Anexo técnico – Especificaciones técnicas

Contenido

Calle 60a #5-54, Oficina 403
Bogotá D.C. Colombia
NIT. 830.101.214-4
+57 3222468120
www.colombiadigital.net

Calle 60a #5-54, Oficina 403
Bogotá D.C. Colombia
NIT. 830.101.214-4
+57 3222468120
www.colombiadigital.net

1 Objeto

Diseñar e implementar una solución integral para los mecanismos, coberturas y/o asistencias que faciliten el acceso a la educación superior y/o mitiguen el riesgo de crédito de conformidad a las necesidades técnicas, funcionales y normativas definidas por la entidad designada por la Corporación Colombia Digital.

2 Contexto

La educación superior constituye un pilar esencial para el progreso social y económico de Colombia. En este contexto, la entidad designada por la Corporación ha consolidado su papel en la promoción del acceso a este nivel educativo mediante el financiamiento de estudios a través de créditos, facilitando el desarrollo del capital humano y la movilidad social.

El Fondo Pasivo Contingente (FPC), se orienta a proporcionar un respaldo integral a los beneficiarios de crédito, mediante la articulación de estrategias y mecanismos que faciliten el acompañamiento continuo en situaciones que puedan afectar la estabilidad económica y académica. En este sentido, se contempla la implementación de una solución tecnológica avanzada que permita gestionar de forma centralizada y eficiente las operaciones del producto de ahorro, integrando funciones de administración de cuentas de ahorro, procesamiento de transacciones de pago de crédito y la ejecución de coberturas y asistencias del FPC a través de interfaces móviles y web. La digitalización de estos procesos operativos optimiza la gestión del recaudo y transforma cada transacción en una inversión directa en la educación superior, promoviendo la disciplina financiera y la planificación a largo plazo en un entorno regulado.

La implementación de este producto de ahorro y la gestión integral de las coberturas del FPC también están en consonancia con la política pública de fomento a la educación superior, que busca garantizar la movilidad social y la igualdad de oportunidades. Al facilitar la permanencia y culminación de los estudios, el FPC actúa como un mecanismo de equidad, reduciendo las barreras económicas que podrían limitar el acceso de los estudiantes a la educación superior. De igual forma, el producto de ahorro se convierte en un instrumento que fortalece la inclusión financiera, permitiendo que los beneficiarios puedan planificar su futuro académico y profesional de manera más efectiva.

La tecnología y los mecanismos digitales desempeñan un papel esencial en esta transformación. La integración de plataformas digitales avanzadas permitirá a la entidad designada por la corporación a gestionar de manera más eficiente tanto el producto de ahorro como las coberturas del FPC, optimizando el uso de los recursos y reduciendo costos operativos. Además, esto facilitará la digitalización de los servicios, permitiendo a los usuarios finales realizar transacciones de manera ágil y segura, lo que a su vez promoverá una mayor autonomía en la gestión de sus recursos.

El impacto social y económico de esta iniciativa se traduce en la ampliación de las oportunidades para los estudiantes, al proporcionarles un instrumento que fomente el acceso, la permanencia y la culminación exitosa de sus estudios. Al transformar el ahorro en una herramienta de inversión

Calle 60a #5-54, Oficina 403
Bogotá D.C. Colombia
NIT. 830.101.214-4
+57 3222468120
www.colombiadigital.net

en educación superior, la entidad refuerza su compromiso con la movilidad social y el desarrollo del capital humano, permitiendo que el producto de ahorro funcione como un catalizador para el fortalecimiento de la inclusión financiera.

La implementación de un producto de ahorro, enmarcado dentro del FPC, se presenta como una respuesta innovadora ante la necesidad de ampliar las oportunidades para que un mayor número de colombianos ingresen, permanezcan y culminen sus estudios superiores. La propuesta se fundamenta en un sólido marco jurídico y operativo, enmarcado en los lineamientos del artículo 5 de la Ley 1002 de 2005, el Decreto 375 de 2018 y las disposiciones del Acuerdo 023 de 2024, lo que permite integrar de manera armónica los mecanismos de financiamiento, coberturas y asistencias que caracterizan este proyecto.

La entidad designada tiene grandes retos con este producto de ahorro, y se espera que pueda ser mejorado y adaptado en el futuro para fortalecer y modernizar su portafolio de servicios. Este proyecto ha sido catalogado como de gran importancia e impacto social, ya que busca cofinanciar la educación superior y contribuir al desarrollo sostenible de Colombia. Entro de las políticas internas de la entidad designada, determina los lineamientos de la cuenta de ahorro educativo voluntario de la misma. Esta cuenta tiene como finalidad fomentar el acceso a la educación superior, permitiendo a los ahorradores financiar su matrícula o el sostenimiento de su educación superior o la de un beneficiario, mejorando su perfil de riesgo crediticio y facilitando el acceso a crédito para los semestres restantes.

El producto de ahorro permitirá a los titulares realizar depósitos periódicos en la entidad designada, con el objetivo de alcanzar una meta de ahorro en un plazo determinado. Estos depósitos generarán intereses, facilitando que los particulares puedan financiar la etapa inicial de los programas de educación superior, una fase que suele ser más costosa y con mayor riesgo de abandono. La entidad, a través de este innovador producto de ahorro y la implementación de una solución tecnológica avanzada, reafirma su compromiso con la educación superior y el bienestar de los estudiantes colombianos. La integración de tecnologías digitales no solo optimiza la gestión de los recursos, sino que también ofrece una plataforma accesible y eficiente para todos los usuarios. Este proyecto es un ejemplo de cómo la innovación y la tecnología pueden transformar la educación y mejorar la calidad de vida de miles de colombianos, garantizando un futuro más prometedor y equitativo para todos.

De esta manera, el producto de ahorro del FPC es un componente estratégico que, en convergencia con la implementación de una plataforma tecnológica avanzada, moderniza la administración del pasivo institucional y habilita un sistema integrado para la gestión de coberturas y asistencias. La propuesta, fundamentada en un riguroso análisis técnico-jurídico, orienta la gestión digital y la humanización de la entidad designada, optimizando los procesos operativos y potenciando el respaldo financiero para los beneficiarios.

Este proyecto representa un paso trascendental en la evolución de la entidad, permitiendo transformar la forma en que se gestionan los recursos y se ofrecen servicios a los usuarios, en consonancia con las mejores prácticas del sector y las exigencias del entorno normativo actual. La iniciativa se presenta, por tanto, como un mecanismo integral que, a través de la convergencia de tecnología y normatividad, impulsa el desarrollo sostenible de la educación superior en

Colombia y refuerza el compromiso de la entidad con el bienestar de sus beneficiarios y el fortalecimiento del sistema educativo.

En el desarrollo del presente documento se encontrarán las especificaciones técnicas de la solución, que detallan los requerimientos operativos, de integración y seguridad que deberá cumplir la plataforma. Dichas especificaciones permiten valorar de manera integral la viabilidad y la capacidad de la solución para responder a las exigencias del entorno normativo y del mercado, constituyéndose en un elemento clave para la transformación digital y la modernización de la gestión del pasivo institucional.

3 Especificaciones técnicas

En el desarrollo del contrato, el oferente deberá considerar los siguientes componentes clave del proyecto de transformación digital para la implementación del Fondo de Pasivo Contingente FPC.

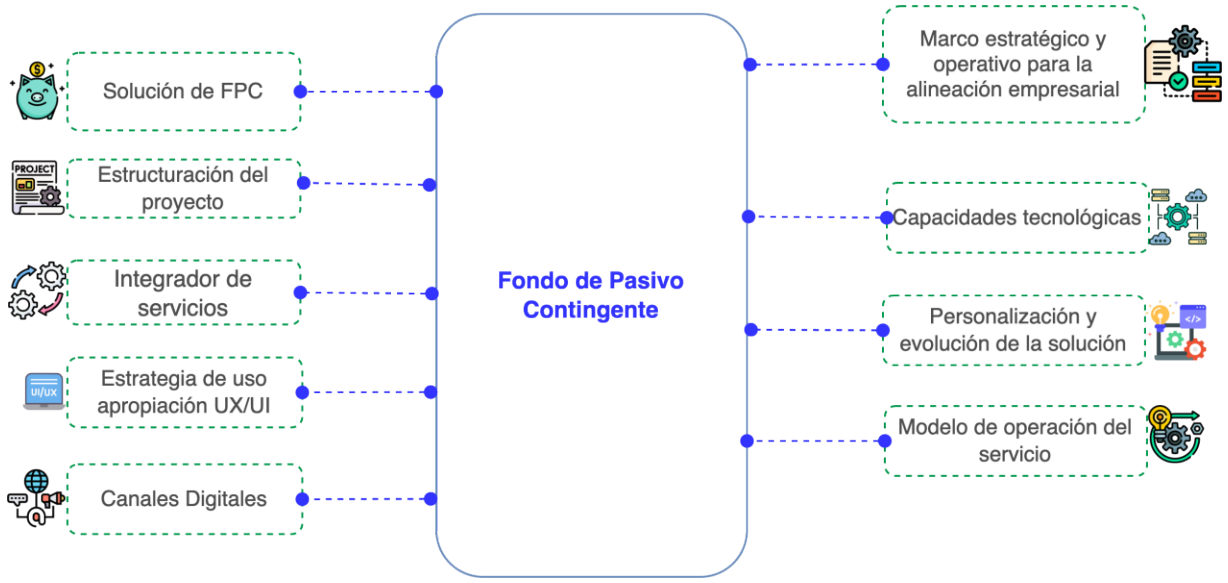


Ilustración 1 Componentes clave FPC

A continuación, se describen conceptualmente cada uno de estos componentes:

3.1 Solución Fondo Pasivo Contingente

Los Fondos de Garantías de la entidad, se consolidaron en el Fondo Pasivo Contingente, creado y reglamentado mediante el Acuerdo interno, con el propósito de potenciar el acompañamiento y el bienestar de sus beneficiarios, contribuyendo a la consecución de las metas académicas y brindando apoyo en los momentos más desafiantes de su formación superior.

El Fondo Pasivo Contingente se encuentra en el marco del Plan Estratégico de la entidad en el cumplimiento de los objetivos estratégicos “O2. Diversificar fuentes de fondeo, para otorgar las mejores condiciones de crédito educativo a los beneficiarios” y “O5. Establecer una red de apoyo que permita generar valor agregado a los grupos de incidencia”, ya que este Fondo proporcionará un esquema de asistencia integral e impulsará proyectos de vida de manera sostenible, a través de la implementación de estrategias y mecanismos que proporcionen coberturas y/o asistencias efectivas, enfocadas en la mitigación del riesgo crediticio.

Así mismo, el Fondo fortalecerá el acompañamiento y el bienestar de sus beneficiarios. Se enfocará en desarrollar e implementar estrategias y mecanismos que proporcionen coberturas y/o asistencias efectivas, con el fin de mitigar el riesgo crediticio ocasionado por dificultades económicas causadas por eventos adversos de salud, desempleo y, en casos extremos, el fallecimiento. Todo lo anterior mediante la integración de las capacidades y recursos financieros y no financieros de los Fondos y Subfondos de Garantías.

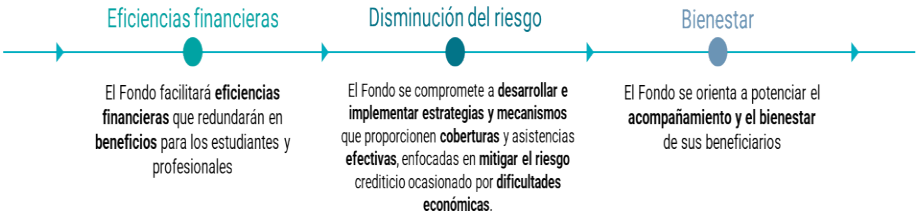


Ilustración 2 Eficiencia de los servicios

El Fondo Pasivo Contingente de la entidad designada provee coberturas y asistencias que protegen a los estudiantes ante eventualidades que puedan comprometer su estabilidad financiera y académica, reforzando el bienestar y la integridad financiera de todos los beneficiarios de créditos educativos, así como de las Instituciones de Educación Superior y de la propia entidad.

Ilustración 3 Estrategias del FPC

Calle 60a #5-54, Oficina 403
Bogotá D.C. Colombia
NIT. 830.101.214-4
+57 3222468120
www.colombiadigital.net

Mediante la implementación de estrategias enfocadas en la minimización del riesgo crediticio, el Fondo Pasivo Contingente refuerza el bienestar estudiantil y la integridad financiera de los estudiantes, profesionales, Instituciones de Educación Superior y de la propia entidad. Cada acción tomada busca fortalecer la confianza en la entidad y contribuir a un futuro educativo prometedor para Colombia.

Por lo anterior, resulta pertinente la creación y puesta en marcha de nuevos mecanismos que generen un impacto beneficioso en la calidad de vida de los estudiantes financiados por la entidad designada. Estos mecanismos estarán destinados a respaldar su recorrido educativo, incentivando de esta manera su permanencia en las IES y contribuyendo a la culminación exitosa de sus programas académicos.

Esta información tiene como objetivo proporcionar una visión de las expectativas y necesidades de la entidad designada por la corporación en relación con los mecanismos y estrategias que permitan ofrecer respaldo y protección integral a los beneficiarios de crédito ante situaciones que puedan comprometer su estabilidad económica y académica.

A continuación, se describe el alcance de los servicios requeridos y sus componentes mínimos necesarios para su correcta implementación y operación de las coberturas de enfermedades catastróficas.

La verificación precisa y oportuna de los eventos cubiertos es fundamental para garantizar que los beneficiarios reciban el apoyo necesario en situaciones críticas. Esto incluye el desarrollo de procedimientos claros y eficientes para la gestión de casos, así como la coordinación con entidades relevantes para validar la documentación y el cumplimiento de las condiciones de las coberturas.

1. **Verificación del cumplimiento de las condiciones para los eventos cubiertos:**
    - Desarrollo de protocolos específicos para la verificación de cada tipo de evento (enfermedades catastróficas y desempleo).
    - Establecimiento de criterios claros y objetivos para la evaluación de los casos.
    - Implementación de procedimientos para la validación de documentos en colaboración con entidades externas

2. **Mecanismos para el registro y seguimiento:**
    - Interoperabilidad con diferentes sistemas y entidades para facilitar la verificación del evento y el seguimiento de casos.
    - Desarrollo e implementación de un sistema digital para el registro, sistematización y seguimiento de los casos u ocurrencia de los eventos.

3. **Elaboración de informes sobre la gestión de eventos y recomendaciones de mejora:**
    - Generación de informes periódicos sobre la gestión de los eventos cubiertos.
    - Análisis de datos para identificar áreas de mejora y recomendaciones para optimizar los procesos.

4. **Identificación de acciones para la mitigación de la materialización de eventos:**
    - Análisis de los casos para identificar patrones y factores de riesgo.

- Desarrollo de acciones afirmativas y programas preventivos para reducir la incidencia de eventos cubiertos.

3.1.1 Producto de ahorro

En un mundo donde la educación es clave para el progreso y la movilidad social, el ahorro se convierte en una herramienta esencial para acceder a oportunidades educativas de calidad. Ahorrar permite a las familias planificar el futuro académico de sus hijos, fortalecer la estabilidad financiera y promover una cultura de responsabilidad económica. En este contexto, el acceso la entidad designada está desarrollando un producto para facilitar a la educación superior a través del ahorro, llevando la educación técnica, tecnológica, profesional y posgradual a todos los rincones del país.

Este producto busca promover la inclusión financiera, consolidar la cultura del ahorro en torno a la educación superior, maximizar la rentabilidad de los ahorros y generar confianza y transparencia en la operación de la entidad designada por la corporación. Es inclusivo para todos los colombianos, ofreciendo beneficios como coberturas de riesgos e incentivos tributarios. Fomenta la cultura del ahorro para la educación en Colombia y en el exterior, facilitando el acceso al crédito educativo con condiciones preferenciales y garantizando el acceso, permanencia y graduación en el sistema de educación superior.

En el marco de la política actual del Estado colombiano, que considera la educación como un pilar fundamental para el desarrollo, este mecanismo de ahorro busca ser una herramienta adicional de financiación para la educación superior, incentivando la cultura del ahorro y promoviendo la inclusión financiera. Además, pretende canalizar recursos de empresas, fundaciones y el sistema educativo en general para promover el acceso, permanencia y graduación en educación superior.

Esta cuenta tiene como finalidad fomentar el acceso a la educación superior, permitiendo a los ahorradores financiar su matrícula o el sostenimiento de su educación superior o la de un beneficiario, mejorando su perfil de riesgo crediticio y facilitando el acceso a crédito para los semestres restantes.

El mecanismo de ahorro permitirá a los titulares realizar depósitos periódicos, con el objetivo de alcanzar una meta de ahorro en un plazo determinado. Estos depósitos generarán intereses, facilitando que los particulares puedan financiar la etapa inicial de los programas de educación superior, una fase que suele ser más costosa y con mayor riesgo de abandono.

El ahorro digital de la entidad transforma cada transacción en una inversión para la educación superior. Con programas de bienestar, asistencias y coberturas, la entidad ofrece un acompañamiento integral que incrementa la rentabilidad del ahorro y protege el capital acumulado, promoviendo la inclusión financiera y la educación superior en Colombia.

Con esta iniciativa, busca promover la cultura del ahorro, garantizar el acceso a la educación superior y contribuir al desarrollo económico y social de Colombia. Este producto de ahorro permitirá a las familias planificar el futuro académico de sus hijos, consolidará la inclusión

financiera y fortalecerá la estabilidad económica de los estudiantes. Además, la entidad pretende ofrecer soluciones tecnológicas avanzadas que optimicen la gestión de los recursos y faciliten el acceso a los beneficios educativos, asegurando un acompañamiento integral durante todo el proceso. Con este proyecto, la entidad reafirma su compromiso con la educación y el bienestar de los estudiantes colombianos, promoviendo un futuro más próspero y equitativo para todos.

El ahorro para la educación superior abre puertas a oportunidades y mejora la calidad de vida. La educación superior es el principal motor de la movilidad social y la mejor inversión para las familias colombianas, no solo en términos de ingresos potenciales, sino también en el desarrollo personal y profesional.

La entidad designada entiende que el acceso, permanencia y graduación en la educación superior son fundamentales para el desarrollo de una sociedad más equitativa y próspera. Por ello, está diseñando un sistema de ahorro inclusivo y eficiente que aprovecha las tecnologías digitales para ofrecer rentabilidad y beneficios adicionales a los usuarios. Este mecanismo de ahorro no solo facilita el acceso a la educación superior, sino que también promueve la inclusión y la educación financiera desde una edad temprana.

Además, el acto de ahorrar fomenta la disciplina financiera y la planificación a largo plazo, habilidades valiosas en todas las áreas de la vida. El enfoque de la entidad incluye la implementación de programas de fidelización que recompensan la constancia en el ahorro y el logro de hitos específicos, así como coberturas y asistencias que protegen el capital acumulado y aseguran que los beneficiarios puedan cumplir sus objetivos educativos, incluso en caso de eventos inesperados.

Con este sistema de ahorro, la entidad busca reducir la carga financiera para los estudiantes y sus familias, combinando ahorros y créditos educativos para minimizar la necesidad de recursos a través de crédito educativo. De esta manera, contribuye a que más colombianos puedan acceder a una educación superior de calidad, mejorando sus perspectivas de futuro y fortaleciendo el desarrollo del país.

3.1.1.1 Objetivo del nuevo mecanismo de ahorro

Fomentar el acceso y permanencia en la educación superior mediante un sistema de ahorro inclusivo y eficiente que aproveche las tecnologías digitales para ofrecer rentabilidad y beneficios adicionales a los usuarios.

3.1.1.2 Objetivos específicos

1. **Facilitar el acceso a educación superior**: Reducir la carga financiera y necesidad de endeudamiento para el estudiante mediante la cofinanciación, combinando ahorros y créditos educativos.
2. **Incrementar la rentabilidad del ahorro**: Proporcionar tasas de interés diferenciadas y competitivas que aumenten la rentabilidad del fondo educativo.
3. **Promover la inclusión y educación financiera**: Integrar programas que enseñen la importancia del ahorro, la gestión financiera efectiva y fomenten la inclusión financiera desde una edad temprana.

4. **Proteger y apoyar con programas de bienestar**: Incluir coberturas, asistencias y programas de bienestar que fomenten la continuidad del ahorro y protejan el capital acumulado.

3.1.1.3 Características del producto de ahorro

El producto de ahorro está diseñado para ofrecer una solución integral que facilite el acceso y permanencia en la educación superior. A través de una plataforma digital inclusiva y eficiente, este producto combina diversas características que promueven la rentabilidad, la protección y el acompañamiento integral de los usuarios. A continuación, se detallan las características esenciales de este innovador producto de ahorro:

1. **Flexibilidad en el ahorro programado**: Los usuarios pueden establecer un rango de ahorro mensual flexible que se ajuste a sus circunstancias financieras, facilitando la participación de familias de diferentes ingresos. Sin costos para el ahorrador y sin letra pequeña.

2. **Apertura de cuenta a nombre del estudiante**: Las cuentas pueden abrirse a nombre de los estudiantes desde temprana edad, fomentando la cultura del ahorro y la inclusión financiera desde una etapa anticipada.

3. **Tasas de interés diferenciales**: Se ofrecen tasas de interés diferenciales y competitivas que incrementan la rentabilidad del ahorro, recompensando la constancia y el compromiso de los usuarios.

4. **Conexión inteligente**: La plataforma digital ofrece una conexión inteligente que permite a los usuarios acceder y gestionar su ahorro educativo de manera intuitiva y eficiente. Esta característica garantiza que los usuarios puedan participar activamente en la construcción de su futuro educativo desde cualquier lugar y en cualquier momento, utilizando dispositivos conectados a internet. La conexión inteligente facilita la interacción con la plataforma a través de una interfaz amigable y fácil de usar, diseñada para adaptarse a las necesidades de los usuarios. Además, proporciona acceso a herramientas y recursos educativos, permitiendo una experiencia de ahorro integrada y personalizada. Con esta característica, la entidad no solo promueve la accesibilidad total, sino que también garantiza que los usuarios puedan aprovechar al máximo las ventajas del ahorro digital, manteniéndose conectados y comprometidos con sus objetivos educativos.

5. **Protección integral**: Este componente del producto de ahorro ofrece coberturas y asistencias diseñadas para proteger el capital acumulado y brindar apoyo en caso de eventos inesperados. Además, se ofrecen asistencias que proporcionan soporte financiero y emocional a los beneficiarios, para que puedan cumplir sus objetivos de ahorro y educación sin interrupciones. Este enfoque integral no solo protege el capital, sino que también ofrece tranquilidad y seguridad a las familias, permitiéndoles enfocarse en el futuro educativo de sus hijos con confianza. En caso de eventos inesperados, como el fallecimiento del titular de la cuenta, garantiza que el beneficiario

reciba el apoyo necesario para cumplir su objetivo educativo, incluyendo la aportación del saldo restante por parte de la entidad designada.

6. **Condiciones preferenciales para créditos educativos**: Los usuarios del producto de ahorro pueden acceder a condiciones preferenciales para créditos educativos, basadas en su historial de ahorro. Esto incluye tasas de interés especiales y la posibilidad de no requerir un deudor solidario, facilitando aún más el acceso a la educación superior. Estas condiciones preferenciales no solo reducen la carga financiera, sino que también incentivan el ahorro constante y responsable.

7. **Enfoque educativo personalizado**: El producto está diseñado para atender las necesidades educativas específicas de cada usuario. Proporciona herramientas para la programación de ahorro de acuerdo con la capacidad económica de cada familia y ofrece orientación personalizada para la consecución de logros académicos. Este enfoque busca que cada estudiante reciba el apoyo necesario para alcanzar sus metas educativas y profesionales.

Por lo anterior se presenta el detalle funcional del negocio

3.1.1.4 Macroproceso de cuenta de ahorro

El macroproceso de cuenta de ahorros está organizado en diferentes etapas y áreas funcionales, que abarcan desde la configuración inicial del producto hasta la gestión operativa y el monitoreo continuo. A continuación, se describe de manera general:

i. **Configurar producto:** Definir las características del producto de ahorro digital, incluyendo tasas de interés, cuentas contables y parámetros de operación, para garantizar su correcto funcionamiento dentro del banco.
ii. **Realizar onboarding:** Proceso mediante el cual un cliente se registra en el banco digital y se le asigna una cuenta de ahorros, asegurando el cumplimiento de normativas de seguridad y validación de identidad.
iii. **Gestión operativa:** Comprende las actividades operativas necesarias para mantener el funcionamiento eficiente del producto.
iv. **Control de políticas de cumplimiento:** Supervisión y aplicación de las políticas internas de la entidad en materia de cumplimiento normativo y prevención de riesgos.
v. **Monitoreo transaccional:** Vigilancia en tiempo real de las transacciones para detectar y prevenir actividades fraudulentas o sospechosas.
vi. **Atención de PQRS (Peticiones, Quejas, Reclamos y Sugerencias)**
vii. Canal de atención para resolver inquietudes y problemas de los clientes en relación con sus cuentas y servicios.
viii. **Gestión contable:** Registro y control de los movimientos financieros de las cuentas de ahorros para garantizar la exactitud contable del mecanismo de ahorro.

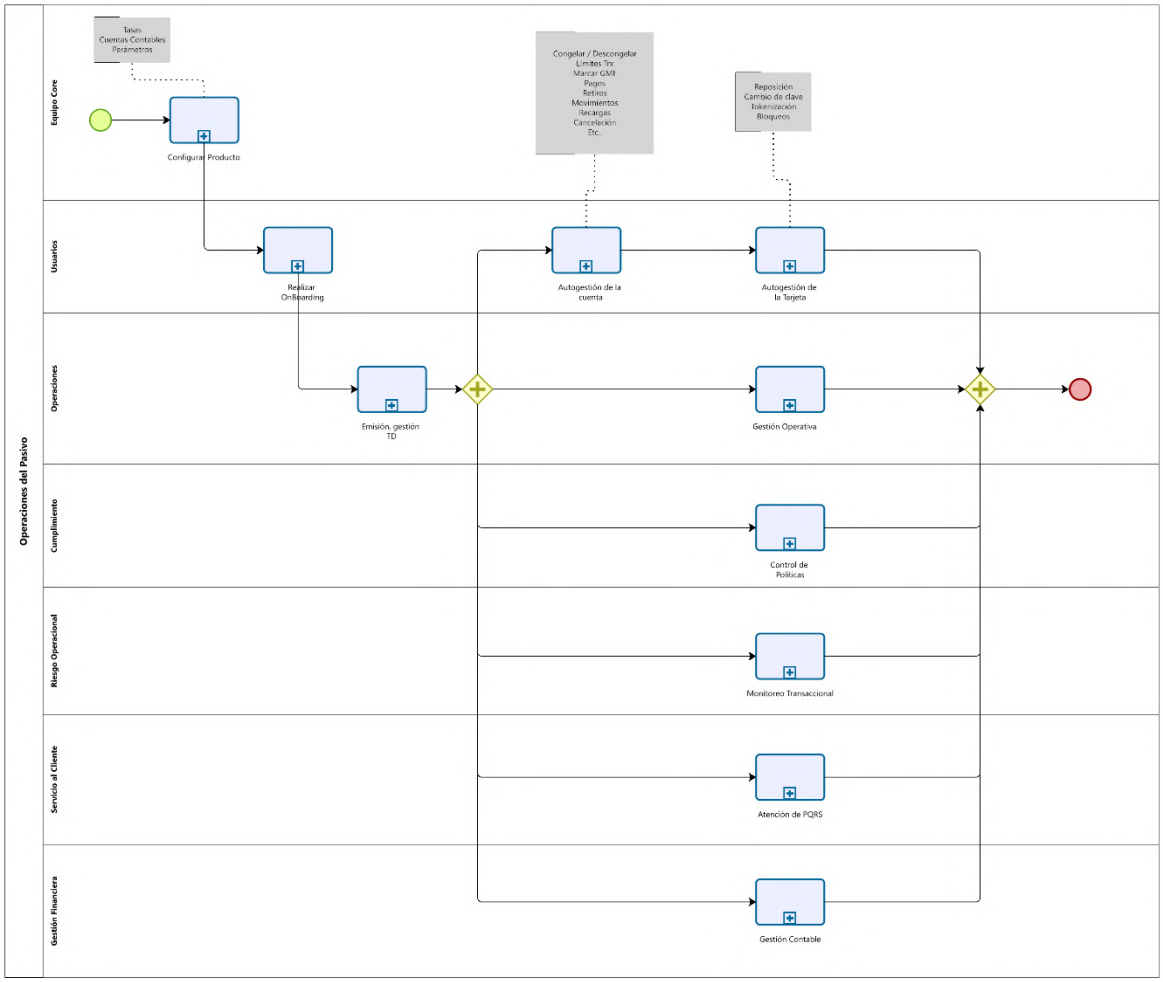


Ilustración 4 Macro proceso cuenta de ahorros

#	Actividad	Entradas	Salidas	Roles
1	Configurar Producto	Políticas de la entidad, normatividad vigente, tasas de interés, parámetros de cuenta, cuentas contables asociadas.	Producto configurado y habilitado para su uso.	Analistas de producto, equipo de riesgos, equipo contable, tecnología.
2	Realizar onboarding	Datos del cliente, documentos de identidad, validaciones KYC (Conozca a su Cliente).	Cuenta creada y activada.	Clientes, equipo de verificación, sistemas antifraude.
3	Emisión y Gestión de Tarjeta Débito (TD)	Solicitud del cliente, datos de la cuenta, validaciones de identidad.	Tarjeta débito emitida, activada y disponible para su uso.	Cliente, área de operaciones, servicio al cliente, tecnología.
3.1	Autogestión de la cuenta	Solicitudes del cliente a través de la app o web.	Cuenta modificada según la acción requerida (congelación,	Cliente, tecnología, soporte.

			configuración de límites, pagos, cancelaciones, etc.).	
3.2	Autogestión de la Tarjeta	Solicitudes del cliente para gestión de la tarjeta.	Tarjeta bloqueada/desbloqueada, clave cambiada, reposición generada.	Cliente, tecnología, soporte.
11	Control de políticas de Cumplimiento	Normativas, parámetros internos del banco.	Reportes de cumplimiento y ajustes necesarios.	Cumplimiento, auditoría, riesgos.
12	Monitoreo transaccional	Movimientos de cuentas, alertas de fraude.	Bloqueo de transacciones sospechosas, reportes de análisis.	Cumplimiento, antifraude, tecnología.
13	Atención de PQRS (Peticiones, Quejas, Reclamos y Sugerencias)	Solicitudes de clientes.	Respuesta y solución a la solicitud.	Servicio al cliente, área legal, operaciones.
14	Gestión contable	Movimientos financieros, registros contables.	Estados financieros precisos y conciliados.	Contabilidad, auditoría, tecnología.

Tabla 1 Actividades del proceso

Este flujo refleja la gestión integral de una cuenta de ahorros desde su configuración hasta la supervisión y atención al cliente, asegurando cumplimiento normativo y operatividad eficiente.

3.1.1.5 Configurar producto

El proceso de *Configurar producto* involucra varias áreas clave dentro de la entidad. A continuación, una descripción general de las etapas principales:

1. **Definir características del producto (Negocio)**
   - Se establecen las características esenciales del producto, como tasas de interés, rendimientos, retención en la fuente y el GMF (Gravamen a los Movimientos Financieros).
   - Se definen los canales de transacción y otros parámetros financieros relevantes.

2. **Definir cuentas contables (Contabilidad)**
   - Se establecen las características esenciales del producto, como tasas de interés, rendimientos, retención en la fuente y el GMF (Gravamen a los Movimientos Financieros).
   - Se definen los canales de transacción y otros parámetros financieros relevantes.

3. **Parametrizar productos (Equipo Core)**
   - Se configuran los parámetros técnicos del producto en los sistemas internos.
   - Se incluyen reglas de operación, validaciones y configuraciones necesarias para su correcto funcionamiento.

4. **Activar productos**
   - Una vez completada la parametrización, el producto se activa y queda disponible para su uso en la entidad.

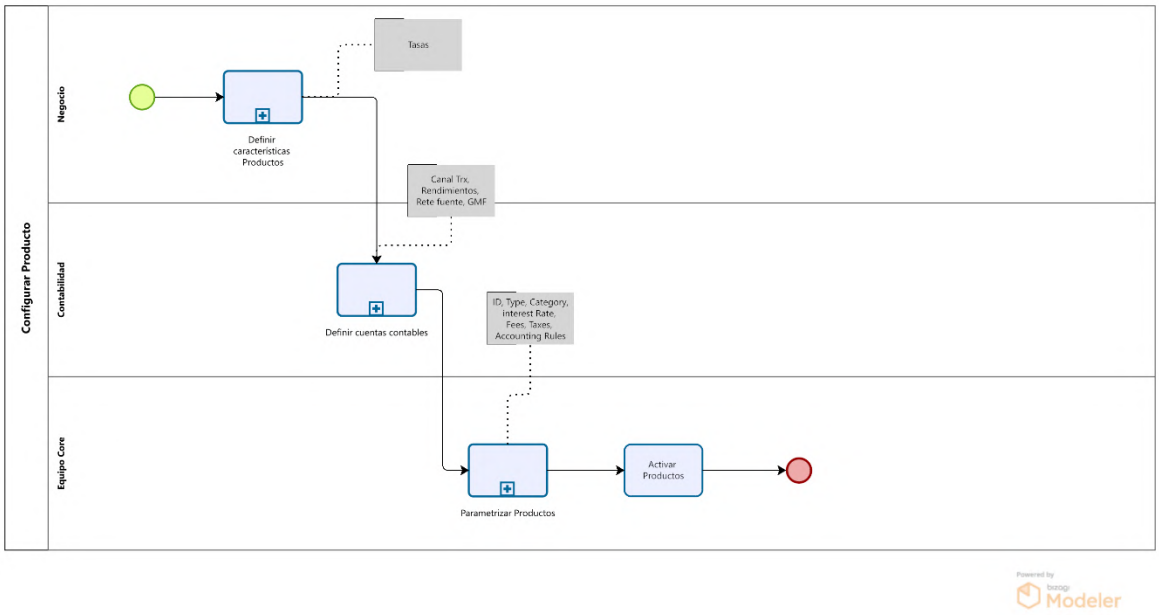


Ilustración 5 Flujo configuración de producto

Este proceso asegura que el nuevo producto de cuenta de ahorros esté correctamente configurado desde el punto de vista de negocio, contabilidad y tecnología antes de su lanzamiento al mercado.

3.1.1.6 Realizar OnBoarding Persona Natural

El proceso de *Onboarding* para la apertura de una cuenta de ahorros incluye aspectos para la validación y registro del usuario.

1. **Registro y validación inicial**
   - Se inicia con el registro del usuario, recopilando información como correo electrónico y número de celular.
   - Se realiza la validación de identidad mediante métodos como captura de tarjeta y prueba de vida (liveness).

2. **Captura de información financiera, comercial y domiciliaria**
   - Se captura información financiera para determinar la fuente de ingresos (ej. Empleado o independiente).
   - Se captura información comercial, verificando si la actividad económica del usuario está permitida.
   - Se valida el domicilio del usuario, registrando país, ciudad y dirección.

3. **Evaluaciones de cumplimiento**
   - Si el usuario es una Persona Expuesta Políticamente (PEP), se recopila información adicional.
   - Si tributa en otro país, se capturan datos para cumplir con regulaciones internacionales

como FATCA/CRS.
- Se validan listas de control y centrales de riesgo para determinar si el usuario está reportado.

4. **Validaciones finales y apertura de la cuenta**
   - Se verifica si hay información incompleta y si los requisitos son subsanables.
   - Si el usuario cumple con todos los requisitos, se procede con la apertura del producto.
   - Si no cumple y los requisitos no son corregibles, el proceso finaliza sin éxito.

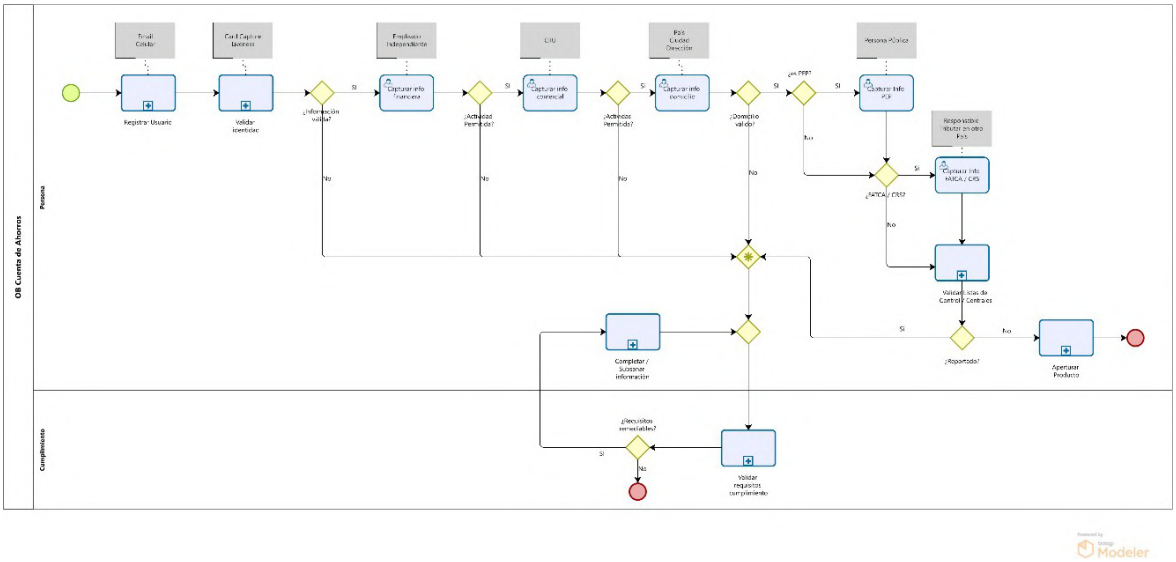


Ilustración 6 Flujo configuración de ahorro

Este proceso garantiza que la apertura de cuentas de ahorro se realice cumpliendo con normativas de seguridad, validación de identidad y regulación financiera.

3.1.1.7 Realizar OnBoarding Persona Jurídica

El proceso de Onboarding de Cuenta de Ahorros para Persona Jurídica (PJ) permite a una empresa abrir una cuenta de ahorros cumpliendo con los requisitos legales y de cumplimiento.

1. Ingreso de información de la empresa
- Se registran los datos de la empresa: NIT, nombre, tipo y representante legal.

2. Registro y validación del Representante Legal
- Se crean las credenciales del representante legal con su email y celular.
- Se verifica su identidad mediante herramientas como **captura de documentos y biometría.**
- Se confirma la existencia legal de la empresa y del representante.

3. Carga y validación de documentos
- Se cargan documentos clave como estados financieros y RUT.

Calle 60a #5-54, Oficina 403
Bogotá D.C. Colombia
NIT. 830.101.214-4
+57 3222468120
www.colombiadigital.net

- Se valida si la actividad comercial es permitida según normativas.
- Se registran datos comerciales y la dirección de la empresa.

4. Validación de cumplimiento y riesgo

- Se determina si el representante legal es una **Persona Expuesta Políticamente (PEP).**
- Se validan listas de control y centrales de riesgo.
- Si hay hallazgos negativos, se revisa si la empresa está reportada.

5. Corrección de Información (si aplica)

- En caso de errores o requisitos incumplidos, se solicita subsanar la información.
- Si los requisitos no son remediables, el proceso se cancela.

6. Apertura de la cuenta

- Si todo es validado correctamente, se procede con la apertura del producto.
- Se registran los **autorizados / beneficiarios para el manejo de la cuenta**.

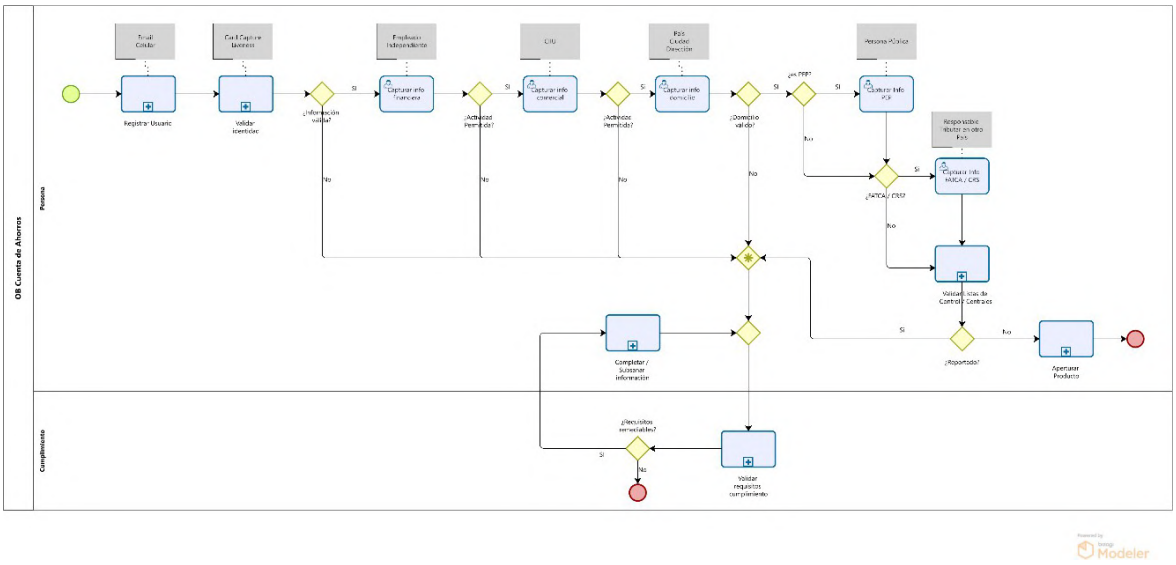


Ilustración 7 Apertura de cuenta

Este flujo asegura el cumplimiento normativo y la correcta identificación de la empresa antes de habilitar su cuenta de ahorros.

3.1.1.8 Autogestión cuenta

El proceso de Autogestión de cuenta permite a los usuarios administrar su cuenta de ahorros de manera autónoma a través de diversas funcionalidades.

1. **Selección de producto y consulta de saldo**
   - El usuario inicia seleccionando el tipo de cuenta que desea gestionar (ej. cuenta con

Calle 60a #5-54, Oficina 403
Bogotá D.C. Colombia
NIT. 830.101.214-4
+57 3222468120
www.colombiadigital.net

intereses, cuenta programada).
- Posteriormente, puede consultar el saldo disponible en su cuenta.

2. **Gestión de movimientos y transacciones**
   - Puede ver los movimientos de su cuenta para revisar sus transacciones.
   - Tiene la opción de realizar transferencias a otras cuentas.
   - Puede retirar dinero sin tarjeta a través de mecanismos como PSE, SPI, corresponsales bancarios o plataformas de pago.
   - También puede recargar su cuenta, lo cual puede hacerse por diferentes medios.

3. **Configuración y personalización de la cuenta**
   - El usuario puede configurar la cuenta, estableciendo metas de ahorro, definiendo el beneficiario o incluso cancelaciones.

4. **Generación de certificados y extractos**
   - Finalmente, si el usuario lo necesita, puede generar certificados o extractos de su cuenta para consulta o trámites administrativos.

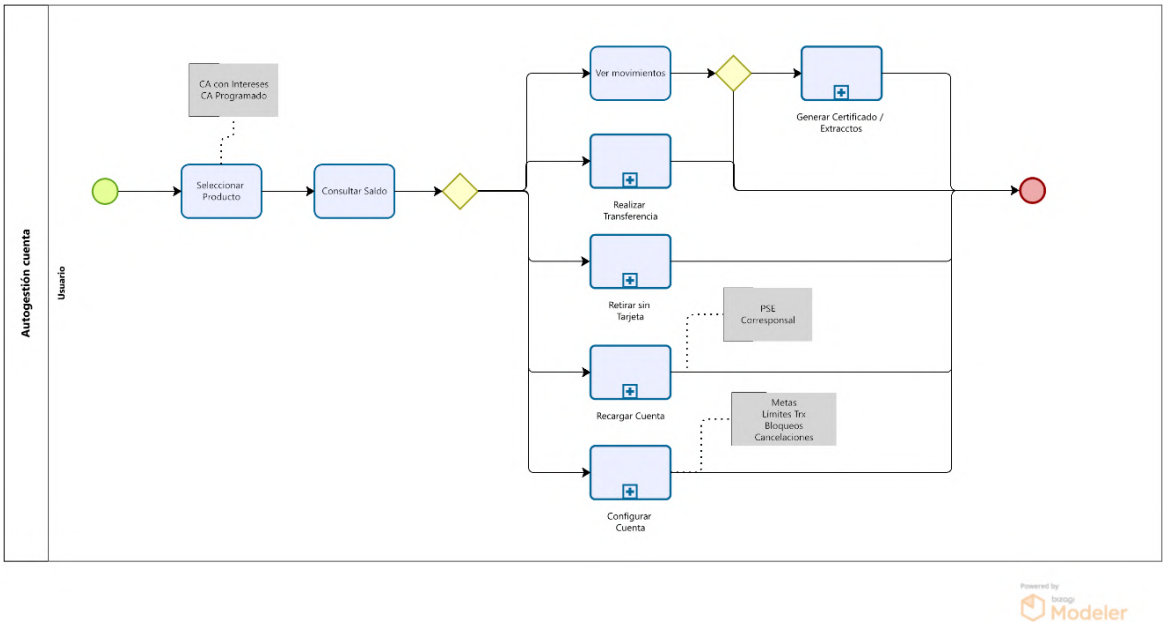


Ilustración 8 Auto gestión de cuenta

Este proceso facilita la administración de la cuenta sin necesidad de asistencia directa del banco, proporcionando autonomía al usuario para gestionar sus finanzas.

3.1.1.9 Reportes normativos

Una de las obligaciones fundamentales para la operación de la plataforma es la generación de reportes normativos. Estos reportes deben ser entregados a los entes de control pertinentes,

asegurando el cumplimiento de las normativas locales e internacionales. La generación de estos reportes es esencial para la transparencia y la vigilancia de las operaciones financieras, garantizando que la plataforma opere de manera íntegra y conforme a las regulaciones establecidas.

3.1.1.10 Solución tecnológica

La solución tecnológica para la gestión de cuentas de ahorro está diseñada para proporcionar una plataforma robusta y eficiente que facilita la administración financiera personal. Esta solución abarca desde la configuración y personalización de la cuenta hasta la generación de certificados y extractos, garantizando autonomía y control para los usuarios. Además, incluye la generación de reportes normativos, esenciales para asegurar el cumplimiento de las regulaciones locales e internacionales y la transparencia en las operaciones financieras. Con módulos como el manejo de perfiles de clientes y auditorías automáticas, la tecnología detrás del Core de depósito asegura alta disponibilidad y escalabilidad, permitiendo gestionar grandes volúmenes de transacciones de manera segura y conforme a la ley.

3.1.1.11 Core de Depósito

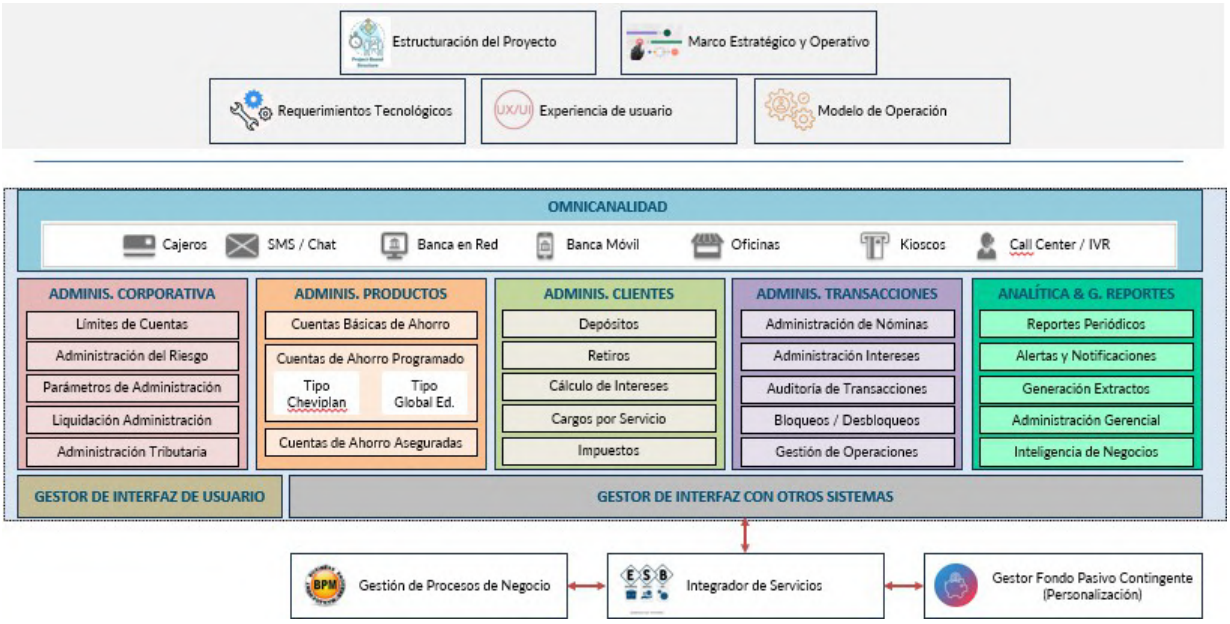
El componente de **Core de Depósitos** debe proveer una solución tecnológica de tipo core bancario de pasivo de cuarta generación, moderna, flexible y segura, que permita gestionar de forma integral productos de ahorro y cuentas transaccionales. Esta solución será la encargada de soportar la operación financiera central de las Cuentas de Ahorro Digital, incluyendo la apertura, administración, operación, liquidación y cierre de las mismas, así como su integración con otros sistemas del ecosistema financiero de la entidad.

Dentro del Core bancario, el módulo o sistema de gestión de pasivos se enfoca específicamente en las operaciones relacionadas con los fondos que los clientes depositan en el banco.

Lo anterior incluye la gestión de cuentas corrientes, cuentas de ahorro, depósitos a plazo fijo, y otros productos de pasivo.

El Core de gestión bancaria de pasivos se encarga de registrar las transacciones de depósito y retiro, calcular los intereses devengados en las cuentas, generar estados de cuenta, y asegurar que las operaciones se realicen de forma segura y eficiente.

Un sistema Core de gestión bancario de pasivos eficiente es crucial para que los bancos puedan ofrecer servicios financieros confiables y accesibles a sus clientes, así como para garantizar la gestión adecuada de sus obligaciones financieras.



3.1.1.11.1.1 Requerimientos Funcionales Principales

La solución propuesta deberá contemplar como mínimo los siguientes aspectos funcionales:

1. **Diseño y Configuración de Productos Financieros**
   - **a.** Creación y gestión de productos de ahorro, cuentas transaccionales, interés de las cuentas, con reglas parametrizables de tarifas, límites, condiciones y periodicidades.
   - **b.** Soporte a modelos de cuentas individuales, conjuntas, cotitulares, beneficiarios y grupos.

2. **Simulador de ahorro**
   - **a.** Monto inicial de ahorro
   - **b.** Valor proyectado
   - **c.** Aportes periódicos:
     - i. Frecuencia: diario, semanal, mensual, anual
     - ii. Monto por periodo
   - **d.** Tasa de interés:
     - i. Nominal o efectiva
     - ii. Fija o variable
   - **e.** Plazo del ahorro:
     - i. En meses o años
   - **f.** Tipo de interés:

i. Simple o compuesto

g. Resultado de la simulación

3. **Originación y Apertura de Cuentas**
   - **a.** Flujo digital completo de apertura de cuenta, con soporte para validación de identidad, aceptación de términos y condiciones, y captura de datos/documentos requeridos.

4. **Gestión del Ciclo de Vida del Producto**
   - **a.** Administración de movimientos financieros (abonos, retiros, pagos, débitos automáticos, etc.).
   - **b.** Liquidación de intereses, generación de extractos, estado de cuenta y cierre de productos.
   - **c.** Cierre manual o automático con reglas configurables.

5. **Contabilidad Automatizada**
   - **a.** Generación automática de asientos contables en tiempo real para cada evento financiero.
   - **b.** Soporte multimoneda, multipaís y adaptabilidad a planes docus locales o internacionales.
   - **c.** Conciliación contable integrada o exportación a ERP externo.

6. **Seguridad y Trazabilidad**
   - **a.** Registro completo y auditable de todas las operaciones realizadas sobre cuentas y productos.
   - **b.** Gestión de usuarios y perfiles con control granular de accesos y funciones.
   - **c.** Notificaciones por eventos (SMS, email, push, Webhooks).
   - **d.** Autenticación multifactor (MFA) y sistemas de autenticación biometricos para acceso seguro.
   - **e.** Cifrado de datos en tránsito y en reposo (AES-256).
   - **f.** Monitoreo de actividad y detección de anomalías.
   - **g.** Configuración de roles y permisos para evitar accesos no autorizados, aplicando el principio de mínimo privilegio.
   - **h.** Reportes Sistema de Administración y Almacenamiento de Reportes.
   - **i.** Reportes Normativos.

7. **Cumplimiento Regulatorio y Normativo**
   - **a.** Soporte a estándares de cumplimiento financiero y operativo (ej. SARLAFT, FATCA, CRS).
   - **b.** Generación de reportes regulatorios e integración con motores de validación externos.

8. **Interoperabilidad**
   - **a.** Exposición de funcionalidades a través de APIs estándar (REST, SOAP, Webhooks, etc.).

Calle 60a #5-54, Oficina 403
Bogotá D.C. Colombia
NIT. 830.101.214-4
+57 3222468120
www.colombiadigital.net

b. Capacidad para integrarse con canales digitales (Web, App, IVR, chatbot), motores de pagos, plataformas de monitoreo y sistemas externos.

9. **Configurabilidad y Escalabilidad**
   a. La solución debe permitir su evolución mediante parametrización, sin necesidad de desarrollos a medida.
   b. Capacidad de gestionar nuevos productos, atributos y reglas sin impacto operativo.

Facilita la generación y administración de informes detallados sobre las operaciones y el comportamiento del sistema. Incluye:

1. Configuración de reportes personalizados por tipo de operación, cliente o período.
2. Exportación de reportes en múltiples formatos (PDF, Excel, CSV).

3.1.1.12 Pasarela de pago

La Pasarela de Pagos será el componente encargado de facilitar los mecanismos de ingreso (Cash In) y retiro de fondos (Cash Out) para los usuarios de la Cuenta de Ahorro Digital, asegurando que las transacciones sean seguras, trazables y cumplan con las normativas del sistema financiero colombiano. Este componente se integrará tanto con la aplicación móvil como con el portal web, actuando como intermediario entre los canales digitales y el Core de Depósitos.

Funcionalidades de Cash In (Ingreso de Fondos)

- PSE (Pagos Seguros en Línea): Se implementará una integración directa con los sistemas de transferencia electrónica de fondos de Colombia a través de un proveedor certificado, utilizando una pasarela homologada.
- SPI como medio de Cash In (P2A - Person to Account): Habilitación de transferencias inmediatas desde cuentas bancarias hacia la Cuenta Digital utilizando SPI.
- Dos opciones de integración: mediante instrucciones desde interfaces bancarias (e.g., “transfiere a tu cuenta SPI con este número”) o, eventualmente, a través de request-to-pay o integración con wallets interoperables.
- La pasarela registra los abonos recibidos y genera la transacción correspondiente en el Core con el identificador del usuario.

Alternativas Digitales Complementarias (opcional en fases futuras): Se podrán incorporar integraciones con botones Bancolombia, Daviplata, Nequi o QR interoperable para mejorar la adopción entre públicos jóvenes no bancarizados o usuarios de wallets.

Funcionalidades de Cash Out (Retiros de Fondos)

- SPI (Sistema de Pagos Inmediatos): Este será el canal principal para permitir retiros desde la Cuenta Digital hacia cuentas bancarias de los usuarios, utilizando una integración directa o indirecta mediante un middleware financiero según el modelo diseñado.
- Alternativas para retiro no inmediato:

- ACH tradicional: En caso de que el banco de destino del usuario no esté disponible en SPI, se podrá utilizar ACH diferido (T+1 o T+2).
- Integración con Wallets: Como evolución, será posible habilitar retiros hacia plataformas como Nequi, Movii y otras, siempre que ofrezcan APIs compatibles y seguras.

Funciones Transversales

- Trazabilidad y Confirmación: Cada operación generará un número de referencia único, visible tanto para el usuario como para el backend operativo, acompañado por un estado de la operación (pendiente, exitosa, fallida, reversada) que será visible en el historial.
- Conciliación Financiera: Registro detallado de cada movimiento en un sistema de conciliación que valida la información con el Core y la pasarela. Además, se ofrecerán reportes descargables y un panel de control para el equipo financiero.
- Reversas y Contingencias: Capacidad para revertir pagos fallidos o inconsistentes basándose en reglas definidas con la entidad designada por la corporación. Cada reversa será registrada por canal y causa (fallo técnico, rechazo bancario, duplicación).
- Alertas y Notificaciones: Los usuarios recibirán mensajes automáticos en la aplicación móvil, y opcionalmente por correo electrónico, tras cada operación de ingreso o retiro. También recibirán alertas en caso de fallos, límites superados o necesidad de intervención manual.
- Controles y Límites: Validaciones integradas según el tipo de usuario, montos, frecuencia diaria y estado de la cuenta, con funcionalidades diseñadas para prevenir fraudes y validación contra listas negras si se habilita conexión con un motor de cumplimiento.

3.1.2 Modelo de operación propuesto para la verificación de eventos de las coberturas de desempleo y enfermedades catastróficas

El modelo de operación contempla un enfoque integral para la gestión de las coberturas, bajo los principios de oportunidad, trazabilidad, eficiencia y control. Este modelo debe incluir, como mínimo, los siguientes componentes:

1. Recepción y registro de solicitudes

- Diseño y habilitación de herramientas y/o canales digitales seguros para la recepción de solicitudes.
- Validación automática de requisitos básicos para prevenir errores u omisiones.

2. Verificación de condiciones y documentos

- **Desempleo:** Integración con fuentes interoperables como ADRES u otras que pueda identificar el proveedor.
- **Enfermedad catastrófica:** Interoperabilidad con Cuenta de alto costo, Minsalud, RIPS u otras que pueda identificar el proveedor.
- De manera transversal, realizar la validación de documentos y fuentes internas de la entidad para garantizar el cumplimiento de condiciones para la aplicación de la cobertura.

3. Evaluación de la solicitud de cobertura

- Evaluación automatizada con reglas de negocio parametrizadas y demás recursos que considere el proveedor.

- Aprobación de la aplicación de la cobertura en la herramienta definida por el proveedor, con log de auditoría e integración con sistemas de la entidad.

4. Aplicación de la cobertura

- Aplicación de la cobertura conforme a los anexos del Acuerdo 023 de 2024 en las herramientas de la entidad.

5. Seguimiento y validación

- Verificación periódica de cumplimiento de condiciones de la cobertura durante el tiempo que este activa.
- Identificación, revisión y reportes de comportamientos inusuales.

6. Control y mejora continua

- Generación de informes periódicos y análisis de tendencias.
- Identificación de posibles fraudes, riesgos o errores del proceso.
- Implementar tableros de seguimiento y control de cada cobertura a las que tenga acceso la entidad designada por la corporación.

Diagramas de flujo de trabajo coberturas de desempleo y enfermedades catastróficas

Cobertura por desempleo

Escenario 1: El proveedor solamente realiza validaciones y la aplicación de las coberturas en cartera son realizadas por el Grupo de Operaciones de la entidad designada por la Corporación:

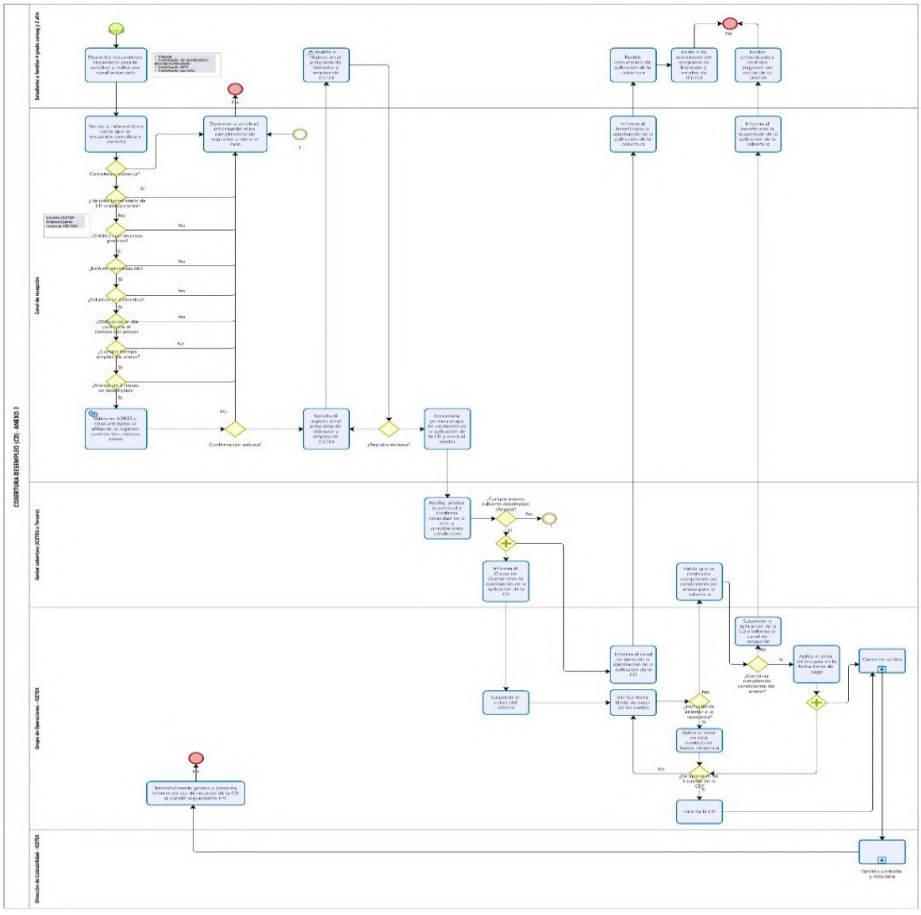
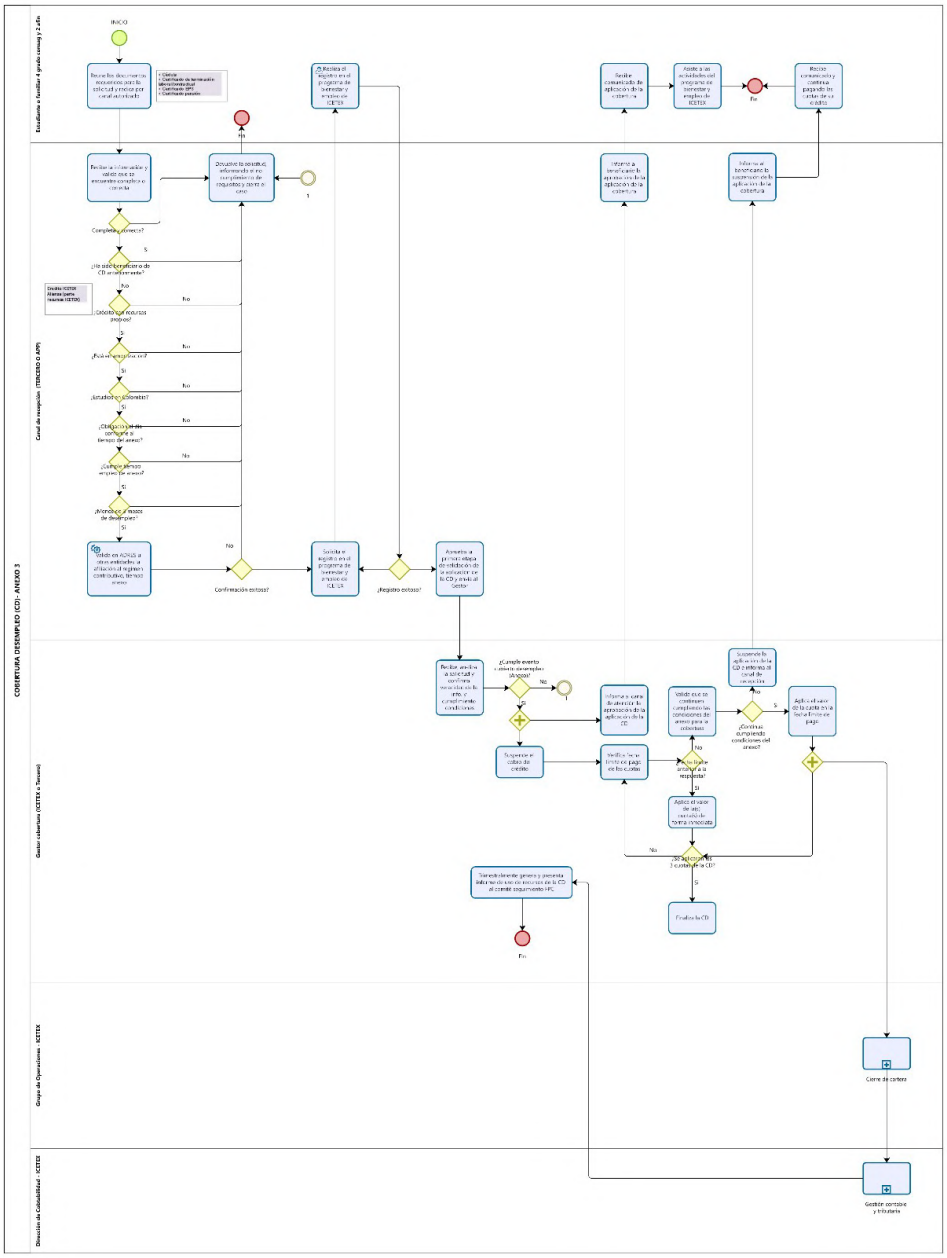


Ilustración 9 Flujo de coberturas

Escenario 2: El proveedor realiza validaciones y la aplicación de las coberturas en cartera:

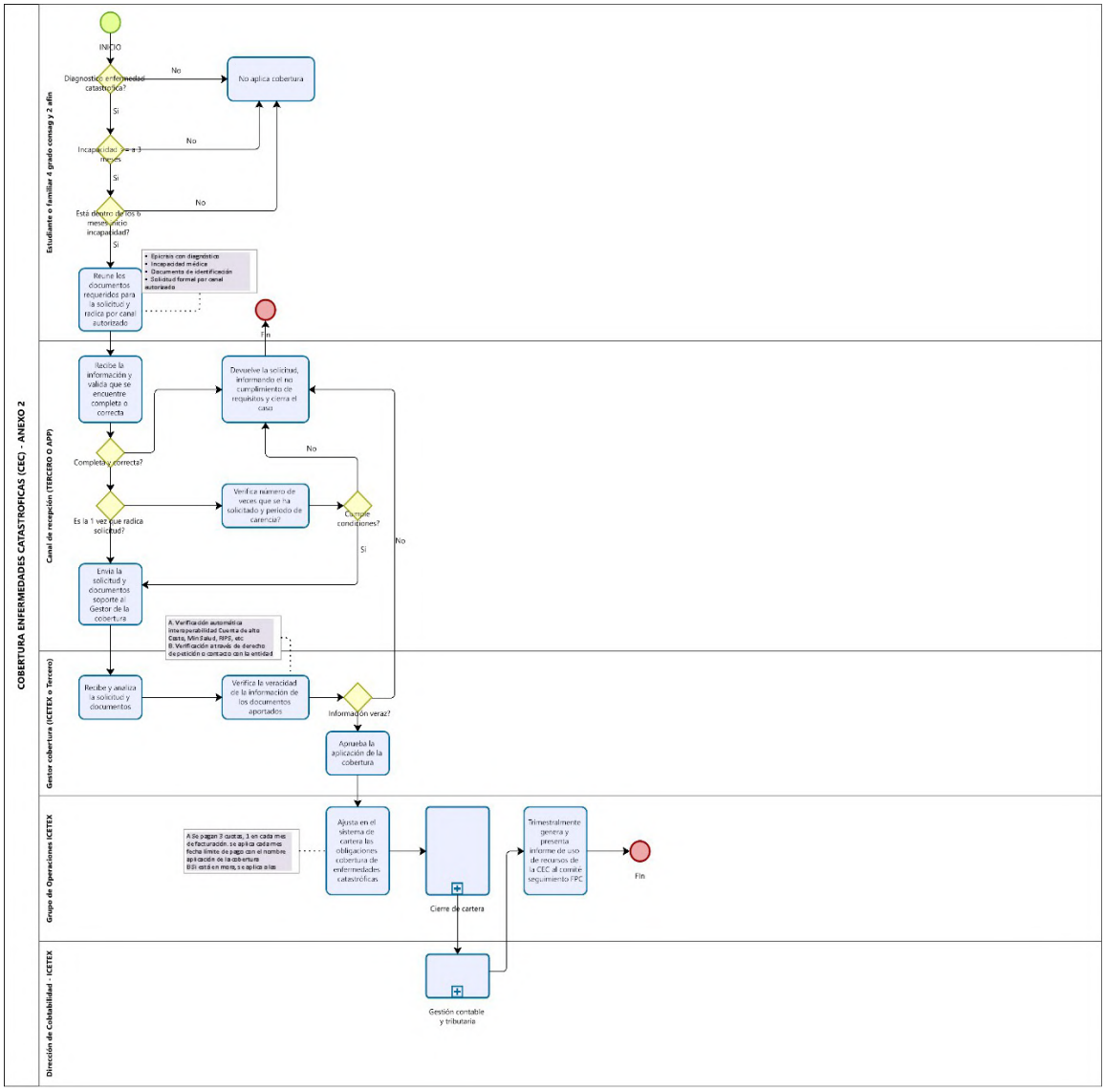


Calle 60a #5-54, Oficina 403
Bogotá D.C. Colombia
NIT. 830.101.214-4
+57 3222468120
www.colombiadigital.net

Ilustración 10 Aplicación de las coberturas

Enfermades catastróficas

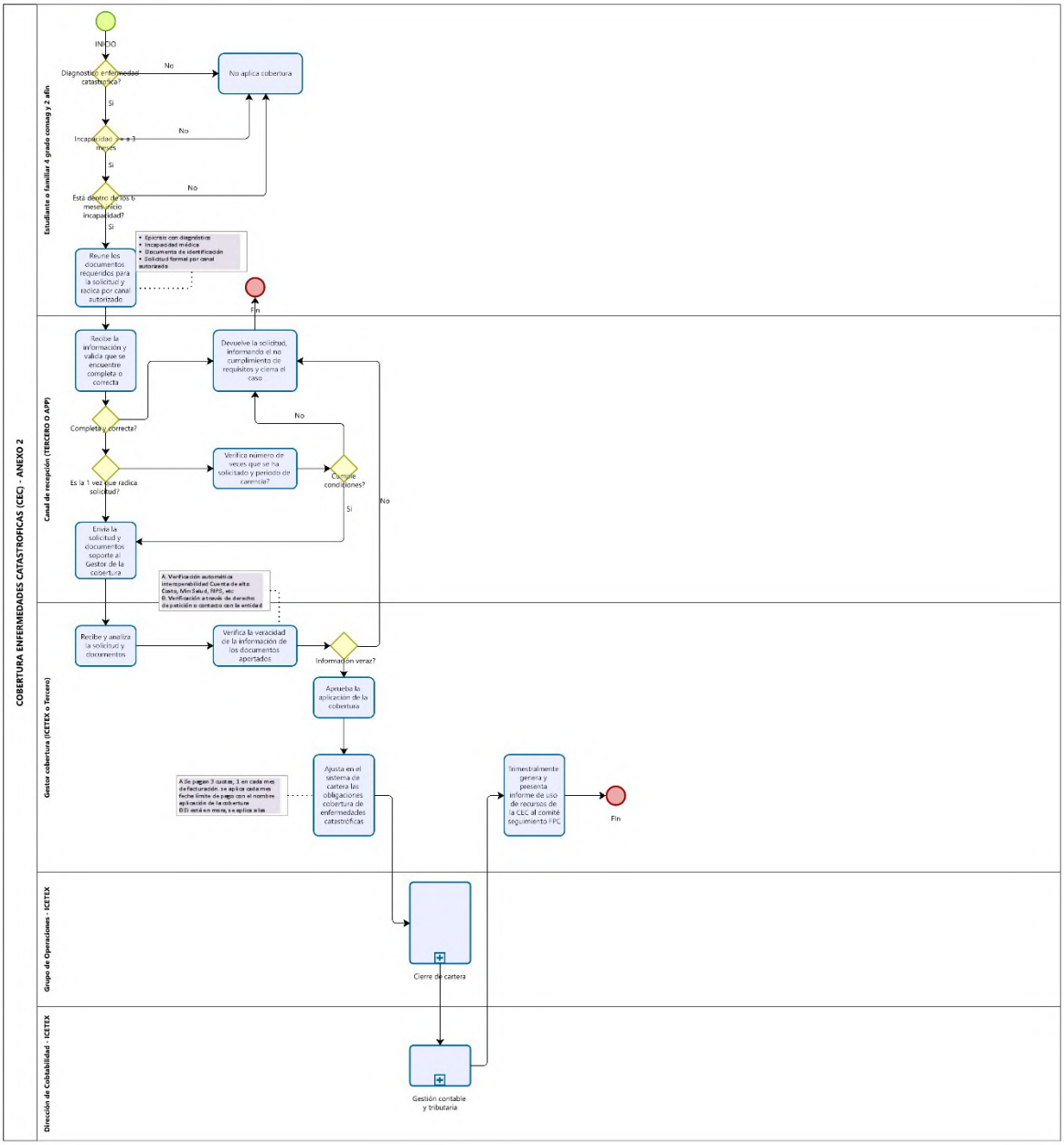
Escenario 1: El proveedor solamente realiza validaciones y la aplicación de las coberturas en cartera son realizadas por el Grupo de Operaciones de la entidad designada:



Calle 60a #5-54, Oficina 403
Bogotá D.C. Colombia
NIT. 830.101.214-4
+57 3222468120
www.colombiadigital.net

Ilustración 11 Enfermedades catastróficas

Escenario 2: El proveedor realiza validaciones y la aplicación de las coberturas en cartera:



Calle 60a #5-54, Oficina 403
Bogotá D.C. Colombia
NIT. 830.101.214-4
+57 3222468120
www.colombiadigital.net

Ilustración 12 validaciones y la aplicación de las coberturas

Impacto de la implementación de las nuevas coberturas de desempleo y enfermedades catastróficas en los procesos actuales de la entidad.

Las nuevas coberturas del Fondo Pasivo Contingente operadas por un tercero impactarán los siguientes procesos de la entidad designada:

- Atención a beneficiarios y/o ciudadanos – M5-1
- Administración de cartera – M3-2
- Gestión de recuperación de cartera - M4-2
- Gestión de archivo – A8-3

Hoja de ruta implementación coberturas desempleo y enfermedades catastróficas

A continuación, se relacionan las fases que se deberán adelantar para el alistamiento operativo e implementación de las coberturas de desempleo y enfermedades catastróficas:

No	Fase	Actividad	Entregable esperado
1	Diagnóstico y diseño	Revisión de lineamientos de la entidad y fuentes de interoperabilidad disponibles.	Diseño funcional y técnico del proceso. Diagramación procesos de coberturas con tiempos de ejecución
2	Desarrollo o configuración de la solución tecnológica	Desarrollo de la solución tecnológica.	Módulo de registro, verificación y decisión de coberturas.
3	Integración Interoperable	Conexión con sistemas de entidades externas y de la propia entidad designada	Interfaces habilitadas y operativas para consulta de datos y aplicación de coberturas.
4	Pruebas y ajustes	Ejecución de pruebas fun-cionales, técnicas y de carga.	Registro de pruebas, ajustes implementados, aprobación.
5	Capacitación y puesta en marcha	Formación de funcionarios recursos del proveedor y socialización con usuarios.	Manuales, videos, talleres de formación y despliegue.
6	Seguimiento y optimización	Recolección de datos, retroalimentación y ajuste de reglas.	Informes de solicitudes (recibidas, en proceso, aprobadas y rechazadas) Mejora del modelo operativo.

Tabla 2 Hoja de ruta implementación coberturas desempleo

3.2 ESTRUCTURACIÓN DEL PROYECTO

La estructuración del proyecto es una etapa clave para garantizar la implementación y habilitación de los productos digitales del Fondo Pasivo Contingente y los diferentes componentes que lo integran. Esta estructuración debe realizarse desde las primeras etapas del proyecto, y debe garantizar la definición de objetivos, alcance, requisitos, cronograma y entregables claves del proyecto, asegurando la alineación estratégica entre las actividades planificadas y los resultados

esperados. Debe identificar y gestionar los stakeholders, habilitar la asignación de roles y responsabilidades, establecer las fases necesarias para integrar los componentes tecnológicos y operativos que permitirán cumplir con los objetivos del proyecto.

3.2.1 Alcance de la estructuración del proyecto

La estructuración del proyecto incluye todas las actividades necesarias para diseñar, implementar e integrar los componentes tecnológicos y operativos del Fondo Pasivo Contingente:

1. **Componentes tecnológicos:**
    1. Core de depósitos.
    2. Payment hub.
    3. Pasarela de pagos
    4. Plataforma omnicanal (web, aplicación móvil, contact center).
    5. Agentes cognitivos para atención automatizada.
    6. Soluciones de BI/BA para analítica avanzada.
    7. Capacidades tecnológicas
    8. reportes normativos.

2. **Procesos Operativos:**
    1. Modelo de negocio.
    2. Mapa de capacidades.
    3. Modelo organizacional.
    4. Modelo de procesos.

3. **Objetivos estratégicos:**
    1. Digitalización completa de servicios financieros.
    2. Optimización de la experiencia del cliente mediante personalización y omnicanalidad.
    3. Cumplimiento con regulaciones financieras, legales y tecnológicas.

4. **Otros componentes de la operación:**
    1. Gestión completa del consumo de horas de desarrollo
    2. Gestión completa del modelo de operación
    3. Gestión completa estrategia de uso y apropiación
    4. Gestión completa de operación del fondo de pasivo contingente
    5. Gestión completa marco estratégico y operativa.
    6. Checklist de cumplimiento de obligaciones debe entregarse los 15 primeros días calendario después de la firma del contrato.

3.3 INTEGRADOR DE SERVICIOS

El componente Integrador tiene como objetivo principal garantizar una interoperabilidad eficiente entre los diferentes módulos tecnológicos, fuentes de datos y actores funcionales que conforman el ecosistema del Fondo Pasivo Contingente (FPC). Su diseño incorpora mecanismos avanzados para integrar y automatizar flujos de información entre plataformas internas, pasarelas de pago, sistemas financieros, entidades externas y otros proveedores tecnológicos. Este enfoque

permite reducir redundancias, minimizar errores manuales y proporcionar una trazabilidad completa de transacciones y operaciones.

En esencia, el componente Integrador se erige como la columna vertebral de la interoperabilidad dentro del ecosistema digital del FPC. Se ha diseñado como una plataforma de integración empresarial que actúa como un nodo estratégico, facilitando la conexión, exposición, orquestación y monitoreo de microservicios tanto internos como externos. Esto se realiza mediante una arquitectura modular, escalable y desacoplada, asegurando altos niveles de trazabilidad y confiabilidad.

Además de ofrecer capacidades tradicionales como un bus de servicios, el Integrador proporciona una estructura flexible que centraliza la gestión de transacciones, la orquestación de flujos de datos y la integración de sistemas. Este ecosistema incluye plataformas internas (como el Core Bancario, BPM, Gestor Documental, ETL o Motor de Reglas) y sistemas externos (tales como entidades regulatorias, servicios de validación biométrica, proveedores de terceros y plataformas de pago).

Gracias a su arquitectura escalable y reutilizable, el Integrador permite que el ecosistema funcione de manera cohesionada. Esto se traduce en una solución adaptable que facilita la incorporación de nuevos flujos y servicios sin necesidad de alterar la lógica de negocio existente en otros módulos. Así, se asegura tanto la adaptabilidad a las necesidades futuras como el cumplimiento de las demandas actuales del negocio y de la regulación.

Funcionalidades Estratégicas

El componente Integrador ofrece un conjunto de capacidades clave para soportar los procesos críticos del FPC:

- Centralización de peticiones entre módulos internos y externos.
- Registro y trazabilidad completa de todas las transacciones realizadas, con cada mensaje registrado y consultable.
- Orquestación de servicios y microservicios mediante comandos y flujos parametrizables y configurables.
- Soporte para múltiples modos de ejecución: sincrónica, asincrónica, por eventos y procesamiento asincrónico.
- Gestión avanzada de errores con reintentos configurables, auditoría automática y control de concurrencia.
- Definición flexible de flujos de integración a través de tipos de peticiones reutilizables.
- Autenticación configurable por host confiable, token, modo de operación y protocolo.
- Control de acceso granular y definición de roles para cada tipo de interacción.
- Mecanismos de integración flexibles: interfaces RESTful estandarizadas, SOAP, colas de eventos, mensajería, archivos y contratos basados en especificación.
- Balanceo de carga interno soportado en un sistema de registro de microservicios propio.
- Interfaz de gestión estándar para monitoreo transversal, configuración y seguimiento operativo con visualización desde tableros de control.
- Conectores reutilizables y parametrizables que reducen los esfuerzos de desarrollo para nuevos sistemas.

- Modelado gráfico de procesos/flujos de negocio.
- Ejecución orquestada de actividades humanas y automáticas.
- Gestión dinámica de variables y parámetros dentro de cada flujo.
- Asignación de tareas mediante reglas de negocio y colas personalizadas.
- Control de versiones y ciclo de vida de los flujos.
- Activación y desactivación de flujos en tiempo real.
- Registro de logs de ejecución para flujos y actividades.
- Seguimiento de flujos activos y actividades/etapas en curso.
- Administración de grupos de usuarios y perfiles de acceso.
- Generación de métricas operativas y tableros de control.
- Configuración de alarmas y notificaciones según tiempos, condiciones o errores.
- Integración nativa con motores de reglas y otros componentes de la arquitectura.
- Capacidad para escalar horizontalmente y distribuir la carga de trabajo.

Estas funcionalidades permiten que el integrador actúe como el sistema nervioso del ecosistema digital, alineado a las mejores prácticas de arquitectura orientada a servicios (SOA) y gobernanza de APIs.

3.3.1 BPM (Business Process Management)

El componente BPM debe automatizar y orquestar los procesos críticos del negocio, desde el onboarding de clientes hasta las validaciones normativas, con trazabilidad total y control de tareas en tiempo real. El BPM debe habilitar la capacidad de modelar procesos parametrizables desde una interfaz gráfica o mediante definiciones técnicas avanzadas. Los procesos definidos pueden incluir actividades humanas, automatizadas, subprocesos, validaciones por condiciones, bifurcaciones lógicas y puntos de integración con sistemas externos.

Con el componente de BPM se busca gestionar y optimizar procesos de negocio relacionados con la cuenta de ahorro digital, debe automatizar flujos de trabajo para mejorar la eficiencia operativa en procesos como:

1. Validación de Identidad / Liveness: Procesos para asegurar que el usuario es quien dice ser (ej. biometría facial, prueba de vida) y no un impostor.
2. KYC (Know Your Customer): Proceso crítico de debida diligencia. Consulta:
    - Listas Restrictivas (OFAC, ONU, PEP - Personas Expuestas Políticamente).
    - Listas Internas.
    - Sistemas de cumplimiento normativo como SARLAFT/UIAF (Colombia).
3. Corrección de errores y validación final.
4. Apertura y gestión de la cuenta.

El BPM debe contar entre sus principales funcionalidades las siguientes:

1. Modelado gráfico de procesos de negocio (BPMN) y configuración técnica avanzada.
2. Ejecución orquestada de actividades humanas y automáticas.
3. Gestión dinámica de variables y parámetros dentro de cada proceso.
4. Asignación de tareas mediante reglas de negocio y colas personalizadas.
5. Control de versiones y ciclo de vida de los procesos.

6. Activación y desactivación de procesos en tiempo real.
7. Registro de logs de ejecución para procesos y actividades.
8. Seguimiento de procesos activos y actividades en curso.
9. Administración de grupos de usuarios y perfiles de acceso.
10. Generación de métricas operativas y tableros de control.
11. Configuración de alarmas y notificaciones según tiempos, condiciones o errores.
12. Integración con motores de reglas y otros componentes de la arquitectura.
13. Capacidad para escalar horizontalmente y distribuir la carga de trabajo.

Debe incorporar mecanismos para la supervisión en tiempo real del estado de cada proceso y actividad, con trazabilidad completa, generación de métricas clave, alarmas configurables, y seguimiento por usuario, producto o canal.

3.4 ESTRATEGIA DE USO APROPIACIÓN Y UX/UI

Se debe diseñar la estrategia integral de marketing para para el lanzamiento del producto Fondo de pasivo contingente (FPC), que incluye en su primera etapa una solución de Ahorro Educativo Digital que busca facilitar el acceso a la educación superior, fomentar la cultura de ahorro desde la primera infancia y contribuir a la reducción de la deserción estudiantil en Colombia. La estrategia de marketing digital del proyecto abarca diversos aspectos fundamentales para

posicionar y promover la solución en el mercado. El Análisis de Situación evalúa el entorno competitivo, tendencias del mercado y comportamiento del consumidor, identificando oportunidades y desafíos. A partir de este diagnóstico, se establecen los Objetivos del Proyecto, alineados con las metas comerciales y de posicionamiento. El estudio del Público Objetivo (Arquetipos de Cliente) permite segmentar la audiencia mediante la definición de perfiles detallados que reflejan sus necesidades, motivaciones y comportamientos digitales.

El Mapa de Arquitectura de Marca estructura la identidad visual y comunicacional, asegurando coherencia y diferenciación en el ecosistema digital. La Propuesta de Valor sintetiza los atributos y beneficios únicos de la oferta, destacando su relevancia para los clientes. A partir de esta propuesta, se diseña el Customer Journey de FPC, un recorrido que visualiza las interacciones clave del usuario con la marca en diferentes puntos de contacto.

La Estrategia de Comunicación 360° define los mensajes y canales que garantizarán una presencia omnicanal efectiva, integrando marketing digital, relaciones públicas y publicidad. Como parte de esta estrategia, el Plan de Medios especifica las plataformas, formatos y presupuesto destinado a la difusión de la campaña.

1. **Análisis de Situación**
   Evaluación del contexto actual del producto de ahorro digital, incluyendo:
   1. Diagnóstico de presencia digital actual (sitio web, redes sociales, métricas de tráfico).
   2. Análisis DOFA.
   3. Benchmarking de competidores directos e indirectos en el sector fintech colombiano.

2. **Objetivos del proyecto**
   Definición de objetivos SMART alineados con el negocio, estos deben incluir Indicadores cuantificables que permitan medir y evolucionar los resultados de la estrategia de marketing.

3. **Público objetivo (Arquetipos de cliente)**
   Creación de buyer personas basadas, de tal manera que el público objetivo se segmente en arquetipos que permitan una mejor descripción y comprensión de los perfiles a los que se dirige el producto de ahorro digital:
   1. Segmentación demográfica (edad, ubicación, nivel socioeconómico) y psicográfica (intereses financieros).
   2. Comportamientos digitales: preferencias de canales, dispositivos usados y frecuencia de interacción.

4. **Mapa de arquitectura de marca**
   Estructuración jerárquica de la marca principal y submarcas (si aplica), definiendo:
   1. Relación entre marca corporativa y producto de ahorro digital.
   2. Coherencia visual y narrativa en todos los puntos de contacto.
5. **Propuesta de valor**

   Articula los diferenciadores clave del producto de ahorro digital, como beneficios únicos y mensajes centrados en inclusión financiera y transparencia:
   1. Beneficios únicos (ej.: tasas competitivas, experiencia 100% digital).

2. Mensajes centrados en inclusión financiera y transparencia.

6. **Customer Journey de FPC**
   Mapea las etapas del usuario desde el descubrimiento hasta la fidelización, permitiendo optimizar cada punto de contacto.

7. **Estrategia de comunicación 360°**
   Integra los diferentes canales de comunicación, incluyendo medios propios, pagados y obtenidos.

8. **Plan de medios**
   Detalla la distribución táctica por canal y establece un calendario de acciones con KPIs específicos.

3.4.1 Estrategia de Uso y Apropiación

La gestión del cambio es un componente crítico para el éxito de la implementación del producto de Cuenta de Ahorro, especialmente en el contexto de la entidad, teniendo en cuenta el impacto que puede tener al interior. Este capítulo aborda las estrategias, procesos y herramientas necesarias para garantizar una transición fluida hacia los nuevos sistemas y procesos definidos en el proyecto, minimizando la resistencia al cambio y asegurando la adopción por parte de todos los actores involucrados.

1. **Objetivos de la Gestión del Cambio**
   1. **Asegurar la Adopción:** Promover la aceptación de los nuevos procesos tecnológicos, como la configuración de productos y el onboarding digital.
   2. **Minimizar Resistencia:** Identificar y abordar posibles barreras al cambio en las áreas funcionales, técnicas y operativas.
   3. **Maximizar el Retorno de Inversión:** Garantizar que los beneficios esperados del proyecto se materialicen a través de una implementación efectiva.

2. **Componentes Clave**
   1. Evaluación Inicial del Impacto

Identificar las áreas afectadas por los cambios, como los equipos de negocio y tecnología.

Acciones Clave:

1. Mapeo de procesos afectados.
2. Evaluación del nivel de madurez digital de los usuarios involucrados.
3. Identificación de riesgos asociados al cambio.

2. Comunicación Estratégica

Diseñar un plan de comunicación que informe a todas las partes interesadas sobre los objetivos, beneficios y cronograma del proyecto.

Acciones Clave:

Calle 60a #5-54, Oficina 403
Bogotá D.C. Colombia
NIT. 830.101.214-4
+57 3222468120
www.colombiadigital.net

1. Realizar sesiones informativas para explicar el impacto de las nuevas plataformas y procesos digitales.
2. Crear canales abiertos para resolver dudas y recibir retroalimentación.

3. Capacitación y Desarrollo

Proporcionar formación específica a los usuarios finales para garantizar que comprendan y puedan operar con los nuevos sistemas.

Acciones Clave:

1. Capacitación técnica para el equipo del proyecto en parametrización y uso de las plataformas digitales.
2. Entrenamiento funcional para las áreas de negocio y cumplimiento sobre las nuevas herramientas digitales.

4. Gestión de Resistencia

Abordar las preocupaciones o resistencias al cambio mediante estrategias proactivas.

Acciones Clave:

1. Involucrar a líderes clave como agentes del cambio dentro de sus equipos.
2. Implementar encuestas periódicas para evaluar la aceptación del cambio.

5. Monitoreo y Seguimiento

Evaluar continuamente el progreso en la adopción del cambio e identificar áreas que requieran ajustes.

Acciones Clave:

1. Definir indicadores clave (KPIs) como tasas de adopción tecnológica o tiempo promedio para completar tareas en el nuevo sistema.
2. Realizar auditorías post-implementación para asegurar que los procesos estén funcionando según lo planeado.

3.4.2 Estrategia Despliegue e Implementación

La estrategia de despliegue e implementación es un componente clave para garantizar el éxito del desarrollo y lanzamiento de la cuenta de ahorro digital y los productos relacionados con el Fondo Pasivo Contingente. Este capítulo establece los lineamientos estratégicos, define el Producto Mínimo Viable (MVP) para pruebas piloto y detalla las fases y actividades necesarias para asegurar una transición fluida desde el desarrollo hasta la operación pasando por la prueba de recorrido para la superintendencia Financiera. Además, se contemplan estrategias específicas de onboarding digital, capacitación interna, integración con otros servicios financieros y preparación para futuras iteraciones.

1. Lineamientos Estratégicos

Los lineamientos estratégicos que se deben tener en cuenta en el despliegue e implementación del producto, asegurando que se cumplan los objetivos del proyecto:

Enfoque en el MVP: Priorizar las funcionalidades esenciales para validar la viabilidad del producto en un entorno controlado.

Calle 60a #5-54, Oficina 403
Bogotá D.C. Colombia
NIT. 830.101.214-4
+57 3222468120
www.colombiadigital.net

Onboarding Digital: Facilitar la inscripción de usuarios mediante procesos rápidos, seguros y 100% digitales.
Escalabilidad: Diseñar la solución para soportar un crecimiento exponencial tras el lanzamiento inicial.
Cumplimiento Normativo: Garantizar que el producto cumpla con todas las regulaciones locales e internacionales aplicables.
Iteración Continua: Preparar el producto para futuras mejoras basadas en retroalimentación de clientes y datos operativos.

2. Definición del MVP

El MVP (Producto Mínimo Viable) se centra en las funcionalidades esenciales para garantizar una experiencia básica pero completa. Las características incluidas son:

- Apertura de cuenta digital con validación de identidad (biometría facial y captura documental).
- Gestión básica de la cuenta (consulta de saldo, movimientos, generación de extractos).
- Onboarding digital automatizado con validación en tiempo real.
- Integración inicial con canales web y aplicación móvil.
- Cumplimiento básico con normativas como FATCA, CRS y listas restrictivas.

El MVP servirá como base para pruebas piloto en un entorno controlado antes de la prueba de recorrido de Superintendencia Financiera y del despliegue a gran escala.

3. Fases del Plan de Trabajo

El plan de trabajo se organiza en cuatro fases principales:

Fase 1: Preparación
Objetivo: Establecer las bases técnicas y operativas para el desarrollo del MVP.
Actividades:
1. Configuración inicial del producto en el core bancario del pasivo.
2. Definición de cuentas contables y parametrización técnica.
3. Diseño del flujo de onboarding digital.
4. Identificación de stakeholders clave y asignación de roles.

Fase 2: Implementación
Objetivo: Instalar, parametrizar e integrar los componentes tecnológicos necesarios para habilitar el MVP.
Actividades:
1. Instalación e implementación del módulo de apertura digital (onboarding).
2. Integración con servicios financieros existentes (core contable, Payment Hub, BI/BA, etc.).
3. Configuración inicial de canales web y aplicación móvil.
4. Pruebas unitarias y funcionales.

Fase 3: Pruebas Piloto
Objetivo: Validar la funcionalidad del MVP en un entorno controlado antes del lanzamiento público.
Actividades:

1. Selección de un grupo limitado de usuarios para realizar pruebas piloto.
2. Monitoreo continuo del desempeño técnico y funcional.
3. Recopilación de retroalimentación para ajustes finales.

Fase 4: Despliegue a Gran Escala
Objetivo: Lanzar el producto al mercado con soporte operativo completo.
Actividades:

1. Capacitación interna a equipos operativos y técnicos sobre nuevas herramientas y procesos.
2. Activación completa de canales omnicanal (web, aplicación móvil, contact center).
3. Campañas informativas para atraer usuarios al nuevo producto.

4. Estrategias Complementarias

Onboarding Digital

- Implementar validaciones biométricas rápidas y seguras para inscripción sin fricciones.
- Automatizar procesos regulatorios como KYC (Conozca a su Cliente) y consulta de listas restrictivas.

Capacitación Interna

- Realizar talleres prácticos sobre uso e integración tecnológica para equipos operativos y comerciales.
- Entrenar a agentes humanos en la interacción con agentes cognitivos para escalamiento inteligente.

Preparación para Iteraciones Futuras

- Diseñar una arquitectura modular que permita agregar funcionalidades sin afectar sistemas existentes.
- Monitorear métricas clave como tasa de adopción y satisfacción del cliente para guiar mejoras continuas.

3.5 MARCO ESTRATÉGICO Y OPERATIVO PARA LA ALINEACIÓN EMPRESARIAL

El proveedor debe desarrollar un marco estratégico y debe asumir una serie de obligaciones claras y estructuradas para garantizar que el resultado cumpla con las expectativas estratégicas y operativas de la organización. Las obligaciones deben cubrir desde el análisis inicial hasta la entrega de una arquitectura operativa y alineada con el modelo de negocio. A continuación, se detallan las obligaciones mínimas que se deben tener en cuenta:

Calle 60a #5-54, Oficina 403
Bogotá D.C. Colombia
NIT. 830.101.214-4
+57 3222468120
www.colombiadigital.net

3.5.1 Análisis del modelo de negocio y modelo estratégico actual

El proveedor deberá llevar a cabo un análisis exhaustivo del modelo de negocio y de la estrategia de la entidad vigente, con el fin de asegurar que la arquitectura propuesta esté alineada con los objetivos estratégicos de la organización. Las obligaciones específicas incluyen:

Revisión y análisis del modelo de negocio:

- Identificar y documentar los segmentos de clientes.
- Identificar las principales propuestas de valor y productos/servicios ofrecidos.
- Evaluar los canales de distribución y comunicación (físicos y digitales).
- Analizar las fuentes de ingresos y la estructura de costos.
- Definir y analizar las principales actividades que habilitan la entrega del producto o servicio.

Evaluación del modelo estratégico:

- Revisar la misión, visión y valores de la entidad.
- Analizar las estrategias actuales y su efectividad.
- Identificar riesgos y oportunidades estratégicas.
- Identificar las iniciativas estratégicas en curso y su alineación con los objetivos de negocio.

Identificación de brechas y oportunidades:

- Identificar inconsistencias o áreas de mejora en el modelo de negocio.
- Proponer ajustes para mejorar la eficiencia y efectividad de las estrategias.

3.5.2 Customer Journey (Mapa de experiencia del cliente)

El proveedor debe desarrollar un mapa de experiencia del cliente que permita entender el recorrido del cliente desde la primera interacción hasta la postventa. Las obligaciones mínimas incluyen:

Identificación de los puntos de contacto (touchpoints):

- Mapear todos los canales y puntos de contacto con el cliente (digitales, físicos, mixtos).
- Identificar las expectativas y necesidades de los clientes en cada punto de contacto.
- Documentar los flujos de interacción y las posibles fricciones o problemas.

Análisis de experiencia y satisfacción:

- Identificar problemas o cuellos de botella en la experiencia del cliente.
- Proponer acciones para optimizar la experiencia y mejorar la satisfacción.

Diseño de mejoras en la experiencia:

- Proponer acciones para mejorar la personalización y consistencia en todos los puntos de contacto.
- Alinear el customer journey con las capacidades y procesos internos.

3.5.3 Mapa de capacidades

El proveedor debe construir un mapa de capacidades que refleje las competencias clave de la entidad y su relación con la estrategia de negocio. Las obligaciones mínimas incluyen:

Identificación y clasificación de capacidades:

- Identificar las capacidades estratégicas, operativas y de soporte.
- Clasificar las capacidades en:
  - **Core:** Capacidades diferenciadoras que generan valor estratégico.
  - **Enabling:** Capacidades que permiten la operación de las capacidades core.
  - **Supporting:** Capacidades que brindan soporte general (por ejemplo, tecnología, finanzas).

Evaluación de capacidades:

- Evaluar la madurez de cada capacidad.
- Identificar brechas entre las capacidades actuales y las requeridas para ejecutar la estrategia.
- Determinar el impacto de las capacidades en la experiencia del cliente y la operación.

Priorización de capacidades:

- Priorizar las capacidades clave para la entrega de valor y diferenciación competitiva.
- Alinear las capacidades con la estrategia de negocio y el modelo de operación.

3.5.4 Modelo de procesos con los principales flujos de actividades

El proveedor debe documentar los principales procesos que habilitan la operación y la entrega de valor al cliente en el marco de los lineamientos del Sistema de Gestión de la entidad. Las obligaciones mínimas incluyen:

Identificación y modelado de procesos:

- Documentar los procesos o procedimientos de cara al cliente (customer-facing).
- Documentar los procesos o procedimientos habilitadores (back-office y soporte).
- Utilizar metodologías estándar como BPMN (Business Process Model and Notation).

Análisis de procesos:

- Identificar redundancias, ineficiencias y cuellos de botella.
- Evaluar la automatización y digitalización de procesos.
- Evaluar el nivel de integración entre procesos y sistemas tecnológicos.

Priorización y optimización de procesos:

- Priorizar procesos críticos para la entrega de productos y servicios.
- Proponer mejoras para optimizar tiempos, costos y calidad.
- Establecer indicadores clave de rendimiento (KPIs) para monitorear la efectividad de los procesos.

3.5.5 Estructura organizacional

El proveedor debe definir y documentar una **estructura organizacional** que soporte el modelo de negocio y las capacidades identificadas. Las obligaciones mínimas incluyen:

Documentación de la estructura actual:

- Levantar y documentar la estructura organizacional actual (organigrama).
- Identificar roles y responsabilidades clave.
- Analizar la efectividad de la estructura en la ejecución de la estrategia y la operación.

Propuesta de ajuste organizacional:

- Alinear la estructura organizacional con el modelo de capacidades y los procesos.
- Proponer cambios en roles y responsabilidades para mejorar la efectividad operativa.
- Identificar necesidades de formación o reentrenamiento.

Gobernanza:

- Definir mecanismos de toma de decisiones y escalamiento de problemas.
- Definir líneas de comunicación y coordinación entre áreas.
- Establecer un modelo de gobernanza para garantizar la ejecución continua de la estrategia.

3.6 REQUERIMIENTOS TÉCNICOS DE LA PLATAFORMA TECNOLÓGICA

En el mundo actual, los canales digitales y la experiencia del cliente ocupan un lugar central en una plataforma tecnológica. Los canales digitales incluyen sitios web, aplicaciones móviles y otras interfaces en línea que los clientes utilizan para interactuar con la entidad financiera. La importancia de estos canales radica en su capacidad para ofrecer servicios bancarios accesibles y convenientes, las 24 horas del día, los 7 días de la semana, independientemente de la ubicación del cliente.

Una experiencia del cliente excepcional en estos canales digitales es crucial para atraer y retener clientes. Las plataformas deben ser intuitivas, rápidas y fáciles de usar, permitiendo que los usuarios realicen sus transacciones y consultas sin complicaciones. Esto no solo mejora la satisfacción del cliente, sino que también fomenta la lealtad y la recomendación, factores vitales para el crecimiento y la competitividad en el sector financiero.

Por esta razón la entidad considera que el proveedor debe cumplir con los siguientes requerimientos mínimos:

3.6.1 Omnicanalidad

El proveedor está obligado a garantizar la correcta gestión, administración, configuración y optimización del enfoque de omnicanalidad, asegurando una experiencia fluida, coherente e integrada en todos los canales digitales y físicos de la entidad. Para ello, deberá implementar una arquitectura unificada de interacción, permitiendo que los clientes puedan iniciar, continuar y finalizar transacciones sin interrupciones, independientemente del canal utilizado. Asimismo, será responsable de la configuración y personalización de los puntos de contacto, asegurando su

sincronización en tiempo real para una comunicación eficiente y consistente. El proveedor deberá garantizar la disponibilidad, escalabilidad y seguridad de la plataforma omnicanal, evitando fallos que afecten la continuidad del servicio. Además, deberá integrar herramientas de análisis y monitoreo, permitiendo evaluar el comportamiento de los usuarios y optimizar la experiencia en función de sus necesidades. Finalmente, será responsable de ofrecer capacitación y soporte técnico especializado, asegurando que el personal de la entidad pueda gestionar la estrategia omnicanal con eficacia y alineación a los objetivos de negocio.

La plataforma debe permitir a los clientes acceder a los servicios a través de múltiples canales de forma fluida y consistente.

3.6.1.1 Canales Digitales principales

Los canales digitales principales son esenciales para garantizar la interacción eficiente entre los clientes y la entidad financiera. Estos incluyen aplicaciones web y móviles que ofrecen interfaces seguras, intuitivas y accesibles, diseñadas para cumplir con altos estándares de calidad y usabilidad.

3.6.1.1.1 Aplicaciones Web y Móvil

- Interfaces intuitivas con acceso seguro a productos financieros.
- Las interfaces deben cumplir como mínimo con los estándares AA con opción de mejora a AAA de la Guía de Accesibilidad de Contenidos Web (Web Content Accesibillity Guidelines - WCAG) en la versión 2.2 o superior.
- Los usuarios podrán operar o gestionar de distintas formas los contenidos de los sitios web, no siendo solamente posible mediante el ratón (mouse), sino por teclado, pantallas táctiles y otros medios.
- El proveedor deberá utilizar la guía de estilos del producto definida entre el proveedor y la entidad teniendo en cuenta el diseño de imagen, tipología y demás componentes que la entidad defina.
- La aplicación móvil debe contar con el cumplimiento de los estandares más reconocidos como Mobile Web Best Practices del World Wide Web Consortium (W3C). Este estándar proporciona directrices para mejorar la experiencia del usuario en dispositivos móviles, asegurando que las aplicaciones sean accesibles, eficientes y seguras.
- Cumplir con las Pautas de Accesibilidad para el Contenido Web (WCAG) que también se aplican a las aplicaciones móviles.
- La aplicación Web deberá como mínimo funcionar correctamente en los principales navegadores como:
    - Google Chrome
    - Safari
    - Microsoft Edge
    - Opera
    - Mozilla Firefox
- La aplicación móvil deberá funcionar correctamente en dispositivos con sistema operativo Android desde su versión 5.0 en adelante.
- La aplicación móvil deberá funcionar correctamente en dispositivos con sistema operativo iOS desde su versión 12 en adelante.

- El sistema de notificaciones debe integrarse perfectamente con el core de depósito y los sistemas de soporte existentes, asegurando una transferencia de datos sin problemas.

A continuación, se detallan los módulos y funcionalidades que debe incluir el portal web del cliente.

1. **Autenticación y seguridad**

   a. Inicio de sesión.
   b. Restablecer contraseña.
   c. Método de seguridad robusto y personalizado para el login y la autorización de las transacciones (MFA, biometría, Face ID, entre otros).
   d. Las demás establecidas en el numeral 3.6.5.4

2. **Consultas**

   a. **Resumen de productos:** Se muestran productos activos (cuentas) con el número de contrato como enlace directo al detalle de los movimientos.
   b. **Consulta de estado de cuenta:** Generación de un informe detallado del estado de cuenta, incluyendo una visión completa de todas las transacciones realizadas durante un periodo de tiempo.
   c. **Calculadora financiera para ahorro:** Que permita visualizar escenarios de ahorro programado, que incluya como mínimo, la meta de ahorro, la periodicidad, el valor del ahorro periódico, el valor opcional del aporte de cobertura por invalidez o muerte.

3. **Transferencias**

   a. **Comprobantes de pago:** Consulta de comprobantes de pago de servicios.
   b. **Transferencias:** Se muestran transferencias a cuentas propias, nacionales/, órdenes por aprobar, últimas transferencias.

4. **Transacciones**

   a. Últimas transacciones.
   b. Revisar transacciones.
   c. Aprobar transacciones.

5. **Perfil del cliente**

   a. **Gestión del perfil del cliente:** Permite actualizar las respuestas a las preguntas de seguridad, alias de las cuentas y preferencias de correo electrónico, entre otros.
   b. **Reinicio de contraseña:** Permite al usuario cambiar la contraseña utilizando un método de seguridad.
   c. **Gestión de beneficiarios:** Agregar/editar beneficiario.
   d. **Administrador del token virtual:** Equipo registrado, olvido de contraseña del token virtual.

Como parte de la solución integral para la Cuenta de Ahorro digital, se debe incluir una aplicación móvil nativa para plataformas Android y iOS. Esta aplicación permitirá a los clientes gestionar sus cuentas y realizar operaciones bancarias de manera rápida y segura desde cualquier lugar, ofreciendo una experiencia de usuario moderna e intuitiva. Es necesario que la aplicación contemple y ofrezca las siguientes características:

- *Disponibilidad en Android y iOS*: La aplicación estará disponible para su descarga en Google Play Store y Apple App Store, asegurando una amplia cobertura y accesibilidad para todos los clientes.
- *Acceso seguro*: Autenticación biométrica (huella digital o reconocimiento facial) y MFA (autenticación multifactor) para garantizar la seguridad en cada inicio de sesión y operación.
- *Experiencia de usuario personalizada*: Interfaz intuitiva y amigable que se adapta a las preferencias del usuario, con navegación sencilla y procesos simplificados.
- *Sincronización en tiempo real*: Las operaciones realizadas en la aplicación móvil se reflejarán automáticamente en la plataforma web y en otros canales digitales.
- *Notificaciones push*: Alertas en tiempo real sobre movimientos de cuenta, pagos programados, transferencias y mensajes de seguridad.
- *Actualizaciones:* Generar actualizaciones de seguridad, funcionalidad y de sistema operativo entre otros.

La aplicación deberá incluir un conjunto de funcionalidades para asegurar que los clientes puedan gestionar su producto financiero:

1. **Consultas de saldos y estados de cuenta**
   - Acceso en tiempo real a saldos y movimientos.
   - Histórico de transacciones y estados de cuenta descargables.

2. **Calculadora Financiera para Productos de Ahorro**
   - Que permita visualizar escenarios de ahorro programado, que incluya como mínimo, la meta de ahorro, la periodicidad, el valor del ahorro periódico, el valor opcional del aporte de cobertura por invalidez o muerte.

3. **Transferencias**
   - Entre cuentas propias y de terceros.
   - Transferencias inmediatas y programadas.

4. **Gestión de Tarjetas**
   - Activación y bloqueo de tarjetas digitales.
   - Reporte de tarjetas extraviadas o robadas.
   - Configuración de límites y alertas de seguridad.

5. **Onboarding Digital**
   - Apertura de cuentas directamente desde la aplicación móvil
   - Validación de identidad mediante biometría y/o reconocimiento facial.
   - Captura de documentos mediante la cámara del dispositivo.

Calle 60a #5-54, Oficina 403
Bogotá D.C. Colombia
NIT. 830.101.214-4
+57 3222468120
www.colombiadigital.net

6. **Centro de Seguridad**
    - Configuración de notificaciones y alertas personalizadas.
    - Control de permisos y accesos.

Chatbots y asistentes virtuales

Para garantizar el uso efectivo de chatbots y asistentes virtuales en la plataforma tecnológica de la entidad, el proveedor deberá cumplir como mínimo con las siguientes obligaciones:

- **Entrenamiento y actualización continua de IA:** Asegurar que los chatbots y asistentes virtuales estén continuamente entrenados y actualizados con los últimos datos y tendencias para proporcionar respuestas precisas y relevantes.
- **Capacidad multilingüe**: Incluir soporte para múltiples idiomas, asegurando que los usuarios de diferentes orígenes puedan interactuar fácilmente con los chatbots.
- **Gestión de escalamiento**: Implementar un sistema eficiente para escalar consultas complejas a agentes humanos cuando sea necesario, garantizando una experiencia de usuario sin interrupciones.

El proveedor deberá garantizar con los siguientes aspectos de omnicanalidad

- Proporcionar herramientas de analítica avanzada para monitorear las interacciones de los usuarios y generar informes detallados que permitan mejorar continuamente el servicio.
- Configurar los chatbots para ofrecer respuestas personalizadas basadas en el perfil del usuario y su historial de interacciones.
- Realizar pruebas exhaustivas y validación del sistema antes de su implementación para asegurar que cumple con los estándares de calidad y funcionalidad requeridos.
- Estos chatbots y asistentes virtuales deben estar Integrados con IA para atención 24/7 en WhatsApp, redes sociales y banca en línea.
- Estos canales deben poder atender todos los servicios en idioma inglés y español.
- Los chatbots y asistentes virtuales debe integrarse con el core de depósito y los sistemas de soporte existentes a través de las arquitecturas de integración diseñadas para ello, asegurando una transferencia de datos.

Enfoque Omnicanalidad

El proveedor deberá garantizar un enfoque de omnicanalidad con los siguientes aspectos como mínimo:

- **Experiencia unificada:** Los clientes pueden iniciar una transacción en un canal (ej. Aplicación móvil) y terminarla en otro (ej. Portal web).
- **Sincronización de datos en tiempo real:** transacciones en línea y actualizaciones de datos en tiempo real.
- **Personalización y contexto:** Cada canal debe reconocer al usuario y su historial de interacciones.

3.6.2 UX/UI Optimizada con diseño accesible y adaptable

El proveedor está obligado a garantizar la correcta gestión, administración, configuración y optimización de la experiencia de usuario (UX) y la interfaz de usuario (UI), asegurando un diseño accesible, adaptable e intuitivo, alineado con los estándares de usabilidad y las necesidades de la entidad. Para ello, deberá implementar principios de diseño centrado en el usuario, asegurando una navegación fluida y eficiente en todos los dispositivos y plataformas. Asimismo, será responsable de la configuración y personalización de la interfaz, permitiendo su ajuste a diferentes perfiles de usuarios, incluidas personas con discapacidad, cumpliendo con normativas internacionales de accesibilidad (como WCAG). El proveedor deberá garantizar la escalabilidad y compatibilidad del diseño con tecnologías emergentes, evitando problemas de rendimiento o incompatibilidad. Además, deberá realizar pruebas de usabilidad periódicas, recolectando retroalimentación para la mejora continua de la experiencia digital. Finalmente, será responsable de ofrecer capacitación y soporte técnico especializado, asegurando que el equipo de la entidad pueda gestionar y evolucionar la plataforma sin afectar la experiencia del usuario.

Una experiencia fluida y atractiva aumenta la retención de clientes y reduce el abandono de procesos bancarios.

Adicional a lo anterior, el proveedor deberá cumplir con los siguientes requerimientos mínimos:

- **Diseño responsive y Mobile-First:** Interfaces adaptadas a distintos dispositivos.
- **Carga rápida y eficiencia:** Uso de caché, optimización de imágenes y CDNs.
- **Simplicidad y claridad:** Formularios cortos, procesos guiados y navegación.
- **Consistencia visual:** Mantener una identidad visual coherente en todos los canales.
- **Pruebas de usabilidad:** Realización de pruebas periódicas con usuarios reales para identificar y resolver problemas de usabilidad.
- **Retroalimentación continua:** Implementación de mecanismos para la recopilación de feedback de usuarios y su incorporación en mejoras continuas.
- Ofrecer los mecanismos necesarios para que los clientes tengan la posibilidad de personalizar las condiciones bajo las cuales realicen operaciones monetarias por los diferentes canales, siempre y cuando éstos lo permitan. En estos eventos se puede permitir que el cliente inscriba las cuentas a las cuales realizará transferencias, registre las direcciones IP fijas y el o los números de telefonía móvil desde los cuales operará.
- Permitir la actualización de datos del cliente para la notificación de operaciones monetarias o generación de alertas (p.ej. correo electrónico, celular).

3.6.3 Notificaciones y alertas en tiempo real

El proveedor está obligado a garantizar la correcta gestión, administración, configuración y operación del sistema de notificaciones y alertas en tiempo real, asegurando su precisión, seguridad y alineación con los requerimientos operativos de la entidad. Para ello, deberá implementar mecanismos de monitoreo continuo y respuesta inmediata, garantizando la entrega oportuna de notificaciones críticas a los clientes y a los sistemas internos de la entidad. Asimismo, será responsable de la configuración y personalización de las alertas, permitiendo su ajuste en función de los niveles de prioridad, canales de comunicación y segmentos de usuarios. El proveedor deberá asegurar la disponibilidad, redundancia y escalabilidad del sistema, evitando

retrasos o fallos en la entrega de mensajes. Además, deberá cumplir con normativas de seguridad y privacidad de la información, asegurando el cifrado y la protección de los datos transmitidos. Finalmente, deberá proporcionar capacitación y soporte técnico especializado, garantizando que el personal de la entidad cuente con el conocimiento y las herramientas necesarias para la gestión eficiente del sistema de notificaciones. Las notificaciones y alertas mantienen a los usuarios informados sobre su actividad financiera y aumentan la seguridad.

Adicional a lo anterior, el proveedor deberá cumplir con los siguientes requerimientos mínimos:

- **Push Notifications:** Para alertas en tiempo real (pagos, depósitos, alertas de fraude).
- **SMS:** Para recordatorios de pagos y OTPs de seguridad.
- **Correo Electrónico:** Comunicaciones detalladas sobre movimientos y productos.
- **WhatsApp/Telegram:** Mensajes transaccionales y atención al cliente.

Además de los métodos de envío, el proveedor debe garantizar lo siguiente:

- Los sistemas deben estar diseñados para ser altamente disponibles y reducir al mínimo los tiempos de inactividad.
- La infraestructura debe ser capaz de manejar un gran volumen de notificaciones simultáneamente sin degradar el rendimiento.
- Implementación de cifrado de extremo a extremo para proteger la información sensible durante el tránsito y almacenamiento.
- Capacidad para personalizar las notificaciones según las preferencias del usuario, incluyendo la frecuencia y el canal de recepción.
- Sistemas de monitoreo en tiempo real y registro detallado de todas las actividades para auditorías y resolución de problemas.
- Compatibilidad con diversas plataformas y dispositivos para asegurar que las notificaciones lleguen a todos los usuarios, independientemente del dispositivo que usen.
- El sistema debe ser accesible desde diferentes dispositivos y plataformas, garantizando una experiencia de usuario consistente.
- Utilizar tecnologías de reconocimiento y procesamiento de voz que permitan una interacción fluida y precisa con los usuarios.
- El sistema de notificaciones debe integrarse perfectamente con el core bancario y los sistemas de soporte existentes, asegurando una transferencia de datos sin problemas.

3.6.4 Personalización basada en IA

El proveedor está obligado a garantizar la correcta gestión, administración, configuración y entrenamiento de los sistemas de personalización basada en inteligencia artificial (IA), asegurando su desempeño óptimo, seguridad y alineación con los objetivos estratégicos de la entidad. Para ello, deberá administrar de manera continua los modelos de IA, optimizando su precisión y eficiencia en la personalización de servicios para los clientes. Además, deberá implementar mecanismos de gobernanza de datos, regulando el acceso, almacenamiento y procesamiento de la información utilizada por los algoritmos. Asimismo, el proveedor será responsable de la configuración, ajuste y mantenimiento de los modelos de IA, asegurando su actualización constante mediante el uso de datos relevantes y técnicas avanzadas de

entrenamiento. Deberá garantizar la transparencia de los modelos utilizados, permitiendo auditorías y supervisión por parte de la entidad y las entidades regulatorias. Finalmente, el proveedor deberá ofrecer entrenamiento especializado al personal de la entidad, asegurando el conocimiento y la correcta interpretación de los resultados generados por la IA, fomentando el uso ético y estratégico de la tecnología en la toma de decisiones. La inteligencia artificial permite adaptar la oferta y mejorar la experiencia del usuario.

Es por esto que para la entidad es fundamental la implementación de agentes cognitivos que permita gestionar solicitudes, responder requerimientos y ejecutar trámites de manera eficiente. Estos agentes, impulsados por inteligencia artificial (IA) y aprendizaje automático (ML), deben integrarse en la arquitectura tecnológica de la solución para ofrecer experiencias personalizadas, consistentes y en tiempo real a través de múltiples canales como web, aplicaciones móviles, contact centers e incluso redes sociales.

Dentro de los principales elementos funcionales están:

a. Gestión omnicanal

a. Capacidad para interactuar con los clientes a través de múltiples canales (web, app móvil, contact center, redes sociales) con una experiencia consistente.
b. Continuidad en las interacciones que permitan que un cliente inicie una consulta en un canal y la continúe en otro sin pérdida de información.
c. Integración con el Core de Deposito y otros sistemas (core contable, plataforma de BI/BA, repositorios de datos estructurados y no estructurados, Gestor Documental y demás componentes de la arquitectura) para acceder a datos del cliente en tiempo real.
d. Implementación de una memoria conversacional para contextualizar respuestas en diferentes sesiones y dispositivos.

b. Procesamiento del Lenguaje Natural (NLP)

a. Comprensión de consultas realizadas en lenguaje natural, tanto por texto como por voz.
b. Capacidad para identificar intenciones, emociones y contexto del cliente.
c. Uso de IA conversacional para comprender y responder consultas en lenguaje natural.
d. Soporte para múltiples idiomas y adaptación al contexto bancario.
e. Corrección de errores tipográficos y aprendizaje de patrones de uso.

c. Automatización de tareas

a. Resolución automatizada de solicitudes comunes como consultas de saldo, bloqueos de tarjetas, generación de estados de cuenta o actualizaciones de datos personales.
b. Escalamiento inteligente a agentes humanos cuando sea necesario, proporcionando contexto completo al operador.
c. Capacidad de ejecutar acciones en nombre del usuario previa autenticación.
d. Integración con el BPM para seguimiento de procesos internos.

d. Personalización y recomendaciones

a. Uso de analítica predictiva para anticipar necesidades del cliente y ofrecer recomendaciones personalizadas (por ejemplo, productos financieros relevantes).

b. Generación de respuestas adaptadas al perfil del cliente basado en su historial transaccional y preferencias.

Adicional a lo anterior, el proveedor deberá cumplir con los siguientes requerimientos mínimos:

- Generar ofertas de crédito cuando aplique.
- Atención en lenguaje natural con NLP.
- Prevención de fraudes y predicción de necesidades.
- Respuestas inteligentes y automatizadas de PQRS

3.7.5 Capacidades tecnológicas

En el entorno financiero actual, la importancia de contar con una plataforma tecnológica robusta, escalable, segura y fácil de utilizar no puede ser subestimada. Una plataforma de este tipo no solo garantiza la eficiencia operativa, sino que también mejora significativamente la experiencia del usuario, lo que es crucial para la retención y satisfacción del cliente.

Una plataforma robusta asegura que los servicios de ahorro estén disponibles de manera continua, minimizando el tiempo de inactividad y las interrupciones. Esto es esencial para mantener la confianza de los clientes y garantizar que puedan acceder a sus cuentas y realizar transacciones en cualquier momento y desde cualquier lugar.

La escalabilidad es otro aspecto fundamental. A medida que la entidad crece y la demanda de sus servicios aumenta, la plataforma debe ser capaz de manejar un mayor volumen de transacciones y usuarios sin comprometer el rendimiento. Esto permite a la entidad adaptarse rápidamente a las cambiantes necesidades del mercado y a las expectativas de los clientes.

La seguridad es, sin duda, una de las principales preocupaciones en el sector bancario. Una plataforma segura protege la información sensible de los clientes y previene el fraude y los ciberataques. Implementar medidas de seguridad avanzadas, como la autenticación multifactor y el cifrado de datos, es crucial para salvaguardar la integridad y la confidencialidad de los datos de los ahorradores.

Finalmente, la facilidad de uso es vital para garantizar que los clientes puedan navegar y utilizar la plataforma sin dificultades. Una interfaz intuitiva y amigable mejora la accesibilidad y la satisfacción del usuario, lo que a su vez puede traducirse en una mayor lealtad y recomendación del servicio.

Entendemos por plataforma tecnológica el conjunto de tecnologías, infraestructuras y servicios que permiten el desarrollo, ejecución y gestión de aplicaciones y procesos digitales dentro de la entidad o la organización. Estas plataformas pueden incluir hardware, software, redes, bases de datos y servicios en la nube, proporcionando un entorno cohesivo para la operación y evolución de soluciones tecnológicas.

3.7.5.1 Arquitectura general

La implementación de una arquitectura de plataforma de cuarta generación, cloud native en una plataforma bancaria moderna se justifica plenamente por la necesidad de escalabilidad, resiliencia, agilidad operativa y capacidad de innovación continua.

En primer lugar, se busca una infraestructura tecnológica sólida y flexible, que combine servidores escalables, almacenamiento seguro y redes de alto rendimiento, como base para ofrecer servicios financieros confiables. En este contexto, la arquitectura cloud native, basada en contenedores, microservicios, orquestación (Kubernetes) y CI/CD o tecnologías superiores, permite responder de forma ágil a los requerimientos del negocio y a la dinámica del mercado financiero digital.

El uso de tecnologías avanzadas como inteligencia artificial y analítica de datos requiere entornos altamente escalables y desacoplados, lo cual es inherente a la filosofía cloud native. Estas capacidades facilitan la entrega de servicios personalizados y proactivos, mejorando la experiencia del cliente y agregando valor estratégico a la entidad.

Además, los enfoques de despliegue continuo (CI/CD) y la automatización garantizan una evolución constante del sistema con mínima intervención manual, reduciendo errores y tiempos de entrega. Esto se traduce en una mayor estabilidad operativa, incluso durante actualizaciones o ante incrementos significativos en la demanda.

La arquitectura cloud native también potencia los beneficios de la nube híbrida, al integrarse perfectamente con entornos públicos y privados, permitiendo ubicar las cargas sensibles en infraestructura local y aprovechar la escalabilidad de la nube pública para otros componentes. Esto se alinea tanto con las necesidades regulatorias del sector financiero como con las estrategias de transformación digital del gobierno nacional.

La entidad hoy en día tiene 1 millón de usuarios activos, los cuales serán los primeros usuarios de la plataforma tecnológica desde sus interfaces Web y Movile, esto quiere decir que la arquitectura debe soportan en primera instancia este número de usuarios, luego de la salida a producción se espera en los 2 primeros meses la llegada de los primeros 50 mil usuarios, así las cosas, la plataforma es importante su atributo de calidad de escalabilidad sin dejar a un lado los demás de disponibilidad, usabilidad, seguridad, y los demás considerados en esta arquitectura.

Por lo anterior y teniendo en cuenta la necesidad de la entidad y del gobierno nacional se ha definido la implementación de una arquitectura para la plataforma tecnológica la cual ofrece los beneficios antes mencionados.

A continuación, se presenta un diagrama de alto nivel de lo que se espera de la arquitectura cloud.

Con lo anterior se presenta la arquitectura general de la plataforma la cual será tenida en cuenta para la presentación de la oferta

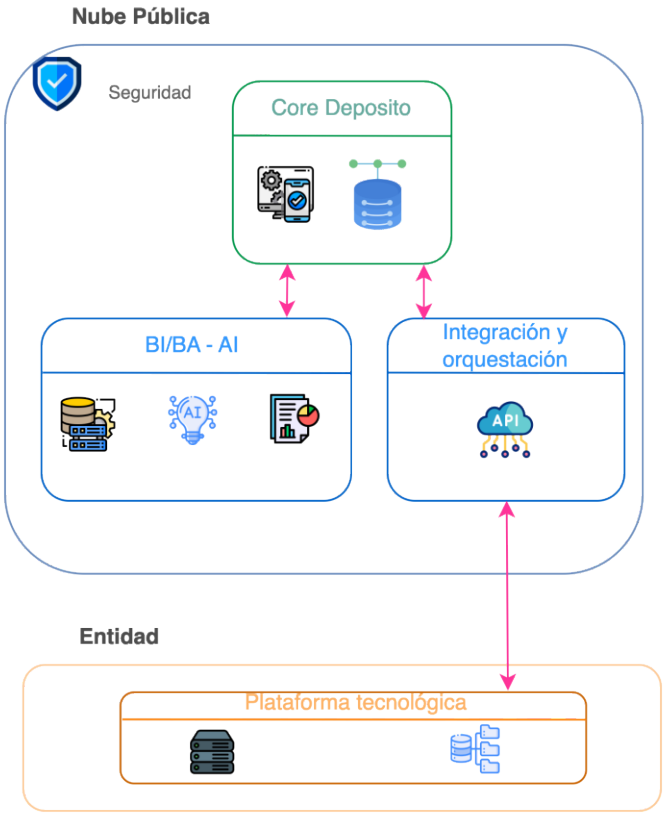


Ilustración 13 Arquitectura general

3.7.5.2 Gestión de nube pública

La gestión de la nube pública desempeña un papel crucial en la infraestructura tecnológica moderna, especialmente en entornos dinámicos y escalables como los de las entidades bancarias. La adopción de soluciones en la nube permite una mayor flexibilidad y agilidad, optimizando recursos y reduciendo costos operativos. Además, facilita la implementación de tecnologías avanzadas y la integración de diversas aplicaciones, mejorando la capacidad de respuesta ante cambios del mercado. La correcta gestión de la nube pública también garantiza la seguridad y el cumplimiento normativo, garantizando que todos los datos y procesos se mantengan protegidos y que las operaciones sean transparentes y auditable.

3.7.5.2.1 Requerimientos clave de infraestructura y despliegue

- El proveedor deberá facilitar el proceso de adquisición y activación de créditos de

consumo en la nube pública, asegurando su disponibilidad oportuna según el crecimiento proyectado. Además, deberá brindar acompañamiento en su aplicación para optimizar costos y evitar interrupciones por agotamiento presupuestal.

- El proveedor debe entregar informes mensuales sobre el estado de la infraestructura
- En el penúltimo bimestre del año, el proveedor deberá presentar a la entidad el plan de capacidad para el año siguiente.
- Además de todo lo anteriormente mencionado, el proveedor debe garantizar la operación de la plataforma con toda la infraestructura tecnológica necesaria para mantener esta en un óptimo funcionamiento y disponible.
- La periodicidad de los informes periódicos solicitados para las capacidades tecnológicas será acordado con la entidad en la reunión de inicio del proyecto.
- El proveedor debe implementar y mantener pipelines de CI/CD utilizando herramientas del mercado que utilicen mejores prácticas y tengan soporte de proveedor para la automatización de compilación, prueba e implementación de código.
- La infraestructura debe integrar controles de seguridad (DevSecOps) en cada fase del pipeline, incluyendo:
    - Escaneo de vulnerabilidades en el código y las dependencias.
    - Pruebas automatizadas de seguridad (SAST, DAST).
    - Validación de políticas de seguridad antes del despliegue.
- El proveedor debe garantizar que cualquier vulnerabilidad crítica detectada se corrija automáticamente o detenga el proceso de despliegue para evitar incidentes de seguridad.
- El proveedor debe garantizar una disponibilidad de al menos el 99.95% en los servicios prestados en la nube en los modelos Iaas y PaaS. Para aquellos proveedores del servicio de computación en la nube en el modelo Saas, la disponibilidad debe ser de al menos el 99.5%. para todos los servicios desplegados, mediante:
    - Implementación de balanceadores de carga en todos los entornos (y pública).
    - Monitoreo proactivo de la capacidad de respuesta y tiempos de respuesta de los servicios.
    - Redistribución automática de tráfico ante fallos o sobrecarga de los servidores.
- El proveedor debe implementar mecanismos de auto escalado en los servicios que así lo soporte y lo requiera, incluyendo kubernetes o tecnologías superiores y estables, para aumentar o reducir automáticamente los recursos en función de la demanda, asegurando que el tiempo de respuesta no supere 500 milisegundos en condiciones de alta carga.
- El proveedor deberá ofrecer soporte técnico especializado 24 horas al día, 7 días a la semana, con disponibilidad inmediata ante incidentes críticos, cubriendo tanto los servicios gestionados como las herramientas de monitoreo, redes, bases de datos, seguridad y los demás requeridos para garantizar la operación de la plataforma.
- Deberá implementar un sistema de monitoreo proactivo en tiempo real sobre el uso de recursos, rendimiento de los servicios y niveles de disponibilidad, incluyendo alertas tempranas ante posibles degradaciones, sobrecostos o interrupciones.
- El proveedor deberá mantener un inventario actualizado de todos los servicios desplegados en la nube y garantizar una política de respaldo automatizado y verificado, con copias cifradas almacenadas en distintas zonas de disponibilidad y cumplimiento del período de retención contractual.
- El proveedor deberá generar estrategias de ahorro cono el suso de instancias reservadas en los casos donde se pueda utilizar.
- Verificar que las jurisdicciones en donde se procesará la información cuenten con normas

equivalentes o superiores a las aplicables en Colombia, relacionadas con la protección de

datos personales y penalización de actos que atenten contra la confidencialidad, integridad y disponibilidad de los datos y de los sistemas informáticos.
- Las condiciones y limitaciones bajo las cuales se puede subcontratar parte del servicio o realizar cambios a los acuerdos establecidos con sus subcontratistas o partners.
- Las causales de terminación del contrato por parte de la entidad, incluyendo, el incumplimiento de los acuerdos o niveles de servicio o el cambio de las condiciones que generen impacto negativo al servicio contratado.

3.7.5.2.2 Respaldo

El proveedor está obligado a garantizar el respaldo de la plataforma tecnológica, asegurando la protección, disponibilidad e integridad de la información a través de mecanismos robustos de backup y recuperación ante desastres (DRP). Para ello, deberá implementar estrategias de respaldo automatizado, cifrado y almacenamiento en múltiples ubicaciones seguras, asegurando la continuidad del negocio ante posibles fallos, ataques cibernéticos o pérdidas de datos. Asimismo, deberá garantizar la disponibilidad de copias de seguridad con retención y versionado adecuado, permitiendo la restauración rápida y eficiente de la información en caso de incidentes. Es necesario articularse con la política de continuidad y recuperación de la entidad.

Además, deberá cumplir con normativas internacionales de gestión de datos y continuidad del negocio, realizando auditorías periódicas, pruebas de recuperación y monitoreo constante para asegurar la confiabilidad del servicio.

Adicional a lo anterior, el respaldo debe contar como mínimo con las siguientes características:

- Definir y ejecutar políticas de respaldo regular de datos críticos, asegurando que los respaldos se realicen de manera frecuente y automática.
- Asegurar la integridad de los respaldos mediante pruebas y verificaciones periódicas. Estas pruebas periódicas deberán realizarse al menos 6 veces al año.
- Guardar los respaldos en ubicaciones seguras y separadas de los sistemas principales para evitar pérdida de datos en caso de desastre.
- Generar el respectivo documento del procedimiento de gestión de respaldo y recuperación alineado con estándares de la industria como ITIL.
- Establecer políticas formales que especifiquen la periodicidad y características de los procedimientos de respaldo de datos e información.
- Mantener al menos tres copias de los conjuntos de datos y toda la información relevante, almacenadas en al menos dos soportes distintos, y asegurar que una de las copias se ubique en una localización diferente a la ubicación principal.
- Implementar sistemas de monitoreo que verifiquen regularmente la realización exitosa de los respaldos y detecten posibles fallos o inconsistencias.
- Mantener registros detallados de todas las actividades relacionadas con el respaldo y la recuperación de datos, facilitando las auditorías y el cumplimiento regulatorio.
- Asegurar que las prácticas de respaldo y recuperación cumplan con las leyes y regulaciones aplicables en materia de protección de datos y privacidad.
- Establecer mecanismos que permitan contar con respaldo de la información que se procesa en la nube, la cual debe estar a disposición de la entidad cuando así lo requiera.

- Garantizar la independencia de su información y de sus copias de respaldo de la información de las otras entidades que procesen en la nube. La independencia se puede dar a nivel lógico o físico.

3.7.5.2.3 Bases de datos

- **Administración y mantenimiento de bases de datos**
  - Garantizar la disponibilidad, integridad y rendimiento óptimo de las bases de datos que soportan la operación de la solución
  - Realizar monitoreo proactivo y continuo del estado de las bases de datos para prevenir interrupciones o degradación del servicio.

- **Configuración y optimización**
  - Configurar adecuadamente los motores de base de datos de acuerdo con las buenas prácticas y requerimientos de seguridad, rendimiento y escalabilidad.
  - Ejecutar tareas de optimización de consultas, índices, planes de ejecución y estructuras de almacenamiento.

- **Gestión de seguridad y cumplimiento**
  - Implementar mecanismos de cifrado en tránsito y en reposo, control de accesos y auditoría para proteger la información sensible de los usuarios y de la entidad.
  - Asegurar el cumplimiento de las normativas nacionales e internacionales relacionadas con la protección de datos personales (como la Ley 1581 de 2012 y sus decretos reglamentarios).

- **Gestión de respaldos y recuperación ante desastres**
  - Diseñar e implementar políticas de respaldo automatizado y recuperación ante fallos (disaster recovery), incluyendo pruebas periódicas de restauración.
  - Mantener una estrategia de alta disponibilidad y continuidad del negocio.
  - Articularse con la política de continuidad de negocio de la entidad.

- **Actualizaciones y parches**
  - Aplicar actualizaciones de software y parches de seguridad sobre los motores de base de datos que así lo requieran sin afectar la disponibilidad del servicio, coordinando con la entidad las ventanas de mantenimiento.

- **Escalabilidad y soporte técnico**
  - Asegurar que la arquitectura de base de datos sea escalable vertical y horizontalmente para responder a la evolución de la demanda y al crecimiento de los datos.
  - Proveer soporte técnico especializado en horarios acordados (24/7 si así se requiere), con niveles de servicio (ANS) claros y mecanismos de atención y escalamiento.

- **Documentación y trazabilidad**

- Entregar documentación técnica actualizada de la arquitectura, configuración, políticas de respaldo, restauración y gestión de usuarios de las bases de datos.
- Registrar y reportar todas las intervenciones, cambios y eventos relevantes ocurridos en las bases de datos.

- **Interoperabilidad y soporte a integraciones**
  - Garantizar que las bases de datos puedan integrarse eficientemente con los sistemas transaccionales, analíticos, de recaudo, de atención al usuario y demás componentes de la plataforma tecnológica.
  - Asegurar que los servicios expuestos por la base de datos (APIs, conectores, etc.) cumplan con estándares abiertos y políticas de interoperabilidad.

- **Participación en el ciclo de vida del sistema**
  - Acompañar los despliegues de nuevas funcionalidades, cambios o migraciones de la plataforma tecnológica que requieran intervención en las bases de datos.
  - Participar en la planeación, diseño, pruebas y puesta en producción de los ambientes de pruebas y productivos.

- **Auditoría y detección de incidentes**
  - Auditar periódicamente las bases de datos y aplicaciones asociadas al producto, asegurando que los registros de auditoría estén activos y capturen todas las acciones realizadas por los usuarios. Esta práctica es esencial para fortalecer la trazabilidad y facilitar la detección y análisis de posibles incidentes de seguridad, permitiendo una respuesta oportuna y eficaz ante cualquier amenaza al entorno tecnológico.

3.7.5.2.4 Seguridad de la nube

El proveedor está obligado a garantizar la seguridad perimetral de la plataforma 100% en línea, implementando y gestionando de manera continua mecanismos de protección avanzados que resguarden la infraestructura contra accesos no autorizados, ciberataques y vulnerabilidades. Esto incluye la configuración y monitoreo de firewalls de nueva generación, sistemas de detección y prevención de intrusos (IDS/IPS), segmentación de red y cifrado avanzado de comunicaciones, asegurando una defensa multicapa que prevenga incidentes de seguridad.

Adicionalmente, deberá garantizar el cumplimiento de normativas internacionales en materia de seguridad de la información, manteniendo auditorías periódicas y reportes de cumplimiento. Esta obligación cobra especial relevancia ante el crecimiento proyectado de nuevos usuarios, lo que demanda una infraestructura escalable y resiliente que permita operar con altos niveles de disponibilidad, integridad y confidencialidad.

Adicionalmente, los componentes de seguridad perimetral deben contar como mínimo con las siguientes características:

3.7.5.2.4.1 Administración y Gestión del Firewall de Nueva Generación (NGFW)

3.7.5.2.4.1.1 Configuración y Endurecimiento del Firewall

- **Definición y administración de reglas**
  - Implementar y mantener reglas de acceso basadas en principio de privilegio mínimo (Least Privilege).
  - Configurar listas de control de acceso (ACLs) estrictas para tráfico entrante y saliente.
  - Implementar reglas de segmentación de red para evitar movimientos laterales en caso de una intrusión.
  - Revisar y optimizar reglas mínimo cada 3 meses para evitar configuraciones obsoletas.

- **Filtrado de aplicaciones y protocolos**
  - Configurar reglas de filtrado de tráfico basadas en aplicaciones y servicios específicos (App Control).
  - Bloquear tráfico no autorizado o aplicaciones de riesgo (P2P, redes sociales, proxies, etc.).
  - Monitorear y restringir el uso de protocolos inseguros (ej. Telnet, FTP, SMB sin cifrado).

- **Filtrado de contenido Web**
  - Implementar políticas de filtrado para bloquear sitios maliciosos, phishing y contenidos inapropiados.
  - Integración con bases de datos de amenazas en tiempo real para detectar sitios peligrosos.

- **Protección contra amenazas avanzadas**
  - Implementar y gestionar mecanismos de detección y bloqueo de malware en el tráfico de red.
  - Integración con herramientas de Threat Intelligence para actualizar listas de amenazas emergentes.

- **Gestión de cifrado y VPN**
  - Configuración de VPNs seguras para acceso remoto con cifrado TLS 1.3 / IPSec AES-256.
  - Aplicación de certificados digitales actualizados para cifrado de tráfico.
  - Cifrado de extremo a extremo para comunicaciones seguras entre usuarios y servicios bancarios.
  - Protección contra interceptación de datos en redes inseguras.
  - Integración con autenticación multifactor (MFA) para mayor seguridad.

- **Consideraciones adicionales**
  - El proveedor deberá garantizar que los firewalls estén configurados siguiendo las mejores prácticas de seguridad y estándares bancarios.
  - El proveedor debe garantizar que la configuración del firewall se realice con expertos en la tecnología de la fabricante seleccionada para proveer el firewall
  - El firewall debe soportar como mínimo los siguientes algoritmos de cifrado:

- AES (Advanced Encryption Standard): AES-256 es ampliamente utilizado debido a su alta seguridad y eficiencia. Es ideal para cifrar datos en reposo y en tránsito.
- TLS (Transport Layer Security): TLS 1.3 es la versión más reciente y segura, utilizada para proteger las comunicaciones en línea, como las transacciones bancarias.
- RSA (Rivest-Shamir-Adleman): Utilizado para el cifrado de datos y la autenticación, especialmente en la protección de claves de cifrado.
- ECC (Elliptic Curve Cryptography): Ofrece un alto nivel de seguridad con claves más pequeñas, lo que lo hace eficiente para dispositivos con recursos limitados.

Mantenimiento preventivo

- **Inspección y validación periódica**
  - Verificación del estado del hardware y rendimiento de los firewalls.
  - Revisión de configuraciones de seguridad para detectar inconsistencias.
  - Aplicación de pruebas de resiliencia y pruebas de carga periódicas para validar capacidad.

- **Gestión de Logs y registros de seguridad**
  - **Almacenamiento de logs** por al menos **12 meses** para auditorías y cumplimiento normativo. Luego de estos 12 meses se enviarán a respaldo para su posterior retención, alineado con la tabla de retención documental de la entidad.
  - Revisión periódica de logs para identificar **comportamientos anómalos o intentos de intrusión**.

- **Pruebas de seguridad y simulación de ataques**
  - **Pruebas de penetración (Pentesting)** cada 6 meses para identificar vulnerabilidades.
  - Simulación de ataques de denegación de servicio (DDoS) para verificar protección.
  - Otras pruebas de seguridad que sean relevantes para la peración.

- **Monitoreo y reportes de seguridad**
  - Monitoreo continuo 24/7
  - Alertas y respuesta automática
  - Monitoreo en tiempo real del tráfico de red y actividad sospechosa.
  - Implementación de alertas automáticas ante detección de ataques, accesos no autorizados o cambios inesperados en reglas de firewall.

- **Análisis de comportamiento y Machine Learning**
  - Integración con herramientas de IA para detectar anomalías y ataques en curso.
  - Generación de perfiles de tráfico para identificar accesos sospechosos.

- **Integración con Sistemas de Detección de Intrusos (IDS/IPS)**
  - Envío de datos a plataformas SIEM (Splunk, QRadar, ArcSight) para correlación con otros eventos de seguridad.

- Implementación de Threat Intelligence Feeds para mitigar amenazas en tiempo real.

- **Reportes de incidentes y auditoría**
  - Generación de informes periódicos detallados sobre intentos de intrusión, reglas modificadas y tráfico bloqueado.
  - Reportes de cumplimiento con estándares de seguridad (ISO 27001, PCI DSS, SWIFT CSP).
  - Reuniones mensuales de evaluación de Seguridad entre la entidad y el proveedor.

- **Cumplimiento normativo y seguridad contractual**

El proveedor debe cumplir como mínimo con las siguientes obligaciones de cumplimiento normativo y contractual:

- **Cumplimiento de Normativas y Estándares Internacionales**
  - ISO 27001: Gestión de seguridad de la información.
  - PCI DSS: Protección de datos de tarjetas bancarias.
  - SWIFT CSP: Seguridad en transacciones financieras internacionales.
  - El proveedor debe garantizar que la administración del firewall cumpla con las regulaciones bancarias y de ciberseguridad actuales, esto implica realizar cualquier cambio que se requiera en los firewalls en caso de alguna regulación o norma nueva.

- **Políticas de seguridad y confidencialidad**
  - Implementación de acceso basado en roles (RBAC) para administración de firewall.
  - Registro de cada cambio realizado en las reglas de seguridad con trazabilidad.
  - Uso de cifrado fuerte (AES-256, TLS 1.3) para comunicaciones con el firewall.

- **Consideraciones adicionales**
  - El proveedor debe realizar mantenimiento continuo para garantizar el correcto funcionamiento y disponibilidad del firewall.
  - Almacenar y revisar los logs de seguridad para detectar comportamientos anómalos y realizar auditorías periódicas
  - Realizar copias de seguridad regulares de las configuraciones de los firewalls para poder restaurarlas en caso de fallos o ataques.
  - Verificar el estado físico del hardware de los firewalls y asegurarse de que esté en condiciones óptimas.

Mantenimiento correctivo

- **Respuesta a incidentes de seguridad**
  - El proveedor deberá contar con protocolos de respuesta inmediata ante incidentes de seguridad.
  - Realizar una evaluación inicial del incidente para determinar su alcance, impacto y origen, a fin de contenerlo rápidamente.

- Establecer un equipo de respuesta especializado para manejar el incidente y coordinar acciones con otras partes involucradas según sea necesario.
- Documentar todas las acciones realizadas durante la gestión del incidente para análisis posterior y mejora de los protocolos de seguridad.

- **Gestión de fallos y recuperación ante desastres**
  - Implementación de firewalls redundantes en alta disponibilidad (HA - High Availability).
  - Restauración de configuraciones desde backups automáticos programados.

- **Soporte 24/7 y mesa de ayuda**
  - Disponibilidad de soporte técnico especializado en modo 24/7/365.
  - Soporte remoto e in-situ en casos de fallos críticos.
  - Asignación de ingenieros certificados en la marca del firewall contratado.

- **Consideraciones adicionales**
  - El proveedor debe garantizar una supervisión continua y reportes periódicos detallados sobre la seguridad del firewall.
  - Disponibilidad garantizada: 99.5%
  - Auditorías externas de seguridad: Cada 6 meses
  - Presentación periódica de hallazgos, incidentes y ajustes recomendados.
  - Validación de efectividad de políticas de seguridad y propuesta de mejoras.

3.7.5.2.4.2 Sistema de Prevención y Detección de Intrusos (IDS/IPS)

El proveedor de tecnología deberá garantizar la administración, gestión y configuración del **Sistema de Prevención y Detección de Intrusos (IDS/IPS)** para proteger la infraestructura y los servicios de la solución contra ataques cibernéticos, accesos no autorizados y vulnerabilidades explotables.

Adicional a lo anterior debe cumplir como mínimo con las siguientes obligaciones

3.7.5.2.4.2.1 Configuración del IDS/IPS

El proveedor será responsable de la implementación, ajuste y optimización del IDS/IPS con base en los requerimientos de seguridad de la entidad. A continuación, las obligaciones mínimas.

Implementación y configuración

- **Definición de políticas de seguridad:**
  - Configuración de políticas de detección y prevención alineadas con estándares como NIST, PCI-DSS e ISO 27001, ISO 27017 y 27018.
  - Implementación de reglas basadas en firma (signature-based) y análisis de comportamiento (anomaly-based).
  - Configuración de listas blancas y negras de direcciones IP y servicios críticos.

- **Segmentación y protección de la red:**

- Implementación de IDS/IPS en zonas estratégicas (frontera perimetral, DMZ, red interna).
- Microsegmentación para proteger tráfico sensible entre aplicaciones bancarias.
- Activación de detección de tráfico lateral para identificar movimientos internos maliciosos.

- **Integración con herramientas de seguridad:**
  - Envío de eventos a un SIEM para correlación de amenazas.
  - Integración con firewall perimetral y sistemas de seguridad de endpoints (EDR/XDR).
  - Uso de Threat Intelligence Feeds para actualizar reglas ante nuevas amenazas.

- **Optimización de reglas y filtros**

A continuación, se presenta las obligaciones mínimas a cumplir de este componente

- **Ajuste fino de sensibilidad del IDS/IPS:**
  - Configuración de umbrales de falsos positivos y falsos negativos para minimizar alertas innecesarias.
  - Ajuste de reglas en función del tráfico legítimo (reducción de alertas irrelevantes).
  - Evaluación mensual de efectividad de firmas y heurísticas para detección de ataques.

- **Bloqueo automático de amenazas (Modo IPS):**
  - Implementación de reglas dinámicas de bloqueo para ataques en tiempo real.
  - Creación de acciones automatizadas ante ataques recurrentes (ejemplo: bloqueo de IPs maliciosas).
  - Pruebas trimestrales de detección y respuesta con ataques simulados.

- **Definición de acciones de respuesta:**
  - Configuración de alertas en tiempo real a equipos de seguridad.
  - Registro de eventos en logs centralizados y encriptados.
  - Implementación de flujos de respuesta automática en caso de ataques críticos.

3.7.5.2.4.2.1.1 Mantenimiento preventivo y correctivo

El mantenimiento del IDS/IPS garantizará su efectividad en la detección y prevención de amenazas, asegurando disponibilidad y actualización constante.

A continuación, las obligaciones mínimas.

Mantenimiento preventivo

- **Actualización de firmas y algoritmos de detección:**
  - Aplicación de nuevas firmas de amenazas cada 24 horas.
  - Evaluación de algoritmos de machine learning para detección de anomalías en tráfico.
  - Pruebas trimestrales de detección de amenazas emergentes.

- **Monitoreo del desempeño del IDS/IPS:**
  - Verificación de carga y latencia del tráfico inspeccionado.

- Evaluación de impacto en el rendimiento de la red y ajustes de reglas si es necesario.
- Implementación de balanceo de carga para alto tráfico.

- **Revisión de configuraciones y pruebas de seguridad:**
  - Auditoría mensual de configuración de reglas activas.
  - Simulación semestral de ataques DDoS, SQL Injection, Ransomware y Zero-day.
  - Pruebas de recuperación ante fallas y reinicio forzado del sistema.

- **Backup de configuración:**
  - Generación de copias de seguridad de la configuración del IDS/IPS cada 7 días.
  - Pruebas de restauración en entornos aislados.

- **Consideraciones adicionales**
  - Aplicar parches y actualizaciones de software de manera oportuna para corregir vulnerabilidades y mejorar la funcionalidad del IDS/IPS.
  - Configurar alertas en tiempo real para notificar al equipo de soporte sobre incidentes críticos.
  - Establecer un protocolo de respuesta a incidentes para gestionar y mitigar cualquier amenaza detectada por el IDS/IPS. Este protocolo debe ser socializado con la entidad en la fecha establecida por las dos partes luego de la firma del contrato.
  - El protocolo debe ser revisado y ajustado cada año de ser necesario.

Mantenimiento correctivo

- **Protocolos de respuesta a fallos:**
  - Análisis y diagnóstico: Revisión de logs, eventos y consumo de recursos.
  - Acciones de contención: Aplicación de medidas temporales para minimizar impacto.
  - Corrección y validación: Aplicación de fix y validación de estabilidad del sistema.
  - Reporte y análisis Post-Incidente: Documento con lecciones aprendidas y mejoras.

- **Recuperación ante desastres:**
  - Implementación de redundancia activa-activa o activo-pasivo del IDS/IPS.
  - Pruebas de failover semestrales para validar conmutación sin interrupciones.
  - Restauración rápida desde backups recientes en caso de corrupción de datos.

3.7.5.2.4.3 Web Application Firewall (WAF)

El proveedor de tecnología será responsable de la administración, gestión y configuración del Web Application Firewall (WAF) para proteger la solución tecnológica de la entidad contra ataques, accesos no autorizados y vulnerabilidades explotables.

3.7.5.2.4.3.1 Configuración del WAF

El proveedor deberá realizar una implementación segura y optimizada del WAF de acuerdo con las mejores prácticas de seguridad y cumplimiento normativo. Adicional a lo anterior, el proveedor deberá cumplir con las siguientes obligaciones mínimas de la configuración.

- **Definición de políticas de seguridad:**
  - Implementación de reglas para detectar y bloquear ataques web (OWASP Top 10: SQL Injection, XSS, CSRF, etc.).
  - Configuración de listas blancas y negras para controlar accesos permitidos y bloqueados.
  - Aplicación de políticas de geolocalización para restringir accesos desde ubicaciones no autorizadas.

- **Protección de APIs y aplicaciones Web:**
  - Configuración de protección específica para APIs REST y SOAP.
  - Inspección profunda del tráfico HTTP/S para detectar solicitudes maliciosas.
  - Implementación de control de acceso basado en identidad (autenticación multifactor).
- **Integración con otros sistemas de seguridad:**
  - Envío de eventos al SIEM para correlación de amenazas.
  - Sincronización con firewall perimetral y sistema de prevención de intrusos (IPS).
  - Uso de Threat Intelligence Feeds para detección proactiva de amenazas emergentes.

3.7.5.2.4.3.2 Mantenimiento preventivo y correctivo

El proveedor garantizará el mantenimiento del WAF para asegurar su **efectividad y disponibilidad** en la protección de aplicaciones web. Adicional a lo anterior, el proveedor deberá cumplir con las siguientes obligaciones mínimas de mantenimiento.

Mantenimiento preventivo

- **Actualización de firmas y reglas de seguridad:**
  - Aplicación de **firmas de amenazas y vulnerabilidades** cada **24 horas**.
  - Evaluación de **nuevas amenazas** y actualización de políticas de mitigación.
  - Pruebas de penetración trimestrales para evaluar la efectividad del WAF.

- **Monitoreo del desempeño del WAF:**
  - Revisión de **latencia y tiempos de respuesta** en tráfico inspeccionado.
  - Verificación de **impacto en el rendimiento de las aplicaciones web**.
  - Ajuste de configuraciones para **optimizar el uso de recursos**.

- **Revisión de configuraciones y pruebas de seguridad:**
  - Auditoría mensual de **configuración de reglas activas**.
  - Simulación semestral de ataques **DDoS, Zero-day y Web Exploits**.
  - Pruebas de recuperación ante fallas y reinicio del sistema.

- **Backup de configuración:**

- Generación de copias de seguridad de la configuración del WAF cada **7 días**.
- Pruebas de restauración en entornos de prueba.

3.7.5.2.4.4 Balanceador de Carga con Seguridad (ADC - Application Delivery Controller)

El proveedor deberá garantizar una implementación robusta y segura del ADC, asegurando el balanceo eficiente de tráfico y la protección contra amenazas. Adicional a lo anterior, el proveedor deberá cumplir con las siguientes obligaciones mínimas de la configuración.

3.7.5.2.4.4.1 Implementación y configuración inicial

- **Definición de estrategias de balanceo:**
  - Implementación de balanceo de carga Layer 4 (TCP/UDP) y Layer 7 (HTTP/HTTPS).
  - Configuración de algoritmos de balanceo según necesidades de la entidad:
    - Round Robin (Distribución equitativa).
    - Least Connections (Menos conexiones activas).
    - IP Hash (Permanencia de sesión por IP).
    - Weighted Least Response Time (Tiempo de respuesta más corto).

- **Alta Disponibilidad (HA) y tolerancia a fallos:**
  - Implementación de clústeres activos-activos o activos-pasivos para redundancia.
  - Configuración de failover automático para continuidad operativa.
  - Sincronización de configuración entre nodos redundantes.

- **Optimización del rendimiento de aplicaciones:**
  - Configuración de compresión y caching de contenido para reducir la latencia.
  - Activación de Offloading SSL/TLS para aliviar la carga en los servidores backend.
  - Implementación de HTTP Keep-Alive y optimización de headers.

- **Protección contra ataques y seguridad integrada:**
  - Configuración de protección contra DDoS en capa 4 y 7.
  - Integración con Web Application Firewall (WAF) para filtrado avanzado.
  - Implementación de políticas de Rate Limiting para mitigar ataques de fuerza bruta.

- **Gestión de sesiones y persistencia:**
  - Configuración de Sticky Sessions cuando la aplicación lo requiera.
  - Habilitación de cookie-based persistence para garantizar continuidad en transacciones.

- **Integración con Infraestructura de la entidad:**
  - Sincronización con Active Directory (AD) o LDAP para autenticación de usuarios.
  - Integración con Sistemas de Monitoreo (SNMP, Syslog, Prometheus, Zabbix, etc.).
  - Configuración de reportes detallados de tráfico, errores y métricas de desempeño.

3.7.5.2.4.4.2 Ajuste y optimización de configuraciones

- **Monitoreo y ajuste de carga:**
  - Implementación de métricas de rendimiento para balanceo dinámico.
  - Ajuste de estrategias de balanceo según demanda y comportamiento del tráfico.

- **Optimización de seguridad y protocolos:**
  - Habilitación de TLS 1.2 y 1.3 con cifrados robustos (AES-256, RSA, ECC).
  - Bloqueo de conexiones con protocolos inseguros (SSL 3.0, TLS 1.0/1.1).
  - Aplicación de restricciones de acceso basadas en listas blancas y negras.

- **Pruebas de resiliencia:**
  - Simulación de pruebas de carga y estrés para validar rendimiento.
  - Evaluación de respuesta ante ataques de inyección de tráfico anómalo.

3.7.5.2.4.4.3 Mantenimiento preventivo y correctivo

El proveedor garantizará el mantenimiento continuo del ADC para asegurar su estabilidad, rendimiento y seguridad. Adicional a lo anterior, el proveedor deberá cumplir con las siguientes obligaciones mínimas de mantenimiento.

Mantenimiento Preventivo

- **Actualización de Firmware y Parches de Seguridad:**
  - Aplicación de actualizaciones trimestrales para corregir vulnerabilidades.
  - Validación de compatibilidad antes de cada actualización.
  - Implementación de parches de emergencia ante vulnerabilidades críticas.

- **Monitoreo Continuo y Análisis de Logs:**
  - Monitoreo en tiempo real del tráfico y detección de anomalías.
  - Análisis de logs de eventos y errores con alertas automáticas.
  - Integración con SIEM corporativo para correlación de eventos.

- **Pruebas de Continuidad Operativa:**
  - Simulación de failover cada 6 meses para validar redundancia.
  - Pruebas de desempeño con tráfico simulado y carga elevada.

- **Revisión de Políticas de Balanceo:**
  - Ajuste de algoritmos según patrones de tráfico y necesidades de la entidad.
  - Análisis de carga en servidores backend y optimización de reglas de distribución.

- **Backups de Configuración:**
  - Copias de seguridad semanales de configuraciones críticas.
  - Almacenamiento en servidores seguros con acceso restringido.
  - Restauración y verificación en entornos de prueba.

3.7.5.2.4.5 Monitoreo y Análisis de Seguridad (SIEM & SOAR)

El proveedor de tecnología será responsable de la implementación, administración y optimización de las plataformas SIEM (Security Information and Event Management) y SOAR (Security Orchestration, Automation, and Response), con el fin de fortalecer la visibilidad de seguridad, la correlación de eventos y la respuesta automatizada ante incidentes en la plataforma.

El proveedor deberá garantizar una implementación robusta y alineada con las mejores prácticas de seguridad, asegurando la correlación efectiva de eventos y una respuesta eficiente ante incidentes. Adicional a lo anterior, el proveedor deberá cumplir con las siguientes obligaciones mínimas de la configuración.

3.7.5.2.4.5.1 Implementación y configuración Inicial

- **Diseño e Implementación del SIEM**
  - Instalación y configuración de la solución SIEM.
  - Definición de **casos de uso de seguridad específicos para el sistema financiero**, como:
    - Detección de accesos no autorizados a sistemas críticos.
    - Identificación de transacciones fraudulentas o anomalías en comportamiento de usuarios.
    - Alertas sobre conexiones sospechosas a firewalls, IDS/IPS y WAF.
    - Monitoreo de tráfico anómalo en balanceadores de carga y VPN.
    - Correlación de eventos entre diferentes fuentes de datos.

- Configuración de **recolección centralizada de logs** desde:
  - Firewalls y dispositivos perimetrales.
  - Servidores y bases de datos críticos.
  - Endpoints y dispositivos móviles.
  - Aplicaciones bancarias y sistemas core.
  - Directorio Activo (AD) y servicios de autenticación.

- **Implementación de reglas de correlación y alertamiento**
  - Desarrollo de **reglas personalizadas** para identificar amenazas avanzadas.
  - Configuración de **umbral de alertas y niveles de criticidad**.
  - Integración con soluciones de threat intelligence para detección de amenazas emergentes.
  - Aplicación de **detección basada en machine learning** para análisis de comportamiento de usuarios (UEBA - User and Entity Behavior Analytics).

- **Integración con SOAR para respuesta automática a incidentes**
  - Implementación de **flujos de automatización** para respuesta rápida ante eventos críticos.
  - Configuración de **playbooks de respuesta** para eventos como:
    - Bloqueo automático de direcciones IP sospechosas.
    - Desactivación temporal de cuentas comprometidas.
    - Notificación y escalamiento automático de incidentes a equipos de respuesta.
  - Orquestación con herramientas de seguridad como **EDR/XDR, IDS/IPS, WAF y antivirus**.

- **Dashboards y reportes en tiempo real**
  - Creación de **tableros personalizados** con métricas clave de seguridad.
  - Generación de **reportes de cumplimiento** con normativas como PCI DSS, ISO 27001 y NIST.
  - Implementación de vistas específicas para el equipo de seguridad y directivos de la entidad.

3.7.5.2.4.5.2 Ajuste y optimización de configuraciones

- **Monitoreo y ajuste de reglas de correlación**
  - Revisión periódica de **falsos positivos y negativos** en reglas de correlación.
  - Ajuste de reglas para mejorar la precisión en la detección de amenazas.
  - Incorporación de **nuevas fuentes de datos y amenazas emergentes**.

- **Optimización del procesamiento de datos**
  - Ajuste de **políticas de retención de logs** según requisitos regulatorios.
  - Optimización del almacenamiento para mejorar la velocidad de análisis.
  - Implementación de **indexación eficiente** para búsqueda rápida de eventos.
  -
- **Evaluación de la eficiencia de la respuesta automática (SOAR)**
  - Análisis de **impacto de las automatizaciones** en la mitigación de amenazas.
  - Refinamiento de **playbooks** para mejorar la efectividad de la respuesta automática.
  - Simulación de incidentes para evaluar la capacidad de respuesta.

3.7.5.2.4.5.3 Mantenimiento preventivo y correctivo

El proveedor garantizará el mantenimiento continuo del SIEM & SOAR para asegurar su disponibilidad, rendimiento y efectividad en la detección de amenazas. Adicional a lo anterior, el proveedor deberá cumplir con las siguientes obligaciones mínimas de mantenimiento.

Mantenimiento preventivo

- **Actualización de la plataforma SIEM & SOAR**
  - Aplicación de **parches y actualizaciones** trimestrales para mejorar funcionalidades y corregir vulnerabilidades.
  - Validación de compatibilidad con nuevos dispositivos de seguridad.
- **Monitoreo del rendimiento del SIEM & SOAR**
  - Evaluación del uso de CPU, memoria y almacenamiento.
  - Optimización de la ingesta y procesamiento de logs para evitar cuellos de botella.
  - Pruebas de carga para validar la capacidad del sistema ante aumentos de tráfico.
- **Revisión de integraciones y conectividad**
  - Verificación de conectividad con dispositivos y fuentes de datos.
  - Revisión de sincronización con sistemas externos como WAF, IDS/IPS y EDR.
  - Informes mensuales de detección de amenazas y tiempos de respuesta.
  - Revisión trimestral con la entidad para optimización de reglas y automatización.
- **Simulación de ataques y evaluación de detección**

- Ejecución de pruebas de **red teaming y ethical hacking** para validar detección de amenazas.
- Ajuste de reglas y algoritmos de machine learning según resultados de simulaciones.

- **Backups de configuración y Logs**
  - Copias de seguridad periódicas de **configuraciones clave**.
  - Almacenamiento seguro y cifrado de logs históricos para auditorías.

Con respecto al monitoreo continuo es necesario que la solución se integre con el nuevo equipo antifraude un monitoreo continuo de las transacciones realizadas en la plataforma, con el fin de identificar actividades sospechosas y generar alertas tempranas. Esto mejora la capacidad de respuesta ante fraudes o comportamientos anómalos, reforzando la prevención y mitigación de riesgos. Es importante continuar implementado un equipo de ciberseguridad.

3.7.5.2.5 Inteligencia de negocios, analítica de negocios e inteligencia artificial

El proveedor debe encargarse de la implementación, gestión y mantenimiento de una plataforma de datos moderna que combine las capacidades de un LakeHouse o tecnologías avanzadas, garantizando la escalabilidad y alta disponibilidad. Es esencial que la plataforma soporte el procesamiento en tiempo real de datos estructurados, semiestructurados y no estructurados, y que garantice la disponibilidad y consistencia de los datos tanto en ambientes on-premise como en nube pública. También es crucial que permita el procesamiento de eventos en tiempo real utilizando tecnologías de Big Data con soporte adecuado, y que soporte la ejecución de modelos de Machine Learning para casos críticos como la predicción de impagos, el análisis de fraudes y el análisis del comportamiento de clientes.

A continuación, se especifica los requerimientos mínimos con que debe contar la plataforma de datos:

a. Implementación, gestión y mantenimiento de una plataforma de datos moderna

- El proveedor debe implementar una plataforma de datos que combine las capacidades de un LakeHouse o tecnologías que lo mejoren en el futuro, asegurando escalabilidad y alta disponibilidad.
- La plataforma debe soportar el procesamiento de datos estructurados, semiestructurados y no estructurados en tiempo real.
- Debe garantizar la disponibilidad y consistencia de los datos en ambientes de nube pública
- El proveedor debe garantizar que la plataforma permita el procesamiento de eventos en tiempo real mediante tecnologías de Big Data con soporte de proveedor
- Debe soportar la ejecución de modelos de Machine Learning para casos de uso críticos como:
  - Scoring de crédito.
  - Predicción de impagos.
  - Análisis de fraudes.
  - Análisis de comportamiento de clientes.
- La infraestructura debe garantizar tiempos de respuesta inferiores a 500 milisegundos para eventos críticos.

- La plataforma debe permitir la integración nativa con herramientas de BI reconocidas del mercado y con soporte de proveedor.
- El proveedor debe asegurar que las interfaces para el consumo de datos estén disponibles mediante APIs y conectores estándar (ODBC/JDBC).
- Debe permitir la creación de paneles y reportes en tiempo real para la toma de decisiones estratégicas.
- El proveedor debe garantizar la capacidad de desarrollar, entrenar, validar e implementar modelos de Machine Learning, e inteligencia artificial en la plataforma.
- Los modelos deben actualizarse automáticamente con base en el comportamiento del mercado y los patrones de los clientes.
- El proveedor debe garantizar que los modelos de Machine Learning y/o inteligencia artificial se ajusten automáticamente mediante **procesos de autoaprendizaje** (reinforcement learning).

b. Gobernanza, seguridad y calidad de datos

- El proveedor debe implementar un modelo de gobernanza de datos que garantice:
  - La integridad y trazabilidad de los datos desde el origen hasta el consumo.
  - La clasificación y catalogación de los datos mediante un diccionario de datos y un catálogo centralizado.
  - El establecimiento de políticas de retención, anonimización y destrucción de datos conforme a normativas nacionales e internacionales (como ISO 27001 y GDPR).
- La plataforma debe permitir el monitoreo y validación automática de la calidad de datos (completitud, consistencia, unicidad y precisión).
- El proveedor debe garantizar que todos los datos en tránsito y en reposo estén cifrados mediante **AES-256** o equivalente.
- La plataforma debe implementar controles de acceso basados en roles (RBAC) y políticas de segregación de datos.
- Debe implementar mecanismos de autenticación multifactor (MFA) y gestión de identidades (IAM).
- El proveedor debe garantizar la protección contra ataques mediante firewalls de aplicaciones (WAF) y detección de intrusiones (IDS/IPS).
- El proveedor debe garantizar que la plataforma permita la exportación e importación de datos entre múltiples plataformas y formatos (Parquet, Avro, CSV, JSON).
- La plataforma debe permitir la migración de datos entre entornos **nubes pública y/o ambientes on premise** sin pérdida de datos o interrupción de servicio.
- Debe asegurar que los datos estén disponibles para consumo mediante protocolos estándar (REST, ODBC, JDBC).

c. Soporte y mantenimiento

- La plataforma debe permitir el escalado horizontal y vertical para soportar incrementos en la carga de trabajo y volumen de datos sin afectar el rendimiento.
- El proveedor debe garantizar un **tiempo de respuesta** inferior a **3 segundos** para consultas complejas sobre datos históricos y en tiempo real.
- La infraestructura debe permitir el procesamiento concurrente de al menos **10,000 eventos por segundo** sin degradación de la calidad del servicio.
- El proveedor debe proporcionar herramientas de monitoreo que permitan:

  - Trazabilidad de datos desde la ingesta hasta el consumo.
  - Registro detallado de todos los accesos y modificaciones en los datos.
  - Detección automática de anomalías y generación de alertas.
- El proveedor debe permitir auditorías periódicas para validar el cumplimiento de políticas de seguridad y gobernanza.
- El proveedor debe garantizar que la plataforma cumpla con las regulaciones aplicables en materia de protección de datos y seguridad
- El aprovechamiento de la información es un factor clave en el proyecto, las soluciones de Business Intelligence (BI) y Business Analytics (BA) son fundamentales para transformar datos en información accionable, optimizar la toma de decisiones y mejorar la experiencia del cliente. Estas herramientas permiten analizar grandes volúmenes de datos estructurados y no estructurados provenientes de múltiples fuentes, como el core de depósito, reposumental, CRM, agentes cognitivos y plataformas omnicanal, para impulsar estrategias basadas en datos.

d. Consolidación de datos:

- Centralización de datos provenientes de diferentes sistemas (core contable, core de depósitos, CRM, agentes cognitivos, canales web y móviles).
- Implementación de un data warehouse o repositorios de datos estructurados y no estructurados para almacenar datos históricos y en tiempo real.

e. Análisis predictivo:

- Uso de algoritmos avanzados de machine learning para predecir tendencias como comportamiento del cliente, riesgo crediticio y probabilidad de abandono.
- Identificación proactiva de oportunidades para cross-selling y up-selling basadas en patrones históricos.

f. Visualización e informes dinámicos:

- Dashboards interactivos que permitan a los usuarios visualizar KPIs clave como rentabilidad por producto, tasa de retención de clientes y costos operativos.
- Generación automatizada de informes regulatorios y financieros en formatos personalizables.

g. Segmentación avanzada:

- Capacidad para segmentar clientes según criterios como comportamiento transaccional, demografía y uso de canales.
- Identificación de segmentos desatendidos para diseñar productos personalizados.

h. Monitoreo en tiempo real:

- Detección inmediata de anomalías en transacciones (fraudes o errores operativos).
- Seguimiento continuo del rendimiento operacional y financiero.

i. Integración con agentes cognitivos:

- Uso de analítica conversacional para mejorar las interacciones del cliente con agentes cognitivos.
- Análisis del sentimiento y contexto del cliente para optimizar respuestas automatizadas.

3.7.5.2.5.1 Inteligencia Artificial como servicio

La implementación de una plataforma de *Inteligencia Artificial como Servicio* (AIaaS) refleja una oportunidad estratégica para impulsar la innovación, mejorar la experiencia del cliente y optimizar procesos internos. Este servicio permitirá diseñar, probar, implementar y desplegar modelos de IA en una arquitectura flexible y escalable, con acompañamiento especializado y costos ajustados al modelo de negocio. A continuación, se describen los aspectos funcionales, técnicos y operativos esperados.

A. Diseño y desarrollo de modelos:

- Permitir a los usuarios crear modelos personalizados para casos específicos como detección de fraudes, análisis predictivo y segmentación avanzada.
- Ofrecer bibliotecas pre entrenadas para tareas comunes como procesamiento del lenguaje natural (NLP) y análisis transaccional.

B. Pruebas y validación:

- Proporcionar entornos seguros para pruebas con datos simulados o reales.
- Implementar herramientas para A/B testing y evaluación del desempeño de los modelos antes del despliegue.

C. Despliegue omnicanal:

- Integración directa con los diferentes canales (web, aplicación móvil, contact center).
- Capacidades para servir modelos como APIs RESTful o gRPC que puedan ser consumidas por otros sistemas.

D. Gestión del ciclo de vida:

- Monitoreo continuo del rendimiento de los modelos en producción.
- Actualización automática basada en nuevos datos o cambios en las condiciones del mercado.

E. Analítica integrada:

- Generación de insights accionables a partir de los datos procesados por los modelos.
- Dashboards interactivos para visualizar métricas clave como precisión, tiempo de respuesta y retorno sobre la inversión (ROI).

3.7.5.2.5.2 Agentes cognitivos

La implementación de agentes cognitivos es fundamental para implementar una estrategia omnicanal que permita gestionar solicitudes, responder requerimientos y ejecutar trámites de manera eficiente. Estos agentes, impulsados por inteligencia artificial (IA) y aprendizaje automático (ML), deben integrarse en la arquitectura tecnológica de la solución para ofrecer experiencias personalizadas, consistentes y en tiempo real a través de múltiples canales como web, aplicaciones móviles, contact centers e incluso redes sociales. Algunos de sus principales elementos funcionales están:

a. Gestión omnicanal

- Capacidad para interactuar con los clientes a través de múltiples canales (web, aplicación móvil, contact center, redes sociales) con una experiencia consistente.
- Continuidad en las interacciones que permitan que un cliente inicie una consulta en un canal y la continúe en otro sin pérdida de información.
- Integración con el Core de Deposito y otros sistemas (core contable, plataforma de BI/BA, repositorios de datos estructurados y no estructurados, y demás componentes de la arquitectura) para acceder a datos del cliente en tiempo real.
- Implementación de una memoria conversacional para contextualizar respuestas en diferentes sesiones y dispositivos.

b. Procesamiento del Lenguaje Natural (NLP)

- Comprensión de consultas realizadas en lenguaje natural, tanto por texto como por voz.
- Capacidad para identificar intenciones, emociones y contexto del cliente.
- Uso de IA conversacional para comprender y responder consultas en lenguaje natural.
- Soporte para múltiples idiomas y adaptación al contexto bancario.
- Corrección de errores tipográficos y aprendizaje de patrones de uso.

c. Automatización de tareas

- Resolución automatizada de solicitudes comunes como consultas de saldo, bloqueos de tarjetas, generación de estados de cuenta o actualizaciones de datos personales.
- Escalamiento inteligente a agentes humanos cuando sea necesario, proporcionando contexto completo al operador.
- Capacidad de ejecutar acciones en nombre del usuario previa autenticación.
- Integración con el BPM para seguimiento de procesos internos.

d. Personalización y recomendaciones

- Uso de analítica predictiva para anticipar necesidades del cliente y ofrecer recomendaciones personalizadas (por ejemplo, productos financieros relevantes).
- Generación de respuestas adaptadas al perfil del cliente basado en su historial transaccional y preferencias.

e. Analítica y reportes

- Captura de datos estructurados y no estructurados para analítica avanzada.
- Generación de reportes normativos y dashboards en tiempo real.
- Integración con BI / BA para la toma de decisiones basada en IA.

3.7.5.2.6 Exposición de APIs públicas

Para integración con terceros permite que diferentes sistemas y aplicaciones se comuniquen y compartan datos entre sí. Las APIs públicas son interfaces accesibles que facilitan la interacción programática, permitiendo a los desarrolladores externos conectar sus propias aplicaciones con la plataforma, automatizar procesos y obtener información en tiempo real de manera segura y eficiente. Esta capacidad de integración es crucial para ampliar la funcionalidad de la plataforma y fomentar la innovación mediante la colaboración con socios y proveedores externos.

3.7.5.2.6.1 Obligaciones técnicas

- Diseño y desarrollo de APIs: Seguir estándares abiertos (REST, GraphQL, SOAP) y buenas prácticas (OpenAPI, JSON: API).
- Versionamiento: Implementar un esquema de versionado para evitar interrupciones a los consumidores de la API.
- Disponibilidad y escalabilidad: Garantizar una infraestructura escalable y altamente disponible (ej. Nivel de Servicio (ANS) de 99.9%).
- Monitoreo y logging: Implementar herramientas de observabilidad (APM, logging estructurado) y auditoría.
- Documentación: Proveer documentación actualizada, clara y accesible (Swagger, Postman, API Gateway).
- Gestión de errores: Definir códigos de error estándar y respuestas consistentes.

3.7.5.2.6.2 Obligaciones de seguridad y cumplimiento

- Autenticación y autorización: Implementar OAuth 2.0, JWT, API Keys o certificados.
- Protección contra amenazas: Aplicar rate limiting, validación de entradas, y mitigación de ataques (DDoS, SQL Injection, XSS).
- Cifrado: Usar HTTPS/TLS en todas las comunicaciones.
- Cumplimiento normativo: Asegurar conformidad con regulaciones como GDPR, ISO 27001, PCI DSS, etc.
- Seguridad en ciclo de vida: Aplicar DevSecOps, análisis de vulnerabilidades y pruebas de penetración.

3.7.5.2.6.3 Obligaciones operativas y de soporte

- Mantenimiento y actualizaciones: Asegurar corrección de errores, parches de seguridad y mejoras continuas.
- Gestión de incidencias y soporte: Brindar canales de atención y tiempos de respuesta acordados en los Niveles de servicio (ANS).
- Política de depreciación: Definir cómo y cuándo se discontinuarán versiones antiguas de la API.
- Reportes de uso: Ofrecer métricas sobre consumo, latencia, errores y rendimiento.

3.7.5.2.6.4 Otras consideraciones

- Niveles de Servicio (ANS) y penalidades: Asegurar disponibilidad mínima, tiempos de respuesta y penalidades por incumplimiento.
- Confidencialidad y propiedad intelectual: Definir el uso de datos y la propiedad de los desarrollos.
- Respaldo y recuperación *ante desastres: Establecer estrategias de backup y planes de continuidad.*

3.7.5.3 Diseño y definición de la arquitectura tecnológica

- El proveedor debe diseñar una arquitectura tecnológica basada en **principios de arquitectura empresarial** y siguiendo estándares internacionales como **TOGAF** y **NIST**.
- La arquitectura debe estar documentada mediante modelos detallados que incluyan:
  - **Arquitectura de infraestructura** (física y virtual).

- **Arquitectura de aplicaciones** (microservicios, contenedores, SOA).
- **Arquitectura de integración** (APIs, ETL, colas de mensajería).
- **Arquitectura de datos** (LakeHouse, pipelines de datos, Base de datos).

- El diseño debe permitir la evolución de la solución tecnológica mediante un modelo de **arquitectura modular** y **desacoplada** para facilitar cambios y mejoras sin impacto en la operación.

3.7.5.3.1 Interoperabilidad y estándares tecnológicos

- El proveedor debe garantizar que la solución tecnológica cumpla con estándares abiertos y protocolos de interoperabilidad como REST, SOAP, gRPC, OAuth 2.0 y OpenAPI para facilitar la integración con otros sistemas internos y externos.
- La solución debe soportar múltiples formatos de datos (JSON, XML, CSV, Parquet, etc.) y ser compatible con plataformas de terceros mediante conectores y adaptadores configurables.
- El proveedor debe implementar una plataforma de orquestación que permita la integración y comunicación entre sistemas de manera segura y eficiente.

3.7.5.3.2 Portabilidad y compatibilidad multi nube

- El proveedor debe garantizar que las configuraciones de infraestructura y aplicaciones sean portables mediante tecnologías de última generación y con soporte de proveedor.
- El proveedor debe permitir la migración de la solución entre diferentes proveedores de nube (ejemplo: **AWS**, **Azure**, **Google Cloud**) sin impacto en la operación o pérdida de datos.

3.7.5.3.3 Gestión de configuración y automatización (IaC)

- El proveedor debe implementar un modelo de **Infraestructura como Código (IaC)** para la gestión automatizada de configuraciones
- Las configuraciones deben estar versionadas y almacenadas en un repositorio de código seguro para garantizar la trazabilidad y control de cambios.
- El proveedor debe establecer procesos de automatización para:
  - Despliegue de infraestructura.
  - Configuración de servicios y redes.
  - Gestión de permisos y acceso.
  - Monitoreo y escalado automático.

3.7.5.3.4 Disponibilidad y Continuidad

- El proveedor debe diseñar la arquitectura para ofrecer un nivel de disponibilidad mínimo del **99.5%** mediante la implementación de:
  - Balanceo de carga mediante servicios de balanceo en la nube.
  - Clústeres redundantes en múltiples zonas de disponibilidad.
  - Replicación síncrona y asíncrona de datos en múltiples regiones.
- La solución debe contar con un **Plan de Recuperación ante Desastres (DRP)** que permita la restauración de servicios críticos en menos de **4 horas** en caso de fallo catastrófico.
- La arquitectura debe incluir **pruebas periódicas** de failover y recuperación para validar la efectividad de los mecanismos de redundancia.

- El proveedor deberá implementar y mantener un Sistema de Gestión de Continuidad del Negocio conforme a los lineamientos establecidos en la norma ISO 22301 y articulado con la política de continuidad de la entidad. Esto incluye, pero no se limita a: identificar y evaluar riesgos potenciales, desarrollar e implementar estrategias de continuidad, realizar simulacros y pruebas periódicas para validar la efectividad de los planes, garantizar la capacitación del personal clave y proporcionar informes regulares que demuestren el cumplimiento continuo de los requisitos de la norma. Además, deberá garantizar la disponibilidad y actualización de los planes de recuperación ante desastres y la coordinación con todas las partes interesadas para minimizar interrupciones operativas y proteger los intereses de la entidad.
- El proveedor debe garantizar que la infraestructura esté replicada en al menos 1 zona geográficas diferentes para asegurar la continuidad operativa ante incidentes de infraestructura o catástrofes naturales.
- Debe implementar mecanismos de conmutación por error (failover) que permitan la activación automática de la infraestructura redundante en menos de 5 minutos en caso de fallo total de la ubicación principal.
- La infraestructura debe realizar copias de seguridad automáticas y replicación de datos entre zonas geográficas para garantizar la integridad y disponibilidad de los datos ante un evento de pérdida de datos o interrupción de servicio.

3.7.5.3.5 Escalabilidad

- El proveedor debe garantizar que la arquitectura de la solución permita la escalabilidad horizontal y vertical para soportar aumentos en la carga de trabajo sin degradación del servicio.
- La infraestructura debe permitir el auto escalado automático mediante herramientas como Kubernetes, Docker Swarm o servicios nativos de la nube (por ejemplo, AWS Auto Scaling, Azure Scale Sets, etc).
- La solución debe soportar un crecimiento de al menos un 30% anual en términos de usuarios, transacciones y volumen de datos sin afectar el rendimiento.

3.7.5.3.6 Documentación y transferencia de conocimiento

- El proveedor debe entregar una documentación detallada que incluya:
  - Diagramas de arquitectura.
  - Configuraciones de infraestructura y seguridad.
  - Procedimientos de operación y mantenimiento.
  - Políticas de recuperación y escalado.
- El proveedor debe capacitar al equipo interno sobre la arquitectura, configuración y operación de la solución tecnológica para garantizar la continuidad operativa.
- La documentación debe actualizarse periódicamente para reflejar cualquier cambio en la configuración o estructura de la solución.
- El proveedor deberá construir y mantener actualizado el o los Manuales de Usuario que describa de manera clara y detallada el uso de la solución, incluyendo:
  - Instrucciones paso a paso para las funcionalidades principales.
  - Descripción de las interfaces gráficas y opciones disponibles.
  - Resolución de problemas comunes (FAQ).
  - Ejemplos prácticos de uso.

  - Procedimientos para recuperación de contraseñas, configuración de accesos y personalización de la interfaz.
- El proveedor deberá construir y mantener actualizado el o los Manuales Técnicos que describan el proceso de configuración e implementación de la solución, incluyendo:
  - Instalación inicial y configuración de parámetros técnicos.
  - Definición de arquitectura y componentes del sistema.
  - Configuración de infraestructura, servidores, redes y bases de datos.
  - Procedimientos para realizar actualizaciones y parches.
  - Configuración de alta disponibilidad, balanceo de carga y escalado automático.
- El proveedor deberá construir y mantener actualizado el o los Manuales de Administración que incluya las instrucciones para gestionar y monitorear la solución, incluyendo:
  - Procedimientos para la gestión de usuarios y roles.
  - Configuración de alertas y umbrales de rendimiento.
  - Gestión de logs y auditoría.
  - Procedimientos para realizar backups y restauración de datos.
  - Documentación de scripts o herramientas automatizadas para monitoreo y análisis de rendimiento.
- El proveedor deberá construir y mantener actualizado el o los Manuales de Soporte que documente los procedimientos para identificar, diagnosticar y resolver incidentes, incluyendo:
  - Clasificación y niveles de severidad de incidentes.
  - Procedimientos de escalamiento y contacto con soporte técnico.
  - Procedimientos para recuperación ante fallos y desastres.
  - Tiempo de respuesta y acuerdos de nivel de servicio (ANS).
  - Registro de incidentes y análisis de causa raíz.

3.7.5.3.7 Rendimiento y eficiencia

El proveedor debe garantizar como mínimo que la solución tecnológica cumpla con los siguientes estándares de rendimiento y eficiencia:

- **Capacidad de procesamiento**: La solución debe procesar un mínimo de **10.000 eventos por segundo** sin degradación de la calidad del servicio, manteniendo una latencia inferior a **200 ms** en el 95% de las transacciones.

- **Resiliencia bajo alta carga**: La solución debe ser capaz de mantener un rendimiento óptimo durante picos de uso de al menos **2 veces** el promedio diario sin afectar la disponibilidad o el tiempo de respuesta.

- **Capacidad de escalado automático**: La infraestructura debe permitir la escalabilidad horizontal y vertical para soportar incrementos en la carga de trabajo mediante mecanismos automáticos de escalado.

- **Optimización de uso de recursos**: La infraestructura debe utilizar mecanismos de optimización automática para reducir el consumo de CPU, memoria y almacenamiento en función de la demanda mediante herramientas como **auto scaling** y **machine learning** para predicción de carga.

- **Gestión de costos**: El proveedor debe garantizar que la solución esté diseñada para minimizar costos operativos mediante:
  - Uso de instancias reservadas o spot en la nube.
  - Reducción de tráfico innecesario mediante balanceo de carga y caché.
  - Optimización de almacenamiento mediante políticas de archivado y eliminación de datos obsoletos.

- **Reducción de tiempos de procesamiento**: El proveedor debe implementar técnicas de procesamiento paralelo y en lotes para reducir el tiempo de ejecución de tareas críticas.

3.7.5.3.8 Trazabilidad y auditoría

El proveedor debe garantizar como mínimo que todos los eventos y acciones dentro de la solución tecnológica estén completamente trazados, registrados y con auditoria:

- **Registro de eventos y transacciones**: La solución debe capturar y almacenar en tiempo real todos los eventos críticos, transacciones y modificaciones mediante sistemas de logging.

- **Identificación de usuario y contexto**: Cada evento debe estar asociado con:
  - ID de usuario o sistema que generó el evento.
  - Marca de tiempo precisa (timestamp).
  - Parámetros de entrada y resultado de la operación.

- **Correlación de eventos**: El proveedor debe garantizar que los eventos estén correlacionados para permitir el análisis de causa raíz y la reconstrucción de transacciones en caso de incidentes o auditorías.

- **Retención de registros**: Los registros deben almacenarse por un período mínimo de **5 años** o superior y deben estar protegidos mediante cifrado y control de acceso.

- **Trazabilidad de datos**: El proveedor debe garantizar la trazabilidad de los datos desde su origen hasta su consumo final, permitiendo reconstruir el ciclo de vida completo de la información.

- **Registro de acceso y actividad**: La solución debe registrar todos los accesos y actividades realizadas por usuarios y sistemas, incluyendo:
  - Intentos de acceso fallidos y exitosos.
  - Acciones administrativas (creación, modificación y eliminación de datos).
  - Cambios en configuraciones de seguridad y permisos.

- **Acceso controlado a registros**: El acceso a los registros debe estar restringido mediante controles basados en roles y requerir doble autenticación (MFA) para acceder a información sensible.

- **Mecanismos de verificación**: El proveedor debe garantizar que los registros de auditoría estén protegidos contra manipulación mediante técnicas de:
    - Cifrado de extremo a extremo.
    - Firma digital.
    - Control de integridad mediante hash (por ejemplo, **SHA-256**).

- **Auditoría periódica**: El proveedor debe permitir la ejecución de auditorías de seguridad y operativas por parte de terceros independientes al menos una vez al año.

3.7.5.4 Seguridad y cumplimiento

En el contexto de una plataforma tecnológica avanzada, la seguridad y el cumplimiento son pilares fundamentales para garantizar la integridad y la confidencialidad de los datos manejados. Estas características no solo aseguran la operación continua y eficiente de la plataforma, sino que también protegen contra riesgos y amenazas externas e internas.

La seguridad implica la implementación de controles robustos y procedimientos que protejan la información tanto en tránsito como en reposo, previniendo accesos no autorizados y garantizando la privacidad de los datos personales. Por otro lado, el cumplimiento refiere al conjunto de regulaciones y normas que la plataforma debe seguir para operar dentro de los marcos legales establecidos, asegurando que todas las actividades de recopilación, almacenamiento, tratamiento y eliminación de datos se realicen conforme a las leyes vigentes.

Dentro de este marco, el proveedor tiene la obligación de garantizar que la plataforma tecnológica cumpla con rigurosos estándares de seguridad y gobernanza, así como con la normativa aplicable en protección de datos. Es esencial que se implementen técnicas avanzadas de cifrado, se obtenga el consentimiento explícito de los titulares de los datos y se habiliten mecanismos para la trazabilidad y auditoría de todos los accesos y modificaciones realizadas. Además, es primordial que se detecten y gestionen cualquier anomalía de manera automática, asegurando siempre la calidad del servicio y la protección de la información sensible.

1. **Protección de datos personales y privacidad (Ley 1581 de 2012 y Decreto 1377 de 2013)**

- El proveedor debe implementar políticas y procedimientos para la recolección, almacenamiento, tratamiento y eliminación de datos personales conforme a la **Ley 1581 de 2012** y el **Decreto 1377 de 2013**.
- Debe garantizar que todos los datos personales estén protegidos mediante técnicas de cifrado robusto (mínimo **AES-256**) tanto en tránsito como en reposo.
- El proveedor debe contar con mecanismos para obtener el consentimiento explícito de los titulares de los datos antes de recolectarlos y tratarlos.
- Debe implementar controles para garantizar el derecho de los titulares de los datos a:
    - Acceso
    - Rectificación
    - Supresión
    - Portabilidad de datos

- El proveedor debe garantizar que los datos personales solo sean accesibles por personal autorizado y para fines previamente definidos.

2. Seguridad de la información y continuidad de negocio - Circular Básica Jurídica (SFC)

- El proveedor debe implementar un **Sistema de Gestión de Seguridad de la Información (SGSI)** basado en estándares internacionales como **ISO/IEC 27001** y **NIST**.
- Debe garantizar la implementación de controles para:
  - Protección contra accesos no autorizados.
  - Cifrado de datos sensibles en tránsito y reposo.
  - Monitoreo y detección de intrusiones (IDS/IPS).
  - Registro y trazabilidad de todos los accesos y modificaciones de datos.
- El proveedor debe establecer un **Plan de Continuidad de Negocio (BCP)** y un **Plan de Recuperación ante Desastres (DRP)**, asegurando la restauración de los servicios críticos en menos de **4 horas** en caso de incidentes.
- Debe realizar pruebas periódicas de los planes de continuidad y recuperación ante desastres, documentando los resultados y aplicando medidas correctivas cuando sea necesario.
- Garantizar que los datos estén cifrados tanto en tránsito como en reposo, utilizando protocolos y algoritmos robustos, como 3DES o AES-256 o superiores, para proteger la información durante su transmisión.
- El proveedor debe cumplir con la normativa de protección de datos aplicable (ISO 27001, ISO 27017, ISO 27018, GDPR) y mantenerla vigente durante todo el periodo contractual.
- El proveedor puede certificarse con estándares o mejores prácticas que reemplacen, sustituyan o modifiquen las anteriores y debe disponer de informes de controles de organización de servicios (SOC1, SOC2, SOC3).
- Asegurar el cumplimiento de normativas del sector financiero (como PCI-DSS, GDPR u otras regulaciones locales), incluyendo auditorías y controles de seguridad.
- Implementar medidas de seguridad como el cifrado de datos en reposo y en tránsito para proteger la información sensible.
- Asegurar que las copias de seguridad estén cifradas tanto en tránsito como en reposo para proteger la confidencialidad y la integridad de la información.
- Mantener una red segregada lógicamente para los servicios prestados, garantizando que los servidores y aplicaciones utilizados no se desplieguen en redes no confiables sin los controles de seguridad adecuados.
- Establecer mecanismos de autenticación y autorización que limiten el acceso a las copias de seguridad únicamente al personal autorizado, previniendo accesos no autorizados.
- El proveedor debe implementar herramientas de Prevención de Pérdida de Datos (DLP) para detectar y bloquear la transmisión de datos confidenciales fuera de la organización.
- Debe establecer políticas para evitar que los empleados o sistemas no autorizados puedan copiar o extraer información sensible.
- El proveedor debe implementar mecanismos fuertes de autenticación, como biometría combinada con un segundo factor de autenticación, certificados de firma digital, OTP (One Time Password), tarjetas que cumplan el estándar EMV, y registro y validación de características de los equipos utilizados.

- El proveedor debe garantizar la confidencialidad, integridad y disponibilidad de la información, asegurando que esta sea precisa, coherente y completa desde su creación hasta su destrucción.
- La información que viaja entre la entidad y los sitios centrales de las entidades debe estar cifrada usando hardware de propósito específico o software, o una combinación de ambos.
- Los servicios y componentes desplegados en entornos cloud-native deben operar sobre plataformas que cuenten con soporte activo por parte del proveedor de servicios en la nube (Cloud Service Provider - CSP) y/o del fabricante de las tecnologías empleadas. Asimismo, deberán implementar controles de seguridad alineados con buenas prácticas de seguridad en la nube (como las recomendaciones de CIS, NIST o ISO/IEC 27017), incluyendo mecanismos de acceso basado en roles (RBAC), autenticación multifactor (MFA), registros de auditoría, cifrado de datos en tránsito y en reposo, y segmentación

lógica de entornos. Estas medidas deben garantizar un acceso controlado, seguro y trazable a los recursos y servicios críticos de la infraestructura cloud.

- Implementar controles de seguridad en los entornos cloud-native que prevengan la introducción, ejecución o persistencia de software malicioso o mecanismos de interceptación de datos en los servicios, contenedores, máquinas virtuales y redes virtuales utilizados. El proveedor deberá asegurar que los entornos donde se procesan o almacenan datos de clientes cuenten con mecanismos de protección contra malware, escaneo continuo de imágenes y artefactos, control de integridad, políticas de ejecución seguras (como allow/deny lists), y monitoreo de comportamiento anómalo. Además, deberá establecer medidas que impidan la inyección de código o dispositivos virtuales no autorizados que puedan comprometer la confidencialidad de la información de los clientes o de las operaciones.
- Si para la implementación del producto se realizan nuevas alianzas o se acude a servicios tercerizados exigir el cumplimiento de normativas clave como la ISO 27001 y la Ley 1581 de protección de datos personales, así como la implementación de planes de continuidad del negocio. Esta medida refuerza la gestión de riesgos legales, operativos y reputacionales, asegurando que los proveedores mantengan estándares equivalentes a los internos.
- Aplicar cifrado de datos para la protección de información sensible de los aportantes del nuevo producto, acompañado de la obtención de autorizaciones expresas e informadas sobre el tratamiento de sus datos. Esta acción fortalece el cumplimiento normativo y la confianza de los usuarios en el manejo de su información.
- Evaluar la capacidad operativa de la plataforma tecnológica que atenderá este producto, identificando necesidades de adecuación para garantizar un desempeño eficiente ante la demanda, sin comprometer la calidad del servicio.
- La propiedad de la información que se procese en los servicios de computación en la nube, haciendo claridad que los datos son propiedad de la entidad vigilada y que no se pueden usar para ningún propósito diferente al establecido en el contrato.
- Dentro del plan de continuidad del negocio la operación en la nube y realizar las pruebas que resulten necesarias para confirmar la efectividad de los procedimientos contingentes.
- El proveedor debe contar con la estrategia de migración a otra plataforma en caso de terminación del contrato por cualquiera de las partes, por la interrupción o la degradación en la prestación del servicio de parte del proveedor de servicios en la nube o por cualquier otro motivo que considere razonable la entidad vigilada.

Auditoría y cumplimiento regulatorio (Ley 964 de 2005 y normas de la SFC)

- El proveedor debe someterse a auditorías periódicas (al menos una vez al año) para verificar el cumplimiento de las normas de seguridad y protección de datos impuestas por la **SFC** y la **SIC**.
- Debe permitir el acceso a la información y las instalaciones para inspecciones realizadas por:
    - Superintendencia Financiera de Colombia.
    - Superintendencia de Industria y Comercio.
    - Autoridades competentes de ciberseguridad y protección de datos.
- El proveedor debe entregar reportes periódicos sobre el estado de seguridad y cumplimiento, incluyendo eventos de seguridad, incidentes y medidas adoptadas.

- Dejar constancia de todas las operaciones que se realicen a través de los distintos canales, la cual debe contener cuando menos lo siguiente: fecha, hora, código del dispositivo (para operaciones realizadas a través de IVR: el número del teléfono desde el cual se hizo la llamada; para operaciones por Internet: la dirección IP desde la cual se hizo la misma; para operaciones con dispositivos móviles, el número desde el cual se hizo la conexión), cuenta(s), número de la operación y costo de la misma para el cliente o usuario.
- Auditar periódicamente las bases de datos y aplicaciones asociadas en relación con el producto, verificando que los registros de auditoría estén activos y capturen todas las acciones de los usuarios.

Administración de acceso y privilegios

- El proveedor debe implementar un modelo de **control de acceso basado en roles (RBAC)** para garantizar que solo los usuarios autorizados accedan a sistemas y datos críticos.
- Debe implementar mecanismos de autenticación multifactor (MFA) para el acceso a servicios y sistemas sensibles.
- El proveedor debe realizar una revisión trimestral de los privilegios de acceso para garantizar que los permisos otorgados estén actualizados y alineados con las funciones del personal.
- Debe implementar herramientas de gestión de identidades y accesos (IAM) para el control centralizado de permisos y accesos a nivel de plataforma, red y aplicación.
- Tener bajo su control la administración de usuarios y de privilegios para el acceso a los servicios ofrecidos, así como a las plataformas, aplicaciones y bases de datos que operen en la nube, dependiendo del modelo de servicio contratado.
- Establecer las medidas necesarias para garantizar que, en el evento de toma de posesión, la SFC, Fogafín, Fogacoop, o quienes éstas designen, puedan acceder a la información y a la administración de los sistemas de información que operan en la nube.

Transferencia y almacenamiento de datos en entornos de nube (Decreto 2364 de 2012 y regulaciones de la SFC)

- Si el proveedor utiliza servicios de nube pública o híbrida, debe garantizar que los datos financieros y personales estén alojados en centros de datos ubicados en países que cumplan con estándares equivalentes a los de la SFC y la SIC en términos de seguridad y protección de datos.
- Debe garantizar que las transferencias de datos entre regiones o centros de datos estén cifradas mediante protocolos seguros (como TLS 1.3).
- El proveedor debe garantizar que los datos almacenados en la nube estén sujetos a las mismas políticas de protección y gobernanza que los datos alojados localmente.

Remisión de información a la SFC

Dentro de los 15 días anteriores al inicio del procesamiento de información en la nube, relacionada con procesos misionales o de gestión contable y financiera, las entidades deben remitir a la SFC la siguiente información:

- El nombre del proveedor que prestará los servicios en la nube y de los subcontratistas o partners que le prestarán servicios asociados al objeto del contrato.
- La relación de los procesos que serán manejados en la nube, incluyendo las aplicaciones, tipo de datos, productos y servicios asociados a éstos.
- La ubicación física o región donde se procesarán y almacenarán los datos.
- Las certificaciones otorgadas al proveedor del servicio y/o sitio de procesamiento.
- La relación de auditorías a las que se somete el proveedor de servicios contratado.
- La información sobre los niveles de servicio establecidos.
- El diagrama con la plataforma tecnológica que soportará los servicios contratados.

Seguridad y análisis de vulnerabilidades

El proveedor debe implementar un sistema robusto de análisis de vulnerabilidades informáticas que permita identificar riesgos potenciales en tiempo real. Este sistema debe generar informes consolidados que detallen las vulnerabilidades detectadas y proporcionar un plan de acción con medidas de remediación claras.

Además, el proveedor debe realizar al menos tres pruebas al año de seguridad de la información y de los sistemas de seguridad perimétrales, asegurando que cualquier hallazgo identificado sea remediado en el menor tiempo posible. Las auditorías deben incluir pruebas de penetración, análisis de configuraciones y revisiones de cumplimiento normativo. Se espera que el proveedor documente cada auditoría con un informe detallado, el cual debe ser compartido con la entidad contratante para su revisión y validación.

Es requisito obligatorio que dichas pruebas de seguridad y análisis de vulnerabilidades sean ejecutadas por una empresa o proveedor distinto e independiente al proveedor de la solución de FPC, con el fin de garantizar la objetividad, imparcialidad y confiabilidad de los resultados obtenidos.

3.7.5.5 Integración de servicios

A continuación, se proporciona mayor detalle de los requerimientos que como mínimo debe cumplir el proveedor.

Garantizar la compatibilidad y conectividad entre plataformas

- El proveedor debe asegurar que la infraestructura y servicios ofrecidos sean compatibles con las plataformas tecnológicas de la entidad, entidades de vigilancia, Fintech y cualquier otro actor que se relacione con la plataforma tecnológica y el negocio.
- Deberá proporcionar conectividad segura mediante protocolos estandarizados (como HTTP, HTTPS, SFTP, REST, SOAP).
- Debe permitir la integración mediante APIs abiertas o conectores personalizados.
- El proveedor debe garantizar los canales necesarios para interoperar o integrarse con los sistemas de la entidad esto incluye conectividad por canales privados y seguros para el consumo de servicios

Implementar y mantener interfaces de integración estandarizadas

- El proveedor debe implementar interfaces estandarizadas para la transferencia y procesamiento de datos.
- Las interfaces deben cumplir con estándares de interoperabilidad como **JSON, XML** y protocolos de autenticación como **OAuth 2.0** o **SAML**.
- El proveedor debe garantizar la actualización y mantenimiento de las interfaces sin afectar la operación.
- El proveedor debe asegurar que los datos en tránsito y en reposo estén cifrados mediante **AES-256** o equivalente.
- La transferencia de datos entre la infraestructura del proveedor y la entidad debe realizarse mediante **canales seguros** (VPN, IPsec, TLS).
- El proveedor debe cumplir con la normativa de protección de datos aplicable (ISO 27001, ISO 27017, ISO 27018, GDPR) y mantenerla vigente durante todo el periodo contractual.
- El proveedor puede certificarse con estándares o mejores prácticas que reemplacen, sustituyan o modifiquen las anteriores y debe disponer de informes de controles de organización de servicios (SOC1, SOC2, SOC3).
- El proveedor debe proporcionar entornos de desarrollo y pruebas para garantizar la compatibilidad y validación de la integración.
- La entidad debe tener acceso a entornos de pruebas para validar las actualizaciones antes de implementarlas en producción.
- El proveedor debe coordinar con la entidad las pruebas de carga, seguridad y rendimiento.
- Gestionar los riesgos de las API o Servicios Web suministrados por el proveedor de servicios en la nube.

Asegurar la continuidad y redundancia de los servicios

- El proveedor debe garantizar la **disponibilidad continua** de los servicios mediante configuraciones de redundancia y alta disponibilidad.
- Asegurar la reanudación de los servicios en un tiempo acordado (RTO y RPO) con la entidad.
- Facilitar la integración mediante mecanismos de autenticación y autorización segura.
- El proveedor debe implementar herramientas de monitoreo que permitan a la entidad:
    - Consultar el estado de los servicios en tiempo real.
    - Generar reportes de desempeño, incidentes y tiempos de respuesta.
    - Recibir alertas automáticas sobre fallos o degradación del servicio.
- El proveedor debe garantizar el acceso a la información de monitoreo mediante interfaces accesibles o APIs.
- El proveedor debe contar con un equipo de soporte técnico especializado disponible 24/7/365.
- La entidad debe contar con una línea de escalamiento directa para la atención de incidentes críticos.
- El proveedor debe proporcionar documentación técnica completa y actualizada sobre las interfaces de integración y servicios.

Interoperabilidad con entidades

- Fiscalía General de la Nación
- Superintendencia Financiera de Colombia

- Registraduría general del estado Civil
- Listas de Control
- Incapacitados
- Dps
- Sisbén
- Dian
- Otras

En caso de que sea necesario establecer un convenio con la entidad que expone el servicio, la entidad designada será responsable de gestionar dicho convenio, contando con el apoyo técnico del proveedor.

Hoja de ruta para integrar la solución con los sistemas existentes de la entidad

A continuación, se relacionan las fases y las actividades que se deberán adelantar para poder integrar la solución con los sistemas actuales de la entidad:

1. Análisis institucional y normativo
Objetivo: Alinear la integración con las políticas de TI de la entidad designada y los lineamientos legales impartidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Revisión legal:
Verificar la Ley de Protección de Datos Personales (Ley 1581 de 2012).
Verificar el marco de interoperabilidad para Gobierno (Arquitectura Empresarial del Estado) definido por MinTIC.
Identificación de actores y procesos clave:
Áreas involucradas (Vicepresidencia de Operaciones y Tecnología, Dirección de Tecnología, Grupo Interno de Trabajo de Operaciones, Vicepresidencia Financiera Jurídica, Dirección de Tesorería, etc.)
Procesos afectados (créditos, pagos, etc.)

2. Levantamiento de requerimientos técnicos y funcionales actualizados
Objetivo: Entender, de manera específica, qué datos y procesos se deben conectar entre la solución y los sistemas que actualmente se utilizan para soportar la operación de la entidad designada por la corporación.

Llevar a cabo una reunión con el equipo de la Vicepresidencia de Operaciones y Tecnología o su delegado.

Fundamentalmente la solución deberá integrarse con los siguientes sistemas que soportan la operación diaria de la entidad:

Core Bancario (sistema desarrollado por un tercero): es una solución de software que integra las operaciones de crédito, cartera y cobranzas de tal forma que le permite a la entidad desarrollar de manera eficiente las actividades de su objeto social.

C&CTEX (desarrollo propio de la entidad): sistema Core de Negocio, donde se almacena toda la información referente a beneficiarios de créditos educativos, proveedores e instituciones de educación superior y permite el control y manejo del plan de pagos del beneficiario, movimientos bancarios, información básica del beneficiario, codeudores, estados de cuenta, cartera, desembolsos, facturación, convocatorias de acceso a un crédito, fondos educativos, constituyentes de fondos, reportes, y reliquidación de créditos.

Desembolsos.net (desarrollo propio de la entidad): sistema que permite realizar y gestionar los giros aprobados a los estudiantes que inician y continúan su estudio de educación superior. Esto se tendrá en cuenta en fases posteriores a la del producto de ahorro

Apoteosys (sistema desarrollado por un tercero): herramienta financiera o ERP que permite la optimización de la operación e integración de la información a través de los módulos del sistema financiero y el sistema administrativo. ERP de la Entidad con el cual se soporta la operación de los Procesos de la Vicepresidencia Financiera para las áreas de Presupuesto, Contabilidad, Tesorería y Activos Fijos.

Vigía (desarrollo propio de la entidad): sistema que administra los reportes de riesgos para su seguimiento y atención.

ControlDoc (sistema desarrollado por un tercero): sistema de información para llevar a cabo la gestión documental de la entidad.

Cosmos CRM (sistema desarrollado por un tercero): sistema de información que permite la administración de contactos, servicios corporativos y oportunidades para canalización de ventas, seguimiento a la adjudicación de créditos, PQRSDs, revisión de estado de procesos jurídicos por demandas o tutelas, a través de informes.

3. Diseño de la integración

Objetivo: Establecer cómo se conectará la solución con los sistemas de la entidad designada.

Determinar el tipo de integración:
Para los casos en los que se ofrezcan **APIs REST o SOAP**, diseñar la conexión cliente.
Si no hay APIs, considerar la integración por **intercambio de archivos (SFTP/ETL)** u otra forma.

Especificaciones técnicas:
Definir el proceso de Autenticación.
Definir el formato de datos (JSON, XML, CSV).

Con respecto a los estándares de interoperabilidad debe tenerse en cuenta el trabajo con una arquitectura SOA, orientada a microservicios, con un bus de integración en el medio que permite hacer conversiones y orquestaciones en diferentes formatos (JSON con servicios REST o XML con protocolo SOAP).

Todo lo anterior bajo el concepto de contenedores.

4. Desarrollo técnico

Objetivo: Construir y probar la conexión entre la solución y los sistemas de la entidad designada. Hacer el desarrollo de conectores/API clients.

Proceder con el envío y recepción de datos de prueba.
Hacer las validaciones y el control de errores pertinentes.
Tener en cuenta las Reglas de negocio según requerimientos de la entidad designada. Logs, auditorías y trazabilidad.

5. Seguridad y cumplimiento normativo
Objetivo: Asegurar que los datos de los usuarios estén protegidos y se cumpla la normativa.
Consentimiento informado del usuario.
Cifrado de datos en tránsito y en reposo.
Auditoría y monitoreo.
Política de privacidad alineada con la SIC y la Ley 1581.

6. Pruebas, despliegue y acompañamiento
Objetivo: Asegurar una puesta en producción estable y conforme a lo pactado.
Hacer pruebas funcionales y de integración.
Hacer una revisión conjunta con el personal funcional y técnico de la entidad desginada. Realizar un despliegue controlado considerando la opción de realizar un piloto. Realizar soporte y monitoreo post-lanzamiento.

7. Mantenimiento y evolución
Objetivo: Garantizar que la integración siga funcionando a largo plazo.
Hacer seguimiento de cambios en los sistemas de la entidad designada. Realizar actualizaciones de API.
Llevar reporte de métricas y uso.
Hacer una gestión de incidentes.

Requerimientos de seguridad para integraciones

El proveedor debe estar alineado con los controles aplicables de la norma ISO/IEC 27001 según el tipo de servicio o producto ofrecido.

El personal asignado al servicio debe estar capacitado en seguridad de la información y privacidad de datos, contar con estudio de seguridad y tener acuerdos de confidencialidad firmados.

Se debe designar un responsable por parte del proveedor que garantice el cumplimiento de los requisitos de seguridad establecidos durante el contrato.

El proveedor debe identificar los riesgos relacionados con seguridad de la información, privacidad y ciberseguridad, y definir planes de tratamiento que garanticen su mitigación.

Todos los dispositivos involucrados en la prestación del servicio deben contar con mecanismos de protección contra malware (por ejemplo, EDR), proceso de aplicación de parches de seguridad, y hardening actualizado al menos una vez al año.

El proveedor debe contar con un procedimiento para detectar, reportar, contener e investigar incidentes de seguridad asociados al servicio contratado.

Las comunicaciones deben ser seguras y emplear mecanismos como VPN (IPSec o SSL), TLS 1.2 o superior y certificados digitales.

Se deben generar y conservar logs o registros de auditoría de los dispositivos usados en la prestación del servicio, incluyendo accesos, errores y eventos críticos. Cuando aplique, estos logs deben integrarse con el SIEM de la entidad designada mediante protocolos como Syslog, WMI o API Rest.

Los desarrollos ofrecidos deben cumplir con OWASP Top 10 y el estándar ASVS, contar con doble o múltiple factor de autenticación, controles tipo CAPTCHA en formularios públicos y gestión de perfiles de usuario. (Cuando aplique)

La solución o servicio debe operar sobre una infraestructura con ambientes separados (desarrollo, pruebas, producción y contingencia), asegurando que la información confidencial de la entidad designada solo resida en producción.

El proveedor debe contar con planes de recuperación ante desastres y continuidad operativa que aseguren la prestación del servicio en caso de eventos adversos.

3.8 DESARROLLO DE PERSONALIZACIONES Y EVOLUCIÓN DE LA SOLUCIÓN

En este sentido, es fundamental mantener la plataforma actualizada con personalizaciones y adaptarse a nuevas necesidades. Esto permitirá la evolución constante de la solución de ahorro, garantizando que se satisfacen las demandas cambiantes del mercado y las necesidades específicas de los usuarios. La capacidad de personalizar y ajustar la plataforma no solo mejora la experiencia del usuario, sino que también fortalece la competitividad y eficiencia del sistema, asegurando una respuesta ágil y efectiva a los retos emergentes.

Por tal razón el proveedor deberá contar con una bolsa de horas para servicios de desarrollo, mantenimiento y soporte tecnológico, garantizando que la cantidad total de horas utilizadas no supere las 4.500 horas en el primer año.

- Las horas contratadas se utilizarán para actividades de desarrollo, mantenimiento, soporte y cualquier otra tarea relacionada con el servicio objeto del contrato.
- En caso de que queden horas sin utilizar en un año, estas podrán acumularse y utilizarse en el siguiente año.
- El proveedor deberá justificar el consumo de horas de los requerimientos de la entidad con historias de usuario o documentos adicionales las cuales servirán como insumo de los requerimientos de desarrollo de software
- La acumulación de horas no podrá exceder las 4.500 horas al término de un año.
- La transferencia de horas no utilizadas no exime al proveedor de garantizar la disponibilidad de los recursos necesarios para la prestación del servicio en los términos del contrato.
- Dos meses antes de finalizar el año se debe se realizará una evaluación del consumo de horas con el objetivo de:

  - Determinar si es necesario aumentar o reducir la bolsa de horas para el siguiente período.
  - Analizar la eficiencia y calidad del servicio prestado por el proveedor.
  - Ajustar la distribución de horas según las necesidades del negocio.
  - Emitir un informe con recomendaciones y posibles ajustes al contrato.
- Garantizar la disponibilidad de los recursos y personal calificado para la ejecución de las actividades enmarcadas en la bolsa de horas.
- Cumplir con los tiempos de respuesta y resolución definidos en los acuerdos de nivel de servicio (ANS).
- Mantener una bitácora detallada de las horas utilizadas y las actividades realizadas.
- Proporcionar reportes mensuales sobre el consumo de horas, el estado de los desarrollos y los incidentes atendidos.
- Asegurar la calidad de los entregables de acuerdo con los estándares técnicos y de seguridad definidos por la empresa.
- El proveedor debe documentar detalladamente todas las personalizaciones a la solución, con manuales, flujos, guías y cualquier documento que apoye el mantenimiento de la solución.
- Toda la información, documentación y desarrollos realizados en el marco del presente contrato serán de propiedad exclusiva de la entidad.
- El proveedor se compromete a no divulgar, compartir o utilizar la información suministrada o generada para ningún otro propósito ajeno al contrato.
- En caso de terminación del contrato, el proveedor deberá entregar toda la documentación y código fuente desarrollado sin costo adicional.
- Cualquier solicitud nueva, ajuste o modificación a la solución deberá ser evaluada en conjunto con el gerente del proyecto y la entidad contratante, con el fin de realizar la estimación necesaria para cada desarrollo antes de su ejecución.
- Se debe tener en cuenta metodologías de desarrollo modernas para realizar entregas en el menor tiempo posible.
- El proveedor deberá desarrollar los servicios necesarios de punta a punta en el caso de que se requiera, esto quiere decir que en el caso de requerirse un desarrollo de un servicio que exponga alguna información desde las plataformas actuales de la entidad el proveedor deberá desarrollar dicha integración, la entidad garantizara el acceso a los datos que y plataformas necesarias.
- El proveedor deberá trabajar con la entidad para evolucionar los componentes, la arquitectura y el uso de cualquier nueva tecnología que surja en el transcurso del contrato.

Para la salida a producción, el proveedor deberá realizar los ajustes necesarios a la solución, asegurando su alineación con las reglas de negocio y las condiciones propias de la plataforma de ahorro, en preparación para la prueba de ruta exigida por la Superintendencia Financiera de Colombia.

Adicionalmente, esta información tiene como propósito brindar una visión clara de las expectativas y necesidades de la entidad designada en relación con los mecanismos y estrategias destinados a ofrecer respaldo y protección integral a los beneficiarios de crédito, especialmente frente a situaciones que puedan afectar su estabilidad económica y continuidad académica.

En ese sentido, a continuación, se presenta el alcance de los servicios requeridos, junto con los componentes mínimos necesarios para garantizar su adecuada implementación y operación, en el marco de las coberturas asociadas a enfermedades catastróficas.

Verificación de eventos para las coberturas de enfermedades catastróficas y desempleo

La verificación precisa y oportuna de los eventos cubiertos es fundamental para garantizar que los beneficiarios reciban el apoyo necesario en situaciones críticas. Esto incluye el desarrollo de procedimientos claros y eficientes para la gestión de casos, así como la coordinación con entidades relevantes para validar la documentación y el cumplimiento de las condiciones de las coberturas.

Componentes mínimos

Verificación del cumplimiento de las condiciones para los eventos cubiertos:
Mecanismos para el registro y seguimiento:
Elaboración de informes sobre la gestión de eventos y recomendaciones de mejora:
Identificación de acciones para la mitigación de la materialización de eventos:
Eventos atendidos por cobertura y rango.

3.9 MODELO DE OPERACIÓN

El proveedor será el encargado de la operación, monitoreo, soporte, mantenimiento y mejora continua de los servicios de seguridad, red y de toda la plataforma tecnológica. Deberá garantizar la continuidad del negocio y la mitigación de riesgos relacionados con la ciberseguridad y la disponibilidad.

Asimismo, será esencial la gestión del Centro de Operaciones de Seguridad (SOC) y el Centro de Operaciones de Red (NOC), asegurando la disponibilidad, seguridad y monitoreo ininterrumpido de la infraestructura tecnológica.

3.9.1 Niveles de atención

El proveedor deberá contar con personal especializado que cubra los siguientes niveles de atención:

- **Nivel 1 (Soporte básico y mesa de ayuda):**
  - Detección y registro de eventos de seguridad y rendimiento de la red y la plataforma tecnológica.
  - Aplicación de procedimientos iniciales de contención y escalamiento.
  - Monitoreo proactivo 24x7 de incidentes de seguridad y disponibilidad de la plataforma.
  - Generación de alertas en tiempo real ante eventos sospechosos.
  - Primera validación de incidentes de seguridad y red para evitar falsos positivos.
  - CMDB: Centraliza la información de cada elemento de configuración CI y Trazabilidad de los CI, conociendo los cambios, incidentes, movimientos,

responsables que ha tenido el activo. Mantener actualizados los documentos de apoyo técnico a la operación.
  - Control y administración del inventario (ficha técnica) de capacidades de cómputo, el cual deberá hacerse de manera remota y automatizada, llevando un seguimiento del historial de cambios de cada servicio.
  - Control y administración del inventario de licencias de software.

- **Nivel 2 (Soporte especializado y administración de plataforma):**
  - Análisis detallado de amenazas, análisis forense y evaluación de impacto.
  - Diagnóstico y corrección de fallas en infraestructura de red, y plataforma tecnológica y seguridad.
  - Aplicación de configuraciones avanzadas y mitigación de ataques.
  - Implementación de medidas correctivas y preventivas para minimizar riesgos futuros.
  - Coordinación con otras entidades o empresas para una gestión más eficiente.
  - El servicio incluye una labor de soporte especializado, con el fin de garantizar la operación permanente del uso de la plataforma de nube pública por parte de los usuarios a la plataforma donde pueden presentarse necesidades que impliquen el apoyo del personal del nivel de especialistas. El servicio deberá prestarse remotamente desde las instalaciones del proveedor y en los casos que se requiera por la Entidad, el servicio brindará soporte en las instalaciones de la Entidad.
  - El servicio incluye una labor de soporte especializado, con el propósito de garantizar la operación continua de la plataforma de nube pública utilizada por los usuarios. Es fundamental brindar el apoyo necesario en situaciones que requieran la intervención del personal con experiencia en niveles especializados. Este servicio se prestará de manera remota desde las instalaciones del proveedor y, cuando la Entidad lo considere necesario, se ofrecerá soporte en sus propias instalaciones.

- **Nivel 3 (Expertos y relación con proveedores):**
  - Resolución de incidentes complejos y análisis profundo de vulnerabilidades.
  - Diseño de estrategias de mejora en ciberseguridad y disponibilidad de red.
  - Coordinación con proveedores de tecnología y reguladores en caso de ataques avanzados.
  - Definición y aplicación de políticas de seguridad y mejores prácticas.
  - Evaluación y recomendación de nuevas soluciones tecnológicas.
  - Administrar y soportar la infraestructura, servicios y la plataforma que sean aprovisionados en las nubes públicas, garantizando la correcta gestión, prestando el soporte técnico especializado de acuerdo con los requerimientos técnicos exigidos por el supervisor, incluyendo en el servicio todos y cada uno de los elementos, mano de obra necesarios y prestando el apoyo técnico y documental en el uso y consumo de servicios cloud.
  - El soporte técnico debe incluir los servicios de migración creación y optimización de los servicios y recursos de la plataforma en nube pública.
  - Implementar y ejecutar los planes de mejoramiento autorizados por el supervisor, tendientes a mantener en correcto funcionamiento de la plataforma en la nube pública.

- Documentar, actualizar y mantener los documentos técnicos en materia de la plataforma tecnológica en la nube pública, de conformidad con los lineamientos establecidos por las partes.
- Generar un informe semestral con la lista de servidores sin utilizar en un período igual o mayor a 1 mes. De igual forma, apoyar todas las actividades de tipo técnico que se requiera para el ajuste de los servicios desplegados.
- Realizar actividades de mantenimiento, configuración, acompañamiento y optimización de la infraestructura, servicios de contenedores, servicios de inteligencia artificial aprovisionados en las diferentes nubes.

3.9.2 Disponibilidad y cobertura

- El proveedor garantizará la operación ininterrumpida del SOC y el NOC bajo un esquema **24x7**, con monitoreo, detección y respuesta a incidentes en tiempo real, acorde a los acuerdos de nivel de servicio (ANS).
- Garantizar la disponibilidad de personal especializado en ciberseguridad, la plataforma tecnológica y gestión de red, con certificaciones y experiencia demostrable.
- Implementar herramientas de monitoreo y detección de amenazas en tiempo real, garantizando su actualización y correcta configuración.
- Asegurar el cumplimiento de los ANS definidos y reportar cualquier desviación en los tiempos de respuesta o resolución.
- Proveer reportes diarios, semanales y mensuales sobre incidentes, tendencias, mejoras implementadas y recomendaciones de seguridad.
- Coordinar con otros proveedores y autoridades en caso de ataques o fallas críticas, asegurando una comunicación efectiva y una respuesta ágil.
- Evaluar cualquier solicitud de ajuste o mejora con el gerente del proyecto y la entidad antes de su ejecución, incluyendo un análisis de impacto y estimación de tiempos y costos.
- Desplegar parches de seguridad y actualizaciones críticas en los sistemas administrados, asegurando la continuidad de la operación.
- Definir e implementar controles de acceso y segmentación de red para minimizar riesgos de seguridad.
- Ejecutar simulaciones y pruebas de respuesta ante incidentes de seguridad y fallos de red de forma periódica.
- Realizar análisis de tendencias de ataques y generar recomendaciones para reforzar la postura de seguridad de la organización.
- Coordinar con otros proveedores y autoridades en caso de ataques o fallas críticas.
- Evaluar cualquier solicitud de ajuste o mejora con el gerente del proyecto y la entidad antes de su ejecución.
- Implementar y mantener una herramienta de **IT Service Management (ITSM)** que permita la gestión completa de tickets, incluyendo registro, categorización, escalamiento, resolución y seguimiento de incidentes y solicitudes.
- Medición y generación en tiempo real de reportes de los índices de gestión del funcionamiento de servicios de soporte técnico y niveles de servicio tanto internos como de terceros mediante reportes estadísticos. La medición de los tiempos de atención y soporte técnico para cada solicitud deberá incluir todos los tiempos asociados hasta la solución definitiva (atención de primer nivel, escalamientos de segundo y tercer nivel que incluye escalamientos a proveedores externos).

3.9.3 Monitoreo y operación

En el marco del contrato para la prestación de servicios de administración, gestión, soporte y mantenimiento de la solución de monitoreo, el Proveedor se obliga a cumplir con las siguientes responsabilidades para garantizar el adecuado funcionamiento, disponibilidad y rendimiento de la plataforma tecnológica en la nube pública donde esta funcionado la solución. Estas obligaciones incluyen la implementación, administración y operación de la solución de monitoreo, así como el soporte técnico y mantenimiento de la herramienta, asegurando que la solución cuente con respaldo directo del fabricante.

Adicional a lo anterior, el soporte y monitoreo debe contar como mínimo con las siguientes características:

1. **Administración y gestión de la solución de monitoreo**

- **Instalar, configurar y poner en operación** la solución de monitoreo, asegurando que la implementación cumpla con las recomendaciones y lineamientos técnicos definidos por el fabricante y las políticas internas de la entidad.
- **Administrar la solución de monitoreo** de manera proactiva, asegurando la correcta configuración y operación de todos los componentes, módulos y agentes instalados en la plataforma tecnológica.
- **Gestionar y mantener la conectividad** entre la solución de monitoreo y los diferentes componentes de la infraestructura tecnológica (servidores, bases de datos, redes, aplicaciones, software de capa media, sistemas operativos, dispositivos de almacenamiento, seguridad, servicios PaaS/SaaS, entre otros).
- **Administrar las políticas de monitoreo** para garantizar que se detecten y gestionen de manera oportuna los eventos relacionados con la disponibilidad, el rendimiento y la capacidad de la plataforma tecnológica.
- **Implementar y actualizar dashboards personalizados** para facilitar la visualización y análisis de métricas clave de rendimiento y disponibilidad de la plataforma tecnológica.
- **Definir y mantener los umbrales de alerta** para la identificación y notificación automática de incidentes en los diferentes componentes de la plataforma tecnológica.
- **Gestionar las credenciales de acceso y permisos** a la solución de monitoreo, asegurando la aplicación de controles de seguridad para proteger la integridad y confidencialidad de la información monitoreada.
- **Realizar revisiones periódicas de la configuración** de la solución de monitoreo para optimizar el desempeño y ajustar las políticas de monitoreo a las necesidades cambiantes de la entidad.

2. **Monitoreo continuo de la plataforma tecnológica**

- **Implementar un esquema de monitoreo continuo 24x7x365** que permita la detección temprana de incidentes, fallas o degradaciones en el desempeño de la plataforma tecnológica.
- **Monitorear el estado y rendimiento** de los siguientes componentes de la plataforma tecnológica:

  - Servidores.
  - Bases de datos y sistemas de almacenamiento.
  - Redes y dispositivos de conectividad.
  - Sistemas operativos y entornos de virtualización.
  - Software de capa media y de servicios de integración
  - Orquestación y contenedores
  - Servicios y aplicaciones empresariales.
  - Dispositivos de seguridad (firewalls, IPS, etc.).
  - Recursos en la nube pública PaaS/SaaS.
- **Generar y gestionar alertas automáticas** basadas en umbrales predefinidos para detectar anomalías, fallas y degradaciones en el rendimiento.
- **Configurar notificaciones en tiempo real** hacia los equipos técnicos y responsables designados por la entidad ante la ocurrencia de eventos críticos o de alto impacto.
- **Realizar un análisis proactivo de tendencias** para identificar patrones de comportamiento y anticipar posibles incidentes antes de que afecten la operación.
- **Generar reportes en tiempo real** sobre el estado de los servicios monitoreados, consolidando métricas clave de disponibilidad, capacidad y rendimiento.
- **Garantizar la precisión y consistencia** de los datos recolectados por la solución de monitoreo, asegurando que las métricas reportadas reflejen el estado real de la plataforma tecnológica.

3. Mantenimiento de la solución de monitoreo

- **Realizar mantenimientos preventivos periódicos** de la solución de monitoreo, asegurando que todos los componentes estén actualizados y configurados correctamente.
- **Aplicar actualizaciones de seguridad, parches y mejoras** recomendadas por el fabricante, garantizando la continuidad del soporte oficial.
- **Validar la compatibilidad** de las actualizaciones con la infraestructura tecnológica de la entidad antes de su implementación.
- **Gestionar el licenciamiento de la solución** para garantizar que las licencias estén vigentes y alineadas con las necesidades de la entidad.
- **Optimizar los procesos de monitoreo** mediante la revisión y ajuste de configuraciones, parámetros y políticas de monitoreo.
- **Realizar pruebas de funcionamiento y rendimiento** posteriores a cada mantenimiento para verificar que la solución opera correctamente.

4. Obligaciones relacionadas con el fabricante de la nube pública

- **Garantizar que la solución esté soportada por el fabricante** y que las versiones implementadas estén dentro del ciclo de vida del soporte oficial.
- **Gestionar directamente con el fabricante** la resolución de problemas complejos que requieran intervención especializada.
- **Participar en sesiones técnicas o capacitaciones** impartidas por el fabricante para mantenerse actualizado sobre mejoras y nuevas funcionalidades.
- **Implementar las recomendaciones técnicas y de seguridad** proporcionadas por el fabricante.

5. **Reportes y documentación**

- **Generar reportes mensuales y trimestrales** que incluyan:
  - Disponibilidad de la plataforma tecnológica.
  - Incidentes y problemas registrados.
  - Tiempo de respuesta y resolución (conforme a los Niveles de Servicio NS).
  - Análisis de causa raíz (RCA) de incidentes críticos.
  - Estado del licenciamiento y soporte de la solución de monitoreo.
  - Recomendaciones de mejora.
- **Proporcionar acceso a la documentación técnica actualizada** de la solución de monitoreo, incluyendo configuraciones, políticas y cambios aplicados.
- **Registrar y documentar todas las actividades** de mantenimiento y soporte realizadas en la solución de monitoreo.
- **Proveer evidencia de la correcta operación** de la solución de monitoreo y de las acciones ejecutadas para garantizar la disponibilidad y estabilidad de la plataforma tecnológica.

6. **Establecer un modelo de gobernanza y gestión del cambio**

- El proveedor debe implementar un modelo de gobernanza que incluya:
- Revisión periódica del cumplimiento de niveles de servicio (ANS) y desempeño.
- Control de cambios mediante un proceso de aprobación documentado.
- Asegurar que las actualizaciones o mejoras de servicios no afecten la continuidad operativa.

El proveedor debe notificar a la entidad con al menos 15 días de anticipación cualquier cambio que afecte la integración o funcionalidad.

3.10 ENTREGA DE OPERACIÓN FIN CONTRATO

- El proveedor deberá elaborar y presentar a la entidad, con al menos seis (6) meses de anticipación al vencimiento del contrato o en el caso de un cambio de proveedor, un Plan de Transición detallado, aprobado por la entidad designada. Este plan deberá incluir cronograma, responsables, entregables, riesgos identificados y medidas de mitigación.
- La transición debe incluir la entrega de la siguiente documentación:
  - Arquitectura tecnológica de la solución.
  - Diagrama de flujo de datos y procesos operativos.
  - Configuraciones de la plataforma y parametrizaciones clave.
  - Manuales técnicos, operativos y de administración del sistema.
  - Manuales de usuario final.
  - Documentación de integraciones y APIs.
  - Base de datos completa y actualizada, en formato reutilizable, acompañada de su respectivo diccionario de datos.
  - Listado completo de licencias de software utilizadas (propias, de terceros, libres y comerciales).
  - Cesión de derechos patrimoniales.

- Copias de contratos/licencias con terceros.
- Certificado en el que se confirme que no existen componentes cuya licencia impida la transferencia, uso o modificación por parte de la entidad designada o el nuevo proveedor.

- Se debe desarrollar una fase de transferencia del conocimiento técnico y funcional al nuevo proveedor o al equipo que la entidad designe. Esto debe incluir sesiones de capacitación, entrega de documentación y acompañamiento durante un período mínimo de 3 meses, para garantizar la curva de aprendizaje y la continuidad del servicio.
- Se proporcionará un informe de cierre con el estado actual de la plataforma y sus componentes, el historial de incidentes presentados durante la operación y las soluciones aplicadas, incluyendo aquellas incidencias que permanezcan pendientes de resolución; el informe también deberá detallar las mejoras y cambios implementados a lo largo del contrato, así como incluir recomendaciones técnicas y operativas que faciliten la continuidad y optimización del servicio por parte del nuevo operador.
- Se asegurarán mecanismos de respaldo y continuidad para evitar interrupciones durante la transición.
- Entrega segura y verificada de todas las credenciales, accesos y claves necesarias para el funcionamiento del sistema, bajo supervisión de la entidad designada por la corporación.
- El proveedor deberá entregar evidencia de cumplimiento de obligaciones legales, regulatorias y contractuales durante la ejecución del contrato, incluyendo aspectos relacionados con la protección de datos personales, seguridad de la información, y gestión de riesgos operativos.

3.11 Operación del Fondo de Pasivo Contingente

Con el fin de implementar las nuevas coberturas otorgadas por el Fondo Pasivo Contingente (FPC), además de los desarrollos tecnológicos para la gestión de las coberturas y/o asistencias, el proveedor deberá disponer de un equipo de trabajo mínimo para dar inicio a la operación de las coberturas de desempleo y enfermedades catastróficas conforme a las condiciones descritas en el reglamento del Fondo.

Actividades del equipo

El equipo deberá realizar, entre otras, las siguientes actividades:

1. **Verificación del cumplimiento de las condiciones para los eventos cubiertos:**
   - Desarrollo de protocolos específicos para la verificación de cada tipo de evento (enfermedades catastróficas y desempleo).
   - Establecimiento de criterios claros y objetivos para la evaluación de los casos.
   - Implementación de procedimientos para la validación de documentos en colaboración con entidades externas.
2. **Mecanismos para el registro y seguimiento:**
   - Interoperabilidad con diferentes sistemas y entidades para facilitar la verificación del evento y el seguimiento de casos.
   - Desarrollo e implementación de un sistema digital para el registro, sistematización y

seguimiento de los casos u ocurrencia de los eventos.

3. **Elaboración de informes sobre la gestión de eventos y recomendaciones de mejora:**
   - Generación de informes periódicos sobre la gestión de los eventos cubiertos.
   - Análisis de datos para identificar áreas de mejora y recomendaciones para optimizar los procesos.
4. **Identificación de acciones para la mitigación de la materialización de eventos:**
   - Análisis de los casos para identificar patrones y factores de riesgo.
   - Desarrollo de acciones afirmativas y programas preventivos para reducir la incidencia de eventos cubiertos.

Adicionalmente, el equipo deberá estar en la capacidad de apoyar el desarrollo de mecanismos y estrategias de bienestar y acompañamiento del FPC. El bienestar de los estudiantes es una prioridad para la entidad designada. Por ello, se diseñarán planes, programas y estrategias que no solo apoyen su trayectoria académica, sino que también mejoren su calidad de vida, ofreciendo orientación y acompañamiento en diversas áreas y momentos de vida, tales como salud mental y vinculación laboral, entre otros.

Estimaciones de reclamaciones

Dado que estas coberturas son nuevas, no se cuenta con información histórica sobre las reclamaciones. Sin embargo, se estima que las reclamaciones por enfermedades catastróficas serán alrededor de 3,000 al año y para desempleo un estimado de 30,000 al año. Estas cifras pueden cambiar y deben ser consideradas como aproximaciones iniciales.