puede hacer la validación con la información de los subsidios en el sistema, interactuar con las bases previamente mencionadas y realizar el llenado de la información de las recuperaciones.
9. Permite generar la visualización de la "Consulta" y la "Visualización de asientos".
10. Permite descargar los archivos ya trabajados con las indicaciones de los fallecidos, los bonos recuperados en partes y los errores identificados, para mandar a corregir a COFIDE.

B) Recaudación - Cartera directa:

La recaudación de la Cartera Directa se encuentra actualmente tercerizada mediante un convenio de servicio de administración de cobranza suscrito con una empresa especializada en gestión de recaudaciones. En el esquema actual, la información de los pagos realizados por los subprestatarios es consolidada mediante cortes operativos de periodicidad mensual, tras lo cual se remite un reporte operativo de recaudación que detalla los pagos efectuados, las fechas de abono, los importes cancelados y los créditos asociados. Sin perjuicio de ello, se requiere que la PLATAFORMA implemente mecanismos de interconexión en línea o mediante servicios de integración (APIs, Web Services o interfaces automatizadas) con las empresas recaudadoras tercerizadas, así como con los canales de recaudación bancarios, tales como los servicios de recaudación del Banco de Crédito del Perú (BCP) u otras entidades financieras que participen en el proceso. Esta interconexión deberá permitir la recepción automática, segura y oportuna de la información de pagos realizados por los clientes, reduciendo

la dependencia de reportes manuales y optimizando la actualización de la información financiera de la cartera.

a. La PLATAFORMA deberá contar con la capacidad de integrarse automáticamente con los sistemas de la empresa recaudadora, mediante mecanismos de intercambio de información estructurada, tales como interfaces de datos, servicios web o carga automática de archivos de recaudación. Dicha integración deberá permitir que la información de pagos recibidos sea procesada en línea o en intervalos programados de alta frecuencia, de modo que la recaudación registrada por los canales externos se refleje de forma oportuna en el sistema de administración de la cartera, garantizando la consistencia de la información y la actualización inmediata del estado de los créditos administrados.

b. La PLATAFORMA deberá ejecutar de manera automática los cálculos necesarios para la correcta aplicación de los pagos recibidos, de acuerdo con las condiciones contractuales de cada crédito y las reglas de imputación establecidas en el sistema financiero.
Para tal efecto, el sistema deberá determinar la distribución del monto recaudado entre los distintos conceptos del crédito, tales como:

   - Intereses vencidos.
   - Intereses corrientes.
   - Capital.
   - Comisiones o gastos asociados.

   Posteriormente, la PLATAFORMA deberá actualizar el cronograma de pagos correspondiente a cada crédito, reflejando los importes cancelados, los saldos pendientes y las nuevas fechas o cuotas pendientes, garantizando la trazabilidad de todas las operaciones realizadas.

c. La PLATAFORMA deberá incorporar funcionalidades que permitan realizar simulaciones de cancelación parcial o cancelación total de los créditos correspondientes a los subprestatarios de la cartera directa.
Estas simulaciones deberán considerar:

   - El saldo de capital pendiente.
   - Los intereses generados a la fecha de la simulación.
   - Los cargos adicionales aplicables.
   - Las condiciones contractuales del crédito.

   Asimismo, el sistema deberá permitir visualizar el impacto financiero de dichas cancelaciones, incluyendo la reducción del saldo de deuda, los intereses aplicables y el monto total requerido para efectuar la cancelación en una fecha determinada.

d. La PLATAFORMA deberá permitir el registro automático tanto a nivel operativo como contable de las recaudaciones recibidas, una vez que estas hayan sido procesadas y aplicadas a los créditos correspondientes. El registro operativo deberá reflejar los detalles de la transacción, tales como:

   - Fecha de pago.
   - Canal de recaudación utilizado.
   - Identificación del cliente.
   - Crédito asociado.
   - Monto pagado.

   En paralelo, el sistema deberá generar los registros contables correspondientes, de acuerdo con la estructura contable definida por la entidad y conforme a las normativas contables aplicables, asegurando la

correcta imputación de los ingresos por capital, intereses y otros conceptos. Este registro deberá realizarse de forma automática y en línea, garantizando la integridad y trazabilidad de la información financiera.

3.4.2.7.4 COBRANZAS

A) Cobranza - COFIDE:

a. La PLATAFORMA deberá procesar en forma diaria la información de cobranzas compartida por **COFIDE** y validar de manera automática. En caso encuentre observaciones deberá mostrar las observaciones en una pantalla.
b. Cada IFI debe transferir los fondos a la cuenta que el **FONDO** determine, la IFI debe comunicar y enviar la constancia del abono realizado y el nombre del cliente. La PLATAFORMA deberá tener opción para que los fondos y la aplicación de la cobranza estén sincronizados
c. La PLATAFORMA debe soportar la transacción de pago por IFI donde valida el pago total de la cuota mensual por IFI, y los pagos masivos donde aplica a cada cuota/cliente respectivamente. Actualización de los cronogramas y generación de la contabilidad.
d. La PLATAFORMA debe procesar los pagos en el cierre diario contable (batch) y generar un reporte de procesadas conformes y no conformes. El reporte debe ser enviado por correo, y configurable para asignar los usuarios destinatarios.
e. La PLATAFORMA deberá permitir realizar los cálculos de los montos a cobrar por interés en la moneda del crédito, los cálculos a realizar son
    - Cálculo del IGV
    - Cálculo de la detracción
    - Cálculo total del interés por cobrar.
f. La PLATAFORMA deberá permitir la interconexión con el Sistema O7 para la generación de los comprobantes electrónicos. El sistema O7 tiene la conexión con SUNAT y genera los comprobantes electrónicos proporcionando los XML y los PDF de cada comprobante electrónico.
g. La PLATAFORMA deberá soportar la emisión de los comprobantes electrónicos y poder enviarlo a los clientes.
h. La PLATAFORMA deberá tener un registro de los comprobantes electrónicos generados y permitiendo adjuntar los archivos XML y PDF generados por el Sistema O7 asociada a cada comprobante electrónico.
i. Los comprobantes electrónicos junto con sus respectivos archivos XML y PDF, son enviados a cada IFI.
j. LA PLATAFORMA deberá generar un reporte por la cobranza mensual ejecutada a las IFI. Luego de ello deberá separar por IFI en moneda soles y dólares, los montos para que se generen los comprobantes electrónicos correspondientes enviando mediante interfase a la plataforma del SIGA las cifras generadas y la plataforma de la SUNAT. Luego de ello cada comprobante electrónico emitido deberá ser enviada de manera automática a cada IFI para su conocimiento respectivo.

B) Cobranza – Cartera Directa:

a. La PLATAFORMA deberá soportar integralmente los distintos procesos de gestión de cobranza de la cartera directa, incluyendo:

- Refinanciación de créditos.
- Reprogramación de obligaciones.
- Gestión de créditos en cobranza prejudicial.

- Gestión de créditos en cobranza judicial.

Asimismo, la PLATAFORMA deberá permitir realizar los cálculos financieros y crediticios asociados a cada una de estas operaciones, incluyendo la generación o actualización del cronograma de pagos correspondiente.

b. La PLATAFORMA deberá contemplar la posibilidad de que las refinanciaciones o reprogramaciones puedan estructurarse con o sin periodo de gracia, permitiendo configurar condiciones tales como:

   - Periodos de gracia para capital.
   - Periodos de gracia para intereses.
   - Modificación de tasas de interés.
   - Ampliación del plazo del crédito.

c. La PLATAFORMA deberá permitir el registro tanto operativo como contable de las operaciones de refinanciación, reprogramación y gestión de cobranza, incluyendo aquellas que se encuentren en etapa prejudicial o judicial. Dichos registros deberán realizarse en conformidad con las normativas y disposiciones regulatorias vigentes emitidas por la Superintendencia de Banca, Seguros y AFP (SBS), garantizando la adecuada clasificación del crédito, el registro de provisiones cuando corresponda y la trazabilidad de todas las modificaciones efectuadas sobre las condiciones del crédito.

d. La PLATAFORMA deberá contar con un módulo de generación y gestión de avisos de vencimiento, orientado a notificar oportunamente a los clientes sobre la proximidad o ocurrencia del vencimiento de sus obligaciones. Estos avisos deberán poder configurarse mediante plantillas parametrizables, permitiendo definir el contenido, formato y canales de envío (correo electrónico, impresión u otros canales habilitados por la entidad).

   Asimismo, la PLATAFORMA deberá mantener un control de versiones de las plantillas utilizadas, de modo que cada aviso emitido pueda ser asociado a la versión específica de la plantilla utilizada, garantizando la trazabilidad documental.

e. La PLATAFORMA deberá permitir realizar los cálculos de los montos a cobrar por concepto de intereses, considerando la moneda en la cual se encuentra denominado el crédito. Dentro de dichos cálculos se deberán contemplar, como mínimo los siguientes conceptos:

   - Cálculo del Impuesto General a las Ventas (IGV) aplicable al interés.
   - Cálculo de la detracción, cuando corresponda conforme a la normativa tributaria vigente.
   - Cálculo del monto total del interés por cobrar, incluyendo todos los componentes tributarios aplicables.

   La PLATAFORMA deberá garantizar que dichos cálculos se realicen de forma automática, precisa y conforme a la normativa tributaria vigente.

f. La PLATAFORMA deberá permitir la interconexión con el Sistema O7, el cual es utilizado para la generación de comprobantes de pago electrónicos, tales como facturas y boletas electrónicas.
Dicho sistema O7 mantiene la integración directa con la SUNAT, permitiendo la validación y emisión de comprobantes electrónicos conforme a los estándares establecidos por la administración tributaria. Como resultado del proceso de emisión, el sistema genera los archivos XML y PDF correspondientes a cada comprobante electrónico, los cuales deberán ser recepcionados o referenciados por la PLATAFORMA.

g. La PLATAFORMA deberá soportar el proceso de emisión de comprobantes electrónicos tales como facturas, boletas de venta, nota de crédito y notas de debido asociadas a las operaciones de cobranza, permitiendo su generación, registro y posterior envío a los clientes correspondientes. Asimismo, el sistema deberá permitir que dichos comprobantes electrónicos puedan ser remitidos a los clientes mediante los canales definidos por la entidad, tales como correo electrónico u otros medios digitales.

h. La PLATAFORMA deberá mantener un registro estructurado de todos los comprobantes electrónicos generadas, permitiendo su consulta, seguimiento y trazabilidad

Adicionalmente, la PLATAFORMA deberá permitir adjuntar o almacenar los archivos XML y PDF generados por el Sistema O7, asociándolos directamente a cada comprobante emitido.

Los comprobantes electrónicos, junto con sus respectivos archivos XML y PDF, deberán ser remitidos a cada Institución Financiera Intermediaria (IFI) correspondiente, asegurando la disponibilidad de la documentación para fines operativos, contables y de auditoría.

3.4.2.7.5 CONCILIACIÓN OPERATIVA VS INFORMACIÓN BANCARIA

La **Conciliación operativa vs información bancaria** es un procedimiento que asegura la exactitud y congruencia entre los movimientos bancarios by los datos que proporciona la operativa transaccional.

Este proceso implica cotejar las transacciones operativas y revisar los extractos bancarios. Así, se puede detectar errores o diferencias y tomar las medidas correctivas necesarias y asegurarse de que la información registrada sea precisa.

Realizar la **Conciliación operativa vs información bancaria** de una serie de beneficios significativos para el **FONDO:**

1) **Detección de errores y diferencias:** Comparar detalladamente los registros transaccionales financieros con los registros operativos internos permite identificar las diferencias, errores involuntarios o actividades fraudulentas.
2) **Exactitud en la información financiera**: La Conciliación operativa vs información bancaria ayuda a que la información operativa de **FONDO** sea confiable, evitando retrabajos, decisiones equivocadas y proporcionando una visión exacta de sus estados financieros.
3) **Control de flujos de efectivo**: Este proceso permite tener una visión detallada de las entradas y salidas de dinero, lo cual facilita la planificación y el control del efectivo.

4) **Gestión de cuentas por cobrar**: Contrastar los datos bancarios con los registros operativos permite comprobar si las facturas o cheques emitidos han sido efectivamente registrados, lo cual es sumamente útil para gestionar cuentas por cobrar.
5) **Toma de decisiones correctas**: Con una información operativa actualizada, los responsables de **FONDO** pueden tomar decisiones estratégicas basadas en datos reales.
6) **Ahorro de tiempo y recursos**: Detectar y corregir errores de manera oportuna ayuda a evitar problemas mayores y reduce el tiempo y recursos necesarios para resolverlos.
7) **Cumplimiento normativo**: La Conciliación operativa vs información bancaria es muy importante para llevar un registro exacto de las operaciones evitando sanciones de los organismos reguladores y de control.

Proceso de la Conciliación operativa vs información bancaria:
Llevar a cabo una Conciliación operativa vs información bancaria efectiva implica seguir una serie de pasos clave:
1) **Recolección de información**: Reúne todos los documentos relevantes, como estados de cuenta bancarios, cheques, recibos y facturas del periodo que se va a revisar.
2) **Identificación de errores y diferencias**: Revisa todas las transacciones y, si hay discrepancias, investigar su origen, ya que pueden deberse a errores de registro o a transacciones pendientes.
3) **Ajustes y correcciones**: Registra cualquier transacción faltante en los registros operativas según sea necesario y guarda un historial de los ajustes realizados para futuras referencias.
4) **Conciliación final**: Una vez realizados los ajustes, verifica nuevamente que los saldos coincidan y que toda la información esté completa y precisa.

Automatización de la Conciliación operativa vs información bancaria:
FONDO requiere automatizar la Conciliación operativa vs información bancaria mediante la PLATAFORMA. Estos programas deberán realizar el proceso en tiempo real, lo que ahorra tiempo y recursos al realizar conciliaciones automáticas y continuas. La automatización no solo incrementa la precisión y rapidez del proceso, sino que también garantiza la integridad de los registros operativos y facilita una gestión financiera eficiente.

La PLATAFORMA debe ser flexible y contar con funcionalidades específicas que permitan a las Instituciones Financieras (IFI) y al **FONDO** llevar un control detallado y preciso de todas las operaciones, así como generar los informes y reportes necesarios para cumplir con los requisitos regulatorios y operativos establecidos. A continuación, se describe de manera detallada las principales funcionalidades y procesos que la plataforma debe contemplar:

1) Cierre Diario y Mensual de los Saldos de los Productos MIVIVIENDA
Uno de los procesos fundamentales de la plataforma es el cierre diario y mensual de los saldos de los productos MIVIVIENDA. Esto implica la generación de varios reportes clave:

a) Reporte Diario de Desembolsos, Saldos y Recuperaciones:
Este reporte debe reflejar las operaciones realizadas durante el día, incluyendo los desembolsos de créditos, los saldos actuales y las recuperaciones de capital e intereses.

b) Reporte Mensual de Desembolsos, Saldos y Recuperaciones:
Similar al reporte diario, pero este debe compilar la información correspondiente a todo el mes.

c) Reporte de Validación de Información:

Este reporte tiene como finalidad validar la integridad y exactitud de los datos, garantizando que toda la información registrada sea coherente y esté correctamente consolidada.

d) Reporte de Saldos Operativos e Intereses:
A nivel diario y mensual, se debe generar un reporte detallado de los saldos operativos, los intereses devengados, los intereses por cobrar y los ingresos por recuperación de capital e intereses.

e) Generación de Asientos Contables:
A partir de la información anterior, la plataforma debe ser capaz de generar los asientos contables necesarios para la correcta contabilización de las operaciones.

f) Generación de Reportes Personalizados:
La PLATAFORMA debe permitir la creación de reportes a medida, según las necesidades específicas de los usuarios.

2) Conciliación de Saldos de Capital e Intereses

La conciliación de los saldos de capital e intereses es un proceso clave para garantizar que los registros sean precisos y estén alineados entre las IFI y el **FONDO**. Para ello, la plataforma debe:

a) Generar reportes detallados que muestren el saldo de capital y de intereses por cada producto y por cada IFI.
b) Elaborar un formato de **Acta de Conciliación** en formato correlativo, para su remisión y suscripción por parte de las IFI. Este proceso debe garantizar que todas las discrepancias sean resueltas y que los saldos finales sean acordados entre las partes.
c) Realizar la conciliación por **Producto**, **IFI** y **Moneda**, permitiendo una revisión detallada y específica de los saldos.

3) Conciliación Operativa y Contable

El proceso de conciliación operativa y contable debe realizarse diariamente, una vez que se hayan recibido los pagos y aplicados tanto por las IFI como por los clientes (subprestatarios). La PLATAFORMA debe:

a) Generar los reportes de conciliación operativa y contable, verificando que todas las transacciones estén correctamente registradas.
b) Contar con transacciones (trx) de pagos y pagos masivos, permitiendo que el Departamento de Operaciones Crediticias y Recuperaciones (AO) pueda validar las aplicaciones de pagos.
c) Generar reportes de cierre de mes para la conciliación, que incluyan un resumen de saldos por IFI, el total de clientes y los pagos no procesados.

La **Conciliación operativa vs información bancaria** es una herramienta esencial en la administración de las finanzas de **FONDO**, ya que permite detectar errores, prevenir fraudes y mantener un control exhaustivo de sus recursos financieros. Al realizar este proceso de manera regular y con precisión se puede asegurar la transparencia de sus registros y tomar decisiones informadas, garantizando así su competitividad y éxito en el mercado.

3.4.2.7.6 PROCESO DE SOLICITUD DE ACTIVACIÓN DE COBERTURA DE RIESGO CREDITICIO

La Cobertura del Riesgo Crediticio corresponde a un “Seguro” que FONDO otorga a las IFI para cubrir el deterioro de un crédito hipotecario otorgado una vez que el crédito hipotecario ha sido reportado como “perdida”.

1. **Activación:** Es el proceso mediante el cual se activa la Cobertura del Riesgo Crediticio asociada a un crédito hipotecario específico. A partir

de este momento, el crédito hipotecario se encuentra cubierto desde el momento en que se registra la partida registral de la garantía hipotecaria constituida A continuación detallamos los procesos de la activación de la CRC:

a) Recepción y Registro de Solicitudes

El primer paso en la activación de un CRC es contar con un check list que facilite la recepción y el registro de las solicitudes de activación remitidas por las Instituciones Financieras (IFI). Este check list debe asegurar que se incluyan todos los documentos requeridos según los reglamentos específicos de cada producto.

La PLATAFORMA permitirá extraer información con la base de garantías del último mes de cierre donde es necesario validar los campos siguientes:

- Estado de la Constitución de garantía
- Validar si cuenta con 1 o 2 tramos
- Validar si el cliente cuenta con crédito vigente o cancelado
- Validar si cuenta con retiro de CRC
- Fecha de desembolso de crédito

LA PLATAFORMA deberá tener la capacidad de carga y validación de expedientes

b) Envío de la Solicitud a la Gerencia Legal

Una vez que se han recibido los documentos y la solicitud de activación del CRC, esta debe enviarse a través del módulo correspondiente. Este módulo permite cargar los archivos digitales enviados por la IFI para su posterior revisión y validación por parte de la Gerencia Legal, quien se encargará de verificar que todo esté en conformidad con la normativa vigente.

c) Cálculo del Capital y Cronograma de Pago

La activación del CRC implica un proceso automatizado para el cálculo del capital que debe ser cubierto y la generación del cronograma de pagos de acuerdo con lo estipulado en el reglamento de cada producto. Este paso es crucial para establecer los plazos y montos a pagar, garantizando que se cumpla con las condiciones contractuales.

d) Activación del Crédito en Cobertura

Una vez que el cálculo del capital y el cronograma de pagos han sido validados, se procede a activar el crédito en cobertura, lo que habilita su inclusión en la plataforma de cobranza mensual correspondiente. De esta manera, el crédito queda registrado como "vigente" y se inicia el proceso de cobranza.

e) Reversión de la Cobertura y Reanudación del Crédito

La PLATAFORMA debe contar con una opción que permita la reversión de la cobertura y la reanudación del crédito en caso de ser necesario. Esta acción se realiza mediante la actualización del calendario de pagos de la IFI, lo que garantiza la correcta reprogramación del crédito.

f) Informe de Estado de Solicitud

También se debe disponer de una opción para enviar a la IFI una carta que detalle el estado de la solicitud de cobertura. Este documento sirve como una herramienta de comunicación que informa a la IFI sobre el avance y la resolución de su solicitud.

2. **Liquidación de CRC Activado:** Es el proceso de ejecutar la Cobertura del Riesgo Crediticio. A continuación, detallamos el proceso de liquidación de la CRC:

    1. **Recepción de Solicitud de Liquidación**
    Cuando se realiza el remate judicial de un inmueble, la IFI puede solicitar la liquidación del CRC correspondiente. Esta solicitud debe ser recibida por el FMV (Fondo de Mitigación de Riesgos) para proceder con la cancelación de la deuda pendiente en el calendario CRC.

    2. **Validación de Gastos Judiciales**
    A continuación, los documentos relacionados con los gastos judiciales, enviados por la IFI, deben ser remitidos a la Gerencia Legal para su revisión y conformidad. Esto asegura que todos los gastos relacionados con el proceso judicial sean debidamente validados antes de proceder con la liquidación.

    3. **Cálculo del Monto a Cargar a la IFI**
    El siguiente paso consiste en sistematizar el cálculo del monto total que se debe cargar a la IFI. Este monto incluye no solo el capital adeudado, sino también los intereses y las penalidades, si las hubiera. Este cálculo debe ser preciso para evitar discrepancias en los pagos y garantizar la correcta liquidación del crédito.

    4. **Notificación a la IFI**
    Una vez que el monto a cargar ha sido determinado, se informa a la IFI sobre el monto a abonar o cargar, así como la fecha de ejecución de la cobranza. Esta comunicación puede realizarse de manera electrónica o física, dependiendo de los procedimientos internos establecidos.

    5. **Generación de Asientos Contables**
    La PLATAFORMA debe generar los asientos contables correspondientes a la cobranza realizada, lo que facilita el seguimiento y registro de los movimientos financieros asociados a la liquidación del CRC.

    6. **Verificación de Movimientos del Día**
    Finalmente, es necesario realizar una verificación de los movimientos contables del día, asegurando que todas las transacciones relacionadas con la liquidación del CRC se hayan registrado correctamente y que no haya errores en los procesos contables.

De acuerdo con lo remitido por GL en la validación de cada cliente, la PLATAFORMA deberá realizar un cruce con la base de provisiones y debe mostrar el tipo de cobertura (CRC – CRCA – Pgmin) considerando:

- Factor de Cobertura
- Factor de Cobertura Total

La PLATAFORMA deberá tener un registro de los seguros de Riesgo Crediticio otorgados (CRC – CRCA – Pgmin) para permitir realizar el seguimiento y control de estos, así como su respectivo reflejo contable, indicando el estado de la activación por IFI, por cliente.

La plataforma, no permitirá el cierre operativo de ninguno de los módulos sin que haya pasado previamente la validación y conciliación de saldos operativos versus saldos contables, generándose un reporte. Luego de la validación cada

área operativa podrá realizar la migración de la data al sistema de contabilidad (SIGA).

La plataforma deberá emitir los siguientes reportes operativos:

FIDEICOMISO COFIDE - REPORTES OPERATIVOS VIGENTE EN EL SAOC

1. Reporte de conciliación de saldos de saldos operativos versus saldos contables. Este reporte, sirve adicionalmente como un validador y debe generarse antes del envío de la información operativa al sistema de contabilidad (SIGA).
2. Detalle y consolidado por programas Anexo T+1-30.06.25
3. Detalle y consolidado por programas de datos a fin de mes-30.06.25
4. Detalle y consolidado por programas formato Líneas 30.06.2025
5. Detalle y consolidado por programas plantillaCarteraConvertida1-30.06.25
6. Detalle y consolidado por programas plantillaCobranzaProyectada1-30.06.25
7. Detalle y consolidado por programas plantillaCreditosVigentes1-30.06.25
8. Detalle y consolidado por programas plantillaTransferenciaBBP-BBP-BMS1-30.06.25
9. Detalle y consolidado por programas plantillaValidacionCOFIDE1-30.06.25
10. DETALLE Y CONSOLIDADO POR PROGRAMAS PREPAGOS MIVIVIENDA III-GF CONVENIO LAIF - 30.06.25
11. DETALLE Y CONSOLIDADO POR PROGRAMAS RECUPERACIONES MENSUAL
12. Detalle y consolidado por programas ReporteAnexos1-30.06.25
    a. Detalle y consolidado por programas saldo de capital
    b. Detalle y consolidado por programas saldo de interés por cobrar
    c. Detalle y consolidado por programas ingreso devengado del interés
    d. Detalle y consolidado por programas ingreso devengado del interés T+1
    e. Detalle y consolidado por programas de intereses en suspenso
13. Detalle y consolidado por programas ReporteBalanceSectorial1-30.06.25
14. Detalle y consolidado por programas ReporteComparativo1-30.06.25
15. Detalle y consolidado por programas ReporteDuplicados-30.06.25
16. Detalle y consolidado por programas ReporteVerInteresDevengado1-30.06.25
17. Detalle y consolidado por programas Saldo FID COFIDE- 30.06.25
18. DETALLE Y CONSOLIDADO POR PROGRAMAS SALDOS POR CONVENIOS CERRADOS MVCS-30.06.25
19. DETALLE Y CONSOLIDADO POR PROGRAMAS SALDOS POR CONVENIOS VIGENTES- SIAF-30.06.25
20. ANEXO 1.1 - REPORTE DE MOVIMIENTOS DE DESEMBOLSOS Y RECUPERACIONES MENSUAL (POR PROGRAMAS)
21. ANEXO 2.1 - REPORTE DE PREPAGOS MENSUAL (POR PROGRAMAS)
22. ANEXO 5 - REPORTE DE EXTORNO MENSUAL (POR PROGRAMAS)
23. ANEXO 6 - REPORTE DE AJUSTE MENSUAL (POR PROGRAMAS)
24. ANEXO 8 - REPORTE CONSOLIDADO DE LOS PROGRAMAS DE MVV POR TRAMOS
25. ANEXO 9 - REPORTE DE SALDOS POR TRAMO DETALLADO (POR PROGRAMAS)
26. INSUMOS PARA LA GENERACIÓN DEL BALANCE SECTORIAL
27. ANEXO 11 - REPORTE DE REPROGRAMACIÓN Y REFINANCIACIÓN DE DEUDA
    a. INTERESES CAPITALIZADOS MENSUAL

b. REPROGRAMACIONES DEL MES DE JUNIO

28. REPROGRAMADOS:
    a. DETALLE Y CONSOLIDADO POR PROGRAMAS DEL SALDO DE CAPITAL REPROGRAMADO.
    b. DETALLE Y CONSOLIDADO POR PROGRAMAS QUE SUSTENTE EL NACIMENTO DEL INGRESO DIFERIDO
    c. DETALLE Y CONSOLIDADO POR PROGRAMAS DEL SALDO DEL DIFERIDO
    d. DETALLE Y CONSOLIDADO POR PROGRAMAS DEL DEVENGADO DEL DIFERIDO

La plataforma deberá emitir los siguientes reportes operativos:

CARTERA DE CREDITOS- REPORTES OPERATIVOS

1. Reporte de conciliación de saldos de saldos operativos versus saldos contables. Este reporte, sirve adicionalmente como un validador y debe generarse antes del envío de la información operativa al sistema de contabilidad.
2. Reporte de saldo de capital (detallado por cliente, sub totalizado por tipo de crédito)
3. Reporte de saldo de intereses por cobrar (detallado por cliente, tipo de crédito, sub totalizado por moneda)
4. Reporte de pase de vigente a vencido (detallado por cliente, tipo de crédito, sub totalizado por moneda)
5. Reporte de interés devengado del mes (detallado por cliente, tipo de crédito, sub totalizado por moneda)
6. Reporte de movimientos del mes (detallado por cliente, moneda y sub totalizado por tipo de crédito)
7. Reporte del devengado y diferido del saldo de capital (detallado por cliente, moneda y sub totalizado por tipo de crédito)
8. Reporte del devengado y diferido refinanciado (detallado por cliente, moneda y sub totalizado por tipo de crédito)
9. Reporte de la aplicación del Premio del Buen Pagado (PBP)
10. Reporte de ingresos por intereses del periodo (detallado por cliente, tipo de crédito y sub totalizado moneda)
11. Reporte de intereses en suspenso y cobranza judicial periodo (detallado por cliente, tipo de crédito y sub totalizado moneda)
12. Reporte de gastos de PBP del periodo (detallado por cliente, tipo de crédito y sub totalizado moneda)
13. Reporte de saldos de las garantías (detallado por cliente, movimiento del mes, tipo de crédito, y sub totalizado por moneda)
14. Reporte de movimientos y saldo del capital por pase de vigente a vencido, vencido a judicial o viceversa (por tipo de cartera, reclasificación)
15. Reporte de movimientos y saldo del diferido por pase de vigente a vencido, vencido a judicial o viceversa (por tipo de cartera, reclasificación)
16. Reporte de interés moratorio (detallado por cliente, tipo de crédito y sub totalizado moneda)
17. Reporte de comisión (detallado por cliente, tipo de crédito y sub totalizado moneda)
18. Reporte de seguro (detallado por cliente, tipo de crédito y sub totalizado moneda)
19. Reporte de reprogramaciones con periodo de gracia
20. Reporte de reprogramaciones sin periodo de gracia

21. Reporte de refinanciamientos con periodo de gracia (con o sin condonación de intereses / con o sin exoneración de intereses moratorios, u otros casos)
22. Reporte de refinanciamientos sin periodo de gracia (con o sin condonación de intereses / con o sin exoneración de intereses moratorios, u otros casos)
23. Reporte de cancelación de vencidos
24. Reporte de reprogramación por facilidades de pagos (detallado por clientes, sub totalizado por moneda)
25. Reporte de reprogramaciones por estado de emergencia – capital cuentas de orden
26. Reporte de reprogramaciones por estado de emergencia – intereses devengado cuentas de orden
27. Reporte de reprogramaciones por estado de emergencia – intereses percibido cuentas de orden
28. Reporte de intereses moratorios condonados (detallado por cliente, tipo de crédito y sub totalizado por moneda)
29. Reporte de intereses moratorios devengados (detallado por cliente, tipo de crédito y sub totalizado por moneda)
30. Reporte de saldo y movimiento del mes de la provisión de incobrabilidad (por tipo de provisión, sub totalizado por moneda)
31. Reporte de Incorporación de Clientes de cartera de Créditos (Detallado por cliente, clasificación de cartera, diferido entre saldo colocado u adeudo y sub totalizado por moneda).
32. Reporte de Provisión de Incobrabilidad de la cartera de crédito por genérica y especifica.
33. Reporte de Recuperaciones Mensuales
34. Reporte de Aplicación Mensual de PBP.
35. Reporte de Cancelaciones Mensuales
36. Reporte de Reprogramaciones y Refinanciaciones Mensuales
37. Reporte de Provisiones de la cartera FDI
38. Reporte Comparativo de Provisiones para la Reserva Legal

A partir de la información anterior, la plataforma debe ser capaz de generar los asientos contables necesarios para la correcta contabilización de las operaciones.

La plataforma deberá emitir los siguientes reportes operativos:

OTRAS CUENTAS POR COBRAR:

CARTERA EXCONEMINSA- REPORTES OPERATIVOS

1. Reporte de Abonos por identificar, por entidad bancaria y moneda
2. Reporte de Cobranza diaria, por fecha y entidad bancaria
3. Reporte de Intereses Devengado de la cartera vigente
4. Reporte de Rendimientos en Suspenso
5. Reporte de Interés Compensatorio SPAD (Detallado mensual por cliente y sub totalizado por moneda)
6. Reporte de Seguros SPAD (Detallado mensual por cliente y sub totalizado por moneda)
7. Reporte de Interés Moratorio (Detallado mensual por cliente y sub totalizado por moneda)
8. Reporte de Diferido por refinanciamientos (Detallado por cliente, mes y año y sub totalizado por moneda)

9. Reporte de saldo de Capital Cartera EXCONEMINSA (Detallado por cliente, capital vigente y vencido así como sub totalizado por moneda)
10. Reporte de saldo de Capital Cartera EXCONEMINSA JUDICIAL (Detallado por cliente, capital vigente y vencido así como sub totalizado por moneda)
11. Reporte de saldo de Capital Cartera SPAD (Detallado por cliente, capital vigente y vencido así como sub totalizado por moneda)
12. Reporte de saldo de Capital Cartera SPAD JUDICIAL (Detallado por cliente, capital vigente y vencido así como sub totalizado por moneda)
13. Reporte de saldo insoluto
14. Reporte de Sustento de identificación de cobros (Detallado por cliente y aplicación de cobro (Capital+interés compensatorio+seguro+interés motarorio+seguros+portes).
15. Reporte de Provisión de incobrabilidad de la cartera EXCONEMINSA
16. Emisión de comprobante electrónico por el cobro de los intereses devengados a través del sistema O7.

A partir de la información anterior, la plataforma debe ser capaz de generar los asientos contables necesarios para la correcta contabilización de las operaciones.

IFIS EN LIQUIDACION – REPORTES OPERATIVOS

1. Reporte de Saldo por Cobrar por IFIS en Liquidación Banco Nuevo Mundo y Banco Republica

2. A partir de la información anterior, la plataforma debe ser capaz de generar los asientos contables necesarios para la correcta contabilización de las operaciones.

La PLATAFORMA debe permitir:

A. Permitir a las Instituciones Financieras Intermediarias (IFI) administradoras de la Cartera Directa acceder a la PLATAFORMA mediante perfiles de usuario debidamente autorizados, con el fin de conectarse y realizar la carga estructurada de información operativa relacionada con la gestión de la cartera. Esta funcionalidad deberá permitir, entre otros aspectos:

   La carga periódica de reportes de recaudación, detallando los pagos efectuados por los subprestatarios, fechas de abono, montos aplicados, canales de pago utilizados y créditos asociados. La carga de reportes de gestión de cobranza, incluyendo el estado de los créditos, acciones de cobranza realizadas y evolución del comportamiento de pago de los clientes.El registro y tratamiento de facilidades de pago otorgadas a los subprestatarios, tales como:

   - Reprogramaciones de créditos.
   - Refinanciaciones de deuda.
   - Exoneración parcial o total de intereses moratorios.
   - Otorgamiento de periodos de gracia u otras condiciones especiales.

La PLATAFORMA deberá garantizar que la información cargada sea validada automáticamente, registrada y vinculada a cada operación crediticia correspondiente, asegurando la integridad, consistencia y trazabilidad de los datos registrados.

B. Permitir a las IFI que administran cartera del programa Mivivienda dentro del Fideicomiso COFIDE cargar, actualizar y mantener en la PLATAFORMA la información relevante de los créditos hipotecarios correspondientes a los subpréstamos otorgados.Dicha funcionalidad deberá permitir registrar y actualizar, como mínimo, los siguientes elementos:

- Cronogramas de pago de los subpréstamos, incluyendo fechas de vencimiento, cuotas, capital, intereses y demás componentes de cada cuota.
- Saldos actualizados de capital e intereses de cada operación crediticia.
- Calificación de riesgo crediticio asignada al cliente conforme a los criterios establecidos por la normativa vigente y las políticas de gestión de riesgo.
- Estado de las garantías asociadas a los créditos, incluyendo información de las garantías hipotecarias, su vigencia, situación registral y cualquier actualización relevante.

La PLATAFORMA deberá permitir realizar validaciones automáticas de consistencia de la información cargada, así como mantener un historial de modificaciones realizadas sobre los datos de cada crédito.

C. Implementar un módulo de seguimiento (tracking) y gestión de solicitudes, consultas y reclamos ingresados por los diferentes canales de atención utilizados por el Fondo MIVIVIENDA S.A., incluyendo:

- El buzón creditostfc@mivivienda.com.pe
- El buzón solicitudescarteradirecta@mivivienda.com.pe
- El Sistema de Gestión Documentaria (SGD)

Este módulo deberá permitir:

- Registrar automáticamente las solicitudes o reclamos recibidos.
- Asignar un número único de seguimiento a cada caso.
- Gestionar el flujo de atención, derivación y respuesta a las áreas responsables.
- Mantener el historial de acciones realizadas durante el proceso de atención.

Asimismo, la PLATAFORMA deberá permitir generar reportes estadísticos y de gestión, tales como:

- Número de solicitudes atendidas por periodo.
- Tiempos promedio de atención.
- Tipología de solicitudes o reclamos.
- Nivel de cumplimiento de plazos de respuesta.

D. Permitir la carga, administración, actualización y mantenimiento del cronograma de pagos correspondiente a cada cliente o subprestatario, asegurando que la PLATAFORMA registre correctamente todas las condiciones financieras y contractuales asociadas a la operación crediticia.La PLATAFORMA deberá garantizar:

- La correcta parametrización de fechas de vencimiento, número de cuotas, montos de capital, intereses y cargos asociados.
- La actualización automática de saldos pendientes y estados de pago conforme a las operaciones registradas.
- La posibilidad de registrar modificaciones derivadas de reprogramaciones, refinanciaciones u otros ajustes contractuales.

Asimismo, la PLATAFORMA deberá mantener un registro histórico de todas las modificaciones efectuadas sobre el cronograma, permitiendo la trazabilidad completa de los cambios realizados, incluyendo fecha, usuario responsable y motivo de la modificación.

E. Permitir el registro, monitoreo y gestión de operaciones relevantes dentro del Sistema de Prevención de Lavado de Activos y Financiamiento del Terrorismo (SPLAFT), en cumplimiento de las disposiciones regulatorias aplicables.La PLATAFORMA deberá permitir:

- Registrar operaciones consideradas inusuales o relevantes conforme a los parámetros definidos por la entidad.
- Integrar mecanismos de alertas automáticas basadas en reglas, umbrales de monto o patrones de comportamiento previamente configurados.
- Mantener un historial detallado de las operaciones evaluadas o reportadas.

Asimismo, la PLATAFORMA deberá asegurar la trazabilidad completa de las operaciones registradas en el módulo SPLAFT, facilitando la generación de reportes y la atención de requerimientos regulatorios o de auditoría.

F. Generar de manera automática y periódica los estados de cuenta correspondientes a los créditos hipotecarios administrados, reflejando la situación actualizada de cada operación crediticia.

Estos estados de cuenta deberán incluir, como mínimo:

- Saldo de capital pendiente.
- Intereses generados.
- Pagos realizados.
- Cuotas vencidas o por vencer.
- Detalle del cronograma vigente.

Asimismo, la PLATAFORMA deberá permitir efectuar el cálculo de liquidaciones totales o parciales de los créditos, considerando los intereses generados a la fecha de cálculo y las condiciones contractuales aplicables.

Los estados de cuenta y liquidaciones generadas deberán estar disponibles para descarga en formato digital y para su envío al cliente a través de los canales definidos por la entidad.

G. Implementar mecanismos de validación automática posterior al cierre operativo, con el fin de verificar la inexistencia de deuda pendiente asociada a un crédito hipotecario. Una vez validado que el crédito ha sido cancelado en su totalidad y que no existen saldos pendientes, la PLATAFORMA deberá permitir la emisión automática de la constancia de no adeudo correspondiente.
El sistema deberá registrar:

- La fecha de emisión del documento.

- El usuario o área responsable de la validación.
- La referencia del crédito asociado.

Asimismo, deberá garantizar la trazabilidad y almacenamiento del documento emitido para fines de consulta, auditoría o requerimientos del cliente.

H. Permitir el registro de la activación de los seguros asociados a cada operación crediticia, tales como seguros de desgravamen, seguros de incendio u otras coberturas vinculadas al crédito hipotecario.

La PLATAFORMA deberá permitir:

- Registrar la fecha de activación del seguro.
- Identificar la compañía aseguradora correspondiente.
- Controlar la vigencia y cobertura de las pólizas.
- Mantener actualizada la información de las pólizas vinculadas a cada crédito.

Asimismo, el sistema deberá permitir la integración de esta información con los módulos de administración de cartera y facturación, con el fin de asegurar la correcta gestión de los cargos asociados a los seguros.

I. Permitir el cálculo automático de las comisiones correspondientes a las IFI administradoras de la cartera, conforme a las condiciones establecidas en los contratos o convenios de administración vigentes.La PLATAFORMA deberá:

- Aplicar las reglas de cálculo definidas contractualmente.
- Validar la correcta aplicación de las comisiones en función de la cartera administrada o la recaudación obtenida.
- Generar los reportes de cálculo correspondientes.

Adicionalmente, el sistema deberá permitir la generación automática de los registros contables asociados a dichas comisiones, asegurando su correcta imputación en el sistema contable.

J. Permitir la revisión integral de la información de cartera correspondiente a cada periodo operativo, previo al cierre operativo mensual.

Este proceso deberá incluir:

- La validación de los totales de cartera.
- La consistencia entre los registros operativos y contables.
- La verificación de saldos, recaudaciones, movimientos y actualizaciones registradas durante el periodo.

Una vez realizadas las validaciones correspondientes, el sistema deberá permitir efectuar la aprobación final del cierre operativo mensual, registrando el usuario responsable y la fecha de aprobación.

K. Permitir la consolidación automática de los principales indicadores clave de desempeño (KPIs) relacionados con la gestión de la cartera, con el fin de facilitar el seguimiento operativo y la toma de decisiones.Entre los indicadores que la PLATAFORMA deberá generar se encuentran, entre otros:

- Niveles de morosidad de la cartera.
- Índices de recaudación.
- Evolución de la cartera vigente y vencida.

- Volumen de refinanciaciones o reprogramaciones.
- Gestión de cobranza.

Asimismo, el sistema deberá permitir la generación automática de reportes de gestión en diferentes formatos, facilitando su análisis por parte de las áreas responsables.

L. Permitir la emisión automática de las declaraciones correspondientes a los seguros asociados a las operaciones crediticias, tales como los seguros de desgravamen y seguros de incendio. La PLATAFORMA deberá asegurar que dichas declaraciones se generen con base en:

- La información actualizada de la cartera de créditos.
- La vigencia de las pólizas de seguro.
- Las condiciones contractuales establecidas con las compañías aseguradoras.

Asimismo, el sistema deberá garantizar la consistencia de la información declarada con los registros de cartera, permitiendo la generación de reportes y el envío de la información a las entidades aseguradoras correspondientes.

3.4.2.7.7 INFORMES NORMATIVOS

La PLATAFORMA deberá tener un módulo que procese y genere en forma automática todos los informes y anexos normativos exigidos por las entidades reguladoras del Mercado Financiero Peruano.

Los informes y Anexos que deberán ser generados en forma automática son los siguientes:

a) **Anexo 5:** El Anexo 5 de la SBS es un documento que considera el total de créditos directos e indirectos de una empresa, según la clasificación del deudor.
   Para la elaboración del Anexo 5, se debe incluir la información del monto del capital de los créditos directos y el equivalente a riesgo crediticio de los créditos indirectos.
   En el caso de que el deudor tenga responsabilidad con una misma empresa en diversas modalidades de crédito, la clasificación del deudor se basará en la modalidad que tenga la categoría de mayor riesgo.
b) **Cuadre del Anexo 5:** El cuadre del Anexo 5 de la SBS (Superintendencia de Banca y Seguros) considera el total de créditos directos e indirectos de una empresa, según la clasificación del deudor. Para elaborar el Anexo 5, se debe incluir la información del monto del capital de los créditos directos e indirectos, sin considerar los intereses y comisiones devengados.
c) Anexo 6: Reporte Crediticio de Deudores (RCD)
d) **Reporte 2-A1 I:** El reporte 2-A1 de la SBS es el reporte de "Activos y Contingentes Ponderados por Riesgo de Crédito – Método Estándar". La Resolución S.B.S. Nº 1088-2024 modificó el Reglamento para el Requerimiento de Patrimonio Efectivo por Riesgo de Crédito, el Reporte N° 2-A1 y el Reporte N° 3 “Patrimonio Efectivo” del Capítulo V del Manual de Contabilidad
e) **Reporte 2-A1 II:** El Reporte 2-A1 de la SBS es un reporte de Activos y Contingentes Ponderados por Riesgo de Crédito, que se realiza mediante el Método Estándar. En este reporte se deben incluir:
   - Exposiciones brutas, incluyendo los rendimientos devengados
   - Provisiones específicas
   - Ingresos diferidos
   - Pérdida por deterioro acumulada
   - Depreciación acumulada

- Amortización acumulada

f) **Reporte 2-A1 III:** El reporte 2-A1-III de la SBS es una distribución por tipos de exposiciones que se realiza de manera mensual. En el reporte 2-A1-III se debe reportar el total de exposiciones ajustadas ponderadas por riesgo de crédito y el requerimiento total de patrimonio efectivo por riesgo de crédito.

g) **Reporte 2-B1 Anexo 1-A**: El reporte 2-B1 Anexo 1-A de la SBS es un método estándar para calcular el requerimiento de patrimonio efectivo por riesgo de tasa de interés en la cartera de negociación. Para calcular el requerimiento de patrimonio efectivo, se debe estimar previamente la duración de Macaulay y la Duración Modificada para cada instrumento. El reporte 2-B1 Anexo 1-B se utiliza para presentar el cálculo del requerimiento de patrimonio efectivo.

h) **Reporte 2-B1 Anexo 1-C:** El reporte 2-B1 Anexo 1-C de la SBS es un método estándar que resume el requerimiento de patrimonio efectivo por riesgo de tasa de interés en la cartera de negociación. El cálculo del requerimiento de patrimonio efectivo requiere la estimación de la Duración de Macaulay y la Duración Modificada para cada instrumento.

i) **Reporte 2-B1 Anexo 3 I:** El reporte 2-B1 Anexo 3 de la SBS es un reporte mensual que se denomina "Método Estándar - Requerimiento de Patrimonio Efectivo por Riesgo Cambiario". El plazo para presentar este reporte es de 15 días calendario después de que finalice el mes al que corresponde la información.

   Para registrar las posiciones en el reporte 2-B1 Anexo 3, se debe:
   - Determinar si cada posición es larga o corta.
   - Expresar el registro de las posiciones en divisas en nuevos soles.
   - Utilizar el tipo de cambio contable correspondiente a la fecha del reporte.
   - Tratar los forward y futuros de monedas como dos posiciones.

j) **Reporte 2-B1 Anexo 3 II:** El reporte 2-B1 Anexo 3 de la SBS es un documento que se presenta para cumplir con el requerimiento de patrimonio efectivo por riesgo cambiario. Se debe presentar en un plazo de 15 días calendario después de que termine el mes al que corresponde la información. Para registrar las posiciones en el reporte 2-B1 Anexo 3, se debe determinar si cada una es larga o corta, de acuerdo con la posición que se asuma frente al activo subyacente. En el caso de los forward y futuros de monedas, se deben tratar como dos posiciones: una en la moneda que se recibe (posición larga) y otra en la moneda que se entrega (posición corta).

k) **Reporte 2-B1 Anexo 1-B-A:** El reporte 2-B1 Anexo 1-B-A de la SBS es un documento que registra posiciones de determinados instrumentos financieros en diferentes bandas temporales. Este reporte tiene dos secciones: una en moneda nacional y otra en moneda extranjera. Para registrar las posiciones en moneda nacional, se deben considerar los instrumentos en nuevos soles indexados a la inflación (VAC). En la sección de moneda extranjera, se deben considerar las posiciones sujetas a tasas flotantes en moneda extranjera. Para cada posición, se debe determinar si es larga o corta, de acuerdo con la posición que se asuma frente al activo subyacente.

l) **Reporte 2-B1 Anexo 1-B-B:** El reporte 2-B1 Anexo 1-B de la SBS es un método estándar para determinar el requerimiento de patrimonio efectivo por riesgo de tasa de interés en la cartera de negociación. Este reporte tiene una sección en moneda nacional y otra en moneda extranjera. En la sección de moneda nacional, se deben considerar las posiciones en instrumentos en nuevos soles indexados a la inflación (VAC). En la sección de moneda extranjera, se deben considerar las posiciones sujetas a tasas flotantes. Para cada posición, se debe determinar si es larga o corta, de acuerdo con la posición que se asuma frente al respectivo activo subyacente.

m) **Reporte 2-C1:** El reporte 2-C1 de la SBS es el Requerimiento de Patrimonio Efectivo por Riesgo Operacional, utilizando el método del Indicador Básico.
n) **Reporte 4-A1:** El reporte 4-A1 de la SBS es un requerimiento de patrimonio efectivo adicional por ciclo económico para empresas que aplican el método estándar. El reporte 4-A1 debe presentarse de acuerdo con la planilla definida por la SBS, y el orden de presentación es primero un registro de cabecera. Algunos de los datos que se incluyen en el reporte 4-A1 son: Ponderadores, Exposiciones directas ajustadas, Exposiciones contingentes, Factores de ponderación marginales.
o) **Reporte 4-B1:** El reporte 4-B1 de la Superintendencia de Banca y Seguros (SBS) es el documento que solicita el patrimonio efectivo por riesgo de concentración crediticia individual. Para presentar el reporte 4-B1, se debe seguir la planilla definida por la SBS. El orden de presentación es:
    - Primero, un registro de cabecera
    - Luego, todos los registros de detalle que sean necesarios para contener los datos a informar

  La Resolución S.B.S. N° 2467-2023 modificó los formatos de los reportes 4-B1, 4-B2, 4-B3, 4-C y 4-D.
p) **Reporte 4-B2:** Requerimiento de Patrimonio Efectivo por Riesgo por Concentración Sectorial
q) **Reporte 4-B3**: Reporte N° 4-B3, que es el requerimiento de patrimonio efectivo por riesgo por Concentración Regional.
r) **Reporte 4-C:** El reporte 4-C de la SBS es el Requerimiento de Patrimonio Efectivo por Riesgo de Tasa de Interés en el Libro Bancario (Banking Book).
s) **Reporte 4-D:** Resumen de requerimientos patrimoniales
t) **Reporte 4-E:** El Reporte N° 4-E de la SBS es un documento que contiene información para calcular el Indicador de Riesgo por Concentración de Mercado. Se encuentra en el Capítulo V del Manual de Contabilidad de la Superintendencia de Banca, Seguros y AFP (SBS).
u) **Reporte 4-F:** El Reporte 4-F de la SBS es un resumen del requerimiento de colchones de conservación, por ciclo económico y por riesgo por concentración de mercado. Se incorporó mediante la Resolución SBS N° 3953-2022, publicada el 27 de diciembre de 2022. El reporte 4-F se expresa en soles y muestra el componente, el requerimiento de colchón en porcentaje y el monto en soles.
v) **Formato 0102 / Anexo 02:** Créditos Directos según Tipo de Garantía
w) **Formato 0103 / Anexo 03:** Stock y Flujo Crediticio por Tipo de Crédito y Sector Económico.
x) **Formato 0110 / Anexo 01:** Colocaciones de la cartera de Créditos Directos.
y) **Formato 0214 / Reporte 14:** Créditos según día de Incumplimiento de la cartera de Créditos Directos
z) **Formato 0225 / Anexo 01:** Monto de la Cartera Directa Transferida en el mes según Tipo Y Situación de Cartera
aa) **Formato 0235 / Anexo 01:** Créditos Reprogramados: Emergencia Nacional Covid-19
bb) **Reporte R 36:** Detalle por Operación de la Cartera de Créditos Directos
cc) **Reporte 29:** El Reporte 29 de la SBS, también conocido como Formato 0229, es el Reporte de Grupos Económicos Deudores.

3.4.2.7.8 SERVICIO CRC (IMPLEMENTANDO EN EL SAOC)

La PLATAFORMA deberá tener un módulo que procese y genere en forma automática todas las solicitudes por parte de las IFI's:

- Plataforma única para recibir solicitudes.
- Validación automática de Excel y anexos.
- Cruce automático entre documentos.

- Seguimiento automático del estado.
- Eliminación del envío por correo.

a) **Fase 1 — Portal de recepción de solicitudes:**
Crear un portal web para IFI o SFTP que permitirá almacenar todos los expedientes presentados.

La IFI: - Ingresa al portal - Carga plantilla Excel F1 - Sube expedientes (PDF o carpetas) - Envía solicitud.

b) **Fase 2 — Motor de validaciones automáticas:**
Se construye un módulo que revise automáticamente:

- Validaciones del Excel
- Campos obligatorios llenos.
- Formato correcto.
- Grado sostenible válido asociado con el proyecto.
- Montos y subsidios coherentes.

Cruces automáticos
El sistema consulta la Base de proyectos registrados – Datos del cliente (actuales como históricos)

c) **Fase 3 — Validación automática de expedientes:**
El sistema revisa documentos subidos:

Validaciones posibles
- DNI coincide con Excel.
- Nombres coinciden.
- Formularios completos.
- Presencia de firmas.
- Documentos obligatorios cargados.

Esto puede hacerse con:
- Lectura automática de documentos.
- Validación por campos estructurados.

d) **Fase 4 — Flujo automático de estados:**
- Notificación automática a IFI
- Registro interno

e) **Fase 5 — Integración con sistemas existentes:**
El nuevo sistema se conecta a:

Sistema	**Para qué**
SAOC	Validaciones actuales
OneDrive/ SFTP	Expedientes
Base proyectos	Validaciones

f) **Fase 6 — Panel de control:**
Permite ver:

- Solicitudes por día
- Tiempos de atención
- Observaciones frecuentes
- Estado por IFI
- Carga de trabajo

3.4.2.7.9 FIDECICOMISO SERVICIO CRC-PBP

La plataforma deberá tener un módulo que permita la administración de los créditos del Fideicomiso CRC-PBP en Moneda Nacional y Moneda extranjera, colocados entre el 2006 y 2009. Estos créditos fueron desembolsados bajo el esquema de los 2 tramos: Concesional y No Concesional.

a. Recepción de solicitudes:

Las Instituciones financieras (IFI) podrán presentar las solicitudes de modificación de calendarios: prepago total, prepago con reducción de monto en cuota, prepago con reducción de plazo, prepago total o cancelación anticipada, refinanciación y recalendarización. También podrán presentar solicitudes de activación de Cobertura o Liquidación de CRC.

Las solicitudes que incluyan cambios en los cronogramas deberán tener la opción de carga del nuevo calendario no concesional a su vez permitir que el FMV genere el cronograma concesional. Los archivos por recibir de la IFI en este punto se denominan: CNC – Cabecera y CNC – Detalle y el archivo a enviar por parte del FMV se denomina CC, los 3 archivos presentan formatos establecidos según reglamento

b. Perfiles:

El módulo debe contemplar que exista para las aprobaciones preliminares de las solicitudes descritas en el punto anterior, un perfil de **Evaluador,** y para el aprobador final un perfil de **Supervisor**. Cada perfil con su respectiva bandeja direccionada a los usuarios designados para ambos perfiles. Cabe mencionar que el registro de las solicitudes puede ser realizado por ambos perfiles o de ser el caso incluir un tercer perfil de menor acceso para la recepción (ingreso) de las mismas y/o consultas de estado de crédito. Asimismo, deberá presentar un perfil para el abogado revisor de las solicitudes de activación de Cobertura dentro de la gerencia legal.

c. Cierre Operativo:

El módulo debe permitir la carga de los archivos que las IFI envían mensualmente, correspondiente a las cuotas canceladas de los créditos vigentes en el Fideicomiso, estas se verán reflejadas en la disminución del saldo capital en su tramo no concesional (frecuencia mensual). Cabe indicar que el módulo permite la carga únicamente de cuotas vencidas a la fecha de carga. El archivo a recibir por parte de la IFI en este punto se denomina: Pago de Cuotas el cual presenta un formato establecido según reglamento.

Asimismo, deberá realizar el cálculo de la cobranza de las comisiones CRC y PBP para cuota vencida en el mes de cierre, y a su vez realizar el cálculo del otorgamiento de los pagos del Premio al Buen Pagador (PBP), estos últimos se verán reflejados en la disminución del saldo capital en su tramo concesional (frecuencia semestral) de acuerdo a la condición del cliente, si es buen pagador lo asume el FMV y si es mal pagador lo asume el cliente.

El detalle tanto de las cobranzas como de los pagos debe ser enviado a cada IFI en correos automáticos generados por la plataforma, brindando las columnas consignadas en los formatos del reglamento del producto.

d. Cuotas pendientes:

El módulo deberá contemplar una base acumulativa de aquellas cuotas no vencidas, pero si reportadas por la IFI (adelanto de cuotas) para realizar una evaluación posterior y carga manual por el evaluador y/o supervisor.

e. Mantenedor:

El módulo debe presentar la flexibilidad de editar las fechas del cobro de las comisiones y de validar las tasas bajo las cuales fueron calculadas dichas comisiones, diferenciándose por moneda y tipo de comisión.

Asimismo, deberá permitir editar los correos de los destinatarios por IFI, mencionados en el punto c)

f. Formatos:

Conforme al reglamento de producto el módulo debe permitir el envío automático de los siguientes formatos:

- FORMATO DE SOLICITUD DE COBERTURA - F.14
- FORMATO DE APROBACION TRÁMITE CRC - F.15
- FORMATO APROBACION DE MODIFICACIÓN DE CALENDARIOS - F.21
- FORMATO OBSERVACIONES A MODIFICACIÓN DE CALENDARIOS - F.22

g. Reportes

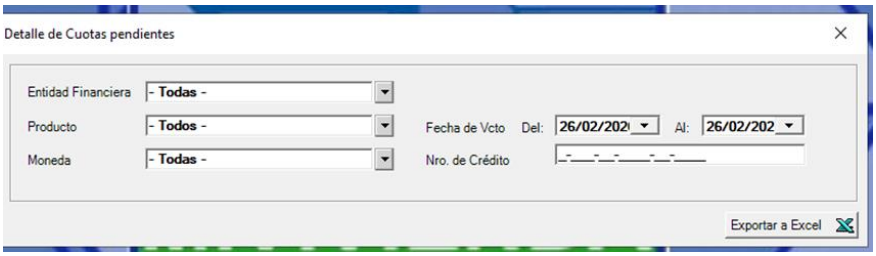
La plataforma deberá emitir los siguientes reportes operativos:

- Detalle de Cuotas Pendientes
- Detalle de PBP Vencidos
- Detalle de Solicitudes Atendidas
- Detalle de Clasificación de Riesgo
- Detalle de Cuotas Pagadas
- Detalle de Ingreso de comisiones
- Detalle de PBP Otorgados
- Detalle de Pronósticos de ingresos
- Detalle de Pronósticos de Egresos PBP
- Saldos por Crédito
- Saldos TNC y TC Proyectados
- Consolidado de Penalidades
- Detalle de Liquidaciones
- Detalle de créditos desembolsados por IFI
- Detalle de extornos mensuales
- Generación de Base de Situación de Expedientes
- Cierre Operativo: Validación de cobranza
- Cierre Operativo: Comisión CRC-PBP
- Cierre Operativo: Pagos PBP
- Indicadores de Cobertura
- Consolidado de Créditos Desembolsados
- Características del Crédito
- Características del Crédito - Promoción

Cabe precisar que los mencionados reportes son generados actualmente por el sistema PRECOSS y que el contenido para cada uno se detalla a continuación:

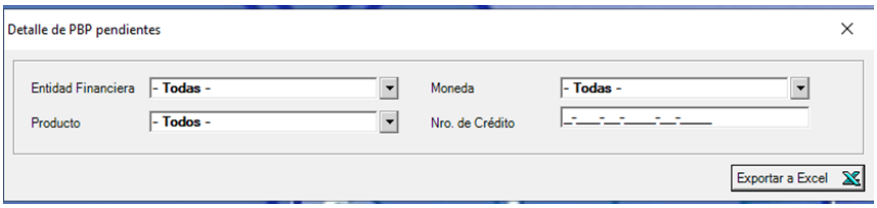
- **Detalle de Cuotas Pendientes**

  Permite realizar la búsqueda en un rango de tiempo, colocando como intervalo fechas de vencimiento de cuotas y mostrar aquellos créditos con cuotas pendientes de carga en el PRECOSS identificando el estado de la misma, es decir indicando si la cuota fue enviada o no enviada por la IFI en el cierre mensual.



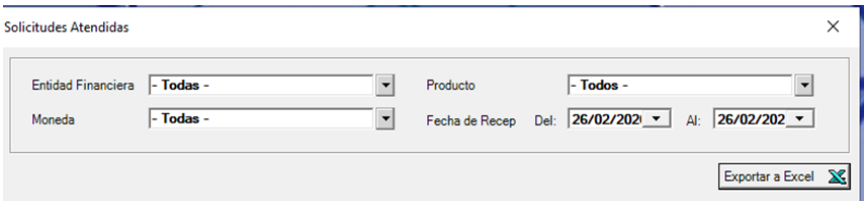
- **Detalle de PBP Vencidos**

  Permite realizar la búsqueda general o por crédito de aquellas operaciones que tengan a la fecha de búsqueda PBPs pendientes de evaluación.



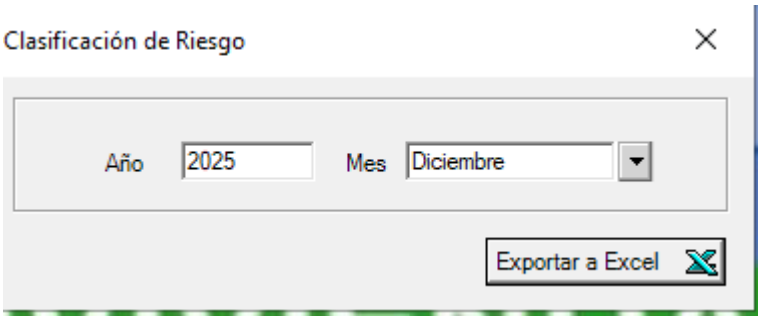
- **Detalle de Solicitudes Atendidas**

  Muestra el estado de las solicitudes ingresadas en un intervalo de tiempo, cabe indicar que además muestra el estado de la misma visualizando en el reporte si la solicitud está aprobada, rechazada u observada, así como las fechas de acción asegurando la trazabilidad de la misma.



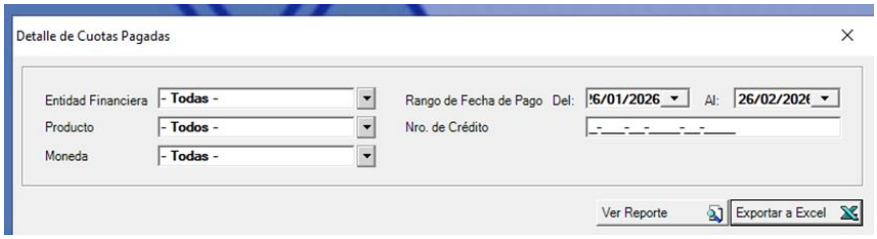
- **Detalle de Clasificación de Riesgo**

  Este reporte muestra el tipo de crédito, código de la SBS, tipo de documento, numero de documento, numero de crédito y clasificación de deudor al último RCC disponible o meses anteriores según se indique en la búsqueda. Este reporte, entre otros, nos sirve de insumo para responder pedidos mensuales y trimestrales a la GR y la GF, los que a su vez permiten cumplir en plazos según el calendario de cumplimiento normativo, dar respuesta a los entes reguladores como la SBS.



- **Detalle de Cuotas Pagadas**

  Permite realizar la búsqueda en un rango de tiempo, colocando como intervalo fechas de vencimiento de cuotas y mostrar aquellos créditos con cuotas pagadas y previamente cargadas en el PRECOSS en el cierre mensual. Muestra la composición de la cuota, la fecha de vencimiento y fecha de pago, además de los datos del cliente como son nombre, apellidos, nro de crédito e IFI.



- **Detalle de Ingreso de comisiones**

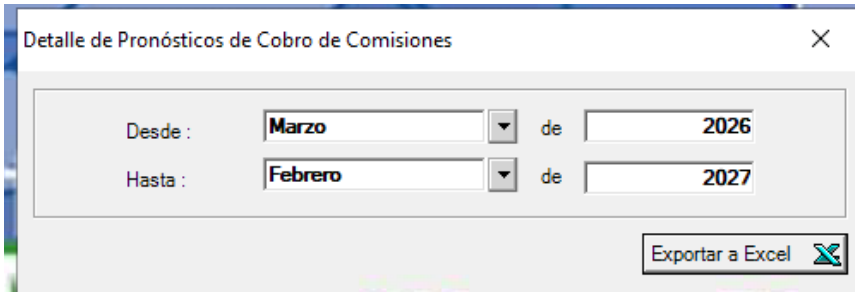
  No se encuentra habilitado desde mi perfil de evaluador.

- **Detalle de PBP Otorgados**

  No se encuentra habilitado desde mi perfil de evaluador.

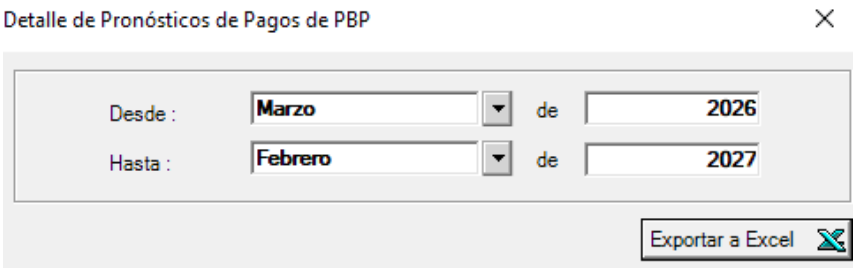
- **Detalle de Pronósticos de ingresos**

  Muestra las proyecciones correspondientes a los ingresos por cobranza de comisiones CRC y comisiones PBP en un periodo de tiempo.



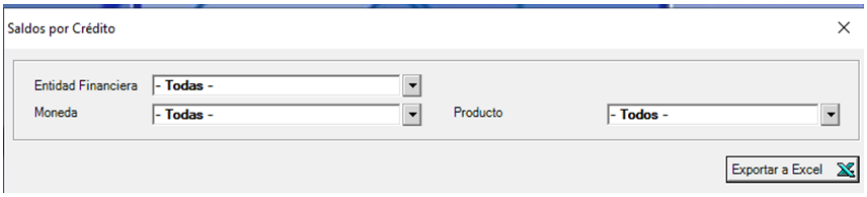
- **Detalle de Pronósticos de Egresos PBP**

  Muestra las proyecciones correspondientes a los egresos por pago de PBP (Premio al Buen Pagador)



- **Saldos por Crédito**

  Este reporte muestra el tipo de crédito, moneda, banco, nombre de beneficiario, fecha de desembolso, saldo del tramo no concesional (TNC) y saldo del tramo concesional (TC). Este reporte permite brindar a GF el estado de la cartera al cierre de cada mes, agrupado por IFI, moneda y nro de operaciones con sus respectivos saldos.



- **Saldos TNC y TC Proyectados**

  Muestra los saldos proyectados por tramos, por mes, por moneda y desde un mes de inicio, así como su resumen anual.

- **Consolidado de Penalidades**
  No se encuentra habilitado desde mi perfil de evaluador.

- **Detalle de Liquidaciones**
  No se encuentra habilitado desde mi perfil de evaluador.

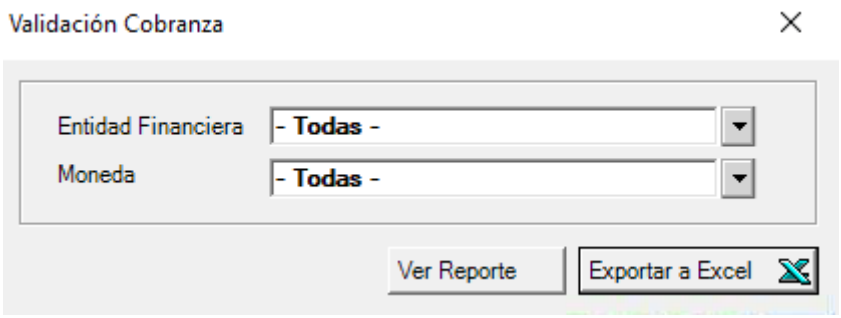
- **Detalle de créditos desembolsados por IFI**
  No se encuentra habilitado desde mi perfil de evaluador.

- **Detalle de extornos mensuales**
  No se encuentra habilitado desde mi perfil de evaluador.

- **Generación de Base de Situación de Expedientes**
  No se encuentra habilitado desde mi perfil de evaluador.

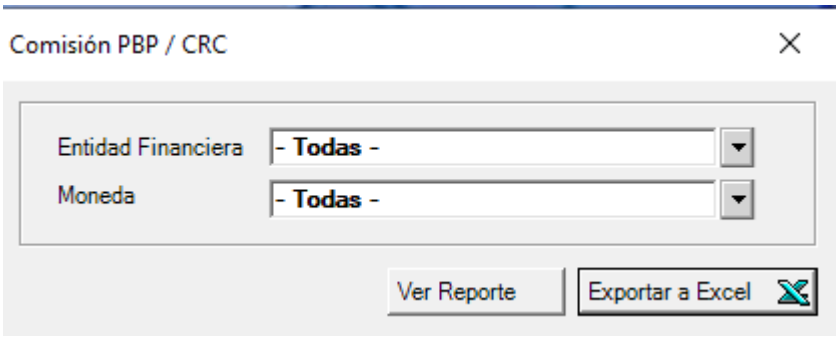
- **Cierre Operativo: Validación de cobranza**

Este reporte muestra IFI, nro de crédito, plazo total, moneda, saldo sobre el cual se calcula la comisión CRC, cuota del TC, fecha de aprobación de expediente, fecha de desembolso y fecha del vencimiento de la primera cuota. Nos permite realizar las validaciones de los importes a cobrar por IFI y por moneda.



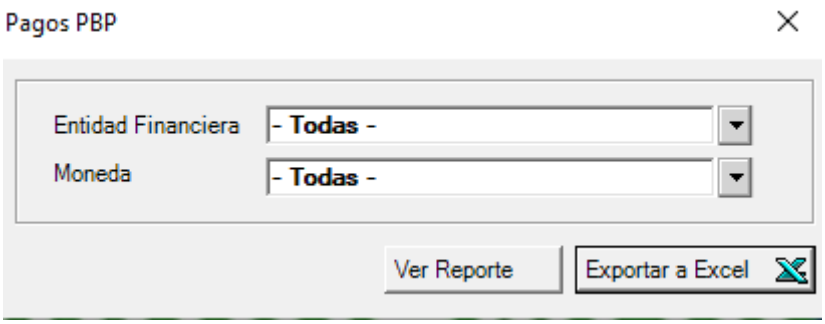
- **Cierre Operativo: Comisión CRC-PBP**

Este reporte muestra IFI, nro de crédito, moneda, cuota vencida en el mes de cierre, comisión PBP y comisión CRC. Es el resumen de la ejecución del cierre operativo.



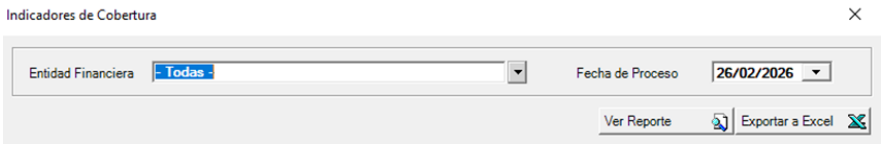
- **Cierre Operativo: Pagos PBP**

Este reporte muestra IFI, nro de crédito, moneda, nro de cuota del TC, capital, interés, monto total, nro de documento, tipo de documento, nombre y una columna pagador donde se muestra si el PBP lo asume el FMV o lo paga el cliente. Este reporte como los 2 anteriores nos ayuda a enviar el memorando a GF respecto a las instrucciones de cobranza y pagos para el cierre mensual.



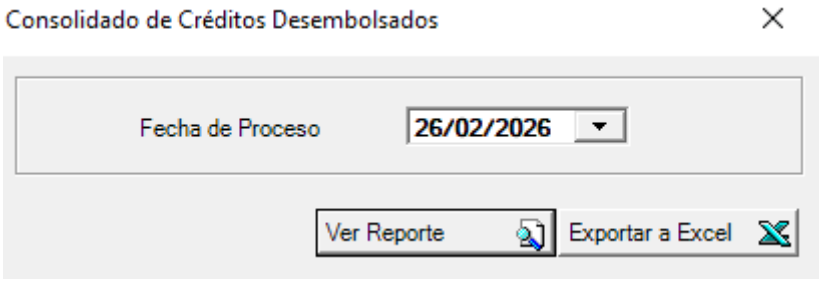
- **Indicadores de Cobertura**

Muestra entidad financiera, cliente, producto, moneda, saldo, valor comercial, valor gravamen, % valor comercial, % valor gravamen, % ltv, % cobertura



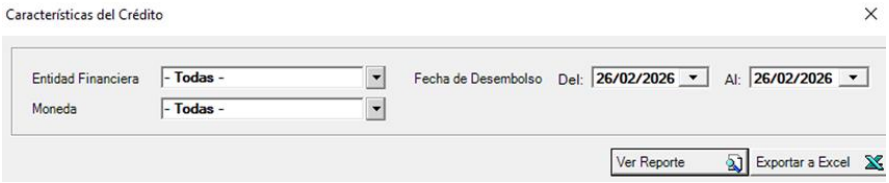
- **Consolidado de Créditos Desembolsados**

Muestra el total de créditos desembolsados por IFI, su saldo, el promedio de cobertura, el promedio LTV, nro de clientes sin garantía y deuda sin garantía.



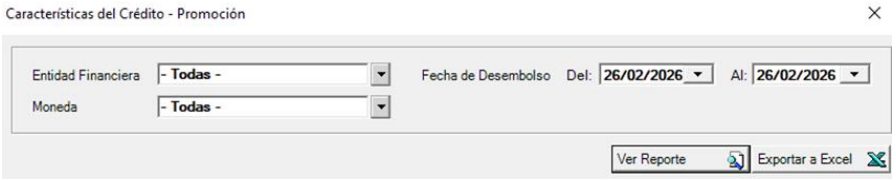
- **Características del Crédito**

Muestra entidad financiera, apellido paterno, apellido materno, nombres, estado civil, sexo departamento, provincia, distrito, producto, tipo de inmueble (departamento o casa), tipo compra/venta (bien futuro o bien terminado), moneda, tasa de interés, plazo, monto, cuota inicial y precio de vivienda



- **Características del Crédito - Promoción**

Muestra entidad financiera, nro de crédito, apellido paterno, apellido materno, nombres, departamento, provincia, distrito, dirección, ciudad, teléfono, producto, moneda, plazo, monto.



3.4.2.7.10 VALIDACION DE CREDITOS MIVIVIENDA CON EL RCC

Necesitamos que la plataforma nos brinde un reporte trimestral correspondiente a los créditos MIVIVIENDA vigentes al cierre de operaciones NO IDENTIFCADOS como créditos otorgados con nuestros recursos en el Reporte Crediticio Consolidado (RCC) de la SBS del mes a trabajar. Los casos encontrados estaran tipificados de 2 formas, como: DNI CORRECTO, NO REPORTADO CUENTA FMV o como DNI NO ENCONTRADO EN EL RCC. Este reporte se denominará Reporte 1.

Como segundo requerimiento se necesita exista la opción de cruzar los documentos del mencionado reporte con la plataforma de RENIEC a fin de validar que los DNI registrados son los correctos. Posterior a ello, el usuario podrá dar conformidad a los casos subsanados en la primera validación siempre y cuando ya se encuentren reportados en el RCC.

Los casos pendientes pasaran a consulta a las IFI a través de un correo automático y conforme a los destinatarios previamente guardados. El tenor del correo será consultar el estado de los subpréstamos en cada IFI, permitiéndome subir las respuestas al sistema registrando de ser necesario comentarios adicionales por caso. Cabe mencionar que, en este paso (previo a las consultas), el sistema debe darnos la opción de excluir algunas IFI de acuerdo con su naturaleza o condición de estas.

Durante el periodo de levantamiento de información con las IFI, el sistema podrá hacer un cruce con las recuperaciones diarias reportadas a fin de validar si existen regularizaciones en el Reporte 1, considérese como regularizaciones a los prepagos totales comunicados por el Fiduciario

Este módulo debe permitir la creación de cartas, ingresando campos como fecha de corte, trimestre trabajado, numero operaciones encontradas (Reporte 1), subsanadas y pendientes. La primera carta por crearse será la enviada a COFIDE y el segundo grupo corresponde a una carta múltiple para todas las IFI, en ambos casos se acompañará con el detalle de las operaciones identificadas por el estado y pendientes de regularizar. El tenor de las cartas es solicitar regularizar ante el Fiduciario, aquellas operaciones respondidas como canceladas, pero aún vigentes en COFIDE, así como solicitar que las operaciones confirmadas como vigentes sean reportadas en las cuentas contables correctas y asignadas para nuestros créditos.

Finalmente, el sistema permitirá hacer un resumen detallado por tipo de error desde el inicio de la gestión del trimestre, indicando las regularizaciones, el motivo y lo pendiente de subsanar, este detalle nos apoyará para la elaboración del memorando que debemos dirigir a nuestra Gerencia de Riesgos conforme a lo establecido en el procedimiento.

3.4.2.7.11 VALIDACION DE ACTAS DE CONCILIACIÓN

La PLATAFORMA deberá permitir la validación de las actas trimestrales de conciliación, mediante la comparación de saldos por producto, moneda e IFI, tomando como referencia la información reportada por COFIDE y la documentación registrada en el SFTP del Fiduciario, según corresponda.

Para ello, la PLATAFORMA deberá considerar el siguiente flujo funcional:

a) Obtención de información fuente
La PLATAFORMA deberá extraer de la carpeta de cierre la información validada y remitida por COFIDE, correspondiente al Anexo 1.1, a fin de identificar los saldos coberturados y vigentes.

b) Validación contra actas registradas en el SFTP
La PLATAFORMA deberá comparar los saldos del Anexo 1.1 con la información contenida en las actas cargadas en el SFTP del Fiduciario, validando su coincidencia por producto, moneda e IFI.

c) Consideración de anexos de sustento por diferencias
En caso se detecten diferencias entre la información del Anexo 1.1 y las actas registradas en el SFTP, la PLATAFORMA deberá verificar la existencia de anexos u otra documentación de sustento asociada a dichas diferencias.

d) Ejecución de la validación
La PLATAFORMA deberá ejecutar el proceso de cruce y validación de manera automática, a través de una funcionalidad que consolide la revisión de la información reportada por COFIDE frente a la documentación disponible en el SFTP.

e) Resultado de la validación
Como resultado del proceso, la PLATAFORMA deberá clasificar la validación en alguno de los siguientes estados:

Aceptada: cuando no existan diferencias, o cuando las diferencias identificadas cuenten con el sustento documental correspondiente.
Observada: cuando existan diferencias sin el respectivo sustento documental.

f) Gestión de observaciones
Cuando la validación resulte Observada, la PLATAFORMA deberá mostrar el detalle de las diferencias identificadas por IFI, producto y moneda, a fin de facilitar su remisión a COFIDE mediante correo electrónico. Asimismo, deberá permitir el registro y subsanación de las observaciones efectuadas.

g) Trazabilidad y almacenamiento de la información
Cuando la validación resulte Aceptada, la PLATAFORMA deberá registrar el resultado y almacenar las actas, anexos y demás documentación relacionada en una ruta o repositorio definido, asegurando su disponibilidad para fines de consulta, control y atención de requerimientos de auditoría.

h) Escenario en ausencia de Fiduciario
En caso no exista Fiduciario, la PLATAFORMA deberá permitir la carga y validación de las actas remitidas directamente por las IFI, verificando que no existan diferencias y, de haberlas, que cuenten con los sustentos correspondientes.

3.4.3 Requerimientos de Seguridad

La PLATAFORMA deberá ser íntegro y confiable, así mismo, deberá incorporar mecanismos de validación de la información.

La PLATAFORMA deberá contar con un módulo de administración y seguridad que permita como mínimo:

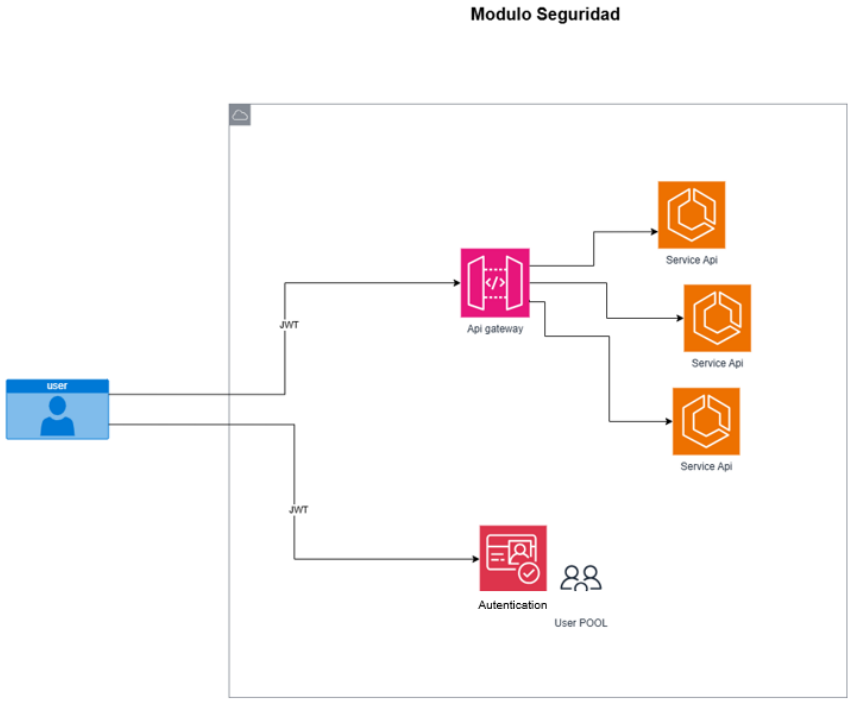
- Registra usuarios, roles, horarios por rol y oficina (para las entidades bancarias y los usuarios internos)
- Gestión de usuarios y contraseñas integrada con el Directorio Activo del FMV
- Gestión de niveles y autorizaciones.
- Gestión de perfiles (La PLATAFORMA debe soportar la administración centralizada para que pueda ser asignada a un responsable para la gestión respectiva)
- Acceso único.
- Disponibilidad de perfil para auditoría (solo lectura). El CONTRATISTA debe atender los requerimientos de información respecto del objeto del servicio de parte de la Unidad de Auditoría Interna del FMV, Sociedades de Auditoría Externa contratadas por el FMV o SBS.
- Logs de auditoría y trazabilidad de la información, que permitan registrar, monitorear y conservar evidencias de las operaciones realizadas en la PLATAFORMA. Como mínimo, deberán contemplar:
    - Logs de acceso a la plataforma, incluyendo registro de inicio y cierre de sesión, identificación de usuario, fecha, hora, dirección IP y dispositivo de acceso.

- Logs de transacciones funcionales, que permitan la trazabilidad de las operaciones realizadas por los usuarios dentro de la PLATAFORMA.
- Logs de cambios a nivel de base de datos, que registren operaciones de inserción, actualización y eliminación (CRUD) sobre las tablas transaccionales.
- Identificación del usuario, fecha y hora, tipo de operación y valores anteriores y posteriores en los cambios realizados, cuando aplique.

Las tablas iniciales sujetas a auditoría deberán corresponder, como mínimo, a aquellas vinculadas a los requerimientos funcionales definidos para la solución, pudiendo ampliarse durante la etapa de análisis y diseño para garantizar la integridad y trazabilidad de la información.

- Reportes de control de transacciones críticas.
- Base de datos cifradas

La Arquitectura de Seguridad, debe contener como mínimo lo siguiente:



Funcionalidades de Autenticación y Gestión de usuarios

- ✓ Registro y autenticación de usuarios (signup/signin).
- ✓ Gestión de sesiones y tokens JWT.
- ✓ Soporte para autenticación multifactor (MFA).
- ✓ Gestión de políticas de contraseñas personalizables, incluyendo complejidad, caducidad y bloqueo por intentos fallidos. Las políticas serán extraídas del Directorio Activo del FMV.

Integración con la Arquitectura

- ✓ Los usuarios, tanto de entornos Web como Mobile, deben registrarse e iniciar sesión a través de la plataforma de autenticación.
- ✓ El módulo de autenticación de la PLATAFORMA emite un token de acceso (JWT), el cual será validado por la pasarela de servicios (API Gateway).
- ✓ La pasarela aplicará políticas de autorización para controlar el acceso granular a cada módulo o microservicio de la plataforma.

- ✓ Cada microservicio validará la autenticidad y vigencia del token mediante middlewares de autenticación distribuidos, asegurando que solo se permita el acceso a usuarios autorizados.

Seguridad Adicional

- ✓ Todos los accesos deben realizarse a través de conexiones cifradas utilizando el protocolo HTTPS (TLS).
- ✓ El token JWT tendrá una vida útil definida así como mecanismos para su revocación en caso de riesgo o cierre de sesión.
- ✓ Uso de refresh tokens para mantener sesiones activas de forma segura.
- ✓ Todas las actividades de acceso y autenticación deberán ser registradas y auditadas mediante herramientas de monitoreo y trazabilidad, permitiendo identificar patrones de comportamiento anómalo o accesos no autorizados.

Buenas Prácticas

- ✓ Implementar la autenticación multifactor (MFA) como obligatoria para usuarios con perfiles administrativos o críticos.
- ✓ Definir y aplicar roles y perfiles de usuario (por ejemplo: cliente, gestor, auditor), con restricciones diferenciadas de acceso y operación.
- ✓ Integrar el módulo de autenticación con el Directorio Activo y la plataforma de control de accesos del entorno tecnológico para limitar el alcance sobre otros recursos.
- ✓ Activar y mantener habilitados los registros de eventos de autenticación, con mecanismos de análisis automatizado para detección temprana de incidentes.

3.4.4 Requerimientos de Integración, Respaldo y Conectividad

Integración con sistemas del FONDO

Durante la **Fase 1**, la plataforma deberá integrarse operativamente con el sistema actual de créditos del FONDO (SAOC), el cual seguirá activo mientras se complete la transición hacia la nueva solución. Esta integración deberá garantizar:

- Interoperabilidad de datos y sincronización de operaciones críticas (desembolsos, recuperaciones, extornos, entre otros).
- Canales de intercambio de información seguros y en tiempo real, mediante servicios RESTful, APIs o mecanismos definidos por el FMV.
- Aseguramiento de la consistencia y trazabilidad de los datos entre ambos sistemas durante el periodo de coexistencia.

Asimismo, la plataforma deberá estar preparada para integrarse con otros sistemas internos del FMV, tales como:

- Siga Contabilidad
- Facturación electrónica
- Tesorería
- Plataforma de gestión documental

Políticas de respaldo y conservación de información

El CONTRATISTA deberá garantizar la implementación de un esquema integral de copias de seguridad (backups), que contemple lo siguiente:

- Backups diarios automáticos, incluyendo datos estructurados (bases de datos), archivos asociados y configuraciones de la plataforma.
- Conservación mínima obligatoria:
  - 3 años en línea, accesibles para consulta directa de la plataforma ante requerimientos operativos o auditorías.
  - 10 años en almacenamiento seguro y de bajo costo, conforme a las políticas de conservación institucional del FONDO y será considerado en la Arquitectura de datos.
- Soporte para restauración completa o granular de información en caso de incidentes o auditorías.
- Validación periódica de la integridad de los backups mediante pruebas de restauración controladas.

- Registro de logs de respaldo y restauración, incluyendo fechas, responsables y resultados.

3.4.5 Requerimientos de Conectividad

Conectividad a la red del FMV
La plataforma deberá habilitar mecanismos de conectividad segura con la **red interna del FONDO**, considerando:

A) Características servicio de interconexión Sede FMV y Data Center del Postor

- El postor deberá suministrar dos enlaces de comunicaciones uno principal y otro backup a través de fibra óptica por diferentes rutas de acceso, desde su Centro de Datos hasta el Centro de Datos de la Sede de FMV, ubicado en Calle Amador Merino Reyna N° 281, San Isidro
- Los enlaces dedicados deben ser de 200 Mbps simétrico con overbooking 1:1, los medios de transmisión de última milla (entendiéndose esta como la infraestructura propia del postor, tales como mangas, buzones, mufas, POP, nodos, entre otros; desde el punto de presencia más cercano hasta las instalaciones de la sede de FMV
- Los enlaces deben estar implementados sobre una red privada y no sobre la red de internet, que permita la transmisión de datos entre el local de FMV y el Data Center del postor. La infraestructura de transporte del backbone de la red para el enlace a suministrar debe ser una red basada en tecnología de Conmutación de Paquetes en Protocolo MPLS, de alta capacidad de 200 Gbps o superior, propia del proveedor y no podrá ser subcontratada a terceros.
- El backbone de la red del postor, deberá contar con al menos un Nodo de nivel Core (el más alto nivel de jerarquía de la red, cuya infraestructura desempeña un papel fundamental y debido a su naturaleza critica, es esencial para mantener la continuidad del servicio y prevenir de interrupciones significativas, asegurando así su correcto funcionamiento) el cual deberá estar ubicado dentro de un centro de datos de propiedad del postor con certificación TIER-3 o RATED-3 en Diseño y/o Construcción. Esta información deberá ser presentada en su propuesta.
- Se deberá dimensionar y suministrar todos los equipos, dispositivos y/o componentes de comunicación necesarios en ambos extremos y realizar los trabajos de ingeniería y obras civiles de ser el caso, a fin de dejar este enlace totalmente operativo.
- Las acometidas de fibra óptica que instale el postor deberán terminar en equipo router que deberá instalar el contratista como parte del servicio.
- El postor debe proveer los equipos routers, para la interconexión donde cada router instalado se conectará a través de puertos Ethernet 10/100/1000 Base-T, RJ-45, a la red de FMV a través de cables UTP categoría 6 certificados. Los equipos routers a proveer deben tener vigencia tecnológica y con soporte de la marca durante el periodo de contrato. Asimismo, el sistema operativo de los equipos a proveer debe ser de la última versión estable durante el periodo de contrato.

B) Características servicio de Internet en el Centro Datos del Postor

- Brindar un enlace dedicado a Internet con un ancho de banda de 500Mbps, simétrico con un overbooking de 1:1, a instalarse en un centro de datos de propiedad del postor, el cual deberá contar con certificación de operación conforme al estándar DCOS-2021, con nivel de madurez operacional 3 (DCOS-3), la misma que deberá ser presentada en la propuesta.
- El backbone del postor deberá ser redundante y la red local que brinda el servicio a la entidad deberá ser propia y 100% en fibra óptica.
- El postor deberá brindar un segmento de direcciones IPv4 de 64 IP’s públicas consecutivas. El postor debe asegurarse que as direcciones IP públicas brindadas no se encuentren listadas en servidores de Blacklist o listas negras.

- El postor debe ser miembro activo del NAP PERÚ (Network Access Point), lo que le permitirá utilizar el intercambio de tráfico entre proveedores y garantizar una conexión continua de internet con baja latencia en la prestación del servicio.

  Para tal efecto, el postor deberá presentar, dentro de su propuesta, un documento emitido por el NAP PERÚ que acredite su condición de miembro de la Asociación, con una antigüedad mínima de diez (10) años. Asimismo, deberá adjuntar la constancia vigente emitida por el NAP PERÚ que acredite que actualmente cuenta con una capacidad mínima de cuatro (4) enlaces de 100 Gbps, en calidad de operador ISP. Igualmente, deberá incluir una impresión del tráfico correspondiente obtenida desde la página web oficial del NAP PERÚ.
- El proveedor deberá contar con salidas internacionales redundantes, al menos con tres (03) proveedores TIER I. La salida principal deberá tener una capacidad mínima de 100 Gbps y la salida de contingencia de 100 Gbps como mínimo. El postor deberá presentar en su propuesta, un diagrama de la salida internacional detallando los nombres de los proveedores TIER I.
- Debe brindar una plataforma de autogestión del DNS (Sistema de Nombres de Dominio) que permitirá al usuario autorizado (Con clave de acceso) poder crear, actualizar, modificar y eliminar configuraciones de los registros del DNS. El contratista debe contar como mínimo, con (02) servidores DNS (Principal y redundado) ubicados en Data Center distintos a nivel nacional. Por seguridad de la información, al menos (01) servidor DNS, deberá estar alojado en el Data center propio del postor, el cual debe estar certificado en la norma ANSI/TIA RATED-3 de Diseño o Construcción.
- Debe brindar una solución de mitigación de ataques de Denegación de Servicios (DDoS) volumétrico, desplegada en la red del postor (nube local) con disponibilidad al 99.5% capaz de mitigar ataques volumétricos de hasta 100 Gbps localmente. La mitigación deberá realizarse cuando el enlace de conexión a Internet sea saturado por un ataque DDoS volumétrico.
- El postor deberá proveer como parte del servicio el equipo de enrutamiento (router) de tecnología vigente, que no se encuentre en fin de vida o fin de soporte. El equipo deberá tener la capacidad de soportar el ancho de banda solicitado y tener la capacidad instalada de soportar un incremento de hasta el 50% de ancho de banda en caso sea necesario durante el tiempo de vigencia del contrato, asimismo el deberá contar con fuente de energía redundante.
- El postor deberá brindar una herramienta web necesaria para monitorear el nivel de consumo del ancho de banda del servicio de internet. La misma que debe ser accedida a través de un usuario y password. Se deberá garantizar la calidad y la precisión de las gráficas, las cuales serán tomadas como válidas para los fines que la entidad estime como conveniente. Por seguridad el acceso al portal web de la herramienta deberá realizarse mediante HTTP o HTTPS. Se podrá brindar desde la red del postor, siendo que la Entidad accederá a ella a través de una página web y que la información histórica que se mostrará será de los últimos 12 meses.
- En caso de consorcios, bastará con que uno de los miembros cumpla con alguna de las disposiciones anteriores.

C) Características servicio de Conexión a nube publica

- La solución debe de poder establecer una conexión entre la plataforma de nube y Fondo mi Vivienda. Para ello se requiere de una capacidad asegurada de un 1 GB como mínimo, Las conexiones deben ser redundantes y asegurar la mínima latencia entre la plataforma de nube y Fondo mi Vivienda.

D) Características del Servicio de Seguridad Gestionada

Con el fin de reducir las brechas de seguridad frente a amenazas existentes de internet, y brechas relacionadas con la infraestructura física que soporta la plataforma, reduciéndose así posibles puntos de falla, el postor deberá brindar una solución de seguridad integral basado en los siguientes componentes:

Solución de seguridad perimetral NGFW

Descripción:

- El Postor deberá brindar una solución de seguridad NGFW desde su nube (Centro de Datos propio y certificado en operación) o en modalidad on premise.
- La solución de seguridad en la nube no deberá ser brindada a través de instancias o contextos virtuales tales como VDOM, VYSYS, LSYS, VSX o similares, es decir no se podrá usar un equipo de seguridad y configurar múltiples firewalls en el mismo appliance para poder brindar el servicio.
- Se deberá brindar la solución con los recursos físicos dedicados de CPU, memoria y disco, para esto el postor podrá colocar un equipo dedicado o una máquina virtual.
- El fabricante de la solución de seguridad debe pertenecer al cuadrante de lideres de Gartner para “Enterprise Network Firewall” o “Hybrid Mesh Firewalls” o “Firewalls de Redes Empresariales” en los últimos 10 reportes de Gartner.
- El fabricante de la solución de seguridad debe estar catalogado como líder en el último informe de Forester Wave Enterprise Firewalls. El postor deberá acreditar que el fabricante de la solución de seguridad es líder en el último informe Forrester Wave Enterprise Firewalls, mediante extracto o captura oficial del informe o carta del fabricante. Esta acreditación deberá para el perfeccionamiento del contrato con la propuesta técnica inicial.

Características:

- Throughput de Threat Prevention: mínimo 1.5 Gbps, medido con tráfico productivo real (64KB HTTP o mixtura de aplicaciones de capa 7) con las siguientes funcionalidades habilitadas simultáneamente: Control de aplicaciones, IPS, Antivirus/Antimalware, Antispyware/Antibot, Control de amenazas de día cero, Seguridad Avanzada en DNS, Filtro de archivos y Logging activo. No se aceptarán cartas de fabricante como fundamento para el cumplimiento del performance esto deberá ser validado con información pública del fabricante.
- La solución debe soportar como mínimo 200,000 sesiones simultaneas (Max Sesiones).
- Debe soportar enrutamiento estático y dinámico (RIPv2, BGP y OSPFv2).
- Permitir configurar el tiempo de almacenamiento en caché de la Tabla ARP.
- Soportar DNS Dinámico en las interfaces.
- La plataforma propuesta por el fabricante debe contar con certificación USGv6 para trabajar IPv6 tanto en Firewall como en IPS.
- Debe ser capaz de operar en los modos Capa 3 (con capacidades completas de Ruteo y NAT), Capa 2, Transparente y Sniffer, de forma simultánea mediante el uso de sus interfaces físicas sin necesidad de tener que hacer uso de contextos o dominios virtuales.
- Soportar VPN Site-to-Site y Cliente-To-Site en protocolos IPSec o SSL.
- Soportar VPN Site to Site: 1,000
- Soportar VPN Client to Site: 500
- La VPN IPSec debe soportar como mínimo:
  - DES y 3DES; AES 128, 192 e 256 (Advanced Encryption Standard)
  - Autenticación MD5, SHA-1, SHA-2;
  - Diffie-Hellman Group 1, Group 2, Group 5 y Group 14;
  - Algoritmo Internet Key Exchange (IKEv1 & IKEv2);
- Permitir la aplicación de políticas de seguridad y visibilidad para las aplicaciones que circulan dentro de los túneles VPN.
- Las VPN client-to-site deben poder operar usando el protocolo IPSec o SSL y permitir la conexión por medio de agente instalado en el sistema operativo.
- Soportar autenticación vía AD/LDAP, Kerberos, TACACS+, SAML, Certificados Digitales y RADIUS, incluyendo Doble Factor de Autenticación (2FA).
- Debe permitir definir segmentos de red para ser agregadas de forma automática en la tabla de rutas de la interfaz túnel del equipo que tenga instalado el agente de VPN.

- Debe soportar Split Tunnel para elegir los segmentos de red que serán enrutados por la VPN.
- El Split Tunnel debe permitir elegir el tipo de tráfico que se enrutará por el túnel VPN, basado en el nombre de la Aplicación y Dominio.
- Debe permitir los siguientes tipos de conexión del cliente al túnel VPN:
- Antes del usuario se autentique en la estación;
- Después de la autenticación del usuario en la estación usando Single Sign On (SSO);
- El agente de VPN client-to-site debe ser compatible al menos con: Windows 7, Windows 8, Windows 10, MacOS X.
- Debe contar con un dashboard gráfico que permita monitorear a los usuarios conectados por VPN.

Threat Prevention:

- Para seguridad del ambiente contra ataques, los dispositivos de seguridad deben poseer módulo de IPS (Intrusion Prevention System), Antivirus/Antimalware, Antispyware/Antibot.
- Capacidad de realizar DNS Sinkhole para la identificación de equipos finales de la Entidad que estén comprometidos por spyware en entornos corporativos
- Las funcionalidades de IPS, Antivirus y Antispyware/Antibot deben operar en carácter permanente, pudiendo ser utilizadas por tiempo indeterminado, incluso si no existe el derecho de recibir actualizaciones debido a caducidad de soporte con el fabricante.
- El servicio deberá soportar el throughput solicitado operando en el máximo nivel o modo de seguridad de inspección de IPS, Antivirus y Antispyware/Antibot.
- Debe identificar las consultas que realizan los hosts infectados hacia dominios maliciosos, de tal forma que el Firewall pueda bloquear dichas consultas DNS.
- Deberá posibilitar la creación de firmas customizadas por la interfaz gráfica del producto.
- Debe ser capaz de detectar y bloquear el virus y malware en general que se propague en, al menos, los siguientes protocolos: HTTP, HTTPS, HTTP/2, FTP, SMB (versiones 1, 2 y 3), SMTP, IMAP y POP3; tanto en IPv4 como en IPv6, para todos los protocolos en mención.
- La solución debe ser capaz de predecir y detener dominios maliciosos de malware basados en algoritmos de generación de dominio (DGA).
- Debe detectar e interrumpir robo de datos ocultos o tunelizados en tráfico DNS.
- Capacidad de bloquear en tiempo real al menos lo siguientes ataques: DGA, Tunneling, Rebinding, NXNSAttack, inclusive si se tratan de solicitudes DNS desconocidas (de las cuales no se tenga firmas)
- Debe soportar la creación de firmas de IPS basadas en el formato de Snort.

URL Filtering:

- Permite especificar la política por tiempo, horario o determinado período (día, mes, año, día de la semana y hora)
- Deberá incluir la capacidad de creación de políticas basadas en la visibilidad e identificar el usuario que accede a una URL a través de la integración con servicios de directorio, autenticación vía Active Directory, LDAP en general y base de datos local.
- Debe soportar un cache local de URLs en el appliance, evitando el delay de comunicación/validación de las URLs
- Debe poseer al menos 70 categorías de URLs, incluyendo las de malware, command and control, proxy, phishing.
- Debe contar con multi categorías de URL, que permita conocer si una web de una categoría determinada está catalogada como riesgo bajo, medio o alto.
- Debido a que diariamente se crean decenas de miles de nuevas páginas web, la solución deberá ser capaz de analizar en tiempo real si la página web tiene contenido malicioso cuando un usuario intenta acceder.
- El análisis en tiempo real deberá determinar si la página web desconocida (no

- categorizada en la base de datos del fabricante), tiene contenido javascript malicioso, phishing, actividad de command and control y otros tipos de contenido malicioso.
- Debe permitir la creación de categorías personalizadas.
- Debe permitir la customización de la página de bloqueo.
- Debe permitir notificar al usuario, mostrándole solo una página de alerta, pero
- permitiéndole continuar la navegación al site.
- Debe identificar cuando un usuario envía credenciales corporativas de red a sitios no autorizados y debe poder bloquear dicho envío, previniendo así ataques de phishing.

Solución Web Application Firewall para servicio Internet

Características:

- La solución propuesta debe ser mediante equipo appliance nuevo y de primer uso y no debe tener anuncios de End-of-life o End-of-Support o End-Of-Sale o similares al momento de la presentación de la oferta, para la acreditación se debe presentar información pública del fabricante en idioma inglés o español o mediante carta del fabricante o partner local autorizado.
- La solución deberá soportar una consola única donde se consolidarán todos los incidentes de seguridad detectados por la herramienta independiente si estos son detectados en la solución cloud u on-premise, esto permitirá a la entidad observar el estado de la seguridad de sus aplicaciones web de forma general como ayuda en la toma de decisiones en la estimación de sus políticas y controles de seguridad.
- La solución deberá ser entregada en modelo de Hardware appliance para el WAF, la cual debe ser propietaria y no estar basada en soluciones OpenSource o depender de firmas de ModSecurity.
- La consola debe soportar la gestión centralizada del firewall de aplicaciones web a través de un navegador web.
- El sistema de administración deberá hacer análisis de los ataques, agregando eventos y alertas individuales en incidentes o narrativas de ataques y amenazas, incluyendo detalles útiles para el análisis de los ataques dirigidos, por ejemplo: Direcciones IP de origen, Vectores de ataque, Aplicaciones y recursos atacados,Historial en el tiempo, incluyendo eventos bloqueados y/o alertados, Muestra de eventos, Análisis estadístico, Integración con información de inteligencia (geolocalización, ataques previos a otros clientes, etc.) y Códigos CVE asociados al ataque.

Web Application Firewall (WAF)

- La solución debe soportar diferentes arquitecturas de despliegues incluyendo Bridge capa2, proxy reverso.
- Número de aplicaciones, dominios o virtual IPs no menor a 10.
- La solución deberá: Inspeccionar y monitorear todos los datos http y la aplicación, incluyendo, los encabezados http, campos de formularios, y el cuerpo http; Inspeccionar las peticiones y respuestas http; asimismo tener la habilidad de decodificar datos a su mínima expresión a partir de diferentes sistemas de encoding Web y validarla y validar todos los tipos de datos ingresados, incluyendo URLs, formularios, cookies, cadenas de queries, campos y parámetros ocultos, métodos http, elementos XML y acciones SOAP.
- La solución deberá permitir la modificación de reglas de seguridad. Los administradores deberán poder definir reglas para el modelo de seguridad positivo o negativo y deberán crear reglas de correlación con múltiples criterios.
- Facilitar la configuración del modelo positivo de seguridad, El dispositivo deberá aprender automáticamente la estructura y los elementos de la aplicación de manera constante y sin intervención humana, la funcionalidad de aprendizaje deberá rastrear cambios continuos en las aplicaciones web, pudiendo reconocer cambios en la aplicación y simultáneamente protegerlas y también deberá aprender los valores aceptables para los campos de ingreso de datos con base en el registro de la actividad.

- Los valores aprendidos podrán ser utilizados como la configuración inicial sobre la que se revisarán los datos ingresados en el modelo positivo de seguridad.
- La configuración aprendida deberá ser accesible y modificable para el administrador del dispositivo.
- La solución deberá correlacionar múltiples eventos de seguridad para distinguir tráfico deseado del tráfico inadecuado.
- La solución debe permitir visualizar cual fue el usuario de aplicación (el que ha iniciado la sesión web) que está involucrado en un incidente. Así mismo la solución debe permitir generar reportes relacionando al usuario de aplicación.
- La solución deberá permitir la modificación de reglas de seguridad. Los administradores deberán poder definir reglas para el modelo de seguridad positivo o negativo y deberán crear reglas de correlación con múltiples criterios.
- Las políticas granulares para control de acceso o generación de alertas deberán de contar con los siguientes criterios para la validación de la actividad en la aplicación Web. Los criterios deberán de poder usarse en cualquier número y cualquier combinación:
    - Por URL, a través del prefijo, ruta o host.
    - Por la existencia o contenido de cualquier Header HTTP
    - Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier customización por expresiones regulares), ya sea en el HTTP Request o el Response por parte del servidor Web
    - Tipo de archivo siendo transmitido en cualquier sentido
    - Métodos HTTP usados
    - La existencia o contenido de cualquier Parámetro web
    - IPs de origen
    - Por la existencia o contenido de Cookies o el identificador de Sesión
    - Response Code y Headers en el Response HTTP por parte del servidor Web
    - Hora del Dia.
    - Por usuario firmado en el aplicativo web
    - User-Agent
    - Tiempo de respuesta o tamaño de la respuesta HTTP
- La solución deberá cubrir todas las vulnerabilidades expresadas en el OWASP Top Ten más reciente y contar con plantillas de políticas pre-definidas para automatizar la protección.
- La solución deberá proporcionar el bloqueo de direcciones IP, sesiones TCP o usuarios de la aplicación web.
- La solución deberá proteger tanto las aplicaciones Web HTTP, como las aplicaciones web SSL y HTTPS.
- La solución deberá tener la capacidad de recibir y utilizar los certificados y pares de llaves público/privadas para los servidores web protegidos.
- La solución deberá desencriptar el tráfico SSL, de las aplicaciones web, entre el cliente y el servidor y re encriptarlo antes de su reenvío.
- En los modos puente (bridge) o sniffer, la solución deberá poder desencriptar el tráfico SSL para inspección, sin terminar o cambiar la conexión HTTPS.
- La solución deberá tener la capacidad de proteger aplicaciones web que incluyan el contenido de servicios web (xml). La protección XML deberá contar con mecanismos automatizados de aprendizaje, similares a los de la protección de aplicaciones web.
- La solución deberá soportar las opciones fail-open y fail-closed
- La solución deberá contar con funcionalidades que permitan:
    - Rastrear e identificar las fuentes de los ataques originadas desde proxies anónimos, direcciones IP maliciosas, Botnet y sitios de phishing.
    - Actualizar las fuentes de ataque para identificar y bloquear el tráfico malicioso.
    - Ajustar dinámicamente las políticas de seguridad con base en la identificación de las fuentes de ataque o de las fuentes que denoten actividad sospechosa.

    - Bloquear solicitudes de acceso basado en la reputación de la fuente del tráfico, como direcciones IP conocidas por su comportamiento malicioso por Botnet, DDoS, Phishing o redes de ocultamiento (TOR y proxies anónimos).
    - Bloquear solicitudes de acceso basado en el país de origen de la conexión.
    - Realice un análisis automático de distribución de alertas en relación con el país de origen, con opción a representar la información a través de un mapa mundial.
    - Detallar y analizar los eventos de seguridad ocurridos, orígenes y método del ataque, dirección IP y localización geográfica del ataque.
- Contar con una comunidad de inteligencia propia del fabricante que permita obtener información en tiempo real sobre los patrones de ataques, reputación de fuentes de tráfico que permita mitigar comportamiento malicioso.
- Identificar y clasificar tráfico generado por Bots, distinguiendo tráfico malicioso.
- La solución deberá contar con una clasificación de BOTs basada en reputación para la distinción de BOTs buenos, malos y sospechosos. Permitiendo el bloqueo de ataques como comment spam, web-scraping y escaneo de vulnerabilidades, y asegurando el acceso de BOTs como Google, Facebook y Pingdom.
- La solución deberá hacer bloqueos a partir del País de Origen (GeoBlocking).
- La solución debe permitir Bloquear solicitudes de acceso basado en la reputación de la fuente del tráfico, como direcciones IP conocidas por su comportamiento malicioso por BOTs, DDoS, phishing o redes de ocultamiento (TOR y proxies anónimos).
- La solución debe permitir tomar acciones personalizadas para las reglas de seguridad, incluyendo bloqueos de sesión, request, envió de Captchas, etc.
- Las alertas de tráfico anómalo deben ser mostradas en un tablero donde se permita visualizar un resumen de la misma, que incluya al menos: Fecha, Hora, Descripción de la alerta y Acción tomada
- La solución debe correlacionar y filtrar los eventos de seguridad en formato de narrativa, con el fin de facilitar la investigación de eventos de seguridad contra las aplicaciones web, mitigar y responder a amenazas de seguridad reales de forma rápida y decisiva; esta debe ser legible, apoyada en el uso de la inteligencia artificial y aprendizaje automático.
- La solución deberá contar con un sistema de seguridad colaborativa para evitar ataques que han sufrido otros sitios web. (Crowdsourcing).
- Contar con una suscripción hacia una herramienta de analítica de incidentes en la nube donde sea posible correlacionar los diferentes eventos y presentar incidentes correlacionados por fuente, tipo de ataque, historia de ataque, reputación y otro.
- La solución de protección de aplicaciones Web (WAF) On-premise de la entidad estará conformado como mínimo un (1) equipo, adicionalmente se deberá proveer 01 equipo de similares características para su uso como spare o instalado en backup on-premise, para la atención de averías para el cambio en un tiempo no mayor a 4 horas desde confirmada la necesidad producto del de los diagnósticos, solo para el caso de la consola de gestión en caso de avería se aceptara su cambio según el tiempo que tome el proceso de RMA con el fabricante pudiendo ser hasta 60 días, dicho equipo WAF con capacidades mínimas:
    - Soportar un Throughput de WAF en capa 7 de 01 Gbps para tráfico exclusivo HTTP/HTTPS
    - La solución deberá contar con tarjetas de aceleración de transacciones SSL en hardware de propósito específico.
    - Contar con 4 interfaces de 1 Gbps en cobre y 4 interfaces SFP GE.
    - Contar con 2 fuentes de poder redundantes.
    - Contar con el licenciamiento que incluya las funcionalidades de WAF, soporte del fabricante y suscripción a servicios de actualizaciones de firmas y funcionalidades de seguridad.

Clasificación de clientes y protección contra Bots

- La solución debe soportar la detección de script y otras herramientas automáticas, a fin de poder identificar y bloquear las consultas que no sean de un navegador web real.
- La solución debe ser capaz de identificar bots (scripts automatizados sin interacción humana) de manera transparente, sin afectar la experiencia de los humanos que acceden a las aplicaciones.
- La solución debe clasificar los bots por tipo y permitir tomar acciones diferentes en base a este criterio, así cómo llevar estadísticas por sitio o aplicativo protegido.
- Se deben poder excluir bots "benignos" como motores de búsqueda, Site Helpers, B2B API clients, redes sociales, etc.
- La solución debe permitir la detección de bots sin la necesidad de integrar código en las aplicaciones
- La solución debe contar con algoritmos complejos y actualizados de detección y clasificación de bots y herramientas automatizadas, excediendo controles básicos de soporte de JavaScript y cookies.
- La solución debe informar el porcentaje de bloqueos en tiempo real y acciones tomadas ante la presencia de Bots y herramientas automatizadas.
- La solución debe proteger ante el uso de herramientas de escaneo automatizadas

Solución Denegación de Servicios (anti DDoS)

Características:

- El postor deberá brindar una solución de mitigación de ataques de Denegación de Servicios Distribuidos (DDoS) volumétrico, desplegada en la red del postor (nube local) capaz de mitigar ataques volumétricos de hasta 100 Gbps localmente.
- La solución debe incluir la protección contra ataques de denegación de servicio a nivel de aplicación sin estados (stateless), por lo que no deberá tener conexiones ni se sesiones concurrentes para el tráfico total (incluyendo tráfico atacante).
- No se aceptarán soluciones “Always on” para este componente debido a que generaría latencia adicional al flujo del tráfico normal lo cual podría provocar una deficiencia crítica para servicios sensibles a la latencia.

Solución de Sandboxing

Características:

- La solución propuesta debe incluir mecanismos de detección de amenazas de día cero, incluyendo una plataforma Sandboxing.
- Como mínimo se requiere el servicio pueda detectar el malware de día cero en un tiempo no mayor a 5 minutos utilizando la emulación completa de malware en entornos Windows, Linux, Android y MacOS.
- Deberá ser capaz de analizar 1800 archivos por hora realizando análisis dinámico (es decir, no uso de firmas ni pre-filter)
- Deberá ser un servicio propio del fabricante, no se aceptarán plataformas que tercericen el servicio de Sandboxing con entidades terceras, debiendo además garantizar la privacidad y confidencialidad del contenido de los archivos analizados, para lo cual se requiere que el servicio cuente como mínimo con certificaciones SOC2 Tipo II de AICPA, ISO 27001, ISO 27017 e ISO 27018.
- Debe proveer información forense sobre las acciones realizadas por el malware y generar automáticamente las firmas de malware y bloquear el acceso a las URLs maliciosas utilizadas por el malware.
- El Next Generation Firewall debe ser capaz de enviar al sandbox de manera automática los archivos sospechosos que se propaguen por los protocolos HTTP, HTTPS, HTTP/2, FTP, SMTP, POP3, IMAP y SMB (versiones 1, 2 y 3). Tanto en IPv4 como en IPv6.
- Debe permitir al administrador la descarga del archivo original analizado por el Sandbox.

- Debe permitir reportar al fabricante eventos que son falso-positivo y falso-negativo en el análisis de malware de día cero a partir de la propia consola de administración.
- Permitir la subida de archivos al sandbox de forma manual y vía API, con el objetivo de automatizar las tareas de análisis dinámico
- Debe detectar técnicas usadas para evadir herramientas de sandboxing como detección de hypervisor (no debe usar hypervisores comerciales), inyección de código a procesos permitidos y deshabilitación de funcionalidades de seguridad del host.
- La solución debe realizar el análisis en un ambiente de hardware real, deshabilitando totalmente la habilidad de la amenaza de evadir sandboxing en máquinas virtuales.

3.4.6 Requerimientos técnicos

La PLATAFORMA deberá soportar las siguientes características técnicas generales

3.4.6.1 Provisión de Infraestructura en la nube

La PLATAFORMA deberá utilizar recursos virtualizados en la nube, que incluyen servidores virtuales (instancias de cómputo), almacenamiento de datos (bloque, objeto y archivo), y redes virtuales (VPC). La PLATAFORMA deberá ser multiplataforma, podrá utilizar como CONTRATISTA de nube AWS, Azure, o Google Cloud, que ofrecen escalabilidad automática, alta disponibilidad y recuperación ante desastres (DR). En el caso de la información / base de datos, el CONTRATISTA deberá implementar configuraciones que permitan mantener la información del FMV aislada de la de otros clientes o de terceros. Además, la infraestructura en la nube debe proporcionar logs de auditoría respecto a los accesos, conexiones y uso de recursos.

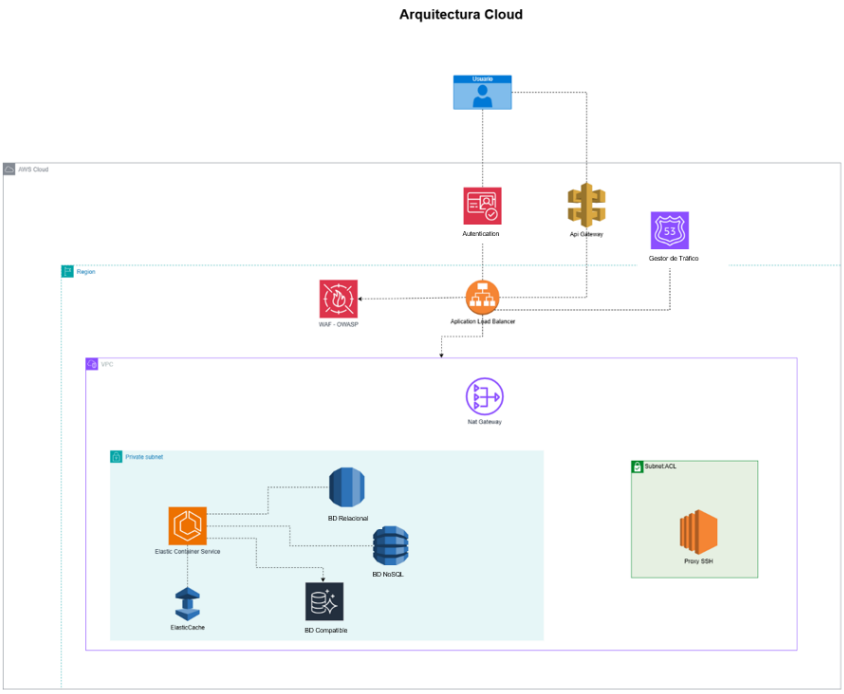
a. Componentes Principales (Zona de Acceso Público)

- **Acceso del usuario final**: Los usuarios podrán acceder a la plataforma desde entornos Web o Mobile, mediante mecanismos seguros de autenticación.
- **Gestión de tráfico DNS**: Un servicio de resolución de nombres dirigirá el tráfico hacia la plataforma, permitiendo balanceo inteligente y alta disponibilidad.
- **API Gateway**: Se encargará de recibir, enrutar y controlar las solicitudes que llegan a los diferentes microservicios.
- **Firewall de aplicaciones web (WAF)**: Protegerá la plataforma contra amenazas comunes del entorno web, como las definidas por OWASP.
- **Balanceador de carga de aplicaciones (ALB)**: Distribuirá el tráfico entrante hacia los servicios internos de forma eficiente y segura.

b. Zona Privada de Procesamiento (Red Privada Virtual - VPC)

- **Elastic Container Service (ECS):** Los microservicios de la plataforma estarán desplegados en un entorno de contenedores orquestados (por ejemplo, Kubernetes o Docker Swarm), permitiendo escalabilidad y aislamiento funcional.
- **Base de datos relacional:** Se utilizará un motor de base de datos estructurada para la gestión transaccional de los procesos del negocio.
- **Motor de base de datos compatible:** Complementariamente, se podrá usar un segundo motor de base de datos estructurada de alta disponibilidad para redundancia o carga distribuida.
- **Base de datos NoSQL:** Para operaciones de alta velocidad y almacenamiento de estructuras no relacionales, se dispondrá de una base de datos NoSQL.
- **ElasticCache (Redis/Memcached):** Mejorará el rendimiento de la plataforma mediante almacenamiento temporal de datos frecuentemente consultados.
- **NAT Gateway:** Permitirá que los servicios desplegados en la red privada accedan a Internet sin exponer directamente las instancias internas.

- **Proxy seguro para administración remota:** Se habilitará un mecanismo de acceso seguro (bastion host o túnel controlado) para tareas administrativas, con políticas de control de acceso basadas en listas (ACLs) y monitoreo de sesiones.



3.4.6.2 Instancias de cómputo:

La PLATAFORMA deberá soportar instancias de cómputo que deben configurarse con capacidades flexibles (escalado vertical y horizontal), optimizadas para soportar cargas transaccionales de la PLATAFORMA. Esto incluye instancias de alta memoria (RAM) para procesos intensivos y de alta capacidad de entrada/salida para tareas de procesamiento.

3.4.6.3 Almacenamiento y Base de Datos:

La PLATAFORMA deberá soportar las siguientes características técnicas dependiendo de la arquitectura propuesta por el CONTRATISTA de la PLATAFORMA.

a. **Almacenamiento Persistente:** Uso de almacenamiento escalable para datos no estructurados y archivos de respaldo.
b. **Bases de Datos Relacionales:** Implementación de bases de datos relacionales para la gestión de datos transaccionales. Se recomienda el uso de bases de datos con capacidades de replicación y clustering para garantizar disponibilidad y consistencia.
c. **Bases de Datos NoSQL:** En caso la propuesta del CONTRATISTA contemple bases de datos no relacionales, se recomienda cachés de alta velocidad.
d. Implementar logs de cambios en las principales tablas transaccionales y según requerimiento del FMV durante la ejecución del servicio

3.4.6.4 Arquitectura de Microservicios:

La PLATAFORMA deberá soportar arquitectura de microservicios con las siguientes recomendaciones.

a. **Microservicios desplegados en contenedores:** La PLATAFORMA deberá ser modular, basada en una arquitectura de microservicios implementados mediante contenedores (Docker) y orquestados con Kubernetes. Esto permite la escalabilidad independiente de cada componente y mejora la resiliencia de la PLATAFORMA.

b. **API Gateway:** Implementación de un API Gateway para gestionar el acceso a los microservicios, proporcionando autenticación, autorización, control de tráfico y enrutamiento seguro.
c. **Mensajería y Gestión de Eventos:** Uso de servicios de mensajería para manejar la comunicación asíncrona entre microservicios, facilitando el procesamiento de eventos y la integración con otros sistemas.

3.4.6.5 Seguridad y Cumplimiento:

La PLATAFORMA deberá soportar

a. **Cifrado de Datos:**
    i. En Tránsito: Uso de protocolos SSL/TLS para cifrar los datos durante la transmisión.
    ii. En Reposo: Cifrado de datos en almacenamiento mediante tecnologías como AES-256.
b. **Autenticación y Autorización:** Implementación de autenticación multifactor (MFA) y protocolos de autenticación robustos como OAuth 2.0 y OpenID Connect. Integración con un Identity Provider (IdP) para la gestión de identidades y accesos.
c. **Firewall de Aplicaciones Web (WAF):** Implementación de un WAF para proteger a la PLATAFORMA contra amenazas comunes como inyección SQL, Cross-Site Scripting (XSS) y ataques DDoS.
d. **Gestión de Identidades y Accesos (IAM):** Uso de políticas IAM para controlar el acceso, asegurando el principio de privilegio mínimo.

3.4.6.6 Monitoreo y Auditoria

Implementación de sistemas de monitoreo continuo o servicios nativos para la revisión de métricas clave, rendimiento y alertas en tiempo real. Registro de auditoría para cumplimiento normativo. Adicionalmente, el CONTRATISTA deberá proporcionar evidencia de los controles de seguridad de la información y ciberseguridad implementados a fin de que el FMV pueda realizar una verificación anual de los mismos.

3.4.6.7 Alta Disponibilidad y Recuperación ante Desastres (Disaster Recovery):

La PLATAFORMA deberá soportar:

a. **Alta Disponibilidad (HA):** Implementación de instancias de aplicación en múltiples zonas de disponibilidad (AZ) dentro de una región para garantizar alta disponibilidad. Configuración de bases de datos en modo multi-AZ o multi-región para asegurar la continuidad del servicio. El CONTRATISTA deberá informar al FMV antes de la etapa de puesta a producción de la PLATAFORMA, de las ubicaciones físicas relevantes para la ejecución del servicio, señalando como mínimo: ubicación de los data centers principal y de contingencia para nube, centro de atención y resolución de incidentes.
b. **Recuperación ante Desastres (DR):** Plan de DR con copias de seguridad automáticas, replicación de datos a una región secundaria y al menos dos pruebas anuales de recuperación. Los escenarios de prueba, Tiempo Objetivo de Recuperación (RTO) y Punto Objetivo de Recuperación (RPO) deben estar claramente definidos y alineados con los requisitos que el FMV establezca.

3.4.6.8 Automatización y DevOps:

Es recomendable que el CONTRATISTA de la PLATAFORMA utilice DevOps e IaC para entrega continua de las nuevas versiones y actualizaciones:

a. **Pipeline de CI/CD:** Uso de herramientas de integración y entrega continua como Jenkins, GitLab CI, o GitHub Actions para automatizar el ciclo de vida de desarrollo y despliegue de aplicaciones. Esto incluye pruebas automatizadas (unitarias, de integración y de seguridad), despliegues automatizados y rollback en caso de fallos.

b. **Infraestructura como Código (IaC):** Implementación para gestionar la configuración y despliegue de recursos en la nube de forma automatizada y versionable.

3.4.6.9 Latencia y Rendimiento.

a. **Optimización de Rendimiento:** La PLATAFORMA deberá disponer de herramientas de monitoreo para identificar cuellos de botella y optimizar el tiempo de respuesta.

3.4.7 GOBIERNO DEL SERVICIO

Con el objetivo de garantizar una adecuada implementación, operación y evolución de la Plataforma Integral para la Gestión de Créditos, el modelo de servicio deberá contemplar un esquema formal de gobernanza y gestión del proyecto, que asegure el cumplimiento de objetivos institucionales, el control sobre la ejecución del servicio, y la mejora continua de la solución entregada.

3.4.7.1 Marco de Liderazgo del Proyecto

3.4.7.1.1 Equipo de Gobierno del CONTRATISTA

La ejecución del servicio estará a cargo de un equipo profesional y técnico especializado, conformado por el CONTRATISTA, con responsabilidades claramente asignadas para asegurar la correcta planificación, implementación, operación y evolución de la Plataforma Integral para la Gestión de Créditos. Este equipo deberá tener experiencia demostrada en el sector financiero y en la ejecución de proyectos tecnológicos complejos.

Liderazgo del Servicio
El CONTRATISTA deberá designar a un Gerente Principal del Servicio, quien será el responsable máximo del cumplimiento integral de los objetivos del contrato. Este profesional tendrá funciones estratégicas y ejecutivas, y será el principal interlocutor con la alta dirección del FONDO. Su responsabilidad incluye la supervisión directa de todo el equipo asignado por el CONTRATISTA, la toma de decisiones críticas, la atención de observaciones relevantes y la representación institucional del CONTRATISTA en instancias de alto nivel.

Estructura del Equipo Clave del CONTRATISTA (por nivel estratégico y funcional)
A continuación, se detalla la estructura del equipo clave ordenada según su nivel estratégico y de responsabilidad:

- **Product Manager**: Define la visión funcional y estratégica del producto. Prioriza funcionalidades, supervisa el roadmap y asegura la alineación de la solución con los objetivos del negocio y los requerimientos normativos.
- **Gestor de Servicios:** Encargado de la operación diaria del servicio. Administra incidencias, y asegura el cumplimiento del alcance definido en los términos de referencia.
- **Jefe de Servicios y Seguridad**: Responsable de la supervisión de los servicios TI asociados a la PLATAFORMA, asegurando su disponibilidad, integridad y cumplimiento con políticas de seguridad, continuidad operativa y planes de recuperación.
- **Project Manager Profesional (PMP) del CONTRATISTA**: Lidera la planificación, ejecución y supervisión del proyecto dentro del equipo del CONTRATISTA. Asegura la entrega oportuna y con calidad de los entregables, coordina al equipo técnico y mantiene la comunicación continua con el Jefe de Proyecto del FMV.
- **Arquitecto de la Nube**: Diseña y mantiene la arquitectura tecnológica de la plataforma en la nube. Garantiza escalabilidad, resiliencia, seguridad y alineación con las mejores prácticas en servicios cloud (AWS, Azure, GCP).

Además de estos perfiles clave, el CONTRATISTA deberá integrar como parte del servicio a personal técnico no clave, incluyendo desarrolladores, analistas funcionales, testers, especialistas en soporte y operación, entre otros. Este personal será responsable de ejecutar las tareas operativas, técnicas y de desarrollo en cada fase del proyecto, actuando bajo la supervisión directa del equipo clave, y será fundamental para el cumplimiento de los entregables, la calidad técnica y la sostenibilidad de la plataforma.

3.4.7.1.2 Equipo de gobierno del FMV

Para efectos de gobernanza, supervisión y control del proyecto, el FONDO designará formalmente equipos responsables y un Jefe de Proyecto que participará activamente en todas las fases del servicio, desde la implementación hasta la operación y mejora continua de la Plataforma para la Gestión de Créditos. Este equipo estará conformado por:

Jefe de Proyecto del FONDO
Al inicio del proyecto el FONDO designará un Jefe de Proyecto con dedicación exclusiva durante toda la vigencia del servicio, quien asumirá el rol de responsable técnico y contractual con las siguientes funciones:

- Verificar el cumplimiento de los entregables, plazos y condiciones técnicas del servicio.
- Emitir pronunciamiento sobre los informes y entregables del CONTRATISTA dentro de los plazos establecidos.
- Coordinar con el Gestor del Servicio las comunicaciones formales de la ejecución contractual.
- Convocar y presidir las reuniones de seguimiento técnico del proyecto.
- Reportar al Equipo Estratégico de Gobierno cualquier incumplimiento, desviación o riesgo crítico.
- Gestionar los vistos buenos de las áreas del FONDO para la conformidad de entregables.
- Proponer la aplicación de penalidades cuando corresponda.

El jefe de Proyecto no podrá modificar el alcance del servicio ni asumir compromisos fuera de las atribuciones expresamente señaladas en el presente requerimiento.

Equipo Estratégico de Gobierno del Proyecto (Nivel Directivo):

Este grupo debe estar conformado por directivos o jefaturas del FMV con capacidad de decisión, que velen por el alineamiento del proyecto con los objetivos institucionales. Se encargarían de:

- Participar en **comités estratégicos y de seguimiento de alto nivel**.
- Tomar decisiones frente a cambios de alcance, prioridades o riesgos críticos.
- Aprobar entregables claves o aceptar hitos del proyecto.
- Validar aspectos normativos, presupuestales o funcionales que superen el ámbito técnico-operativo.

Lo conformaran:
- El **Jefe de Proyecto**
- Gerente General
- Gerente de Operaciones.
- Gerente de Finanzas
- Gerente de Riesgos
- Jefatura de Tecnología de la Información.

- Otros directivos, Gerentes o Jefes designados por resolución o documento interno.

Equipo Técnico-Operativo del Proyecto (Nivel de ejecución):

Este es el equipo que trabaja de forma directa y continua con el CONTRATISTA. Se encarga de:

- Supervisar la ejecución técnica, funcional y documental del servicio.
- Participar en las reuniones de avance, pruebas, certificaciones, marchas blancas, etc.
- Validar entregables operativos.
- Canalizar requerimientos internos hacia el CONTRATISTA.
- Participar en el Comité de Seguimiento mensual.

Este grupo incluye:

- El Jefe de Proyecto del FONDO.
- Especialistas de las áreas usuarias de la Gerencia de Operaciones, Finanzas, Administración y Riesgos del FMV (originación, formalización, cobranza, etc.).
- Personal de la Oficina de Tecnologías de la Información del FMV: Analistas funcionales, arquitectos o especialistas de infraestructura, especialistas de seguridad del FMV.
- Personal de legal o normativo del FMV (cuando el tema lo amerite).

3.4.7.2 Marco de Coordinación y Gestión del Proyecto

Para asegurar una adecuada gestión, coordinación y trazabilidad del proyecto, se requiere que el CONTRATISTA designe a su costo **un (01) Project Manager Profesional (PMP)**:

a) PMP del CONTRATISTA

El CONTRATISTA deberá contar con su Jefe de Proyecto, quien liderará la ejecución interna del proyecto desde su organización. Este profesional desarrollará actividades de forma exclusiva y obligatoria hasta la FASE 3. Sus principales funciones serán:

- Planificar, ejecutar y supervisar las actividades del equipo técnico y funcional del CONTRATISTA.
- Garantizar la entrega oportuna y con calidad de los entregables establecidos.
- Elaborar informes de avance y mantener actualizada la matriz de riesgos, plan de comunicaciones y cronograma.
- Gestionar los mecanismos de control de cambios y velar por el cumplimiento de SLA y KPI acordados.
- Coordinar permanentemente con el Jefe de Proyecto asignado por el FONDO, asegurando la alineación de expectativas y objetivos.

3.4.7.3 Comités de Gestión, Seguimiento y Mejora Continua del Servicio

3.4.7.3.1 Conformación y Participación

El Comité estará conformado por el **Equipo Estratégico** del FONDO, así como por el personal clave del CONTRATISTA. La participación de todos los integrantes designados por ambas partes será de carácter obligatorio.

Será requisito indispensable la asistencia presencial de todos los miembros del comité conforme a lo estipulado en los presentes Términos de Referencia, de ser necesario se incluirán especialistas técnicos, funcionales y de soporte, según los temas establecidos en la agenda correspondiente.

Las reuniones del Comité se desarrollarán en las instalaciones del FONDO. Solo en casos excepcionales, debidamente justificados y aprobados por el FONDO, se podrá autorizar otra modalidad de participación.

3.4.7.3.2 Frecuencia y Funcionamiento

El Comité se reunirá con una periodicidad **mensual** como mínimo, pudiendo convocarse de manera extraordinaria ante eventos críticos, contingencias o situaciones que ameriten atención inmediata. El FONDO podrá solicitar la conformación de **comités especializados** adicionales (por ejemplo, comité técnico, de seguridad, de interoperabilidad, de migración, entre otros), en función de la criticidad o especificidad de determinadas fases o componentes del servicio. Las reuniones del Comité deberán desarrollarse bajo principios de **mejora continua** (Ciclo PDCA: Planificar – Hacer – Verificar – Actuar) y **buenas prácticas de gestión de servicios y gobierno de TI**, tales como ITIL y COBIT.

3.4.7.3.3 Funciones Principales

El Comité tendrá, entre otras, las siguientes funciones:

- Monitorear el avance del proyecto respecto al cronograma, entregables y metas establecidas.
- Evaluar el cumplimiento de los **indicadores clave de desempeño (KPI)**, los **acuerdos de nivel de servicio (SLA)** y demás niveles comprometidos.
- Analizar incidentes críticos y proponer acciones correctivas, preventivas o de mejora evolutiva.
- Revisar, validar y priorizar **requerimientos de cambio**, bajo procesos formales de gestión del cambio.
- Evaluar propuestas de mejoras funcionales o técnicas que aporten valor institucional.
- Verificar el cumplimiento normativo, la seguridad, y la alineación con los estándares de calidad requeridos.
- Validar todos los **entregables técnicos, funcionales y documentales** presentados por el CONTRATISTA.

3.4.7.3.4 Documentación y Acuerdos

Al término de cada sesión del Comité, se deberá elaborar un **acta oficial**, la cual deberá ser **firmada por ambas partes el mismo día de la reunión**. Esta acta deberá contener como mínimo: los temas tratados, acuerdos adoptados, responsables asignados, plazos de cumplimiento y observaciones relevantes. Las actas deberán ser remitidas como parte integral de los entregables correspondientes a cada fase del proyecto.

3.4.8 Gestión del Servicio durante la Fase 4, 5 y 6

Durante la etapa Operativa y de soporte bajo modalidad de horas a demanda (Fases 4, 5 y 6), se mantendrá el esquema de gobernanza descrito, adaptado a la naturaleza de la operación. El comité de seguimiento continuará activo, manteniendo la supervisión sobre los niveles de servicio (SLA), evolución funcional, atención de incidentes y soporte técnico.

El PMP del CONTRATISTA deberá mantenerse vigente como responsable del servicio durante toda la etapa operativa, mientras que el FMV evaluará la continuidad o reemplazo de su Jefe de Proyecto asignado conforme a sus necesidades internas.

3.4.9 DOCUMENTOS PARA PRESENTACIÓN DE OFERTA

El postor deberá presentar, como parte de su propuesta, la documentación que acredite lo siguiente:

- Ser **partner de desarrollo** de al menos una de las principales nubes públicas:
  - Amazon Web Services (AWS), o

- Google Cloud Platform (GCP), o
- Microsoft Azure.
- Oracle Cloud Infraestructure (OCI)

- Contar con al menos **una (01) solución certificada** por la nube correspondiente, por ejemplo:
  - AWS Certified Solutions,
  - Google Cloud Partner Advantage, o
  - Azure Marketplace Certification

- Certificación vigente de Diseño y/o Construcción de Data Center bajo alguno de los siguientes estándares:
  - Uptime Institute Tier III, y/o
  - ANSI/TIA-942-B Rated-3, y/o
  - ANSI/TIA-942-C-2024.
- Contar con acreditación vigente que certifique que el NOC y SOC son de propiedad del postor y operan de manera ininterrumpida.

Asimismo, deberá remitir la siguiente documentación, conforme a lo dispuesto en la Resolución SBS Nº 504 – 2021, Reglamento de Seguridad de Información y Ciberseguridad.

- Certificación vigente del ISO 9001:2015
- Certificación vigente del ISO/IEC 27001:2022
- Reportes: SOC 2 Tipo II u otros equivalentes

3.4.10 NIVELES DE SERVICIO

Los niveles de servicios se comenzarán a medir a partir del inicio de la etapa operativa. La aplicación de las penalidades se realiza una vez concluido la etapa de marcha blanca de la FASE

Los niveles de servicio serán revisados por el FMV, con una periodicidad mensual y, de ser necesario, se realizarán los cambios pertinentes, con la finalidad de mejorar la calidad del servicio.
La siguiente tabla, resume los niveles de servicios por indicador establecidos a razones imputables el CONTRATISTA para el presente servicio, los mismos que se medirán con una frecuencia mensual.

3.4.10.1 Acuerdos de Nivel de Servicio

Código	Forma de Medición	SLA	Supuesto de Aplicación de la Penalidad	Penalidad
SLA-01	Disponibilidad de la plataforma	99.6% de uptime	Si la disponibilidad cae por debajo del 99.6%.	Penalización aplicada según el porcentaje de disponibilidad perdido.
SLA-02	Clasificación de incidentes – Crítico	Respuesta < 2 horas desde la notificación de la incidencia por parte del FONDO. Resolución < 4 horas desde la notificación de la	Si el tiempo de respuesta o resolución excede los valores establecidos. Incidencias Criticas: Estas son incidencias que afectan gravemente el funcionamiento de la plataforma, causando	Penalización por cada incidente no resuelto en el tiempo establecido.

		incidencia por parte del FONDO. Dicha notificación será vía correo o plataforma.	interrupciones totales en la plataforma o impidiendo el acceso a funciones clave.	
SLA-03	Clasificación de incidentes – Alto	Respuesta < 4 horas desde la notificación de la incidencia por parte del FONDO. Resolución < 6 horas desde la notificación de la incidencia por parte del FONDO. Dicha notificación será vía correo o plataforma.	Si el tiempo de respuesta o resolución excede los valores establecidos. Incidencias Alto: Impactan el servicio de manera significativa, pero no provocan una interrupción total de la plataforma. Pueden incluir problemas con algunos módulos específicos de la plataforma o dificultades en la ejecución de ciertos procesos importantes	Penalización por cada incidente no resuelto en el tiempo establecido.
SLA-04	Clasificación de incidentes - Medio	Respuesta < 8 horas, desde la notificación de la incidencia por parte del FONDO. Resolución < 16 horas desde la notificación de la incidencia por parte del FONDO. Dicha notificación será vía correo o plataforma.	Si el tiempo de respuesta o resolución excede los valores establecidos. Incidencias Medio: o Son problemas que no afectan gravemente la operatividad de la plataforma y tienen un impacto limitado o parcial. Pueden incluir fallos menores, como errores en informes no críticos o problemas con funcionalidades secundarias de la plataforma.	Penalización por cada incidente no resuelto en el tiempo establecido.
SLA-05	Clasificación de incidentes - Bajo	Respuesta < 12 horas desde la notificación de la incidencia por parte del FONDO. Resolución < 24 horas desde la notificación de la incidencia por parte del FONDO.	Si el tiempo de respuesta o resolución excede los valores establecidos Incidencias Bajo: Son incidencias menores que tienen un impacto limitado en la plataforma y no afectan la funcionalidad principal de la plataforma	Penalización por cada incidente no resuelto en el tiempo establecido.

		Dicha notificación será vía correo o plataforma.		
SLA-06	Soporte 24/7 para momentos críticos	Garantizar soporte 24/7 Respuesta < 15 minutos desde la notificación de la incidencia por parte del FONDO. Resolución < 1 hora desde la notificación de la incidencia por parte del FONDO.	Si el soporte no está disponible en momentos críticos los como cierres mensuales, cierres contables o generación de reportes regulatorios.	En caso de indisponibilidad del soporte en algún momento crítico, se aplicará una penalización.
SLA-07	Tiempo de respuesta de la PLATAFORMA por causas imputables al Contratista	Respuesta < 3 segundos desde iniciado la interacción.	Si el tiempo de respuesta de la PLATAFORMA en todas las operaciones, salvo las operaciones que sean más complejas debidamente coordinadas entre ambas partes, excede los 3 segundos.	Penalización por cada medición que supere el tiempo establecido.
SLA-08	Tiempo de procesamiento de transacciones	Cierre de operaciones diarias < 3 horas desde iniciado el cierre del día. Cierre de operaciones mensuales < 5 horas desde iniciado el cierre mensual.	Si el tiempo de procesamiento de operaciones diarias o mensuales excede lo establecido.	Penalización por cada incumplimiento de tiempo en procesos de cierre.
SLA-09	RTO (Recovery Time Objective)	Restauración del servicio < 4 horas desde notificado la indisponibilidad de cualquier componente del servicio.	Si el tiempo de restauración de cualquier componente del servicio excede las 4 horas, y esto sea por causas atribuibles al Contratista.	Penalización por cada incidente que supere el tiempo establecido.
SLA-10	RPO (Recovery Point Objective)	Cantidad de datos perdidos.	Si se registra una pérdida de datos, y esto sea por causas	Penalización basada en la cantidad horas irrecuperables

			atribuibles al Contratista.	
SLA-11	Pruebas de recuperación	Realizar pruebas de recuperación de desastres al menos dos veces al año	Si no se realizan las pruebas de recuperación según la periodicidad establecida.	Penalización en caso de incumplimiento de pruebas de recuperación.
SLA-12	Pérdidas de información por fallas o vulnerabilidades	0 incidentes de pérdida de información	En caso se produzca un evento de pérdida de información sensible derivado de accesos no autorizados o vulneración de la arquitectura/plataforma.	Penalización del 15% de la facturación mensual por cada incidente reportado.

3.4.11 FASES DEL SERVICIO

La implementación de la PLATAFORMA para el FONDO se llevará a cabo en varias etapas claramente definidas, cada una con objetivos y actividades específicas que deben ser cumplidas por el CONTRATISTA de la PLATAFORMA. A continuación, se detallan las 6 FASES del proceso, desde la implementación de la PLATAFORMA hasta el soporte continuo.

Fase	Alcance
FASE 1	a. Diseño e Implementación de la Arquitectura de la Nube b. Desarrollo e Implementación de la Plataforma para la Gestión de Créditos – Nuevos Productos y Migración de Carteras (Reemplazo del NSCC), la cual debe contener desde el desarrollo, pruebas y puesta en producción de los siguientes 6 módulos: - Módulo de originación - Módulo de configuración - Módulo de clientes - Módulo de créditos - Módulo Contable - Módulo Normativo - Módulo de Reportes - Módulo Exconeminsa, IFI en Liquidación c. Marcha Blanca, para validar el funcionamiento completo de la solución implementada en un entorno de operación real y supervisado.
FASE 2	a. Implementación de la Plataforma para la Gestión de créditos - Fideicomiso, Garantías y Provisiones (Reemplazo de actual sistema SAOC y SIR), la cual debe contener desde el desarrollo, pruebas y puesta en producción de los siguientes 6 módulos:

	- Módulo de fideicomisos - Módulo CRC - PBP - Módulo de Garantías - Módulo de tesorería - Servicio CRC - Servicio CRI b. Marcha Blanca, para validar el funcionamiento completo de la solución implementada en un entorno de operación real y supervisado.
FASE 3	Migración de datos históricos Durante esta fase se debe realizar la migración de toda la información del Fideicomiso COFIDE hacia la nueva plataforma.
FASE 4	Corresponde a la operación continua del servicio implementado.
FASE 5	Transición de salida
FASE 6	Bolsa de horas

3.4.11.1 FASE 1

Etapa 1: Diseño e Implementación de arquitectura de la nube

Su finalidad es diseñar e implementar una arquitectura tecnológica en la nube, que servirá como base fundamental sobre la cual se desplegará, de manera integral y segura, la Plataforma para la Gestión de Créditos del FONDO. Esta infraestructura deberá estar diseñada para alojar de forma óptima todos los componentes técnicos y funcionales de la plataforma, garantizando el cumplimiento de los requerimientos de rendimiento, escalabilidad, seguridad, interoperabilidad e integración con los sistemas actuales del FMV.

La infraestructura cloud será de titularidad exclusiva del FONDO, quedando registrada a su nombre y configurada para su uso institucional permanente, lo que asegurará independencia tecnológica, soberanía sobre los datos y sostenibilidad a largo plazo. No obstante, el CONTRATISTA será responsable de gestionar integralmente dicha infraestructura en calidad de partner tecnológico, encargándose del diseño, provisión, configuración, monitoreo, operación, mantenimiento y soporte continuo de los servicios en la nube, de acuerdo con los niveles de servicio (SLA) establecidos.

Asimismo, esta arquitectura servirá como habilitador para poner a disposición de las Instituciones Financieras Intermediarias (IFI) una plataforma digital moderna e interoperable, la cual podrán utilizar directamente o integrar con sus propios sistemas de información. Esto facilitará procesos clave como la originación, evaluación, desembolso, seguimiento y extornos de créditos hipotecarios y fideicomisos, en coordinación con el FMV.

Para alcanzar estos objetivos, la etapa comprende los siguientes subprocesos:

1. Levantamiento de requerimientos técnicos, normativos y operativos

Durante este periodo, el CONTRATISTA deberá identificar y documentar los requerimientos técnicos, normativos y operativos necesarios para el diseño de la arquitectura de nube. La recopilación debe considerar aspectos de seguridad, escalabilidad, normativas SBS, integración con sistemas existentes y requerimientos funcionales del entorno actual.

Entregable	Contenido mínimo
Informe de Requerimientos	• Necesidades técnicas, operativas y regulatorias.

Técnicos, Normativos y Operativos	• Condiciones del entorno tecnológico actual. • Requerimientos de integración e interoperabilidad. • Consideraciones de cumplimiento normativo y seguridad.

2. **Diseño de la arquitectura de nube**
   En esta etapa se elaborará el diseño lógico y físico de la arquitectura de nube, definiendo la topología, componentes, ambientes, seguridad, respaldo y modelo operativo.

Entregable	Contenido mínimo
Documento de Diseño de Arquitectura de Nube	• Diagramas lógicos y físicos. • Topología de red y estructura de ambientes. • Políticas de seguridad, respaldo y contingencia. • Estrategia de escalabilidad y disponibilidad

   El diseño de arquitectura de nube deberá ser presentado formalmente al FONDO para su revisión y aprobación. La aprobación expresa del FMV será condición indispensable para que el CONTRATISTA pueda iniciar cualquier actividad de despliegue, implementación o configuración de la infraestructura en nube. En consecuencia, el CONTRATISTA no podrá avanzar a la etapa de despliegue mientras el Documento de Diseño de Arquitectura de Nube no cuente con la conformidad correspondiente del FMV.

3. **Despliegue de la infraestructura cloud**
   Este subproceso comprende la creación, configuración y puesta en funcionamiento de los recursos en la nube según el diseño aprobado. Incluye la habilitación de los entornos definidos (producción, pruebas, preproducción), configuraciones de red, accesos, firewalls, almacenamiento y demás componentes requeridos.

Entregable	Contenido mínimo

Informe de Despliegue de Infraestructura Cloud	• Recursos aprovisionados y su configuración.
	• Evidencias de habilitación de lo diferentes ambientes tales como:
	  ○ Ambiente Productivo
	  ○ Ambiente Pre Producción
	  ○ Ambiente Calidad o Pruebas
	• Configuración de políticas de acceso y respaldo por cada ambiente.
	• Validación inicial de los entornos y/o ambientes operativos (Produccitivo, Pre Producción, Calidad o Pruebas) .

4. **Pruebas de validación de la infraestructura**
   Durante esta fase se ejecutarán pruebas técnicas para verificar el correcto funcionamiento, rendimiento, disponibilidad y cumplimiento de los parámetros establecidos en el diseño de la arquitectura.

Entregable	Contenido mínimo

Informe de Validación de Infraestructura	• Plan de pruebas ejecutado y resultados obtenidos. • Validación de conectividad, rendimiento y seguridad. • Registro de incidencias y acciones correctivas aplicadas. • Conformidad técnica por el lado del FMV del diseño implementado.

5. Cierre de la Etapa 1

El informe de cierre de la Etapa 1 deberá ser presentado por el Contratista máximo al día siguiente de culminada dicha etapa. Su aceptación estará sujeta a la evaluación y conformidad expresa del FMV, la cual deberá emitirse en un plazo máximo de siete (07) días calendario contados desde el día siguiente de la recepción del informe.

En caso se identifiquen observaciones, estas deberán ser subsanadas por el contratista en un plazo no mayor a cinco (05) días calendario contados a partir del día siguiente de la notificación correspondiente.

Entregable	Contenido mínimo
Informe de cierre de la Etapa 1	• Documento de Diseño de Arquitectura de Nube aprobado por el Jefe de la Oficina de Tecnologías • Informe de Despliegue de Infraestructura Cloud aprobado por el por el Jefe de la Oficina de Tecnologías • Informe de Validación de Infraestructura aprobado por el por el Jefe de la Oficina de Tecnologías

Etapa 2: Desarrollo e Implementación de la Plataforma para la Gestión de Créditos – Nuevos Productos y Migración de Carteras (Reemplazo del NSCC)

Esta etapa se desglosa en varios subprocesos clave que permitirán desarrollar la PLATAFORMA de acuerdo a las necesidades del **FONDO**.

1. Análisis del entorno

En esta etapa, el CONTRATISTA deberá realizar el relevamiento, revisión y análisis detallado de la situación actual del FONDO, con la finalidad de identificar los procesos, sistemas, integraciones, información, necesidades funcionales, técnicas, operativas, normativas y de seguridad que deberán ser considerados para la implementación de la Plataforma para la Gestión de Créditos.

El análisis deberá comprender la revisión de los procesos actuales vinculados a la gestión crediticia, así como la identificación de brechas funcionales y técnicas —GAP Analysis— entre la situación actual del FONDO, las funcionalidades requeridas y la solución tecnológica a implementar.

Como mínimo, el análisis deberá considerar los siguientes módulos o componentes funcionales:

Módulo de originación.
Módulo de configuración.
Módulo de clientes.
Módulo de créditos.
Módulo contable.

Módulo normativo.
Módulo de reportes.
Módulo de gestión de carteras especiales, incluyendo Ex CONEMINSA e IFI en liquidación.
Integraciones con sistemas internos y externos necesarios para la operación de la plataforma.

El CONTRATISTA deberá identificar las necesidades de integración con los sistemas internos del FONDO, entidades externas, Instituciones Financieras Intermediarias —IFI— y demás plataformas que intervengan en los procesos de originación, administración, seguimiento, cobranza, conciliación, liquidación, registro contable, reportes y control de los productos financieros administrados por el FONDO.

Entregable	**Contenido mínimo**
Informe del Discovery GAP Análisis del entorno	El Informe de Discovery y GAP Analysis del Entorno deberá contener, como mínimo: • Análisis del estado actual de los sistemas, procesos y operaciones del FONDO vinculados a la gestión de créditos, fideicomisos, garantías, carteras especiales, cobranza, conciliación, contabilidad y reportes. • Identificación de los sistemas actuales que serán reemplazados, integrados, consultados o considerados durante la implementación de la plataforma. • Identificación de brechas funcionales y técnicas —GAP Analysis—, precisando su descripción, impacto, prioridad, responsable y recomendación de tratamiento. • Identificación preliminar de requerimientos funcionales por módulo o proceso. • Identificación preliminar de requerimientos no funcionales, incluyendo seguridad, disponibilidad, rendimiento, escalabilidad, trazabilidad, interoperabilidad, usabilidad y mantenibilidad. • Requerimientos preliminares de integración con sistemas internos del FONDO, entidades externas, IFI, servicios de autenticación, sistemas contables, plataformas de cobranza, repositorios documentales y demás sistemas necesarios para la operación. • Identificación de riesgos iniciales asociados al entorno actual, tales como dependencia de sistemas heredados, calidad de datos,

	integraciones, continuidad operativa, seguridad, disponibilidad o restricciones normativas.

2. **Plan de Desarrollo**

En este subproceso el CONTRATISTA deberá presentar un plan de trabajo detallado a los interesados del **FONDO**, donde se definirán los objetivos del proyecto, el alcance del desarrollo y la implementación, el equipo de trabajo y las responsabilidades de cada parte involucrada. Este plan servirá como la guía para todas las actividades subsecuentes.

Este proceso debe concluir con el plan de desarrollo e implementación, el cual deberá incluir como mínimo.

Entregable	Contenido mínimo
Plan de desarrollo	• Objetivos del proyecto • Alcance de la implementación. • EDT del proyecto. • Organigrama del proyecto y la responsabilidad de cada rol • Riesgos iniciales del proyecto con su plan de mitigación • Métodos y frecuencia de comunicación entre el equipo y los interesados • Lista de personas clave o grupos que serán informados del progreso del proyecto • Estrategia de migración de los datos históricos. • Cumplimiento con los requisitos técnicos y de seguridad del punto 7.

3. **Definición del Alcance detallado**

En esta etapa, el CONTRATISTA deberá trabajar de manera coordinada con el FONDO para definir de forma clara el alcance funcional y técnico de la Plataforma para la Gestión de Créditos.
Para ello, el CONTRATISTA deberá revisar los procesos, productos, necesidades funcionales, requerimientos técnicos e integraciones identificadas durante el análisis del entorno, a fin de precisar qué funcionalidades serán implementadas, qué parámetros deberán configurarse, qué reglas de negocio serán consideradas y qué integraciones serán necesarias para el correcto funcionamiento de la plataforma.
Asimismo, el CONTRATISTA deberá realizar una presentación funcional de la solución propuesta, a fin de explicar al FONDO cómo se implementarán los principales procesos, productos, funcionalidades, parametrizaciones e integraciones identificadas. Esta presentación servirá como mecanismo de validación inicial del entendimiento del alcance y permitirá recoger precisiones antes del desarrollo e implementación de la plataforma.
Como resultado de esta etapa, el CONTRATISTA deberá elaborar el Documento de Alcance Funcional y Técnico, el cual deberá ser presentado al FONDO para su revisión y aprobación. Este documento constituirá la base para las actividades de diseño, desarrollo, configuración, construcción de integraciones, pruebas e implementación de la plataforma.
La aprobación del Documento de Alcance Funcional y Técnico por parte del FONDO será condición necesaria para continuar con las actividades de desarrollo e implementación correspondientes a la fase respectiva.Asimismo, el CONTRATISTA deberá elaborar el guion de pruebas modulares e integrales, el cual permitirá validar que las funcionalidades, reglas de negocio, integraciones,

reportes, parámetros y componentes implementados cumplen con el alcance aprobado antes de su despliegue y puesta en producción.

El Documento de Alcance Funcional y Técnico aprobado por el FONDO constituirá la línea base funcional y técnica de la fase correspondiente, por lo que las funcionalidades, integraciones, reportes, reglas de negocio, parámetros y componentes allí definidos formarán parte de la prestación principal del servicio, siempre que se encuentren vinculados al objeto y alcance del presente requerimiento.
Este subproceso debe concluir con el documento del alcance aprobado, el cual deberá contener como mínimo:

Entregable	Contenido mínimo
Documento de Alcance Funcional y Técnico	Documento funcional donde se considere como mínimo lo siguiente: • Definición de los productos del FONDO a implementar en La PLATAFORMA, con su alcance definición, parámetros y sus reglas de negocio. • Los requisitos funcionales de los productos a implementar • Los requisitos no funcionales (rendimiento, seguridad, usabilidad y mantenibilidad) • Identificación de las integraciones necesarias para el funcionamiento de la plataforma con sistemas internos del FONDO, entidades externas, IFI u otras plataformas vinculadas al proceso. Para cada integración se deberá precisar, como mínimo: - sistema origen; - sistema destino; - finalidad de la integración; - datos a intercambiar; - método de conexión; - periodicidad o momento de ejecución; - responsable funcional y técnico. • Detalle de las funcionales que quedan fuera del alcance. • Los criterios de aceptación: Detalles de cómo se evaluará si un entregable cumple los requisitos. • Indicadores de éxito: Medidas que permitan evaluar si el proyecto ha cumplido sus objetivos (KPIs, métricas). • Cualquier requisito legal, de cumplimiento, o de estándares que deba respetarse. • Lista de posibles riesgos y problemas que podrían surgir durante el proyecto. Incluyendo un plan de mitigación: Acciones preventivas o correctivas para minimizar los riesgos.

4. Desarrollo de la PLATAFORMA

En este subproceso, el CONTRATISTA de la PLATAFORMA implementará lo definido en el documento del alcance para habilitar los productos del FONDO, las interfaces requeridas con otras plataformas, los procesos automatizados de carga de información, los requisitos funcionales y requisitos no funcionales. Este subproceso concluirá con el informe por parte del CONTRATISTA que ha realizado sus pruebas unitarias de manera exitosa según los criterios de aceptación acordados con el FONDO.

Entregable	Contenido mínimo
Informe de pruebas unitarias	• Objetivo de las pruebas unitarias • Módulos, funciones o componentes probados • Tecnologías y frameworks de prueba • Descripción del entorno de pruebas (Hardware y software) • Describir la estrategia de pruebas • Cantidad total de pruebas unitarias realizadas, defectos corregidos, % de cobertura de las pruebas • Casos de pruebas, resultado esperado y resultado obtenido, estado de la prueba.

5. Capacitación

En este subproceso, el CONTRATISTA de la PLATAFORMA llevará a cabo sesiones de capacitación con un mínimo de 40 horas lectivas de formación para cada una de las 75 personas designado por el FMV, para asegurar que los usuarios y el personal del FONDO estén preparados para operar e. El Plan de Capacitación es un entregable previo a la etapa de Pase a Producción.

Este subproceso concluirá con el informe de capacitación por parte del CONTRATISTA de la PLATAFORMA:

N	Entregable	Contenido mínimo

1	**Plan de Capacitación**	• Objetivo General
		• Público Objetivo
		  ○ Descripción y segmentación de los grupos a capacitar (por ejemplo: usuarios funcionales, personal técnico, operadores, personal de seguridad de la información).
		• Modalidad de Capacitación
		• Estructura Curricular
		  ○ Módulos temáticos diferenciados por perfil (funcional, operativo, técnico, seguridad de la información).
		  ○ Temario detallado por módulo (temas, subtemas).
		  ○ Relación de los módulos con los roles del usuario en la plataforma.
		• Duración
		  ○ Cronograma de ejecución (fechas estimadas por grupo y módulo).
		• Metodología
		  ○ Enfoques pedagógicos o metodológicos (aprendizaje práctico, basado en escenarios reales, talleres guiados, etc.).
		• Docentes
		  ○ Relación de instructores propuestos (CVs abreviados) y asignación de los docentes por módulo.
		• Materiales y Recursos

		○ Listado de materiales a entregar (manuales, presentaciones, accesos a entornos de prueba, etc.). ○ Idioma de los materiales (preferiblemente en español). • Evaluación del Aprendizaje ○ Mecanismos de evaluación por módulo (pruebas prácticas, exámenes, simulaciones, etc.). ○ Criterios de aprobación. ○ Registro de asistencia y control de participación. • Indicadores de Cumplimiento % de participación, % de aprobación, % de satisfacción de los participantes (encuestas de calidad).
1	**Informe final de la capacitación**	• Objetivo de la capacitación • Alcance y contenido de la capacitación • Estrategia de la capacitación • Fechas, duración, lugar de la capacitación. • Información de los instructores • Información de los participantes • Evaluación de la capacitación • Resultados de la capacitación • Conformidad de los participantes del FMV • Conclusiones de la capacitación.

6. Certificación

En esta etapa se realizarán las pruebas necesarias para verificar que la Plataforma para la Gestión de Créditos funcione correctamente y cumpla con los requisitos funcionales, requisitos no funcionales, integraciones, reglas de negocio, reportes, parametrizaciones y criterios de aceptación definidos en el Documento de Alcance Funcional y Técnico aprobado por el FONDO.

El CONTRATISTA será responsable de conducir, coordinar, preparar, ejecutar y documentar todo el proceso de certificación de la plataforma, incluyendo la planificación de las pruebas, preparación de ambientes, carga de datos de prueba, elaboración y ejecución de casos de prueba, registro de evidencias, atención de observaciones, corrección de defectos y presentación de los resultados correspondientes.

La participación del FONDO en esta etapa estará orientada a revisar, validar y otorgar conformidad sobre los resultados de las pruebas, así como a formular observaciones cuando corresponda. Dicha participación no traslada al FONDO la responsabilidad de la ejecución técnica ni funcional del proceso de certificación, la cual corresponde al CONTRATISTA.

La etapa de certificación deberá concluir con la presentación del informe correspondiente, en el cual el CONTRATISTA sustente que la plataforma ha sido probada satisfactoriamente, que las observaciones y defectos identificados han sido atendidos, y que la solución se encuentra en condiciones de continuar con las actividades de despliegue, puesta en producción o marcha blanca, según corresponda.

Las actividades mínimas que debe realizar el CONTRATISTA son:

- **Planificación de las pruebas**

b. Definición de objetivos: Establecer los objetivos principales de las pruebas (Encontrar defectos, validar funcionalidades y evaluar rendimiento).
c. Alcance de las pruebas: Delimitar las características, módulos o funcionalidades del software que serán sometidos a prueba.
d. Tipos de pruebas a realizar: Definir los tipos de pruebas a incluir (pruebas unitarias, de integración, de rendimiento y de aceptación).
e. Criterios de entrada y salida: Establecer los criterios para iniciar y finalizar las pruebas (cuándo una prueba es satisfactoria o cuándo detener las pruebas).

- **Preparación del Entorno de Pruebas**
  a. Configuración del entorno: Preparar el entorno de pruebas (servidores, bases de datos, sistemas operativos) para simular el entorno real donde funcionará el software.
  b. Datos de prueba: Crear o definir datos de prueba representativos para evaluar diferentes escenarios.
  c. Herramientas de pruebas: Seleccionar y configurar herramientas necesarias para la ejecución de las pruebas.

- **Diseño de casos de prueba**
  a. Identificación de casos de prueba: Desarrollar casos de prueba detallados que cubran diferentes escenarios, tanto positivos como negativos.
  b. Especificación de pasos: Detallar los pasos a seguir para cada caso de prueba, incluyendo las entradas, acciones y resultados esperados.
  c. Prioridad de los casos de prueba: Clasificar los casos de prueba según su prioridad (alta, media, baja) basándose en el impacto y la criticidad de la funcionalidad evaluada.

- **Ejecución de pruebas**
  a. Ejecución manual o automatizada: Realizar pruebas manuales o automatizadas según lo planificado.
  b. Registro de resultados: Documentar los resultados de cada caso de prueba, especificando si pasó o falló.
  c. Registro de defectos: Identificar y registrar los defectos encontrados en una herramienta de seguimiento.

- **Gestión de defectos**
  a. Identificación y descripción de defectos: Documentar los defectos con una descripción clara, pasos para reproducir el problema, severidad e impacto.
  b. Asignación de defectos: Asignar los defectos a los equipos responsables para su corrección.
  Seguimiento de resolución: Hacer un seguimiento del estado de los defectos (abierto, en proceso, resuelto, cerrado).

- **Ejecución de pruebas para validación de correcciones**
  a. Pruebas de regresión: Ejecutar pruebas para asegurarse de que los cambios o correcciones no hayan introducido nuevos defectos en la plataforma.
  b. Validación de correcciones: Verificar que los defectos identificados hayan sido corregidos correctamente

- **Pruebas de rendimiento y seguridad.**

  a. Pruebas de rendimiento: Evaluar el comportamiento del software bajo diferentes cargas (pruebas de carga, estrés, volumen).
  b. Pruebas de seguridad: Realizar pruebas para identificar vulnerabilidades de seguridad (análisis de penetración, pruebas de autenticación y autorización).
  c. Pruebas de usabilidad: Evaluar la experiencia de usuario (UX) para garantizar una interacción fluida y amigable.

La etapa de certificación concluirá con el informe de certificación y el cumplimiento del objetivo de las pruebas de certificación.

Entregable	Contenido mínimo

Informe de la certificación	• Planificación de la certificación:
	  ○ Objetivo, alcance, tipos de pruebas, y criterios de entrada y salida.
	  ○ Módulos, funciones o componentes probados
	  ○ Tecnologías y frameworks de prueba
	  ○ Descripción del entorno de pruebas (Hardware y software)
	  ○ Describir la estrategia de pruebas
	• Informe de los resultados de la Certificación.
	  ○ Cantidad total de pruebas realizadas, defectos corregidos, % de cobertura de las pruebas
	  ○ Casos de pruebas, resultado esperado y resultado obtenido, estado del caso de prueba.
	  ○ Resultado de las pruebas no funcionales
	• Acta de los criterios de aceptación firmada por los usuarios designados como equipo funcional del FMV.
	• Casos de prueba firmados y aprobados por los usuarios designados como equipo funcional del FMV
	• Aceptación formal por parte de la Gerencia de Operaciones, Gerencia de Finanzas y Gerencia de Riesgos.
	• Aceptación formal por parte de la Oficina de Tecnología sobre el lanzamiento a producción.

7. Pase a producción

Esta etapa incluirá el despliegue en producción de la PLATAFORMA configurado para el FONDO, junto con la migración de los datos históricos necesarios para el funcionamiento de lo implementado en la Fase 1, permitiendo así el inicio oficial de las operaciones.

a. **Planificación del pase a producción:** El plan deberá considerar con los siguientes puntos:
   i. El cronograma del pase a producción, recursos necesarios y roles asignados para asegurar que todo esté alineado, un procedimiento de rollback en caso se presente algún contingente.
   ii. Checklist de preproducción: Asegurando de que todas las configuraciones necesarias, pruebas y validaciones estén completas.
   iii. Comunicación del plan: Informar a los equipos de stakeholders sobre el plan de pase a producción y las fechas programadas.

b. **Despliegue a producción:** Una vez validadas las pruebas, La PLATAFORMA se desplegará en el entorno de producción. El FONDO deberá aprobar el lanzamiento antes de proceder. Se llevará a cabo el despliegue de la solución con las configuraciones validadas y aprobadas, y la plataforma comenzará a operar oficialmente.

c. **Migración de los datos históricos a producción:** Para la migración de los datos a producción se recomienda
   i. Planificar un periodo de corte (downtime) para realizar la migración final de los datos históricos. Se recomienda seleccionar el periodo de tiempo con la menor transaccionalidad.

ii. Realizar una auditoría final y reconciliación de datos para confirmar que todos los registros han sido transferidos correctamente y que no hay datos perdidos o duplicados.

Esta etapa del pase a producción concluye con el informe del pase a producción. El soporte post implementación se realizará durante la Fase 4 de la Operación del Servicio e inicia desde el momento en que se realiza el pase a producción.

Al finalizar esta Etapa de Pase a Producción deberá firmarse una Acta de Culminación del Pase a Producción donde se indicará la fecha inicio de la marcha blanca de la fase 1 del Servicio.

Entregable	Contenido mínimo
Informe del pase a producción	• Planificación del pase a producción o Objetivo y alcance o Cronograma, recursos y roles asignados o Procedimiento de rollback o Checklist con las configuraciones, pruebas y validaciones • Informe de los resultados del pase a producción. • Aceptación formal por parte de la Oficina de Tecnología sobre el lanzamiento a producción. • **Entregables Documentarios y Técnicos de la Plataforma** El CONTRATISTA deberá adjuntar y documentar la entrega formal de: **a) Documentación técnica:** Manual de arquitectura técnica. Diseño funcional y técnico. Diccionario de datos. Modelo entidad-relación y documentación de bases de datos. Diagramas de flujo y flujos de procesos. **b) Documentación operativa:** Manual de instalación y despliegue. Manual de administración de la plataforma (cloud,seguridad, respaldos). Guía de operación para soporte técnico de primer y segundo nivel. **c) Documentación para usuarios:** Manual de usuario (cliente externo, gestor interno, supervisor). Guía rápida por perfil de usuario. Videos/tutoriales si están contemplados. **d) Entregables digitales:** Código fuente Paquetes de instalación o despliegue (scripts,contenedores, imágenes). Configuraciones exportables o parametrizadas. Backups iniciales y configuraciones base del entorno productivo.

8. Cierre de la Etapa 2

El informe de cierre de la Etapa 2 deberá ser presentado por el contratista máximo al día siguiente de culminada dicha etapa. Su aceptación estará sujeta a la evaluación y conformidad expresa del FMV, la cual deberá emitirse en un plazo máximo de siete (07) días calendario contados desde la recepción del informe.

En caso se identifiquen observaciones, estas deberán ser subsanadas por el contratista en un plazo no mayor a cinco (05) días calendario contados a partir de la notificación correspondiente.
Cabe precisar que sin la conformidad del FMV respecto al informe de cierre, no se podrá dar inicio formal a la siguiente etapa del proyecto.

Entregable	Contenido mínimo
Informe de cierre de la Etapa 2	• Informe final de la capacitación aprobado por el FMV. • Informe del pase a producción aprobado por el FMV

Etapa 3: Marcha Blanca de FASE 1
La Marcha Blanca de la Fase 1 comenzará inmediatamente después del pase a producción de dicha fase y tendrá una duración máxima de 90 días calendario. Durante este período, la Plataforma para la Gestión de Créditos deberá operar en un entorno real supervisado, con monitoreo continuo y acompañamiento técnico por parte del FMV, con el objetivo de validar su correcto funcionamiento, estabilidad y cumplimiento funcional antes del cierre formal de la fase.

Durante la marcha blanca, se deberán ejecutar las siguientes actividades mínimas:

- Ejecución supervisada en entorno real con validación de procesos clave como: desembolsos, prepagos, extornos, generación de cronogramas, recuperación y gestión de carteras.
- Interoperabilidad activa con IFI, habilitando el registro de subprestatarios mediante interfaz web segura o integración vía API.
- Verificación de integraciones con los sistemas internos del FMV (facturación electrónica, contabilidad, tesorería, monitoreo, entre otros), así como la integración operativa con el sistema actual (SAOC) durante el periodo de coexistencia.
- Pruebas de rendimiento y estabilidad, con medición de KPIs como tiempos de respuesta, disponibilidad, consumo de recursos y posibles cuellos de botella.
- Monitoreo de incidencias y atención inmediata a eventos críticos detectados durante la operación supervisada. Las observaciones menores serán registradas y tratadas posteriormente, siempre que no comprometan la funcionalidad.
- Verificación de seguridad operativa, incluyendo gestión de accesos, autenticación, trazabilidad y control de integridad transaccional.
- Generación y validación de reportes contables y regulatorios, incluyendo el cierre operativo diario automático, conciliaciones y reportes exigidos por entidades como la SBS.
- Evaluación del cumplimiento de SLA, conforme a los indicadores establecidos en el TDR.
- Evaluación funcional por parte del FMV, con levantamiento y corrección de observaciones realizadas por las áreas usuarias.
- Conformidad técnica y funcional por parte del responsable de la Oficina de Tecnologías y el Gerente de Operaciones.

Cierre de la etapa 3:
Finalizada la marcha blanca, la Plataforma para la Gestión de Créditos deberá encontrarse plenamente operativa, con un funcionamiento 100% estable y libre de incidencias críticas, habiéndose validado satisfactoriamente todas las etapas funcionales y técnicas contempladas en la Fase 1.
En caso subsistan incidencias críticas no resueltas al cierre de la etapa, el contratista deberá subsanarlas en un plazo máximo de cinco (05) días calendario contados desde la fecha de culminación de la marcha blanca. La subsanación de estas

observaciones será condición indispensable para la aprobación del informe de cierre de la etapa 3.

Entregables:

Entregable	Contenido mínimo
Informe de cierre de la Etapa 3	• Resumen de actividades ejecutadas durante la marcha blanca. • Resultados de validación funcional, integración, rendimiento y seguridad. • Registro de incidencias, tratamiento efectuado dentro de la etapa de Marcha blanca y estado. • Evaluación del cumplimiento de SLA. • Aceptación formal por parte de los usuarios designados como equipo funcional del FMV • Aceptación formal por parte de la Gerencia de Operaciones, Gerencia de Finanzas y Gerencia de Riesgos. • Aceptación formal por parte de la Oficina de Tecnología.

Cierre de FASE 1
El Acta de Cierre será presentada el último día de la Fase 1 y su firma estará condicionada a la conformidad total del FMV, expresada mediante la firma de todos los integrantes del Equipo Estratégico de Gobierno del Proyecto del FMV (Nivel Directivo), la cual deberá emitirse en un plazo máximo de siete (07) días calendario contados desde la recepción del informe.

En caso se identifiquen observaciones, estas deberán ser subsanadas por el contratista en un plazo no mayor a cinco (05) días calendario contados a partir de la notificación correspondiente.

Cabe precisar que sin la conformidad total del FMV respecto al acta de cierre, no se podrá dar inicio a la Fase 4 – Operación Oficial.

Entregable	Contenido mínimo
Acta de cierre de la FASE 1	• Informe de cierre de la etapa 1 aprobado por el FMV. • Informe de cierre de la etapa 2 aprobado por el FMV. • Informe de cierre de la etapa 3 aprobado por el FMV.

3.4.11.2 FASE 2

Etapa1: Implementación de la Plataforma para la Gestión de créditos - Fideicomiso, Garantías y Provisiones (Reemplazo de actual sistema SAOC y SIR)

Esta etapa se desglosa en varios subprocesos clave que permitirán adaptar La PLATAFORMA a las necesidades del **FONDO**.

a. Análisis del entorno
En esta segunda fase, el CONTRATISTA de la **PLATAFORMA** realizará un relevamiento detallado de la situación actual del **FONDO**, incluyendo la identificación de brechas funcionales ("gaps") y requerimientos específicos para la implementación de la PLATAFORMA.

Se identificarán necesidades técnicas, operativas y normativas, evaluando las funcionalidades de la PLATAFORMA frente a los procesos actuales del FONDO:

- Módulo de fideicomisos
- Módulo CRC - PBP
- Módulo de Garantías
- Módulo de tesorería
- Módulo Exconeminsa, IFI en Liquidación

Entregable	Contenido mínimo
Informe del Discovery GAP Análisis del entorno	• Análisis del estado actual de la plataforma y operaciones del FONDO • Identificación de brechas funcionales y técnicas (GAP Analysis) • Requerimientos de integración con otros sistemas • Cronograma detallado del proyecto con hitos y responsables

b) Plan de Desarrollo

Este proceso debe concluir con el plan de desarrollo e implementación, el cual deberá incluir como mínimo.

Entregable	Contenido mínimo
Plan de desarrollo	• Objetivos del proyecto • Alcance de la implementación. • EDT del proyecto. • Organigrama del proyecto y la responsabilidad de cada rol • Riesgos iniciales del proyecto con su plan de mitigación • Métodos y frecuencia de comunicación entre el equipo y los interesados • Lista de personas clave o grupos que serán informados del progreso del proyecto • Estrategia de migración de los datos históricos. • Cumplimiento con los requisitos técnicos y de seguridad del punto 7.

c) Definición del Alcance detallado

En este subproceso el CONTRATISTA de la PLATAFORMA trabajará estrechamente con el **FONDO** para definir los parámetros de los productos que se implementaran. Este proceso incluye la presentación funcional de la plataforma, la identificación de las necesidades del **FONDO**, y la definición de nuevos productos a implementar. Además, se deberán definir las parametrizaciones de la plataforma, las brechas funcionales ("gaps") y los requerimientos de integración con otros sistemas del **FONDO**. Finalmente, se elaborará un guion de pruebas modulares e integrales que sirvan para validar la solución antes de su despliegue.

Este subproceso debe concluir con el documento del alcance aprobado, el cual deberá contener como mínimo:

Entregable	Contenido mínimo
Documento del alcance	• Definición de los productos del FONDO a implementar en La PLATAFORMA, con sus reglas de negocio en La PLATAFORMA.

	• Los requisitos funcionales de los productos a implementar • Los requisitos no funcionales (rendimiento, seguridad, usabilidad y mantenibilidad) • Detalle de las interfaces con otros sistemas o plataformas, indicando métodos de conexión y la disponibilidad de los datos a intercambiar • Detalle de las funcionales que quedan fuera del alcance. • Los criterios de aceptación: Detalles de cómo se evaluará si un entregable cumple los requisitos. • Indicadores de éxito: Medidas que permitan evaluar si el proyecto ha cumplido sus objetivos (KPIs, métricas). • Cualquier requisito legal, de cumplimiento, o de estándares que deba respetarse. • Lista de posibles riesgos y problemas que podrían surgir durante el proyecto. Incluyendo un plan de mitigación: Acciones preventivas o correctivas para minimizar los riesgos.

d) Desarrollo de la PLATAFORMA

En este subproceso, el CONTRATISTA de la PLATAFORMA implementará lo definido en el documento del alcance para habilitar los productos del FONDO, las interfaces requeridas con otras plataformas, lo procesos automatizados de carga de información, los requisitos funcionales y requisitos no funcionales. Este subproceso concluirá con el informe por parte del CONTRATISTA que ha realizado sus pruebas unitarias de manera exitosa según los criterios de aceptación acordados con el FONDO.

Entregable	Contenido mínimo
Informe de pruebas unitarias	• Objetivo de las pruebas unitarias • Módulos, funciones o componentes probados • Tecnologías y frameworks de prueba • Descripción del entorno de pruebas (Hardware y software) • Describir la estrategia de pruebas • Cantidad total de pruebas unitarias realizadas, defectos corregidos, % de cobertura de las pruebas • Casos de pruebas, resultado esperado y resultado obtenido, estado de la prueba.

e) Capacitación

En este subproceso, el CONTRATISTA de la PLATAFORMA llevará a cabo sesiones de capacitación con un mínimo de 40 horas lectivas por persona de formación para 75 personas designadas por el FONDO, para asegurar que los usuarios y el personal del FONDO estén preparados para operar la plataforma. El Plan de Capacitación es un entregable previo a la etapa de Pase a Producción.

Este subproceso concluirá con el informe de capacitación por parte del CONTRATISTA de la PLATAFORMA:

N	Entregable	Contenido mínimo
1	**Plan de Capacitación**	• Objetivo General • Público Objetivo

		○ Descripción y segmentación de los grupos a capacitar (por ejemplo: usuarios funcionales, personal técnico, operadores, personal de seguridad de la información). • Modalidad de Capacitación • Estructura Curricular ○ Módulos temáticos diferenciados por perfil (funcional, operativo, técnico, seguridad de la información). ○ Temario detallado por módulo (temas, subtemas). ○ Relación de los módulos con los roles del usuario en la plataforma. • Duración ○ Cronograma de ejecución (fechas estimadas por grupo y módulo). • Metodología ○ Enfoques pedagógicos o metodológicos (aprendizaje práctico, basado en escenarios reales, talleres guiados, etc.). • Docentes ○ Relación de instructores propuestos (CVs abreviados) y asignación de los docentes por módulo. • Materiales y Recursos ○ Listado de materiales a entregar (manuales, presentaciones, accesos a entornos de prueba, etc.). ○ Idioma de los materiales (preferiblemente en español). • Evaluación del Aprendizaje ○ Mecanismos de evaluación por módulo (pruebas prácticas, exámenes, simulaciones, etc.). ○ Criterios de aprobación. ○ Registro de asistencia y control de participación. • Indicadores de Cumplimiento % de participación, % de aprobación, % de satisfacción de los participantes (encuestas de calidad).
2	**Informe de la capacitación**	• Objetivo de la capacitación • Alcance y contenido de la capacitación • Estrategia de la capacitación • Fechas, duración, lugar de la capacitación. • Información de los instructores • Información de los participantes • Evaluación de la capacitación • Resultados de la capacitación

		• Conclusiones de la capacitación.

f) Certificación

Se realizarán las pruebas exhaustivas para verificar que la plataforma funcione correctamente y que cumpla con los criterios de aceptación detallados en el documento del alcance

La etapa de certificación concluirá con el informe de certificación y el cumplimiento del objetivo de las pruebas de certificación.

Entregable	Contenido mínimo

Informe de la certificación	• Planificación de la certificación:
	  ○ Objetivo, alcance, tipos de pruebas, y criterios de entrada y salida.
	  ○ Módulos, funciones o componentes probados
	  ○ Tecnologías y frameworks de prueba
	  ○ Descripción del entorno de pruebas (Hardware y software)
	  ○ Describir la estrategia de pruebas
	• Informe de los resultados de la Certificación.
	  ○ Cantidad total de pruebas realizadas, defectos corregidos, % de cobertura de las pruebas
	  ○ Casos de pruebas, resultado esperado y resultado obtenido, estado del caso de prueba.
	  ○ Resultado de las pruebas no funcionales
	• Acta de los criterios de aceptación firmada por los usuarios.
	• Casos de prueba firmados y aprobados por la Gerencia de Operaciones.
	• Aceptación formal por parte de la Oficina de Tecnología sobre el lanzamiento a producción.

g) Pase a producción

Esta etapa incluirá el despliegue en producción de la fase 2 de la PLATAFORMA configurado para el FONDO, junto con la migración de los datos históricos necesarios para el funcionamiento de todos los módulos del alcance, permitiendo así el inicio oficial de las operaciones.

El informe de cierre de la Etapa 1 deberá ser presentado por el contratista al día siguiente del vencimiento del plazo establecido para dicha etapa. Su aceptación estará sujeta a la evaluación y conformidad expresa del FMV, la cual deberá emitirse en un plazo máximo de siete (07) días calendario contados desde la recepción del informe.

En caso se identifiquen observaciones, estas deberán ser subsanadas por el contratista en un plazo no mayor a cinco (05) días calendario contados a partir de la notificación correspondiente.

Cabe precisar que sin la conformidad del FMV respecto al informe de cierre, no se podrá dar inicio formal a la siguiente etapa del proyecto.

Entregable	Contenido mínimo
Informe de cierre de la etapa 1 – Fase 2	**Informe de culminación del Pase a Producción** • Planificación del pase a producción

	○ Objetivo y alcance ○ Cronograma, recursos y roles asignados ○ Procedimiento de rollback ○ Checklist con las configuraciones, pruebas y validaciones • Informe de los resultados del pase a producción. • Aceptación formal por parte de la Oficina de Tecnología sobre el lanzamiento a producción. • **Entregables Documentarios y Técnicos de la Plataforma** El CONTRATISTA deberá adjuntar y documentar la entrega formal de: **a) Documentación técnica:** Manual de arquitectura técnica. Diseño funcional y técnico. Diccionario de datos. Modelo entidad-relación y documentación de bases de datos. Diagramas de flujo y flujos de procesos. **b) Documentación operativa:** Manual de instalación y despliegue. Manual de administración de la plataforma (cloud,seguridad, respaldos). Guía de operación para soporte técnico de primer y segundo nivel. **c) Documentación para usuarios:** Manual de usuario (cliente externo, gestor interno, supervisor). Guía rápida por perfil de usuario. Videos/tutoriales si están contemplados. **d) Entregables digitales:** Código fuente Paquetes de instalación o despliegue (scripts,contenedores, imágenes). Configuraciones exportables o parametrizadas. Backups iniciales y configuraciones base del entorno productivo.

3.4.10 Etapa 2: Marcha Blanca de la FASE 2

La marcha blanca de la Fase 2 de la **PLATAFORMA** comienza una vez culminado el pase a Producción de la fase 2 y tiene un plazo máximo de 30 días calendario para su culminación.

Al finalizar esta etapa, la Plataforma para la Gestión de Créditos deberá encontrarse plenamente operativa y disponible para ser utilizada por las Instituciones Financieras Intermediarias (IFI), ya sea a través de acceso directo o mediante integración con sus propios sistemas de información.

Durante esta fase, se llevará a cabo una operación supervisada en entorno real controlado, bajo la observación y acompañamiento del equipo técnico del FMV, con el fin de validar el funcionamiento completo de la plataforma antes del cierre formal de la Fase 1.

Cierre de la etapa 2:
Finalizada la marcha blanca, la Plataforma para la Gestión de Créditos deberá encontrarse plenamente operativa con todos los módulos y funcionalidades especificadas en el alcance de la Fase 2, con un funcionamiento 100% estable y libre de incidencias críticas, habiéndose validado satisfactoriamente.

En caso subsistan incidencias críticas no resueltas al cierre de la etapa, el contratista deberá subsanarlas en un plazo máximo de cinco (05) días calendario contados desde la fecha de culminación de la marcha blanca.

Cabe precisar que sin la conformidad del FMV respecto al informe de cierre, no se podrá dar inicio formal a la siguiente a la Fase 3 del proyecto.

Entregables:

Entregable	Contenido mínimo
Informe de cierre de etapa 2 – Fase 2	Informe de culminación de Marcha blanca: • Fecha de inicio y fin de la marcha blanca. • Detalle de pruebas realizadas en entorno real controlado. • Incidencias detectadas, tratamiento efectuado y estado. • Validación de funcionalidades clave por parte del FMV. • Registro de participación y acceso de las IFI (pruebas reales o simuladas). • Aceptación formal por parte de los usuarios designados como equipo funcional del FMV • Aceptación formal por parte de la Gerencia de Operaciones, Gerencia de Finanzas y Gerencia de Riesgos. • Aceptación formal por parte de la Oficina de Tecnología.

3.4.11 Cierre de FASE 2

El Acta de Cierre será presentada el último día de la Fase 2 y su firma estará condicionada a la conformidad total del FMV, expresada mediante la firma de todos los integrantes del Equipo Estratégico de Gobierno del Proyecto del FMV (Nivel Directivo), la cual deberá emitirse en un plazo máximo de siete (07) días calendario contados desde la recepción del informe.

En caso se identifiquen observaciones, estas deberán ser subsanadas por el contratista en un plazo no mayor a cinco (05) días calendario contados a partir de la notificación correspondiente.

Cabe precisar que sin la conformidad total del FMV respecto al acta de cierre, no se podrá dar inicio a la Fase 3 – Migración de datos históricos.

Entregable	Contenido mínimo
Acta de cierre de la FASE 2	• Informe de cierre de la etapa 1 – Fase 2 aprobado por el FMV • Informe de cierre de la etapa 2 – Fase 2 aprobado por el FMV

3.4.11.3 FASE 3

Migración datos históricos (COFIDE)

El CONTRATISTA y el FONDO en coordinación y/o trabajo conjunto se encargarán de la migración de la información histórica del FONDO, asegurando que todos los datos relevantes sean trasladados de manera correcta a la nueva plataforma. El CONTRATISTA deberá contar con sus interfaces automatizadas para migrar los datos históricos. Se utilizará como entrada la estrategia de migración de datos históricos definida en el plan de implementación. Los pasos recomendados para la migración de datos históricos al **PLATAFORMA** son:

1. **Planificación y evaluación inicial**
   a. **Análisis de datos existentes:**
      - Identificar todas las fuentes de datos que serán migradas, incluyendo bases de datos, archivos, y otros sistemas legados.
      - Determinar el volumen, la calidad y la estructura de los datos históricos. Realizar un análisis de calidad para identificar datos duplicados, inconsistentes o incompletos.

   b. **Definición del alcance de la migración:**
      - Establecer qué datos específicos serán migrados (datos de transacciones, clientes, productos financieros) y cuáles se archivarán o descartarán.
      - Definir los requisitos de cumplimiento y normativas de seguridad para la migración, especialmente si involucra datos sensibles o regulados.

   c. **Elaboración del plan de migración:**
      - Crear un plan detallado que incluya cronograma, recursos, roles y responsabilidades, junto con los riesgos identificados y las estrategias de mitigación.

2. **Diseño de la estrategia de migración**
   a. **Estrategia de migración:** Se recomienda el método de migración Big Bang (todos los datos se migran en un solo momento) y no el método de migración gradual (los datos se migran progresivamente en grupos). Sin perjuicio de lo antes definido el FMV y el Proveedor podrá definir la mejor estrategia según se requiera en el momento de su aplicación.
   b. **Selección de herramientas de migración:** El CONTRATISTA de la PLATAFORMA deberá habilitar las interfaces automatizadas para cargar la información en la PLATAFORMA.
   c. **Definición del mapeo de datos:** Diseñar un mapeo detallado de datos entre los sistemas legados y la PLATAFORMA, especificando cómo se transformarán los campos y se migrarán las estructuras de datos.

3. **Preparación del entorno de migración**
   a. Preparar el entorno de migración, asegurando que se cuenta con los recursos necesarios (almacenamiento, cómputo, red).
   b. Pruebas de conectividad y seguridad:
      Verificar la conectividad entre la plataforma legado y La PLATAFORMA. Asegurarse de que los mecanismos de autenticación y cifrado estén configurados para garantizar la seguridad durante la transferencia de datos.

4. **Extracción, transformación y carga de datos**
   a. **Extracción de datos:** Extraer datos de los sistemas legados según el plan definido. Realizar una extracción incremental o completa, dependiendo del volumen de datos y la estrategia seleccionada.
   b. **Transformación de datos**: Limpiar, normalizar y transformar los datos para que cumplan con los estándares de la PLATAFORMA. Esto puede incluir la corrección de datos corruptos, eliminación de duplicados y ajuste de formatos.
   c. **Carga inicial de datos:** Realizar una carga inicial de datos en el entorno de prueba de la PLATAFORMA. Ejecutar las pruebas unitarias para verificar que los datos se han transferido correctamente y cumplen con los requisitos.

N	Entregable	Contenido mínimo
1	**Informe de la migración de datos históricos**	• Plan de la migración. o Objetivos y alcance o Entorno de migración o Estrategia de migración o Procedimiento de limpieza, normalización y transformación de datos

		• Tiempo histórico de datos migrados. • Informe de validación y consistencia de datos. • Pruebas unitarias firmadas y aprobados por el equipo funcional designado por el FMV. • Aceptación formal por parte de la Gerencia de Operaciones, Gerencia de Finanzas y Gerencia de Riesgos. • Aceptación formal por parte de la Oficina de Tecnología.

Cierre de FASE 3

El Acta de Cierre será presentada el último día de la Fase 3 y su firma estará condicionada a la conformidad total del FMV, expresada mediante la firma de todos los integrantes del Equipo Estratégico de Gobierno del Proyecto del FMV (Nivel Directivo), la cual deberá emitirse en un plazo máximo de cinco (05) días calendario contados desde la recepción del informe.

En caso se identifiquen observaciones, estas deberán ser subsanadas por el contratista en un plazo no mayor a tres (03) días calendario contados a partir de la notificación correspondiente.

Cabe precisar que sin la conformidad total del FMV respecto al acta de cierre, no se podrá dar por culminada la Fase 3 – Migración de datos históricos.

Entregable	Contenido mínimo
Acta de cierre de la FASE 3	• Informe de migración de datos históricos aprobado por el FMV. • Informe de aceptación final de la plataforma aprobado..

3.4.12 FASE 4

3.4.12.1 Operación

Durante esta fase, la Plataforma para la Gestión de Créditos se encontrará en operación oficial en entorno productivo, con disponibilidad para usuarios internos del FONDO y para las Instituciones Financieras Intermediarias (IFI), según los esquemas de acceso definidos.

Las actividades clave de esta fase incluyen:

1. **Inicio de la operación oficial de la plataforma**

   Esta fase marca el inicio del funcionamiento oficial de la Plataforma para la Gestión de Créditos en entorno productivo. A partir de este momento, la plataforma deberá encontrarse plenamente operativo y disponible para los actores involucrados, cumpliendo con los siguientes criterios mínimos:

   - Habilitación completa de funcionalidades por cada fase para el registro, procesamiento, gestión y seguimiento de créditos hipotecarios, fideicomisos, garantías u otros productos financieros del portafolio del FONDO, de acuerdo con los flujos aprobados por el FMV.
   - Acceso habilitado para las Instituciones Financieras Intermediarias (IFI), ya sea a través de una interfaz web segura o mediante integración directa con sus propios sistemas utilizando APIs estandarizadas y seguras, conforme a los lineamientos técnicos definidos por el FMV.
   - Validación previa por parte del FMV de que todas las condiciones técnicas, funcionales y de seguridad se encuentran implementadas de manera satisfactoria para dar inicio a la operación oficial.

2. **Administración de la infraestructura en la nube**

Durante la Etapa Operativa, el contratista será responsable de la gestión proactiva y continua de toda la infraestructura tecnológica alojada en la nube que soporte la Plataforma para la Gestión de Créditos, asegurando su disponibilidad, rendimiento, escalabilidad y seguridad, conforme a los niveles de servicio establecidos.

Las responsabilidades mínimas en esta materia incluyen:

- Mantenimiento preventivo y correctivo de la infraestructura cloud, incluyendo revisión periódica de componentes, actualizaciones de la plataforma operativo, parches de seguridad, y ajustes de configuración necesarios para prevenir fallas y mantener la estabilidad del servicio.
- Gestión de escalamiento de recursos, para asegurar la adecuada capacidad de procesamiento, almacenamiento y transferencia de datos ante incrementos de carga o nuevas necesidades funcionales.
- Monitoreo de la infraestructura en tiempo real, incluyendo CPU, memoria, almacenamiento, tráfico de red, salud de servicios, y disponibilidad de las integraciones clave.
- Aplicación de medidas de seguridad y cumplimiento, tales como control de accesos, cifrado de datos en tránsito y en reposo, monitoreo de eventos de seguridad y respuesta ante incidentes.
- Ejecución del Plan de Continuidad Operativa y Recuperación ante Desastres (DRP), con protocolos claros de activación, recuperación y restauración, previamente validados por el FMV.
- Cumplimiento del SLA de disponibilidad del servicio, con un mínimo de 99.6% de uptime mensual, monitoreado y reportado en los informes de operación.

La administración de la infraestructura en la nube deberá realizarse de manera autónoma por el contratista, con total visibilidad para el FMV a través de herramientas de monitoreo y reportes documentados. El incumplimiento de estas condiciones será sujeto a penalidades conforme al régimen de SLA del presente TDR.

3. **Gestión de Monitoreo continuo**

Durante la Etapa Operativa, el contratista deberá implementar y mantener un sistema integral de monitoreo preventivo y proactivo sobre todos los módulos críticos de la Plataforma para la Gestión de Créditos, con el objetivo de anticipar, detectar y alertar sobre condiciones que puedan derivar en fallas operativas, interrupciones del servicio o impactos económicos para el FMV.

Este monitoreo deberá estar alineado con los SLA establecidos en este TDR, y contemplar los siguientes elementos obligatorios:

- Monitoreo en tiempo real de disponibilidad, rendimiento, uso de recursos, carga de procesos, integraciones activas y cumplimiento de los tiempos de respuesta de la plataforma.
- Monitoreo de procesos críticos como cierres diarios y mensuales, operaciones masivas, sincronizaciones, integraciones entre sistemas, y uso anómalo de recursos que puedan afectar la continuidad operativa.
- Generación de alertas automáticas y notificación anticipada al FMV ante la detección de comportamientos inusuales, degradación del rendimiento, cuellos de botella, fallos en procesos programados o riesgos de indisponibilidad
- Implementación de mecanismos de detección y prevención de incidentes, especialmente en procesos financieros sensibles como la liquidación, desembolso, consolidación y cierre de operaciones.
- Documentación y trazabilidad de todas las alertas generadas, incluyendo: fecha y hora de emisión, causa identificada, acciones preventivas o correctivas realizadas, y estado de resolución. Esta información deberá incorporarse en los informes mensuales de operación.

- Integración con una herramienta de monitoreo de plataforma, que deberá estar habilitada desde el inicio de la Etapa Operativa y contar con:
  - Acceso directo y seguro para el equipo técnico del FMV.
  - Visualización en tiempo real de indicadores clave: disponibilidad, consumo de recursos, estado de integraciones, tiempos de respuesta, generación de alertas, entre otros.
  - Capacidad para emitir reportes automáticos mensuales y alertas configurables con parámetros definidos conjuntamente con el FMV.

4. Soporte técnico y funcional continuo

Durante la Etapa Operativa, el contratista deberá garantizar un servicio de soporte técnico y funcional continuo, con atención oportuna y eficaz a todos los incidentes, requerimientos y consultas que puedan surgir durante el funcionamiento de la Plataforma para la Gestión de Créditos, tanto por parte de los usuarios internos del FMV como de las Instituciones Financieras Intermediarias (IFI).

Las responsabilidades del contratista incluirán como mínimo:

- Atención de incidentes de primer y segundo nivel, según su nivel de severidad y conforme a los tiempos de respuesta y resolución establecidos en los SLA del servicio:
  - Incidentes Críticos.
  - Incidentes de Alta, Media y Baja severidad.
  - Soporte 24/7 en casos críticos que comprometan la continuidad del servicio.

- Recepción, clasificación, priorización, resolución y seguimiento de los incidentes reportados a través de la mesa de ayuda, herramienta de gestión o canal habilitado, asegurando trazabilidad total de las acciones realizadas.

- Registro detallado de cada incidente o requerimiento, incluyendo fecha y hora de reporte, descripción del problema, clasificación de severidad, responsable asignado, acciones tomadas y tiempo de resolución.

- Aplicación de actualizaciones evolutivas menores que no afecten la operación de la plataforma ni requieran interrupciones en el servicio. Estas actualizaciones deberán ser previamente validadas en ambientes controlados y coordinadas con el FMV.

- Generación de reportes mensuales de soporte, consolidando:
  - Número de incidentes atendidos por nivel de severidad.
  - Requerimientos funcionales y técnicos resueltos.
  - Tiempo promedio de atención y cumplimiento de SLA.
  - Alertas críticas y acciones de mejora aplicadas.

  El servicio de soporte deberá contar con recursos humanos calificados y herramientas adecuadas para asegurar la continuidad, estabilidad y eficiencia operativa de la plataforma en todo momento, alineado con las buenas prácticas de ITSM (IT Service Management).

5. Gestión de respaldos y continuidad del servicio

Durante la Etapa Operativa, el contratista será responsable de garantizar la continuidad del servicio y la integridad de la información mediante la ejecución de políticas robustas de respaldo, recuperación y preservación de datos, conforme a los lineamientos institucionales del FMV y los niveles de servicio establecidos.

Las obligaciones mínimas del contratista en esta materia serán:

- Ejecución automática de respaldos diarios de todos los entornos productivos de la Plataforma para la Gestión de Créditos, incluyendo bases de datos, archivos de configuración, logs relevantes, integraciones y componentes críticos de la plataforma.

- Validación periódica de las restauraciones, asegurando que los respaldos puedan ser recuperados exitosamente y se encuentren libres de errores o inconsistencias. Estas pruebas deberán realizarse de forma controlada al menos una vez al mes.

- Conservación y custodia de la información conforme a las políticas institucionales del FMV, asegurando:
  - Un mínimo de 3 años de retención en línea para acceso inmediato.
  - Un mínimo de 10 años en almacenamiento seguro, con mecanismos de cifrado, control de acceso y registro de auditoría.

- Gestión de incidentes críticos asociados a pérdida de datos o interrupción del servicio, aplicando el Plan de Recuperación ante Desastres (DRP) en caso corresponda. El DRP deberá estar actualizado, probado y aprobado por el FMV antes del inicio de la Etapa Operativa.

  Cumplimiento de los niveles de servicio relacionados con continuidad del negocio:

  SLA-09: Tiempo de recuperación del servicio (RTO) menor a 4 horas.
  SLA-10: Punto de recuperación de datos (RPO) con pérdida de datos.
  SLA-11: Ejecución de pruebas de recuperación de desastres al menos dos (2) veces al año, con resultados documentados y entregados al FMV.

- Documentación y reporte de cada respaldo y evento de restauración, incluyendo fecha, alcance, medio utilizado, validación de integridad y responsable.

6. Monitoreo y trazabilidad

Durante la Etapa Operativa, el contratista deberá implementar mecanismos de auditoría continua y trazabilidad completa sobre todos los componentes críticos de la Plataforma para la Gestión de Créditos, con el fin de garantizar la seguridad, integridad, transparencia y control de los procesos ejecutados en la plataforma.
Las obligaciones mínimas en esta materia serán:

- Implementación de monitoreo en tiempo real de los módulos, servicios activos e integraciones, con visibilidad sobre su funcionamiento, tiempos de respuesta y disponibilidad.
- Auditoría detallada y continua de todos los accesos a la PLATAFORMA, incluyendo usuarios internos del FMV, IFI, administradores técnicos y otros actores autorizados. Esta auditoría deberá registrar:
  - Identidad del usuario o sistema que accede.
  - Fecha, hora y duración del acceso.
  - Acciones realizadas dentro de la plataforma (consultas, aprobaciones, modificaciones, eliminaciones, etc.).
  - Ubicación y dispositivo desde el cual se realizó el acceso.
- Registro y trazabilidad completa de transacciones sensibles, tales como: solicitudes de crédito, modificaciones de datos financieros, gestiones de garantías, liquidaciones, cierres contables, migraciones y aprobaciones administrativas.
- Detección y reporte de comportamientos inusuales o sospechosos, tales como accesos fuera del horario habitual, múltiples intentos fallidos de autenticación, modificaciones masivas inesperadas o accesos desde ubicaciones no reconocidas.

- Generación de reportes automáticos de auditoría, los cuales deberán ser entregados mensualmente al FMV e incluir:
  - Actividades de usuarios.
  - Análisis de patrones de uso.
  - Eventos de seguridad y alertas relevantes.
  - Recomendaciones de mejora o acciones correctivas.
- Conservación de los logs de auditoría conforme a la política institucional del FMV, con mecanismos de protección contra alteraciones y acceso no autorizado.

Estos mecanismos de auditoría serán claves para respaldar el cumplimiento normativo, la rendición de cuentas, la trazabilidad de decisiones y la prevención de fraudes o usos indebidos de la plataforma.

7. Seguimiento y cumplimiento de SLA

Durante la Etapa Operativa, el contratista será responsable de asegurar el cumplimiento riguroso de los Acuerdos de Niveles de Servicio (SLA) establecidos en el presente TDR, los cuales constituyen compromisos contractuales medibles que garantizan la calidad, disponibilidad, continuidad y eficiencia del servicio prestado.

Las obligaciones mínimas del contratista en esta materia serán:

- Monitoreo permanente del cumplimiento de cada SLA, a través de mecanismos automáticos y trazables que permitan validar de manera objetiva los siguientes indicadores:
  - Disponibilidad de la plataforma (SLA-01).
  - Tiempos de respuesta y resolución de incidentes según su severidad (SLA-02 al SLA-05).
  - Disponibilidad del soporte técnico 24/7 (SLA-06).
  - Tiempo de respuesta de la plataforma (SLA-07).
  - Tiempos de procesamiento de transacciones críticas (SLA-08).
  - RTO y RPO (SLA-09 y SLA-10).
  - Ejecución de pruebas de recuperación (SLA-11).
  - Generación de alertas preventivas ante contingencias (SLA-12).
- Generación y entrega de reportes mensuales de cumplimiento de SLA, que deberán incluir como mínimo:
  - Resultados detallados por cada indicador.
  - Incidentes ocurridos y tiempos de atención.
  - Alertas generadas y acciones preventivas aplicadas.
  - Casos de incumplimiento y su justificación, si corresponde.
  - Aplicación de penalidades, cuando sea el caso.
- Identificación proactiva de desvíos en los niveles de servicio, con propuesta de medidas correctivas y planes de mejora continua, a ser validados por el FMV.
- Trazabilidad completa del cumplimiento de SLA mediante el uso de herramientas que permitan al FMV verificar en cualquier momento los indicadores del servicio, ya sea en tiempo real o mediante consulta histórica.

El incumplimiento de los SLA será sancionado con la aplicación de las penalidades específicas definidas en el presente documento, sin perjuicio de otras acciones contractuales que correspondan.

N	Entregable	Contenido mínimo
1	**Informe mensual de Operación**	- Resumen ejecutivo del mes: principales hitos, estado general del servicio, eventos relevantes. - Reporte funcional y técnico: disponibilidad de la plataforma, estadísticas de uso, actualizaciones aplicadas. - Gestión de incidencias y requerimientos: consolidado mensual por nivel de severidad,

		tiempos de atención y resolución, pendientes justificados. - Cumplimiento de SLA: tabla comparativa de indicadores comprometidos vs. resultados reales, con justificaciones y penalidades si corresponde. - Monitoreo y alertas: detalle de alertas generadas, eventos preventivos, comportamientos anómalos detectados. - Auditoría y trazabilidad: registro de accesos, acciones críticas, eventos de seguridad. - Gestión de respaldos y continuidad: evidencia de respaldos diarios, validaciones realizadas, incidentes relacionados. Recomendaciones de mejora: sugerencias técnicas o funcionales para optimización o escalamiento.

3.4.13 FASE 5: Transición de salida

El objetivo es asegurar una transición ordenada, segura y plenamente documentada de la gestión de la plataforma y de su infraestructura tecnológica en la nube, la cual es de titularidad exclusiva del FONDO (FMV). Esta transición deberá garantizar la continuidad operativa sin interrupciones, así como la entrega completa de configuraciones, datos, accesos y documentación necesarios para su administración directa por parte del FMV o para su administración directa por parte del FMV o por el operador que este designe.

Al término del contrato, el FMV conservará de manera íntegra:

- El acceso, control y titularidad plena sobre la infraestructura en la nube donde se encuentra alojada la plataforma.

- El código fuente, documentación técnica y funcional, configuraciones y bases de datos, conforme a las disposiciones de entrega y transferencia establecidas en el contrato.

- La continuidad operativa de la plataforma, sin requerimiento de migración a otra infraestructura, salvo decisión expresa del FMV.

En consecuencia, el CONTRATISTA deberá garantizar que no existan restricciones, bloqueos, dependencias técnicas ni condiciones que impidan al FMV continuar con la operación de la plataforma una vez finalizado el contrato, ya sea bajo un modelo de gestión directa o a través de un nuevo CONTRATISTA designado por la entidad.

Actividades clave:

1. Planificación de la salida del servicio

- Definición del cronograma de retiro del servicio.
- Coordinación con el equipo de la Oficina de Tecnología de la Información (OTI) del FMV para definir responsables, formatos y procedimientos de recepción.

2. Transferencia de conocimiento

- Entrega formal del código fuente, diccionario de datos, y el acrivo en cvs de la data almacenada.
- Revisión conjunta de la arquitectura implementada y sus parámetros de operación.
- Capacitación técnica (transferencia de conocimiento) al personal designado por el FMV.

3. Exportación de información y respaldo completo

- Proporcionar un repositorio compartido para la Validación del acceso a este y resguardo de toda la data exportada () y no estructurada (archivos cargados, reportes, documentos generados).
- Generación y entrega de respaldos completos en formato cvs para que pueda ser importado a los entornos tecnológicos del FMV.
- Validación de la integridad, legibilidad y trazabilidad de los datos entregados.
- Entrega del código fuente de la aplicación al inicio de la transición de salida, donde ya no se realizará cambios al código en producción

4. Desvinculación del CONTRATISTA

- Eliminación de cuentas, accesos y roles asignados al personal del CONTRATISTA en los entornos productivos del FMV.
- Cierre de sesiones, herramientas de monitoreo y servicios administrados por el CONTRATISTA.
- Entrega de la documentación técnica y operativa final, incluyendo:
    - Manuales funcionales actualizados
    - Diagramas y configuraciones de la arquitectura
    - Diccionario de datos
    - Inventario descripción de los componentes de la arquitectura y de la plataforma.

5. Cierre del servicio y soporte post-retiro

- Finalización formal del contrato con acta de cierre.
- Eliminación segura de datos del FONDO en los servidores del CONTRATISTA, garantizando el cumplimiento de normativas de protección de datos.

Entregable	Contenido mínimo
Informe de exportación de datos con detalles de los archivos generados	Documento detallado con la descripción completa de los datos extraídos de la plataforma. **Contenido mínimo:** • Descripción de los datos exportados (tipos de información, estructuras, tablas, volúmenes). • Formato de entrega (ej. CSV, JSON, XML, SQL Dump, entre otros). • Detalles de cifrado o compresión si aplica. • Fecha y hora de generación de la exportación. • Evidencia de validación de integridad mediante sumas de verificación (hash). • Procedimiento recomendado para la importación en los sistemas del FONDO.
Documentación técnica de configuración y parametrización	Este entregable debe incluir información detallada sobre la configuración y personalización realizada en la plataforma del CONTRATISTA, de modo que el FONDO pueda comprender su estructura y, en caso de ser necesario, replicarla en otra Plataforma. **Contenido mínimo:** • Parámetros generales de la plataforma (configuraciones clave, reglas de negocio, validaciones). • Estructura de bases de datos (tablas, relaciones, diccionario de datos). • Interoperabilidad con otras plataformas y/o sistemas (APIs, integraciones, protocolos de comunicación). • Seguridad y accesos (roles, permisos, políticas aplicadas). • Histórico de cambios y ajustes en la configuración.

Acta de conformidad de los entregables solicitados	Este documento oficial será firmado por ambas partes (CONTRATISTA y FONDO) y certificará que los datos han sido exportados, entregados y validados conforme a los requisitos del contrato. **Contenido mínimo:** • Fecha y participantes en el proceso de entrega. • Resumen de los datos entregados y su validación por parte del FONDO. • Cláusula de cumplimiento y cierre formal del servicio. • Firmas de los representantes del CONTRATISTA y del FONDO.
Plan de evidencias de eliminación de datos del CONTRATISTA	Este entregable detalla el acompañamiento que brindará el CONTRATISTA durante un período posterior a la migración para eliminar cualquier dato derivado de la transición. También incluirá la evidencia de eliminación de la información del FONDO en la infraestructura del CONTRATISTA. **Contenido mínimo:** • Alcance de la eliminación • Estrategia y procedimiento de eliminación • Cronograma • Evidencias de eliminación • Acta de conformidad

3.4.14 FASE 6: Bolsa de Horas (900)

Durante la etapa de operación del servicio, el CONTRATISTA deberá poner a disposición del FONDO una bolsa de 900 horas. Estas horas corresponden a una prestación accesoria del servicio, de carácter complementario y bajo demanda.

El uso de esta bolsa estará orientado exclusivamente a la atención de requerimientos adicionales que no hayan sido contemplados en el alcance inicial del servicio contratado, pero que guarden relación directa con el mismo. Se incluyen, de forma referencial, nuevas funcionalidades, mejoras evolutivas, ampliaciones funcionales, optimizaciones o adaptaciones de la plataforma que respondan a nuevas necesidades institucionales del FONDO.

Queda expresamente establecido que la bolsa de horas no podrá ser utilizada para la atención de incidencias, errores o problemas relacionados con funcionalidades ya implementadas dentro del alcance principal del servicio. Dichas situaciones deberán ser atendidas en el marco del soporte técnico regular incluido en la prestación principal.

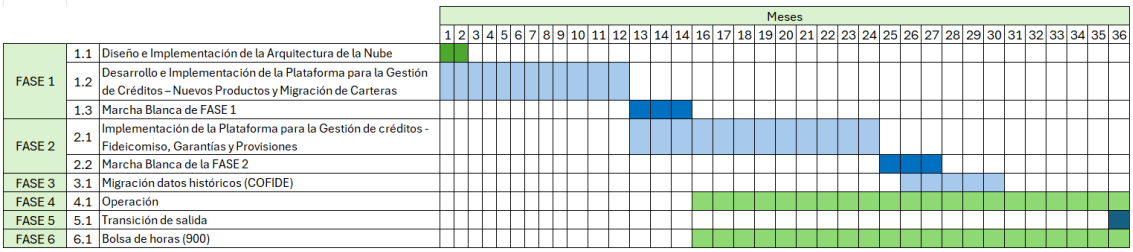
Toda solicitud para el uso de estas horas deberá ser gestionada de manera formal por el Supervisor de Aplicaciones del FONDO, a través de comunicación por correo electrónico, con una anticipación mínima de 24 horas. Esta solicitud deberá contener la descripción técnica del requerimiento, su justificación, el tiempo estimado de ejecución y la prioridad asignada. Ningún desarrollo podrá ejecutarse sin la aprobación previa y expresa del FONDO.

N	Entregable	Contenido mínimo

1	**Informe mensual de uso de Bolsa de Horas**	**-Detalle de requerimientos atendidos durante el mes.** **-Actividades ejecutadas y horas consumidas por cada una.** **-Estado de avance de cada solicitud.** **-Saldo acumulado de horas disponibles.** **-Identificación de entregables asociados (documentos técnicos, configuraciones, evidencias, etc.).**

3.4.12 Resumen del cronograma

En el siguiente grafico se muestra el resumen de las FASES descritas anteriormente.



Nota: La imagen del cronograma es referencial y corresponde a un escenario ideal de ejecución**.**

3.4.13 ENTREGABLES Y PLAZOS

Para el proceso de entrega de documentos y materiales relacionados con el proyecto, se ha dispuesto que todos los entregables sean enviados a través de la Mesa de Partes Virtual del **FONDO**, utilizando el siguiente enlace: https://www.mivivienda.com.pe/sgd.mpv/. Los documentos deberán ser dirigidos a la Oficina de Tecnología de la Información del **FONDO** para su correspondiente recepción y revisión. A continuación, se detallan los entregables esperados y los plazos correspondientes para su entrega.

Fase	N.º	Entregable	Plazo máximo de entrega	Responsable de Conformidad
FASE 1	Etapa 1	Informe de cierre de la etapa 1	Máximo al día siguiente de culminada la etapa 1- Fase 1	-Jefe de la Oficina de Tecnología de la Información
	Etapa 2	Informe de cierre de la etapa 2	Máximo al día siguiente de culminada la etapa 2- Fase 1	-Gerente de Finanzas -Gerente de Operaciones -Gerente de Riesgos -Gerente de Administración -Jefe de la Oficina de Tecnología de la Información
	Etapa 3	Informe de cierre de la etapa 3 ***Acta de cierre de la Fase 1***	Máximo al día siguiente de culminada la etapa 3- Fase 1	
FASE 2	Etapa 1	Informe de cierre de la etapa 1 – Fase 2	Máximo al día siguiente de culminada la etapa 1 – Fase 2	-Gerente de Finanzas -Gerente de Operaciones -Gerente de Riesgos -Gerente de Administración -Jefe de la Oficina de Tecnología de la Información
	Etapa 2	Informe de cierre de la etapa 2 – Fase 2 ***Acta de cierre de la Fase 2***	Máximo al día siguiente de culminada la etapa 2 – Fase 2	
FASE 3	3.1	Informe de culminación de Migración de datos históricos (COFIDE)	Máximo al día siguiente de	-Gerente de Finanzas -Gerente de Operaciones

		Acta de cierre de la Fase 3	culminada la etapa 3 – Fase 3	-Gerente de Riesgos -Gerente de Administración -Jefe de la Oficina de Tecnología de la Información
FASE 4	4.1	Informe mensual de Soporte de operación	Máximo al día siguiente del cierre de cada mes de soporte	-Gerente de Finanzas -Gerente de Operaciones -Gerente de Riesgos -Gerente de Administración -Jefe de la Oficina de Tecnología de la Información
FASE 6	6.1	Soporte a demanda (bolsa de 900 horas)	Máximo al día siguiente de cada consumo ejecutado que se desee facturar	-Gerente de Finanzas -Gerente de Operaciones -Gerente de Riesgos -Gerente de Administración -Jefe de la Oficina de Tecnología de la Información

3.4.15 RESPONSABILIDADES DEL FONDO

En el marco de la ejecución del servicio establecido entre el FONDO y el CONTRATISTA de la PLATAFORMA, se establece que el FONDO actuará como la entidad contratante encargada de proporcionar toda la información y documentación necesaria para la correcta realización del servicio. Los documentos y datos para entregar incluyen lo siguiente:

1. **Manuales de Procedimientos Operativos:** El FONDO proporcionará los manuales detallados que describen los procedimientos operativos estándar que deben seguirse durante la ejecución del servicio. Estos manuales servirán como guía para asegurar la correcta implementación de los procesos establecidos.
2. **Manuales de los Sistemas de Información Involucrados:** Se entregarán los manuales correspondientes a los sistemas de información que estarán involucrados en el servicio. Estos manuales incluirán detalles sobre el funcionamiento, la configuración y el uso de las plataformas y herramientas tecnológicas que serán esenciales para la realización de las tareas pactadas.
3. **Arquitectura de los Sistemas de Información Afectados:** Se pondrá a disposición la información sobre la arquitectura de los sistemas de información que se verán impactados por el servicio, lo que permitirá comprender el impacto de las modificaciones o integraciones necesarias y coordinar el trabajo de manera efectiva.
4. **Accesos a los Sistemas de Información Involucrados en el Entorno No Productivo:** El **FONDO** otorgará los accesos necesarios a los sistemas de información involucrados en el servicio, en un entorno no productivo, con el fin de que el contratista pueda realizar las pruebas y verificaciones pertinentes sin afectar el entorno en vivo de la organización.
5. **Acceso al Personal Relevante:** Se garantizará el acceso al personal clave del FONDO que estará involucrado en la ejecución del servicio, facilitando así la colaboración directa y eficiente entre ambas partes.
6. **Designación de un responsable como punto de Contacto:** El **FONDO** designará un responsable específico que actuará como punto de contacto para todas las cuestiones relacionadas con el servicio. Esta persona será la encargada de coordinar la comunicación y resolver cualquier consulta o inquietud durante la ejecución del servicio.

3.4.16 OBLIGACIÓN DEL CONTRATISTA

El CONTRATISTA de la PLATAFORMA deberá cumplir con varias responsabilidades para garantizar la correcta prestación del servicio de soporte y mantenimiento:

1. **Asignación de un Sectorista**: El CONTRATISTA designará a un **sectorista** que se encargará de coordinar y gestionar todos los incidentes y solicitudes relacionadas con el software.
2. **Gestión Centralizada del Soporte**: Todo el soporte será gestionado mediante una herramienta de **mesa de ayuda** proporcionada por el CONTRATISTA, que permitirá hacer un seguimiento eficiente de las incidencias.
3. **Modelo de Organización del Soporte**: El CONTRATISTA deberá detallar en su propuesta cómo se organizará el equipo encargado de brindar el soporte, incluyendo:
   - Personal dedicado con las cualificaciones técnicas necesarias.
   - Niveles de soporte: **in situ**, telefónico y remoto.
   - Organigrama del equipo de soporte.
   - Políticas de escalado y resolución de problemas.
   - Flujo de trabajo detallado para la atención de incidentes, desde la recepción hasta la resolución.
4. **Tiempos de Respuesta y Resolución**: El CONTRATISTA se compromete a responder y resolver los incidentes dentro de los niveles de servicio acordados.
5. **Modalidad de Soporte:** El soporte se brindará de forma remota desde el centro de desarrollo del CONTRATISTA de la PLATAFORMA. Si es necesario, se podrá brindar soporte in situ.
6. **Horarios de Atención**: El soporte estará disponible de lunes a viernes, de **8:30 a 18:30 horas**. Para incidentes **críticos** y de **alta criticidad**, el CONTRATISTA de la PLATAFORMA dispondrá de un **hotline 24/7**, disponible en cualquier momento.
7. **Atención Fuera del Horario Regular**: Las incidencias reportadas fuera del horario laboral se atenderán al día siguiente, dependiendo de la criticidad del problema. En ningún caso se generarán costos adicionales por atención fuera del horario regular, salvo en situaciones que impliquen servicios fuera del alcance del contrato.
8. **Actualizaciones y Modificaciones**
   El servicio de mantenimiento forma parte de la **prestación accesoria** del contrato, específicamente dentro del alcance de la Fase 4, e incluye la implementación de actualizaciones periódicas durante toda la vigencia del servicio, que comprenden:

   - Adecuaciones normativas impuestas por organismos reguladores como la SBS o SUNAT.
   - Corrección de fallos o errores identificados en funcionalidades ya implementadas dentro del alcance original del servicio.

   Estas actividades no generan costos adicionales para el FONDO ni podrán ser imputadas a la bolsa de horas de la prestación accesoria. Las actividades que surjan como nuevos requerimientos o ampliaciones funcionales no contempladas en el alcance original serán atendidas exclusivamente mediante la **bolsa de horas**.

   El CONTRATISTA será responsable de asegurar que la plataforma se mantenga actualizado, tanto en términos de cumplimiento normativo como en mejoras tecnológicas, durante todo el período del contrato. Estas actualizaciones se realizarán de manera que no afecten la disponibilidad de la plataforma, preferentemente fuera del horario laboral o con la debida planificación. Además, dichas actualizaciones no generarán costos adicionales para la empresa.

   Es importante destacar que no existe un tiempo específico dedicado a cada tipo de actualización, pero el CONTRATISTA deberá realizar estos cambios de manera oportuna y sin interrumpir la operatividad.

El servicio de mantenimiento y soporte proporcionado por el CONTRATISTA tiene como objetivo garantizar la operatividad continua y la adaptación de la plataforma a nuevas normativas o mejoras. Con un equipo calificado y un proceso de soporte estructurado, el CONTRATISTA se compromete a atender los incidentes en tiempos definidos y a mantener la plataforma actualizado durante los **36 meses** de duración de la operación del servicio. De esta manera, se asegura que la plataforma funcione de manera eficiente, sin que esto genere costos adicionales para la empresa.

9. EL CONTRATISTA se obliga a asumir las sanciones, multas u otro concepto impuestas a EL FMV S.A. por un organismo supervisor competente, en caso de infracción de la normativa vigente, siempre que las causas sean atribuibles a EL CONTRATISTA sin perjuicio de la indemnización por los daños y perjuicios que se hayan generado y el cobro de las penalidades que corresponda.

3.4.17 CONFORMIDAD

a) La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 144 del Reglamento de la Ley 32069. La conformidad será otorgada por el Jefe de la Oficina de Tecnologías de la Información, previo Visto Bueno de Gerente de Operaciones, Gerente de Finanzas, Gerente de Riesgos y Gerente Comercial, de aplicar, según el entregable y de acuerdo con la función; la conformidad se emite en un plazo máximo de siete (07) días de presentado el entregable.

Fase	N.º	Entregable	Plazo máximo de entrega	Responsable de Conformidad
FASE 1	Etapa 1	Informe de cierre de la etapa 1	Máximo al día siguiente de culminada la etapa 1- Fase 1	-Jefe de la Oficina de Tecnología de la Información
	Etapa 2	Informe de cierre de la etapa 2	Máximo al día siguiente de culminada la etapa 2- Fase 1	-Gerente de Finanzas -Gerente de Operaciones -Gerente de Riesgos -Gerente de Administración -Jefe de la Oficina de Tecnología de la Información
	Etapa 3	Informe de cierre de la etapa 3 ***Acta de cierre de la Fase 1***	Máximo al día siguiente de culminada la etapa 3- Fase 1	
FASE 2	Etapa 1	Informe de cierre de la etapa 1 – Fase 2	Máximo al día siguiente de culminada la etapa 1 – Fase 2	-Gerente de Finanzas -Gerente de Operaciones -Gerente de Riesgos -Gerente de Administración -Jefe de la Oficina de Tecnología de la Información
	Etapa 2	Informe de cierre de la etapa 2 – Fase 2 ***Acta de cierre de la Fase 2***	Máximo al día siguiente de culminada la etapa 2 – Fase 2	
FASE 3	3.1	Informe de culminación de Migración de datos históricos (COFIDE) ***Acta de cierre de la Fase 3***	Máximo al día siguiente de culminada la etapa 3 – Fase 3	-Gerente de Finanzas -Gerente de Operaciones -Gerente de Riesgos -Gerente de Administración -Jefe de la Oficina de Tecnología de la Información

FASE 4	4.1	Informe mensual de Soporte de operación	Máximo al día siguiente del cierre de cada mes de soporte	-Gerente de Finanzas -Gerente de Operaciones -Gerente de Riesgos -Gerente de Administración -Jefe de la Oficina de Tecnología de la Información
FASE 6	6.1	Soporte a demanda (bolsa de 900 horas)	Máximo al día siguiente de cada consumo ejecutado que se desee facturar	-Gerente de Finanzas -Gerente de Operaciones -Gerente de Riesgos -Gerente de Administración -Jefe de la Oficina de Tecnología de la Información

b) De existir observaciones, el Departamento de Logística las comunica al CONTRATISTA, indicando claramente el sentido de éstas, otorgándole un plazo para subsanar dependiendo de la complejidad o sofisticación de las subsanaciones a realizar. El plazo de subsanación no debe ser mayor de dos (2) días. Subsanadas las observaciones dentro del plazo otorgado, no corresponde la aplicación de penalidades.
c) El mismo plazo establecido para la subsanación de observaciones resulta aplicable para que el FMV se pronuncie sobre el levantamiento de observaciones.
d) Si pese al plazo otorgado, el contratista no cumpliese a cabalidad con la subsanación, el FMV puede otorgar al contratista periodos adicionales, conforme a lo señalado en el numeral 144.4 del Reglamento de la Ley, u optar por resolver el contrato, de acuerdo con el supuesto de resolución establecido en el literal b) del numeral 68.1 del artículo 68 de la Ley. En caso se otorgue periodos adicionales corresponde aplicar la penalidad por mora desde el vencimiento del plazo inicial para subsanar, sin considerar los días en los que pudiera incurrir la entidad contratante para efectuar las revisiones y notificar las observaciones correspondientes.
e) Este procedimiento no resulta aplicable cuando los bienes, servicios y/o consultorías manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso la entidad contratante no efectúa la recepción o no otorga la conformidad, según corresponda, debiendo considerarse como no ejecutada la prestación, aplicándose la penalidad que corresponda por cada día de atraso.

3.4.18 FORMA DE PAGO

Se detalla a continuación el procedimiento y las condiciones bajo las cuales se realizará el pago de la contraprestación pactada.

1. El pago se realiza de conformidad con lo establecido en el artículo 67 de la Ley.
2. La entidad contratante paga las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días hábiles siguientes de otorgada la conformidad por parte del área usuaria, y es prorrogable, previa justificación de la demora, por cinco (05) días hábiles.
3. El FMV realiza el PAGO A CUENTA de la contraprestación pactada a favor del contratista de acuerdo con el siguiente detalle:

ítem	**Descripción**	**Fases**	**Entregables**	**Pago**

1	**Prestación Principal:**	FASE 1	Etapa 1	Informe de cierre de la etapa 1	70% del monto total del costo de la FASE 1
	Desarrollo e implementación de una PLATAFORMA para la GESTIÓN DE CRÉDITOS		Etapa 2	Informe de cierre de la etapa 2	20% del monto total del costo de la FASE 1
			Etapa 3	Informe de cierre de la etapa 3 ***Acta de cierre de la Fase 1***	10% del monto total del costo de la FASE 1
		FASE 2	Etapa 1	Informe de cierre de la etapa 1 – Fase 2	80% del monto total de la Fase 2.
			Etapa 2	Informe de cierre de la etapa 2 – Fase 2 ***Acta de cierre de la Fase 1***	20% del monto total de la Fase 2.
		FASE 3	Etapa 3	Informe de Migración datos históricos (COFIDE) ***Acta de cierre de la Fase 3***	100% del monto total de la Fase 3: Migración de datos históricos.
2	**Prestación Principal: Operación**	FASE 4	Etapa 4	Soporte	1/24 meses del monto total de la Fase 4: Operación.
3	**Prestación accesoria: Servicio de Bolsa de horas (300 horas)**	FASE 6	Etapa 5	Soporte a demanda	Las horas ejecutadas en la correspondiente a la cantidad de horas consumidas.

Cabe precisar que la Fase 5: Transición de salida no tendrá costo para el FONDO, dado que su ejecución se encuentra condicionada a la no continuidad del servicio y corresponde únicamente a actividades de cierre.

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la entidad contratante debe contar con un expediente de pago con la siguiente documentación:

1. Documento en el que conste la conformidad de la prestación efectuada suscrita por el servidor responsable de la Oficina de Tecnologías de la Información previo informe del Supervisor de Aplicaciones de Tecnologías de la Información y el entregable respectivo que motivo la emisión de la conformidad, correspondiente a lo indicado en el numeral 4.4.

2. Comprobante de pago electrónico que deberá ser presentado en versión PDF y XML, posterior a la emisión del documento en el que conste la conformidad, además deberá indicar el número de contrato y ser emitida a nombre de:

    - Razón Social: FONDO MIVIVIENDA S.A.

- Dirección: Cal. Amador Merino Reyna N° 285 - Edificio Targa - San Isidro RUC: 20414671773

3. Copia del contrato y/u orden de servicio.

4. Consulta de Autorización de Comprobantes de pago (ingresando a la página web de la SUNAT).

El contratista debe presentar el expediente de pago con los documentos señalados previamente, debe presentar la documentación a nuestro canal de Mesa de partes virtual: https://www.mivivienda.com.pe/sgd.mpv/ o al módulo de Mesa de Partes sito en Calle Amador Merino Reyna N° 285 – Edificio Targa – San Isidro, dirigido al Departamento de Logística.

3.4.19 GARANTÍA

El CONTRATISTA de la PLATAFORMA se compromete a subsanar, sin costo adicional para el FONDO, cualquier defecto o vicio oculto que afecte la correcta implementación o funcionamiento de los entregables, incluso con posterioridad a la conformidad otorgada por el FONDO.

La subsanación deberá realizarse en un plazo máximo de **siete (07) días calendario**, contado desde el día siguiente de la notificación efectuada por el FONDO, con la finalidad de garantizar la exigibilidad de la obligación.

El plazo de garantía será de **tres (3) años**, contado a partir de la conformidad otorgada por el FONDO.

3.4.20 RESOLUCIÓN DE CONTRATO

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 68.1 del artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas. De encontrarse en alguno de los supuestos de resolución del contrato, LAS PARTES proceden de acuerdo con lo establecido en el artículo 122 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

3.4.21 RESPONSABILIDAD POR VICIOS OCULTOS

La recepción conforme de la prestación por parte de LA ENTIDAD CONTRATANTE no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 69 de la Ley N° 32069, Ley General de Contrataciones Públicas, y el artículo 144 de su Reglamento, aprobado por Decreto Supremo N° 009-2025-EF.

El plazo máximo de responsabilidad del contratista es de tres (3) años contado a partir de la conformidad otorgada por LA ENTIDAD CONTRATANTE.

3.4.22 REQUISITOS MÍNIMOS

Todos los perfiles de personal solicitados deberán cumplir con los requisitos mínimos establecidos, incluyendo las certificaciones exigidas en las presentes bases, las cuales deberán ser presentadas obligatoriamente para la suscripción del contrato

1. Profesional N° 01 – (01) Un Product Manager

Certificación:

- Certificación CSPO (Certified Scrum Product Owner)
- Curso y/o Bootcamp de Liderazgo mínimo de 30 horas lectivas

- Taller y/o Curso en Gestión de Proyecto, Agilidad mínimo de 30 horas lectivas
- Curso y/o Seminario de Alta Dirección Entidades Financieras mínimo de 30 horas lectivas
- Curso y/o programa Marketing y Ventas mínimo de 30 horas lectivas
- Curso y/o programa en Marketing Digital mínimo de 30 horas lectivas

2. Profesional N° 02 -Un (01) PMP (Project Manager Profesional)

a) Certificación:
- Certificación PMP (Project Management Professional); y,
- Certificación –-ITIL® (ITIL Foundation v3); y,
- SCRUM Fundamentals Certified Credential SFC® y SCRUM Master Certified SMC®; y,
- Certificación CSPO® - Scrum Product Owner; y,
- SAFe SASM – Advanced Scrum Master; y,
- PMO VALUE RING® – Certified Practitioner; y,
- PM4R MASTER PROFESSIONAL®

3. Profesional N°03 - Un (01) Gestor del servicio

Requisito:
- Certificado en Gestión de Proyectos como PMP – Activo
- Certificado en buenas prácticas de agilidad como Scrum Master por Scrum Alliance o Scrum Org
- Certificado como Devops Fundatios y/o ITIL v4

4. Profesional N°04 - Un (01) Jefe de Servicios y Seguridad

Requisitos:
- Certificado como ITIL Foundations v3; y,
- Certificado como ITIL® Foundation Certificate in IT Service Management; y,
- Certificado como ITIL® Service Operation Certificate; y,
- Certificado como IT Service Management Foundation based ISO/IEC 20000; y,
- Certificado como Cloud Computing Foundation Certificate; y,
- Certificado como Information Security Foundation based ISO/IEC 27002; y,
- Certificado como Integrator Secure Cloud Services; y,
- Certificado PRINCE2® Foundation Certificate in Project Management; y,
- Certificado como ITIL® Service Strategy Certificate; y,
- Certificado como ITIL® Service Design Certificate; y,
- Certificado como ITIL® Service Transition Certificate; y,
- Certificado como ITIL® Continual Service Improvement Certificate; y,
- Certificado como ITIL® Expert Certificate in IT Service.

5. Profesional N°5- Un (01) Arquitecto de la nube

- Certificación vigente que demuestre conocimiento en los fundamentos y arquitectura de la nube.

3.4.23 Procedimiento de reemplazo de personal

a) El contratista deberá informar al personal propuesto, las condiciones del servicio, a fin de evitar desistimientos durante el desarrollo del servicio.
b) El personal que preste servicio durante la vigencia del contrato, no tendrán ningún vínculo ni relación laboral con el FONDO S.A. el contratista es su empleador, por

tanto, se compromete a pagar a su personal las remuneraciones, sueldos y salarios de acuerdo con las leyes y beneficios conforme a los dispositivos legales vigentes en materia laboral y especiales, de ser el caso.
c) Para el cambio de personal propuesto, en el caso de renuncia de alguno de los profesionales a cargo del servicio, o a pedido del Contratista o del FMV, EL CONTRATISTA deberá remitir a la Oficina de Tecnologías de la información, con una anticipación de cinco (5) días calendarios a la desvinculación del profesional, un documento dirigido a Mesa de Partes virtual del FMV, indicando el motivo de la renuncia y adjuntando el CV documentado del nuevo profesional propuesto, y/o una terna de potenciales profesionales que cumplan con los mismos requisitos solicitados. La aprobación del profesional de reemplazo será dentro de los dos (2) días calendario siguientes de presentada la solicitud de reemplazo. No se podrá realizar ningún reemplazo de profesional o profesionales, sin la aprobación comunicada por el FMV al contratista dentro del plazo indicado. En caso el personal se retire sin autorización del CONTRATISTA, este tendrá el mismo plazo para presentar al profesional o a la terna de profesionales (cinco días calendario de ocurrido el hecho) y el plazo para que el FMV apruebe al personal será de dos (2) días calendario.

3.4.24 SEGURIDAD DE LA INFORMACIÓN

a) El contratista se compromete a mantener en reserva y a no revelar a terceros, sin previa autorización escrita del FMV, toda información que le sea suministrada por ésta última y/o sea obtenida en el ejercicio de las actividades a desarrollarse o conozca directa o indirectamente durante el proceso de selección o para la realización de sus tareas, excepto en cuanto resultare estrictamente necesario para el cumplimiento del contrato. cualquier información y documentación a la que se tenga acceso a consecuencia del procedimiento de selección y la ejecución del contrato, quedando prohibida revelarla a terceros.

b) Dicha obligación comprende la información que se entrega, como también la que se genera durante la realización de las actividades previas a la ejecución del contrato, durante su ejecución y la producida una vez que se haya concluido el contrato.

c) Dicha información puede consistir en informes, recomendaciones, cálculos, documentos y demás datos compilados o recibidos por el contratista. Asimismo, aun cuando sea de índole pública, la información vinculada al procedimiento de contratación, incluyendo su ejecución y conclusión, no podrá ser utilizada por el contratista para fines publicitarios o de difusión por cualquier medio sin obtener la autorización correspondiente del FMV.

d) **Obligaciones de Confidencialidad del Contratista**

El CONTRATISTA de la PLATAFORMA, junto con su personal, se compromete a no revelar ni compartir ningún dato o documento obtenido durante la ejecución del contrato con terceros, ya sea de forma directa o indirecta. Este acuerdo incluye la prohibición de uso de la información para fines ajenos al cumplimiento del contrato o para beneficio propio. Es importante recalcar que toda la información que el CONTRATISTA de la PLATAFORMA maneje en virtud del contrato es de propiedad exclusiva de FONDO y, por lo tanto, el Contratista no podrá utilizarla de ninguna manera que no esté explícitamente permitida por el FONDO. Al culminar el servicio, el FMV comunicará al CONTRATISTA para que proceda a eliminar toda información generada durante el periodo contratado.

e) Responsabilidad por Violación de la Confidencialidad

El CONTRATISTA de la PLATAFORMA es responsable de mantener y proteger la confidencialidad de la información a la que acceda durante la ejecución del contrato. Cualquier violación a este principio, ya sea mediante la divulgación no

autorizada, la modificación o la alteración de la información, conllevará responsabilidades legales y administrativas para el CONTRATISTA de la PLATAFORMA. Dichas violaciones pueden generar consecuencias que van desde sanciones administrativas hasta acciones legales, incluidas posibles demandas civiles y/o penales, dependiendo de la gravedad de la infracción. Además, el CONTRATISTA de la PLATAFORMA deberá asumir el costo de cualquier indemnización que pueda derivarse de la divulgación no autorizada de información, en caso de que esta genere perjuicios para FONDO o terceros.

f) Medidas Técnicas y Organizativas de Protección

El CONTRATISTA de la PLATAFORMA tiene la obligación de implementar todas las medidas técnicas y organizativas necesarias para proteger la información confidencial. Esto incluye, pero no se limita a, garantizar que sus empleados, directores, CONTRATISTA es, y cualquier otra persona vinculada al CONTRATISTA de la PLATAFORMA no divulguen información a terceros sin la debida autorización por parte de FONDO. Dichas medidas deben asegurar no solo la confidencialidad de los documentos y datos, sino también su integridad y disponibilidad. El Contratista deberá tomar todas las precauciones necesarias para evitar que los datos sean alterados, destruidos o comprometidos de cualquier otra forma.

g) Vigilancia de la Seguridad de la Información

Durante la ejecución del contrato, el CONTRATISTA de la PLATAFORMA también se compromete a estar alerta a cualquier vulnerabilidad o debilidad en los sistemas, infraestructura o servicios de FONDO que pueda comprometer la seguridad de la información. información. Para tal efecto, el CONTRATISTA debe contar con un reporte SOC 2 Tipo II u otro equivalente a fin de garantizar la seguridad de la información. Además, el CONTRATISTA deberá sustentar que su infraestructura de nube cuenta con certificaciones internacionales vigentes en esta materia, tales como ISO/IEC 27001, ISO/IEC 27701 e ISO/IEC 27018. Estas documentaciones deberán ser remitidas por el CONTRATISTA para la presentación de ofertas.

3.4.25 SANCIONES

La potestad de imponer sanción a CONTRATISTAS, participantes, postores, contratistas y subcontratistas, referida en el artículo 88 de la Ley, por infracción a la Ley y el Reglamento, recae en el TCP. También le corresponde imponer sanciones en regímenes especiales de contratación, cuando dichas normas le atribuya expresamente esa potestad.

3.4.26 CLAUSULA ANTICORRUPCIÓN Y ANTISOBORNO:

a) A la suscripción de este contrato, EL CONTRATISTA declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de la entidad contratante.

b) Asimismo, EL CONTRATISTA se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente.

c) Aunado a ello, EL CONTRATISTA se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o CONTRATISTA es de servicios del área

usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

d) Adicionalmente, EL CONTRATISTA se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con LA ENTIDAD CONTRATANTE.
e) Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacioncitas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato

f) Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato4. Cuando lo anterior se produzca por parte de un CONTRATISTA adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que se excluido de los Catálogos Electrónicos de Acuerdo Marco5. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera.

3.4.27 PREVENCIÓN DEL LAVADO DE ACTIVOS Y DEL FINANCIAMIENTO DEL TERRORISMO:

a) EL CONTRATISTA, sus socios, accionistas, asociados, aportantes, directores, representantes, funcionarios, empleados, asesores, agentes o, y/o personas vinculadas, en adelante “los Vinculados”, declaran conocer las normas peruanas en materia de prevención del lavado de activos y del financiamiento del terrorismo y, por consiguiente, se obligan a presentar a EL FONDO la información y/o documentación que le sea solicitada para su adecuada identificación y la de sus “Vinculados”, conforme a sus políticas y procedimientos para la prevención y gestión de los riesgos de lavado de activos y del financiamiento del terrorismo.

b) EL CONTRATISTA declara que ella y/o sus vinculados no han sido condenados en el país o en el extranjero, mediante sentencia consentida o ejecutoriada por la comisión del delito de lavado de activos, financiamiento del terrorismo y/o delitos precedentes o equivalentes; asimismo, que no tienen mandato de prisión preventiva vigente o que, directamente o a través de sus representantes, hubiesen admitido y/o reconocido la comisión de los delitos antes mencionados, ante alguna autoridad nacional o extranjera competente.

c) EL CONTRATISTA se obliga a poner en conocimiento inmediato de EL FONDO cualquier cambio referente a los antecedentes antes mencionados, que se produjeran con posterioridad a la firma del presente Contrato, de lo contrario se presumirá que no ha se ha producido ningún cambio en lo anteriormente declarado, sin perjuicio de lo estipulado en el siguiente párrafo.

d) EL CONTRATISTA acepta expresamente que la falsedad a estas declaraciones o la omisión de comunicación de información o la negativa a proporcionar la información y/o documentación solicitada implica un incumplimiento sustancial del presente Contrato y, por consiguiente, su ocurrencia dará lugar a la resolución automática del mismo.

e) En caso EL FONDO incurriera en costos y/o multas establecidas por una resolución administrativa o sentencia judicial firme, como consecuencia del

incumplimiento de lo establecido en la presente clausula, EL CONTRATISTA se hará totalmente responsable por dichas multas y/o penalidades y/o indemnizaciones y/o pagos similares, asumiendo el importe de las mismas, sin reserva ni limitación alguna.

3.4.28 MEDIDAS DE SEGURIDAD Y SALUD EN EL TRABAJO EN LA PRESTACIÓN DE LA CONTRATACIÓN

El contratista deberá cumplir con lo estipulado en el Reglamento de la Ley de Seguridad y Salud en el Trabajo en lo que respecta al cumplimiento de las normas de seguridad y salud en el trabajo, prevención de riesgos, accidentes de trabajo y enfermedades ocupacionales.

3.4.29 CLAUSULA DE GESTIÓN DE RIESGOS:

LAS PARTES realizan la gestión de riesgos de acuerdo con lo establecido en el contrato y los documentos que lo conforman, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación.

3.4.30 CONFIDENCIALIDAD DE LA INFORMACION:

a) El contratista se compromete a firmar una cláusula de confidencialidad, tomar conocimiento de la Política de SI-C de FMV y lo pertinente del Reglamento de SI-C, mantener reserva, y no revelar a tercero alguno sin previa conformidad escrita de FMV, toda información que le sea suministrada en el marco del contrato que se suscriba.

b) El contratista se compromete a mantener en reserva y a no revelar a terceros, sin previa autorización escrita del FMV, toda información que le sea suministrada por ésta última y/o sea obtenida en el ejercicio de las actividades a desarrollarse o conozca directa o indirectamente durante el proceso de selección o para la realización de sus tareas, excepto en cuanto resultare estrictamente necesario para el cumplimiento del contrato.

c) El contratista deberá mantener la confidencialidad y reserva absoluta en el manejo de cualquier información y documentación a la que se tenga acceso a consecuencia del procedimiento de selección y la ejecución del contrato, quedando prohibida revelarla a terceros.

d) Dicha obligación comprende la información que se entrega, como también la que se genera durante la realización de las actividades previas a la ejecución del contrato, durante su ejecución y la producida una vez que se haya concluido el contrato.

e) Dicha información puede consistir en informes, recomendaciones, cálculos, documentos y demás datos compilados o recibidos por el contratista.

f) Asimismo, aun cuando sea de índole pública, la información vinculada al procedimiento de contratación, incluyendo su ejecución y conclusión, no podrá ser utilizada por el contratista para fines publicitarios o de difusión por cualquier medio sin obtener la autorización correspondiente del FMV.

g) EL CONTRATISTA deberá presentar, para la suscripción del contrato, una Declaración Jurada comprometiéndose a cumplir y hacer cumplir al personal clave destacado lo estipulado en el párrafo precedente.

3.4.31 CLÁUSULA DE RIESGO OPERACIONAL:

a) Las partes declaran tener conocimiento de lo dispuesto por la normativa sobre Gestión Integral de Riesgos aprobada por la Superintendencia de Banca, Seguros y AFP – SBS, la cual tiene por objeto que las empresas supervisadas gestionen adecuadamente los riesgos operacionales asociados a la subcontratación, así como establecer políticas y procedimientos apropiados para evaluar, administrar y monitorear los procesos subcontratados. En ese sentido, EL CONTRATISTA se obliga a ejecutar las prestaciones materia del presente contrato aplicando estándares razonables de control, seguridad, continuidad y confidencialidad acordes con la naturaleza del servicio o bien contratado y con las obligaciones contractuales asumidas.

b) Asimismo, las partes acuerdan que las prestaciones a cargo de EL CONTRATISTA podrán ser objeto de revisión, monitoreo o verificación por parte del FMV, directamente o a través de terceros autorizados, cuando este lo considere necesario para verificar el adecuado cumplimiento contractual. Para tales efectos, EL CONTRATISTA se obliga a facilitar la información y documentación vinculada exclusivamente a los servicios prestados al FMV, así como brindar las facilidades razonables a las personas designadas para efectuar dichas revisiones.

c) EL CONTRATISTA reconoce que, a fin de obtener información sobre la prestación de los servicios a una fecha determinada, el FMV podrá solicitar la revisión de las prestaciones mediante aviso previo, el cual podrá efectuarse incluso el mismo día de la revisión cuando las circunstancias lo justifiquen. En salvaguarda de la protección de datos y de la confidencialidad de la información de EL CONTRATISTA, dichas revisiones únicamente podrán efectuarse respecto de los servicios prestados al FMV. Asimismo, EL CONTRATISTA deberá comunicar al FMV, mediante correo electrónico y dentro del plazo máximo de un (1) día hábil de haber tomado conocimiento, cualquier incidente o evento vinculado directamente a la prestación contratada que pudiera afectar de manera relevante la continuidad del servicio, la disponibilidad de la información, la seguridad de los accesos o el adecuado cumplimiento de las obligaciones contractuales.

3.4.32 CLÁUSULA DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD:

1. Toda información que EL FMV S.A. suministra a EL CONTRATISTA es confidencial y este último deberá mantener su integridad y disponibilidad, así como adoptar un sistema de gestión de seguridad de la información.
2. EL CONTRATISTA declara conocer de manera integral los alcances normativos contemplados en el Reglamento de Gestión de Seguridad de la Información y Ciberseguridad aprobado con Resolución SBS N° 504-2021, y demás normas modificatorias o complementarias, así como las responsabilidades y consecuencias ante su incumplimiento.
3. EL CONTRATISTA no podrá usar la información que le suministra u obtiene a nombre de EL FMV S.A., para fines distintos a los pactados mediante el presente contrato, asimismo no podrá revelarla a terceros, sean personas naturales y/o jurídicas, tampoco podrá realizar anuncios públicos con los datos e información brindada, ni mencionar posibles procesos, actividades, tareas, operaciones, transacciones que se estén realizando o realicen a futuro, salvo autorización por escrito de EL FMV S.A. Esta obligación se extiende adicionalmente a sus socios, representantes, funcionarios, asesores, personal en general, a título de trabajadores o no y al personal destacado por contratos de intermediación o tercerización, a quienes deberá capacitar, instruir, comunicar y obtener su aceptación por escrito al inicio de sus actividades y periódicamente, respecto de las limitaciones señaladas en el presente y sus efectos, consecuencias contractuales, penalidades y responsabilidades, debiendo tener acceso a dicha información solo el personal de EL CONTRATISTA que sea estrictamente necesario. Hacerse responsable ante el incumplimiento de estas obligaciones, ya sea por sus empleados o por terceros.

4. EL CONTRATISTA asegura que, al momento de la suscripción del presente, no tiene en su poder ningún tipo de información de EL FMV S.A. que pueda afectar su gestión de seguridad de la información.
5. Si EL CONTRATISTA considera tener algún tipo de información obtenida con anterioridad a la suscripción del presente, y que deba ser excluida de esta cláusula, deberá comunicarlo a EL FMV S.A. para que se suscriba el documento pertinente detallando la información, y EL CONTRATISTA quede liberada de algún reclamo futuro por parte de EL FMV S.A. con respecto al uso de la misma.
6. En caso EL CONTRATISTA deba revelar información y/o entregar documentación confidencial por mandato de resolución administrativa o jurisdiccional, deberá informar inmediatamente a EL FMV S.A. de tal hecho, con el fin de hacer valer los mecanismos de defensa correspondientes que permitan evitar la divulgación de la documentación e información señaladas y protegerlas en caso tengan que ser reveladas.
7. Sin perjuicio de lo anterior, EL CONTRATISTA cumplirá con el mandato administrativo y/o jurisdiccional indicado, limitándose a entregar aquella parte o sección que resulte indispensable para evitar la sanción correspondiente. En este caso, se deberá además solicitar a la autoridad competente que brinde a la documentación e información reveladas el tratamiento de reserva y confidencialidad que les corresponda; y, remitirá a EL FMV S.A. copia de la información presentada a la autoridad administrativa o jurisdiccional requirente. EL CONTRATISTA, al finalizar la vigencia del presente, se obliga a devolver inmediatamente a EL FMV S.A. toda la información que tenga en su poder, y a destruir aquella de la que se hayan obtenido copias.
8. La obligación de medidas de seguridad de información se mantendrá durante toda la vigencia del presente contrato, mientras subsista cualquier obligación pendiente a cargo de EL CONTRATISTA, y hasta por un plazo adicional de cinco años computados desde el término de la vigencia del presente.
9. Cuando EL CONTRATISTA con motivo de la ejecución del presente contrato, requiera justificadamente el acceso a los equipos, o cualquier soporte de infraestructura de EL FMV S.A., ya sea en sus locales o a través de acceso remoto, debe garantizar que los dispositivos utilizados por sus empleados cuenten de manera obligatoria con las medidas de seguridad y técnicas requeridas por EL FMV S.A..
10. Además, debe abstenerse de realizar almacenamientos o tratamientos de datos suministrados por EL FMV S.A. en la nube, para los casos en que la solución tecnológica se encuentre alojada en la Nube, este procedimiento se deberá realizar previa evaluación, para lo cual EL CONTRATISTA deberá brindar la información prevista en los reglamentos de EL FMV S.A.
11. En caso amerite, deberá implantar las medidas de seguridad perimetral apropiadas para la protección de la información de EL FMV S.A., implementando los mecanismos necesarios para garantizar que las comunicaciones entre su infraestructura y la de EL FMV S.A. debiendo conservar la confidencialidad, integridad y disponibilidad de la información, limitándose a las necesidades del servicio
12. Asimismo, deberá almacenar únicamente los datos necesarios para la ejecución del servicio, debiendo abstenerse de realizar cualquier almacenamiento de información sin el conocimiento y autorización expresa por parte de EL FMV S.A.
13. En caso los datos ó información generada por LAS PARTES, sufran pérdida o robo, acceso no autorizado, divulgación, alguna violación de seguridad o cualquier incidente, EL CONTRATISTA deberá notificarlo a EL FMV S.A. de forma inmediata.

3.4.33 CLÁUSULA DE CONTINUIDAD DEL NEGOCIO:

1. Las partes declaran tener conocimiento de que EL FMV S.A., en su condición de empresa supervisada por la Superintendencia de Banca, Seguros y AFP – SBS, debe adoptar medidas orientadas a garantizar la continuidad de sus operaciones y de los servicios contratados con terceros. En ese sentido, EL CONTRATISTA se obliga a ejecutar las prestaciones materia del presente contrato aplicando

medidas razonables de continuidad, disponibilidad, recuperación y contingencia acordes con la naturaleza del bien o servicio contratado, a fin de reducir el riesgo de interrupciones que puedan afectar el cumplimiento de las obligaciones contractuales asumidas.

2. EL CONTRATISTA declara que cuenta con un Plan Actualizado de Continuidad del Negocio vigente y acorde con la naturaleza de la prestación contratada, el cual contempla medidas para asegurar la continuidad del bien o servicio ante eventos imprevistos, incluyendo casos fortuitos o de fuerza mayor. EL FMV S.A. podrá solicitar la remisión de la documentación que sustente la existencia y actualización de dicho plan, únicamente respecto de los servicios materia del presente contrato.
3. EL CONTRATISTA deberá contar con mecanismos de comunicación para informar oportunamente cualquier evento que genere o pudiera generar interrupción relevante en la prestación contratada. Dicha comunicación deberá efectuarse al FMV dentro del plazo máximo de tres (3) horas de tomado conocimiento del evento. Asimismo, dentro del plazo máximo de cuatro (4) días hábiles de realizada la comunicación inicial, EL CONTRATISTA deberá remitir un informe que contenga, como mínimo: a) las causas del evento; b) el tiempo estimado o real de afectación; c) los servicios o entregables afectados; d) las medidas implementadas para la atención y recuperación; y, e) el estado situacional actualizado del evento.
4. EL CONTRATISTA se obliga a participar, cuando sea requerido por EL FMV S.A. y durante la vigencia contractual, en las pruebas de continuidad relacionadas con las prestaciones materia del presente contrato, brindando las facilidades razonables necesarias para su ejecución. La participación en dichas pruebas no implicará la obligación de efectuar simulaciones o pruebas ajenas al alcance de la prestación contratada.

3.4.34 CLAUSULA DE PROTECCIÓN DE DATOS PERSONALES:

Son considerados datos personales, para efectos del presente contrato, cualquier tipo de información o documentos que identifican o hacen identificables a personas naturales. Datos que pueden estar contenidos en medios o soportes razonablemente utilizables (banco de datos) de acuerdo con la Ley 29733 Ley de Protección de Datos Personales (LPDP), Reglamento, directivas y demás normas modificatorias o complementarias.

De corresponder, **EL CONTRATISTA** declara:

1. Ser titular del banco de datos personales que en virtud de la presente relación contractual transfiere a **EL FMV** para su tratamiento.
2. Contar con el consentimiento previo, informado, expreso e inequívoco de las personas naturales cuyos datos personales se encuentran contenidos en el banco de datos, para que éstos, puedan ser objeto de tratamiento por **EL FMV**;
3. Que la información contenida en el banco de datos que se transfiere ha sido obtenida de manera legítima;
4. Que el banco de datos, materia del presente, se encuentra debidamente inscrito en el Registro Nacional de Protección de Datos Personales a cargo de la Dirección Nacional de Protección de Datos del MINJUS,
5. Que el banco de datos cumple con las obligaciones de seguridad, protección, calidad y legalidad establecida en la LPDP, modificatorias y sus Directivas.

En caso EL FMV transfiera Datos Personales a EL CONTRATISTA, este se obliga de manera taxativa mas no limitativa a:

1. Acceder únicamente al banco de datos personales que **EL FMV** le transfiera, con la finalidad exclusiva de la ejecución del presente contrato;
2. Una vez ejecutada la prestación materia del presente contrato, **EL CONTRATISTA** deberá devolver, a su costo y asumiendo las medidas de seguridad exigidas en la Directiva de Seguridad de la Información de la LPDP

toda la información entregada por **EL FMV;** también deberá eliminar de forma permanente los datos personales que le fueron transferidos así como cualquier copia de los mismos en los diversos soportes de activos de información (equipos, papeles, etc.) salvo que de manera justificada y con conocimiento y aceptación de **EL FMV** deba conservarla para la atención de posibles reclamos derivados del tratamiento efectuado por **EL FMV**, en cuyo caso la mantendrán como información reservada y confidencial, hasta que transcurra el plazo de prescripción legal;

3. Cuando **EL CONTRATISTA** con motivo de la ejecución del presente contrato, requiera justificadamente el acceso a los equipos, o cualquier soporte de infraestructura de **EL FMV,** ya sea en sus oficinas o a través de acceso remoto, se obliga a adoptar las medidas de seguridad y técnicas necesarias descritas en la LPDP, reglamento, directivas y modificatorias, salvaguardando que los datos a los que tiene acceso, no sean trasladados a soportes distintos que no sean de propiedad de **EL FMV** o a soportes de su propiedad, siempre que cuente con la autorización de **EL FMV;**
4. Cuando la ejecución del presente contrato requiera que los datos transferidos sean tratados por **EL CONTRATISTA** en la nube o locales ajenos a los de **EL FMV**, **EL CONTRATISTA** deberá comunicar y poner a disposición de **EL FMV** un documento que acredite que cumple con las medidas de seguridad de información y otros aspectos señalados en el Reglamento de la Ley de PDP, La Directiva de Seguridad de la Información de la Ley en mención y debe evidenciar anualmente que **EL CONTRATISTA** y/o sus subcontratistas mantienen vigente las certificaciones ISO/IEC 27001, y que cuentan con un reporte SOC 2 tipo 2 u otros equivalentes, relevantes al servicio provisto y a la zona o región desde donde se provee el bien o servicio.
5. Mantener indemne a **EL FMV** por cualquier reclamo de algún tercero, fundado en el incumplimiento de la presente clausula.
6. **EL CONTRATISTA** no podrá usar la información que le suministra u obtiene a nombre de **EL FMV**, para fines distintos a los pactados mediante el presente, asimismo no podrá revelarla a terceros, sean personas naturales y/o jurídicas, tampoco podrá realizar anuncios públicos con los datos e información brindada, ni mencionar de posibles procesos, actividades, tareas, operaciones, transacciones que se estén realizando o realicen a futuro, salvo autorización por escrito de **EL FMV**. Esta obligación se extiende adicionalmente a sus trabajadores y personal dependiente, sea directa o indirectamente, a quienes deberá capacitar, instruir, comunicar y obtener su aceptación por escrito al inicio de sus actividades y periódicamente, respecto de las limitaciones señaladas en el presente y sus efectos, consecuencias contractuales, penalidades y responsabilidades, debiendo tener acceso a dicha información solo el personal de **EL CONTRATISTA** que sea estrictamente necesario. Hacerse responsable ante el incumplimiento de estas obligaciones, ya sea por sus empleados o por terceros.
7. En caso **EL CONTRATISTA** deba revelar información y/o entregar documentación personal de clientes de **EL FMV** por mandato de resolución administrativa o jurisdiccional, deberá informar inmediatamente a **EL FMV** de tal hecho, con el fin de poder hacer valer los mecanismos de defensa correspondientes que permitan evitar la divulgación de la documentación e información señaladas y protegerlas en caso tengan que ser reveladas. Sin perjuicio de lo anterior, **EL CONTRATISTA** cumplirá con el mandato administrativo y/o jurisdiccional indicado, limitándose a entregar aquella parte o sección que resulte indispensable para evitar la sanción correspondiente. En este caso, se deberá además solicitar a la autoridad competente que brinde a la documentación e información reveladas, el tratamiento de reserva y confidencialidad que les corresponda; y, remitirá a **EL FMV** copia de la información presentada a la autoridad administrativa o jurisdiccional requirente.
8. **EL CONTRATISTA**, al finalizar la vigencia del presente, se obliga a devolver inmediatamente a **EL FMV** toda la información que tenga en su poder, y a destruir aquella de la que se hayan obtenido copias.

9. Cumplir con todas las demás disposiciones contenidas en la Ley, su Reglamento y cualquier otra normativa referida a la protección de datos personales, no descritas expresamente en la presente clausula.

3.5. REQUISITOS DE CALIFICACIÓN

2.5.1. REQUISITOS DE CALIFICACIÓN OBLIGATORIOS

A. EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

Requisitos:

El postor debe acreditar un monto facturado acumulado equivalente a **S/ 5,000,000.00 (Cinco millones con 00/100 soles)**, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los quince años anteriores a la fecha de la presentación de ofertas que se computa desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran servicios similares a los siguientes:

- Desarrollo e Implementación de sistemas bancarios tercerizados
- Desarrollo e Implementación de software como servicio (SaaS)
- Desarrollo e Implementación de software de procesamiento de productos crediticios
- Servicio de migración de servicios on premise a la nube
- Servicios de migración de plataformas SaaS
- Servicio de desarrollo de software
- Servicio de fábrica de sotfware.
- Servicio de soporte especializado para los servicios de tecnología de información y comunicaciones
- Servicio de alojamiento (Housing)

Acreditación:

La experiencia del postor en la especialidad se acredita con un máximo de veinte (20) contrataciones, mediante copia simple de: (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con constancia de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago[1], o comprobante de retención electrónico emitido por SUNAT por la retención del IGV[2]. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados[3], para acreditarla debe presentar de forma obligatoria lo indicado en el numeral (ii) del presente párrafo; no es posible que acredite su experiencia únicamente con la presentación de contratos u órdenes de servicio con conformidad o constancia de prestación.

En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo correspondiente** referido a la

---

[1] El solo sello de cancelado en el comprobante de pago, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación fehaciente de la cancelación. Es válido el sello colocado por el cliente del postor (sea utilizando el término “cancelado” o “pagado”).

[2] De acuerdo con el Régimen de Retenciones del Impuesto General a las Ventas (IGV).

[3] Se entiende “privados” como aquellos que no son entidades contratantes.

Experiencia del Postor en la Especialidad.

En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los quince años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso de que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo correspondiente**

Las personas jurídicas resultantes de un proceso de reorganización societaria no pueden acreditar como experiencia del postor en la especialidad aquella que le hubieran transmitido como parte de dicha reorganización las personas jurídicas sancionadas con inhabilitación vigente o definitiva.

Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicio o de cancelación del comprobante de pago, según corresponda.

Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo correspondiente** referido a la Experiencia del Postor en la Especialidad.

Advertencia
En el caso de consorcios, solo se considera la experiencia de aquellos integrantes que ejecutan conjuntamente el objeto del contrato.

2.5.2. REQUISITOS DE CALIFICACIÓN ADICIONALES

B. CAPACIDAD TÉCNICA Y PROFESIONAL

C.1. EXPERIENCIA DEL PERSONAL CLAVE

Requisitos:

a. **Profesional N°01 – Product Manager (01):**
Deberá acreditar experiencia de siete (07) años como Gerente de Producto en el Sistema Financiero y/o Gerente de Producto en Bancos del sistema financiero Peruano.

b. **Profesional N°02 – PMP (1):**
Deberá acreditar experiencia mínima de cinco (05) años como Sub-Gerente o Gerente de Soluciones de Negocios o Gerente de Tecnología de la Información o Gerente de desarrollo de sistemas o software o soluciones tecnológicas en el sistema Financiero Peruano.

c. **El profesional N°03 – Gestor de Servicios (1):**
Deberá acreditar experiencia mínima de cinco (05) años como jefe o supervisor o coordinador de proyectos de tecnología de la información o desarrollo de

sistemas o software o soluciones tecnológicas o soporte y mantenimiento TI en el sistema Financiero Peruano.

d. El profesional N°04 – Jefe de Servicios y Seguridad (1):
Deberá acreditar experiencia mínima de siete (07) años como jefe de servicios de TI, SMO, o supervisor o coordinador de servicios de tecnología de la información o supervisor de sistemas o soporte y mantenimiento TI en el sistema Financiero.

e. El profesional N° 05 - Arquitecto de la nube (1):
Deberá acreditar experiencia mínima de cuatro (4) años realizando actividades de diseño de arquitecturas escalables, seguras, resilientes y de alto rendimiento, implementando políticas de seguridad, cifrado (en tránsito y en reposo) y auditoría. Mantenimiento de soluciones en la nube utilizando los servicios y mejores prácticas de AWS, GCP o Azure.

Acreditación:

El postor debe señalar la denominación del puesto, cargo y/o posición, y tiempo de experiencia del personal clave propuesto (años, meses y días) en el **Anexo correspondiente**, adjuntando en su oferta, copia simple de cualquiera de los siguientes documentos: (i) contratos y su respectiva conformidad; (ii) constancias; (iii) certificados; o (iv) cualquier otra documentación que, de manera fehaciente, demuestre la experiencia del personal propuesto.

Estos documentos deben señalar los nombres y apellidos del personal clave; el cargo desempeñado indicando el día, mes y año de inicio y culminación; el nombre de la entidad u organización que emite el documento; la fecha de emisión y nombres y apellidos de quien suscribe el documento.

En caso los documentos que acreditan la experiencia establezcan esta en meses sin especificar los días se debe considerar el mes completo. Se considera aquella experiencia que no tenga una antigüedad mayor a veinticinco años anteriores a la fecha de la presentación de ofertas. De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo de la misma solo se considera una vez el periodo traslapado. En ningún caso corresponde exigir que el mismo personal clave acredite experiencia en más de un cargo.

Advertencia
Al calificar la experiencia del personal, se debe valorar de manera integral los documentos presentados por el postor para acreditar dicha experiencia. En tal sentido, aun cuando en los documentos presentados la denominación del cargo o puesto no coincida literalmente con aquella prevista en las bases, se deberá validar la experiencia si las actividades que realizó el personal corresponden con la función propia del cargo o puesto requerido en las bases.

C.2. CALIFICACIONES DEL PERSONAL CLAVE

C.2.1 FORMACIÓN ACADÉMICA

Advertencia
Como requisito de calificación solo puede consignarse “grado de bachiller” o “título profesional”, según el perfil del personal clave definido por el área usuaria considerando, entre otros aspectos, la normativa que resulte aplicable.

Requisitos:

a) Profesional N°01 – Product Manager (01):

Titulado en las especialidades de Ingeniería de Sistemas y/o Ingeniería Informática y/o Ingeniería Industrial y/o Ingeniería de Computación y Sistemas y/o Ingeniería de Sistemas Empresariales y/o Ingeniería Estadística e Informática y/o Ingeniería de Software y/o Ingeniería Industrial y/o Ingeniería Electrónica y/o Ingeniería de Telecomunicaciones y/o Licenciado (a) en Economía y/o Licenciatura en Sistemas Computacionales y/o Ingeniera Mecánico Electrónica y/o Ingeniería de Redes y Comunicaciones y/o Ingeniería Empresarial y de Sistemas y/o Ingeniería Industrial y de Sistemas y/o Ingeniería de Sistemas e Informática y/o Ingeniería de Sistemas de Información y/o Ingeniería de Telecomunicaciones y Redes y/o Ingeniería de Seguridad Informática y/o Ingeniería de Sistemas y Cómputo y/o Ingeniería Empresarial y/o Computación e Informática y/o Ingeniería de Computación y/o Licenciado (a) en Computación y/o Ingeniería de Sistemas y Computación y/o Ciencias de la Computación y/o Ciencias de la Información y/o Ingeniería Informática y de Sistemas y/o Ingeniería de Telecomunicaciones y Telemática y/o Ingeniería de Sistemas de Información y Gestión y/o Licenciado (a) Administración y Sistemas y/o Certificado y/o Título de Profesional Técnico en Computación e Informática y/o Técnico en Informática y/o Técnico en sistemas y/o técnico en Electrónica y/o técnico en Redes y Comunicaciones de Datos y/o técnico en Administración de Redes y Comunicaciones y/o técnico en Administración y Sistemas y/o Técnico en Sistemas de Información y/o Técnico en Desarrollo de Sistemas de Información y/o Técnico en informática y computación y/o Técnico en Administración de Redes y Comunicaciones y/o Ingeniería Electrónica con mención en Telecomunicaciones y/o Ingeniería de Sistemas de Información y Gestión.

b) Profesional N°02 – PMP (1):

Titulado en las especialidades de Ingeniería de Sistemas y/o Ingeniería Informática y/o Ingeniería Industrial y/o Ingeniería de Computación y Sistemas y/o Ingeniería de Sistemas Empresariales y/o Ingeniería Estadística e Informática y/o Ingeniería de Software y/o Ingeniería Industrial y/o Ingeniería Electrónica y/o Ingeniería de Telecomunicaciones y/o Licenciatura en Sistemas Computacionales y/o Ingeniera Mecánico Electrónica y/o Ingeniería de Redes y Comunicaciones y/o Ingeniería Empresarial y de Sistemas y/o Ingeniería Industrial y de Sistemas y/o Ingeniería de Sistemas e Informática y/o Ingeniería de Sistemas de Información y/o Ingeniería de Telecomunicaciones y Redes y/o Ingeniería de Seguridad Informática y/o Ingeniería de Sistemas y Cómputo y/o Ingeniería Empresarial y/o Computación e Informática y/o Ingeniería de Computación y/o Licenciado (a) en Computación y/o Ingeniería de Sistemas y Computación y/o Ciencias de la Computación y/o Ciencias de la Información y/o Ingeniería Informática y de Sistemas y/o Ingeniería de Telecomunicaciones y Telemática y/o Ingeniería de Sistemas de Información y Gestión y/o Licenciado (a) Administración y Sistemas y/o Certificado y/o Título de Profesional Técnico en Computación e Informática y/o Técnico en Informática y/o Técnico en sistemas y/o técnico en Electrónica y/o técnico en Redes y Comunicaciones de Datos y/o técnico en Administración de Redes y Comunicaciones y/o técnico en Administración y Sistemas y/o Técnico en Sistemas de Información y/o Técnico en Desarrollo de Sistemas de Información y/o Técnico en informática y computación y/o Técnico en Administración de Redes y Comunicaciones y/o Ingeniería Electrónica con mención en Telecomunicaciones y/o Ingeniería de Sistemas de Información y Gestión.

c) El profesional N°03 – Gestor del Servicio (01):

Titulado en las especialidades de Ingeniería de Sistemas y/o Ingeniería Informática y/o Ingeniería Industrial y/o Ingeniería de Computación y Sistemas y/o Ingeniería de Sistemas Empresariales y/o Ingeniería Estadística e

Informática y/o Ingeniería de Software y/o Ingeniería Industrial y/o Ingeniería Electrónica y/o Ingeniería de Telecomunicaciones y/o Licenciatura en Sistemas Computacionales y/o Ingeniera Mecánico Electrónica y/o Ingeniería de Redes y Comunicaciones y/o Ingeniería Empresarial y de Sistemas y/o Ingeniería Industrial y de Sistemas y/o Ingeniería de Sistemas e Informática y/o Ingeniería de Sistemas de Información y/o Ingeniería de Telecomunicaciones y Redes y/o Ingeniería de Seguridad Informática y/o Ingeniería de Sistemas y Cómputo y/o Ingeniería Empresarial y/o Computación e Informática y/o Ingeniería de Computación y/o Licenciado (a) en Computación y/o Ingeniería de Sistemas y Computación y/o Ciencias de la Computación y/o Ciencias de la Información y/o Ingeniería Informática y de Sistemas y/o Ingeniería de Telecomunicaciones y Telemática y/o Ingeniería de Sistemas de Información y Gestión y/o Licenciado (a) Administración y Sistemas y/o Certificado y/o Título de Profesional Técnico en Computación e Informática y/o Técnico en Informática y/o Técnico en sistemas y/o técnico en Electrónica y/o técnico en Redes y Comunicaciones de Datos y/o técnico en Administración de Redes y Comunicaciones y/o técnico en Administración y Sistemas y/o Técnico en Sistemas de Información y/o Técnico en Desarrollo de Sistemas de Información y/o Técnico en informática y computación y/o Técnico en Administración de Redes y Comunicaciones y/o Ingeniería Electrónica con mención en Telecomunicaciones y/o Ingeniería de Sistemas de Información y Gestión.

d) El profesional N°04 - Jefe de Servicios y Seguridad (01):

Titulado o Bachiller en las especialidades de Ingeniería de Sistemas y/o Ingeniería Informática y/o Ingeniería Industrial y/o Ingeniería de Computación y Sistemas y/o Ingeniería de Sistemas Empresariales y/o Ingeniería Estadística e Informática y/o Ingeniería de Software y/o Ingeniería Industrial y/o Ingeniería Electrónica y/o Ingeniería de Telecomunicaciones y/o Licenciatura en Sistemas Computacionales y/o Ingeniera Mecánico Electrónica y/o Ingeniería de Redes y Comunicaciones y/o Ingeniería Empresarial y de Sistemas y/o Ingeniería Industrial y de Sistemas y/o Ingeniería de Sistemas e Informática y/o Ingeniería de Sistemas de Información y/o Ingeniería de Telecomunicaciones y Redes y/o Ingeniería de Seguridad Informática y/o Ingeniería de Sistemas y Cómputo y/o Ingeniería Empresarial y/o Computación e Informática y/o Ingeniería de Computación y/o Licenciado (a) en Computación y/o Ingeniería de Sistemas y Computación y/o Ciencias de la Computación y/o Ciencias de la Información y/o Ingeniería Informática y de Sistemas y/o Ingeniería de Telecomunicaciones y Telemática y/o Ingeniería de Sistemas de Información y Gestión y/o Licenciado (a) Administración y Sistemas y/o Certificado y/o Título de Profesional Técnico en Computación e Informática y/o Técnico en Informática y/o Técnico en sistemas y/o técnico en Electrónica y/o técnico en Redes y Comunicaciones de Datos y/o técnico en Administración de Redes y Comunicaciones y/o técnico en Administración y Sistemas y/o Técnico en Sistemas de Información y/o Técnico en Desarrollo de Sistemas de Información y/o Técnico en informática y computación y/o Técnico en Administración de Redes y Comunicaciones y/o Ingeniería Electrónica con mención en Telecomunicaciones y/o Ingeniería de Sistemas de Información y Gestión.

e) El profesional N° 05 - Arquitecto de la nube (01):

Titulado o Bachiller en las especialidades de Ingeniería de Sistemas o Ingeniería Electrónica o Ingeniería de Telecomunicaciones y Redes o Ingeniería Industrial o Ingeniería Electrónica o Ingeniería de Computación y Sistemas o Ingeniería de

Software o Ingeniería de Sistemas de Información o Ingeniería de Computación o Ingeniería Informática o Ingeniería de Seguridad o Ingeniería de Computación o Ciencias de la Computación o Ciencias de la Información o Administración y Sistemas-

Acreditación:

El postor debe señalar los nombres y apellidos, documento de identidad, el nombre de la universidad o institución educativa que expidió el grado de título profesional, y el grado o título profesional obtenido en el **Anexo correspondiente**, adjuntando en su oferta copia del grado de bachiller o título profesional. En caso se acredite estudios en el extranjero del personal clave, debe presentarse, adicionalmente, copia simple de la revalidación o reconocimiento del grado o título ante la SUNEDU.

Los evaluadores o la DEC, según corresponda, verifican los grados o títulos profesionales en el Registro Nacional de Grados Académicos y Títulos Profesionales de la Superintendencia Nacional de Educación Superior Universitaria – SUNEDU, a través del siguiente link: https://enlinea.sunedu.gob.pe/ o en el Registro Nacional de Certificados, Grados y Títulos del Ministerio de Educación, a través del siguiente link: https://titulosinstitutos.minedu.gob.pe/ según corresponda.

C.2.2 CAPACITACIÓN DEL PERSONAL CLAVE

Requisitos:

a) Profesional N°01 – Product Manager (01):

- Curso y/o Programa Internacional de Alta Dirección en Productos Financieros mínimo de 30 horas lectivas
- Curso de Product Manager mínimo de 30 horas lectivas
- Curso de Dirección Estratégica para la Defensa y la Administración de Crisis mínimo de 30 horas lectivas
- Gobierno Corporativo para liderar Comités mínimo de 30 horas lectivas

Acreditación:

Se acredita con copia simple de constancias, certificados u otros documentos.

Advertencia
• Las horas indicadas pueden ser lectivas, académicas y/o pedagógicas sin distinción entre estas. • Al evaluar la incorporación de este requisito, la entidad contratante debe sustentar que el tipo de capacitación seleccionado se encuentre vinculado con las actividades que va a desempeñar el personal clave. • Se podrá acreditar la capacitación mediante certificados de estudios de postgrado, considerando que cada crédito del curso que acredita la capacitación equivale a dieciséis horas, según la normativa de la materia.