# BASES DESAFÍO:
# "MEJORAR LAS FORMAS DE PAGO EN BANCA PERSONA"

## 1. Antecedentes

El Banco República Oriental del Uruguay (BROU) y la Agencia Nacional de Investigación e Innovación (ANII) establecieron un acuerdo de cooperación con el objetivo de promover la colaboración entre el sector Fintech de Uruguay y el BROU, sirviéndose para ello de la experiencia que posee ANII en la evaluación y gestión de proyectos de innovación. Así como para facilitar el intercambio de conocimientos y experiencias, que oficien como aceleradores para el desarrollo de una cultura de innovación dentro del BROU.

En ese sentido se crea un fondo concursable para la financiación de proyectos innovadores en modalidad de desafío, que permitan plantear soluciones relacionadas con las áreas de interés de el BROU.

Los desafíos buscan resolver problemas relevantes que afectan la eficiencia, el alcance o la calidad en los servicios brindados a los ciudadanos con el objetivo de mejorarlos.

## 2. Problema/oportunidad

En la actualidad, presenciamos una transformación acelerada en la manera en que se llevan a cabo las transacciones de pago tanto a nivel local como global. Este cambio acelerado trae consigo la incorporación de nuevas modalidades y tecnologías innovadoras que están revolucionando el ecosistema financiero.

La evolución constante de las transacciones de pago nos muestra un escenario en el que los métodos tradicionales están siendo desafiados por soluciones más ágiles, seguras y convenientes. La digitalización y la adopción masiva de dispositivos móviles han impulsado el surgimiento de modalidades de pago electrónicas, como billeteras digitales y pagos sin contacto, que ofrecen comodidad y simplicidad en cada transacción.

Este vertiginoso ritmo de cambio nos desafía a estar constantemente actualizados y preparados para adoptar estas nuevas modalidades y tecnologías. Los bancos y las instituciones financieras deben adaptarse rápidamente para ofrecer a sus clientes una amplia gama de opciones de pago que se ajusten a sus necesidades y preferencias.

En este contexto, el BROU busca promover una mejora en las transacciones de pago que refleje el impulso constante hacia la eficiencia, la seguridad y la comodidad financiera. En un mundo cada vez más interconectado, el BROU reconoce la importancia de adaptarse y adoptar modalidades y tecnologías innovadoras como un factor clave para brindar a sus clientes una experiencia de pago óptima y satisfactoria.[1]

## 3. Desafío

El desafío consiste en explorar nuevas soluciones que permitan mejorar las formas de pago en la banca persona, alineadas con la hoja de ruta del Banco Central del Uruguay (BCU).[2]

[1] El BROU se reserva el derecho de proporcionar información sobre los trabajos en ejecución relacionados con esta temática, conforme a sus políticas de confidencialidad.

[2] https://www.bcu.gub.uy/Sistema-de-Pagos/Documents/Sistema%20de%20Pagos-hoja-de-ruta-2025.pdf

A modo de ejemplo, mencionamos algunos aspectos a considerar:

- Idea innovadora: Soluciones originales, creativas y/o disruptivas con un enfoque original al problema o desafío planteado, que vayan más allá de la aplicación de tecnología innovadora.

- Innovación tecnológica: Soluciones que incorporen tecnologías emergentes, como blockchain, inteligencia artificial, internet de las cosas u otras tecnologías disruptivas que puedan agilizar y asegurar las transacciones de pago.

- Seguridad: Soluciones que garanticen la seguridad de las transacciones y la información sensible.

- Interoperabilidad: Soluciones que permitan la interoperabilidad con otros sistemas y entidades financieras, para facilitar la adopción y el uso generalizado.

- Cumplimiento normativo: Las soluciones alineadas con las regulaciones y normativas establecidas por el Banco Central del Uruguay y otras autoridades competentes.

- Experiencia del usuario: Soluciones intuitivas, fáciles de usar y que se adapten a las necesidades y preferencias de los clientes.

- Eficiencia operativa: Soluciones que optimicen los procesos internos de la banca, mejorando la eficiencia en la gestión de pagos y reduciendo costos.

Objetivos esperados:

1- Obtener una solución innovadora que aporte un diferencial para el Banco respecto al resto del sistema financiero.

2- Mejorar la rapidez y eficiencia de las transacciones de pago para los usuarios de banca persona, reduciendo los tiempos de procesamiento y agilizando el flujo de las transacciones.

3- Optimizar la experiencia del usuario al realizar pagos.

4- Garantizar la seguridad de las transacciones, implementando medidas robustas de protección y prevención de fraudes para salvaguardar la información financiera y personal de los usuarios.

5- Impulsar la confianza y la satisfacción del usuario, brindando una experiencia de pago ágil, segura y conveniente que cumpla con las expectativas y necesidades de los usuarios de banca persona.

El proyecto deberá entregar el **prototipo funcional no productivo** de la solución operativa, la documentación correspondiente, así como cualquier elemento surgido de los trabajos realizados, otorgando al BROU el uso irrestricto del desarrollo asociado al prototipo, así como la posibilidad de modificación por un tiempo ilimitado sin coste adicional.

Adicionalmente el solucionador seleccionado, al entregar la versión final del prototipo funcional no productivo deberá entregar conjuntamente un documento, **"plan de adecuación**", donde se detallen los apartamientos del prototipo entregado respecto de los requerimientos exigidos para su integración en BROU, así como un plan de alto nivel, para adecuar el mismo a los estándares exigidos para su implantación en las instalaciones del Banco.

## 4. Participantes

Podrán participar de este desafío aportando potenciales soluciones empresas del sector privado en forma individual o en conjunto con organizaciones de I+D+i[3], que estén radicadas en el país.

## 5. Condiciones de financiamiento

La solución seleccionada será financiada en forma total.

El financiamiento puede alcanzar un monto máximo de hasta **UYU 4.260.000** (cuatro millones doscientos sesenta mil pesos uruguayos), impuestos incluidos.

Se contará con un plazo de 6 (seis) meses para el desarrollo de la solución. El plazo podrá ampliarse en caso de solicitud fundada del adjudicatario.

Rubros financiables:

- Materiales e insumos
- Software y licencias
- Personal técnico[4]
- Consultores
- Servicios
- Protección propiedad intelectual
- Otros costos
- Imprevistos

Con recursos provenientes del desafío no se podrán financiar actividades que no estén directamente relacionadas con el proyecto, quedando explícitamente excluidas, entre otras, las siguientes:

- Inversión en activos fijos.
- Inversiones (por ejemplo equipos e instalaciones) que se destinen a la actividad y/o operación habitual de la empresa.
- Personal administrativo de las proponentes.
- Inversiones financieras, tales como depósitos a plazo, fondos mutuos, compra de acciones.
- Pago de deudas de cualquier tipo de la empresa.
- Gastos operacionales recurrentes de la empresa.

El BROU y la ANII no se comprometen a continuar con un vínculo con el solucionador posterior al desarrollo del proyecto comprendido en este desafío.

Los proyectos no podrán centrarse en la adquisición de tecnología llave en mano.

[3] Nos referimos a instituciones académicas, centros de investigación, centros tecnológicos, entre otros.

[4] Rigen los topes de remuneraciones financiables para personal dependiente.

## 6. Etapas del desafío

A. Llamado a perfiles de solución. Llamado a presentación de perfiles de solución completando el formulario en el sitio de ANII. **Los postulantes tendrán tiempo hasta el viernes 14 de junio de 2024 a las 14h** para la presentación del perfil.

Los perfiles son propuestas básicas, basadas en información general y en los elementos centrales del desafío que permitan tener una primera idea sobre la posible solución a desarrollar. Esto implica considerar los siguientes ítems: descripción de la propuesta de solución, antecedentes del equipo de trabajo, objetivos y metodologías, recursos humanos y materiales necesarios, así como un presupuesto inicial.

La descripción de la propuesta de solución deberá contener elementos tales como:

- Necesidad que resuelve o diferencial que aporta al Banco y/o a sus clientes la idea una vez implementada
- Indicar si está alineado a tendencias de mercado
- Cómo enmarca su solución en el contexto local y regional
- Componentes o bloques a alto nivel de la solución
- Propuesta indicando cómo el Banco rentabilizaría la solución. (opcional)
- Que evolución / explotación a futuro prevé (opcional)

B. Selección de perfiles de solución. El Comité de evaluación y seguimiento (CES), hará la evaluación de los perfiles y seleccionará los que formularán el proyecto final.

C. Formulación de proyectos finales en base a perfiles de solución aprobados. Se invitará a los perfiles de solución seleccionados previamente a formular los proyectos de solución finales. En el mismo se deberá profundizar en los antecedentes del proponente, capacidad del equipo de trabajo, descripción del proyecto de solución, incluyendo: mérito innovador o valor diferencial propuesto, viabilidad técnica, objetivos, resultados, cronograma de ejecución.

Adicionalmente deberá profundizar en la descripción de su propuesta de solución e incorporar elementos tales como:

- Documentación técnica que sustente la idea a implementar
- Funcionalidades que incluirá el prototipo
- Diagramas básicos de casos de uso de las principales funcionalidades
- Componentes y tecnologías clave utilizadas
- Arquitectura general de la solución y sus componentes clave

A su vez el proyecto deberá contener un presupuesto detallado por rubros financiables. Los postulantes de soluciones tendrán ***30 días corridos*** para completar la formulación del proyecto final.

D. Evaluación de proyectos finales. Una vez completada la etapa de formulación de proyectos, el Comité de Evaluación y Seguimiento (CES) realizará la evaluación y selección de un proyecto final. Como parte de este proceso de evaluación se podrá solicitar la presentación oral del proyecto a través de una instancia virtual o presencial a aquellos postulantes que el CES entienda pertinente y oportuno, previo a realizar la selección de la propuesta que desarrollará la solución.

Al momento de evaluar los proyectos se tendrán en cuenta los siguientes aspectos.

Criterios de elegibilidad:

- La organización deberá estar radicada en la República Oriental del Uruguay.

- La organización radicada en el país puede asociarse con una organización radicada en el exterior.
- Estar al día con sus obligaciones fiscales.
- Presentación de un responsable.
- Formulario debidamente completado.

Criterios de pertinencia:

- Se evaluará la adecuación propuesta a las bases del llamado.
- La propuesta debe incluir todos los requerimientos descritos en el punto tres de estas bases.
- La propuesta debe demostrar que se genera una solución y que es aplicable a los fines de este desafío.

Criterios para la evaluación de la solución:

- Mérito innovador y valor agregado diferencial: Evalúa el tipo y grado de innovación que implicaría la ejecución del proyecto, así como el valor agregado propuesto.
- Viabilidad técnica: El proyecto debe demostrar que la propuesta que se pretende desarrollar es tecnológicamente factible y que cumplirá con los requisitos técnicos exigidos en el punto 7.1. Es importante también la coherencia de los objetivos con el problema planteado, su claridad, así como los tiempos y los costos. Se evaluará cuán detallada y clara es la explicación de la implementación de la idea propuesta, los componentes y tecnología utilizada, la interacción propuesta y su arquitectura, entre otros.
- Impacto en la eficiencia, alcance o calidad del producto o servicio ofrecido por el organismo público: Es importante destacar los beneficios que se obtendrían de implementar la solución propuesta, tanto para el organismo que propone el desafío cómo para la población que utilice el producto o servicio.
- Capacidad del equipo de trabajo: La organización que presenta el proyecto deberá demostrar que dispone de las capacidades para llevarlo a cabo, es decir, que dispone de los recursos humanos capaces de gestionar y supervisar las actividades establecidas en el proyecto.
- Plan de Proyecto: Debe establecer una propuesta de plan de proyecto incluyendo el cronograma de trabajo organizado en etapas y considerando los artefactos que entienda relevantes.
- Presupuesto: El proyecto debe establecer un presupuesto razonable y balanceado.

Para completar la evaluación, se podrá solicitar la incorporación de un video explicativo de la solución planteada en el formulario, así como convocar a una entrevista presencial o virtual a los actores cuyo involucramiento y/o participación considere relevante para la implementación de la propuesta.

Se podrá aprobar (de forma total o parcial) un proyecto de solución para el desafío, así como sugerir la asociatividad entre distintas propuestas recibidas. En caso de no resultar satisfactorio o pertinente ningún proyecto presentado, el desafío podrá declararse desierto.

## 7. Requisitos técnicos

Dada la amplitud y diversidad de los estándares técnicos manejados por el BROU para desarrollos de software, se ha definido exigir para la propuesta de **prototipo** un conjunto básico reducido de los mismos (detallados en el punto 7.1), con el fin de facilitar el desarrollo para el solucionador seleccionado, permitiendo centrarse en la idea propuesta y funcionalidades asociadas, y que puedan presentar el prototipo de un producto que luego eventualmente pueda evolucionar a una solución corporativa.

Asimismo, al momento de entregar el prototipo desarrollado por parte del solucionador seleccionado el mismo deberá presentar también un **plan de adecuación de alto nivel** del prototipo a los estándares y lineamientos tecnológicos que forman parte de los requisitos obligatorios del BROU para soluciones corporativas (detallados en el punto 10.1), indicando para cada caso, aspectos tales como la dificultad o complejidad de la adecuación, el tiempo de trabajo necesario y los principales pasos requeridos para efectuarla. Adicionalmente deberá identificar los distintos componentes de hardware y software necesarios.

Se valorará positivamente que el solucionador incorpore en su propuesta de prototipo la mayor cantidad de estándares posible del punto 10.1 y que, para aquellos estándares no contemplados inicialmente, la adecuación requiera un esfuerzo menor.

En caso que el proyecto requiera el uso de un framework de desarrollo o cierta tecnología para la cual aún no se cuenta con un estándar técnico definido, el plan de adecuación deberá consistir en una breve investigación y análisis de alternativas justificando la elección propuesta e identificando el licenciamiento requerido. La tecnología elegida como definitiva no tiene por qué coincidir con la utilizada en el prototipo, en cuyo caso deberá presentar también la información de adecuación tecnológica correspondiente. El Banco se reserva el derecho de la aceptación de la tecnología propuesta para un uso posterior.

La solución deberá asumir la existencia de un sistema core bancario que disponibiliza servicios a través de interfaces de software definidas, mediante las cuales, podrá obtener información y realizar diversas operaciones como transferencias bancarias/interbancarias o pagos. La solución propuesta deberá resolver estas operaciones a través de dichas interfaces del mencionado sistema core bancario.

Se debe tomar como base las interfaces publicadas en el siguiente enlace: https://support.dlya.com.uy/apibanking/#introduccion donde se describen, entre otros, un conjunto de servicios del Core Bancario indicando datos de entrada, salidas, tipos de datos, códigos de error e invocaciones. De no existir en la lista provista el servicio específico necesario, podrá proponer uno.

Para la implementación del prototipo el solucionador no contará con interconexión a la infraestructura tecnológica del Banco, en su lugar deberán simular dichas interfaces y generar los datos de prueba necesarios para la implementación y validación de la solución.

A solicitud del Banco deberá realizar una demostración presentando el avance del prototipo implementado, sus funcionalidades y mostrar el cumplimiento de requisitos técnicos.

### 7.1. Requerimientos técnicos a tener en cuenta en la etapa de formulación de proyectos finales para el prototipo.

#### 7.1.1. Arquitectura

La solución debe basarse en arquitectura web en al menos tres capas (presentación, negocio y datos), debiéndose contar con un bajo acoplamiento entre ellas. Dichas capas deben poder instalarse en servidores diferentes ubicados en distintas zonas de seguridad, y la comunicación entre los componentes distribuidos debe hacerse mediante API REST o SOAP.

Como modelo de despliegue se acepta el uso de máquinas virtuales o contenedores. En caso de utilizar contenedores, deberán ser compatibles con OCI (Open Container Initaitive).

La solución deberá poder ser utilizada en Alta disponibilidad y ser escalable horizontalmente.

#### 7.1.2. Base de datos

La persistencia de la solución deberá basarse en modelos relacionales utilizando algún DBMS estándar del mercado.

En caso de requerir el uso de bases de datos NoSQL u otra tecnología para la persistencia de datos, para algún componente de la solución que no requiera transaccionalidad ni las mismas exigencias de persistencia de los datos, podrá hacerlo justificándolo apropiadamente.

#### 7.1.3. Lenguajes de desarrollo y frameworks

Para el FrontEnd podrá usarse cualquier framework de desarrollo siempre que se genere un sitio web con diseño responsive o una aplicación móvil nativa. Si bien para el prototipo será suficiente generar una aplicación móvil Android, deberá utilizarse un framework que viabilice una fácil migración de lo desarrollado a IOs

Para el BackEnd se admitirá cualquier framework de desarrollo, teniendo en cuenta que se valorará la migración a bajo costo hacia los lenguajes aceptados por el Banco.

#### 7.1.4. Integración

Debe utilizarse API REST o SOAP como mecanismos de integración con el resto de las aplicaciones del Banco o externas que sean requeridas.

#### 7.1.5. Seguridad

Se deberán implementar buenas prácticas de desarrollo que tengan en cuenta la seguridad, así como contemplar en el mismo los vectores de ataques descritos en el OWASP Top Ten y OWASP Top Ten mobile[5].

Se debe implementar diversas recomendaciones estándar de seguridad, algunas de las cuales son de aplicación al desarrollo de WebServices, como ser:

- Implementar seguridad robusta a nivel de transporte,
- Utilizar protocolo HTTPS,
- Realizar autenticación de endpoints mediante certificados,
- Realizar la autorización basada en principios de mínimo privilegio y separación de funciones,
- Realizar validación del contenido del mensaje previo a su procesamiento por la capa de negocio,
- Tomar medidas de protección contra Cross-site scripting attacks, asegurando que las respuestas son consumidas como datos y no como scripts
- Restringir la cantidad máxima de mensajes a procesar por unidad de tiempo y la cantidad de transformaciones criptográficas simultaneas soportadas para minimizar impacto de ataques DoS,

[5] https://owasp.org/www-project-mobile-top-10/

- Evitar generar mensajes de respuesta que expongan detalles de la tecnología utilizada,
- Generar servicios que eviten las invocaciones duplicadas (pej generar servicios idempotentes y utilizar id único de transacción)
- Deberá poder integrarse con la tecnología Middleware utilizada como proxy y WAF en el Banco, Los servicios serán accedidos a través de dichas tecnologías que actuarán como intermediario.

En caso de implementar integración con SOAP, se debe adoptar protección de mensajes con WS-Security. En caso de implementar API REST se debe utilizar mensajería con token de autenticación y autorización en cada mensaje.

Los certificados utilizados para la autenticación y/o cifrado deberán cumplir con estándar X.509 (RFC5280), siendo los mismos avalados por una autoridad certificadora válida para el cifrado de clave pública.

El control de acceso de la solución debe implementarse en la capa de presentación o negocio, ya que la conexión a la base de datos debe realizarse con un usuario genérico con permisos restringidos, no debiendo ser el dueño del esquema.

Los permisos deben otorgarse de acuerdo al principio de mínimo privilegio / necesidad de hacer-necesidad de saber.

Las contraseñas deben resguardarse de forma segura con un cifrado estándar o utilizar Key Derivation Functions y deben poder modificarse periódicamente.

Para el manejo de usuarios de clientes se admitirán métodos robustos de autenticación tales como Identidad Digital (validadas por AGESIC), o mecanismos propios que implementen más de un factor de autenticación. Para la autorización se deben implementar protocolos seguros como OAuth 2.0 que validen contra un sistema centralizado.

En cuanto al manejo de usuarios internos de la institución, la autenticación debe realizarse mediante integración con un LDAP corporativo utilizando protocolos seguros. La autorización de usuarios, se gestionará mediante funcionalidades de LDAP o módulo de seguridad incluido en la solución según corresponda, deberá existir segregaciones por roles, cuyos permisos deben poder asignarse de forma parametrizable.

Deberá utilizar canales de comunicación seguros entre módulos o componentes externos e internos.

Se deben identificar y habilitar la cantidad mínima de puertos abiertos necesarios para el funcionamiento de la solución.

#### 7.1.6. Auditoría

La solución deberá implementar un mecanismo propio de auditoría, no pudiéndose utilizar la auditoría de la base de datos.

#### 7.1.7. Logs

Los logs deberán ser almacenados en formatos legibles en archivos.

Se deberán permitir diferentes niveles de log (debug, warn, info, error) de acuerdo a criterios de los desarrolladores de la solución.

Deberá poder centralizar los logs a un servidor independiente centralizado utilizando la tecnología definida en el Banco.

#### 7.1.8. Correo electrónico

Para el caso que la solución interactúe con correo electrónico interno o externo, esta comunicación se realizará al servidor de correo corporativo mediante protocolos SMTP para correo saliente y POP3S o IMAP para correo entrante.

#### 7.1.9. Documentación

Deberá presentar la documentación básica de la solución y su funcionamiento contemplando entre otros los siguientes documentos:

- Manual de usuario y manual de instalación.
- Diagramas del diseño de Arquitectura de la solución, componentes y despliegue
- Diagrama del Modelo Entidad Relación o similar utilizado y Diccionario de Datos
- Otros diagramas UML o similares (de clases, casos de uso, etc)
- Código fuente comentado.
- Plan de adecuación del prototipo a los estándares tecnológicos

## 8. Formalización, desembolsos y seguimiento de los proyectos

El ganador del desafío firmará un contrato con la ANII.

El contrato incluirá un cronograma de desembolsos asociados a hitos. La aprobación de cada hito será realizada por un Comité de seguimiento técnico, y será condición necesaria para la liberación del desembolso correspondiente.

Se retendrá el 10% del monto total hasta la aprobación del informe final.

## 9. Propiedad intelectual (PI) y garantía

La PI del desarrollo/prototipo de la solución será del proponente seleccionado. No obstante, éste le cede al BROU en forma irrevocable, ilimitada y sin costo adicional al derivado del Proyecto, el derecho al uso, modificación, adaptación, etc. ya sea a través de recursos propios o contratados, debiendo el proponente transferir los códigos y la información que el BROU requiera a estos efectos.

Por su parte el proponente seleccionado se obliga a no utilizar, ceder, licenciar, comercializar, etc., el desarrollo/ prototipo, adaptación, etc., hasta cumplidos 5 años a contar desde la entrega del prototipo desarrollado al BROU.

El proponente garantizará que no infringirá derechos de autor, de propiedad industrial e intelectual de terceros y que mantendrá indemne al BROU y ANII ante cualquier reclamo derivado de violaciones de derechos de propiedad intelectual y/o derechos de autor.

Garantía: para el caso de la constatación de fallas en los sistemas, imputables a su construcción o errores humanos del equipo solucionador/proponente, la garantía implica para la institución solucionadora la obligación de restaurar y/o corregir las fallas dejándolo/s en perfecto estado de funcionamiento, siendo exclusivamente de su costo la totalidad de los gastos y daños que por tal situación se originase. La duración de la garantía deberá ser de 6 meses una vez finalizado el desarrollo de la solución. En caso de querer

modificar el alcance y características de la garantía será responsabilidad de las partes involucradas establecer un acuerdo específico con dicho detalle según entiendan oportuno.

Por otro lado, el BROU y ANII no se comprometen a encomendar la fabricación de la solución corporativa final al ganador del desafío.

## 10. Comentarios adicionales

Previo a la implementación del prototipo el solucionador deberá firmar un acuerdo con el BROU que incluirá cláusulas de confidencialidad. Este acuerdo es necesario para poder brindar la información requerida para viabilizar la implementación de algunos puntos solicitados.

En caso que el prototipo evolucione y se alcance la oportunidad de crear una eventual relación comercial con BROU, se debe tener en cuenta que:

- El solucionador deberá declarar conocer y adherir a las políticas de prevención de lavado de activos y financiamiento del terrorismo del Banco, las cuales se encuentran publicadas en la página web del Banco en la siguiente dirección: https://www.portal.brou.com.uy/web/guest/institucional/otros

- La solución deberá ser compatible con la normativa nacional e internacional referida a la gestión de riesgos asociados al sistema de pago y a la Prevención de Lavado de Activos.

- Según el alcance del servicio que el BROU pueda solicitar al solucionador o la modalidad de vinculación que resulte del mismo y considerando las reglamentaciones previstas del TOCAF y del Banco Central a las cuales el Banco se debe ajustar, en el momento de concretar el servicio se podrán pedir las condiciones formales y/o técnicas que el solucionador deberá cumplir para establecer dicho vínculo con el BROU.

- El solucionador deberá cumplir de forma individual o en asociación con un tercero los requisitos estándar del Banco exigidos en adquisiciones de estas características (por ejemplo TOCAF, pliego único, pliego particular, etc.) y aquellos particulares que se entiendan de aplicación para el caso concreto.

- El solucionador de forma individual o en asociación con un tercero deberá demostrar solvencia económica, capacidad de respuesta (por ejemplo, para resolución de incidentes, el cumplimiento de un SLA, la administración y el mantenimiento evolutivo de la solución), capacidad de llevar adelante el plan de implantación, y que cuenta con las certificaciones y recursos técnicos profesionales necesarios, así como antecedentes en el mercado, que brinden el respaldo necesario al Banco.

En caso de que el producto se aloje en las instalaciones del Banco y pase a ser parte de la infraestructura de BROU, deberá cumplir las siguientes condiciones:

- Se deberá proteger la información en ejecución, tránsito y reposo.

- El control de acceso se basará en la autenticación de usuarios mediante Active Directory y la autorización estará basada en roles.

- Cuando la información sea crítica, atendiendo requerimientos normativos y/o de negocio, podrá requerirse Autenticación Multifactor (MFA).

- Se deberá garantizar la trazabilidad de todas las transacciones realizadas, permitiendo identificar operaciones y registros tanto exitosos como fallidos.

- La seguridad en el desarrollo de software debe ser asegurada, protegiendo todos los ambientes utilizados.

- Se deben seguir estándares como OWASP (móvil o web, según corresponda a modo de ejemplo TOP 10, ASVS/MASVS, MASTG) para prevenir vulnerabilidades. La solución propuesta deberá implementarse tomando las medidas oportunas para maximizar la seguridad de las aplicaciones, siguiendo los estándares adoptados por el Banco.

- Las pruebas de seguridad deben ser regulares desde el inicio del ciclo de vida del desarrollo de software (CVDS), incluyendo análisis de código estático para identificar y corregir vulnerabilidades antes de la implementación en producción, debiéndose proveer evidencia documental de las mismas.

- Se deberán considerar buenas prácticas para el desarrollo de software, así como reutilizar software existente para evitar introducir vulnerabilidades.

- El software debe ser configurado de forma segura por defecto y documentarse para los administradores.

- La solución deberá cumplir con los requerimientos funcionales y técnicos completos, es decir los básicos para el desarrollo del prototipo, los identificados como requeridos para una solución corporativa en el punto 10.1 y aquellos adicionales que posterior a la finalización del proyecto determine el Banco que sean de aplicación para el caso concreto. El Banco podrá exigir una prueba de concepto que contemple el cumplimiento de estos puntos.

En caso de que Banco decida modificar el producto por su cuenta:

- Una vez culminado el proyecto de diseño de la solución y construcción del prototipo, las modificaciones que se pudieran hacer al producto por el BROU o a cargo del BROU serán de propiedad intelectual del BROU a menos que se acuerde lo contrario con el solucionador.

- El Banco podrá realizar modificaciones al prototipo o solución y su evolución (solución modificada o actualizada), sin ningún tipo de costo ni restricción y sin requerir previo conocimiento del solucionador, ya sea que lo realice directamente o a través de un tercero.

### 10.1. Requerimiento Técnicos para la posible solución corporativa a implantar en el Banco

Una posible solución corporativa deberá cumplir con los requisitos técnicos básicos establecidos para el prototipo en el punto 7.1 más los indicados a continuación:

#### 10.1.1. Arquitectura

Deberá contemplar los siguientes puntos:

- No se aceptarán soluciones que tengan componentes y/o almacenen datos en la nube pública, todos los componentes deberán estar alojados en los servidores del Banco.
- La solución debe ser compatible para su ejecución en la tecnología de contenedores utilizada en el Banco.

- La solución corporativa debe estar en alta disponibilidad activo/activo, poder ser balanceada por una balanceador de carga y poder trabajar detrás de un proxy server corporativo.

### 10.1.2. Base de datos

A excepción del posible componente NoSQL mencionado en el punto 7.1.2, se aceptarán únicamente los DBMSs y conjuntos de caracteres estándar del Banco.

Se deberá describir el procedimiento de conexión a la base de datos y utilizar los drivers validados por el Banco. En el caso de modelos relacionales, la integridad deberá implementarse al menos en la Base de datos.

Se debe indicar los usuarios, permisos y roles necesarios a nivel de Base de datos.

Realizar un diseño y utilizar funcionalidades del DMBS que permitan la escalabilidad de la solución.

Codificar las sentencias SQL utilizando variables bind y no con el valor literal.

Se debe definir un método de depuración de datos históricos y reincorporación.

### 10.1.3. Lenguajes de desarrollo y frameworks

Se deberá utilizar JEE o Microsoft .NET, siendo recomendada la primera mencionada. En el caso de basarse en JEE, no deberán utilizarse componentes propietarios o extensiones a la especificación que impidan o dificulten la portabilidad de la aplicación.

Es viable plantear el uso de otros frameworks de desarrollo para el frontend, en cuyo caso, el plan de adecuación consistirá en una breve investigación y análisis de alternativas justificando la elección propuesta e identificando el licenciamiento requerido. El Banco se reserva el derecho de la aceptación de la tecnología propuesta para un uso posterior.

Con respecto a las versiones del software de base en los servidores para los distintos ambientes del Banco se deberá cumplir con los estándares definidos por el Banco.

La solución deberá ser compatible tanto con Android como con IOs.

### 10.1.4. Seguridad

La base de datos debe implementarse definiendo un usuario genérico de conexión y éste no debe ser el dueño del esquema. Esto significa que el usuario de conexión contará con permisos DML (data manipulation language) y no DDL (data definition language). La contraseña de este usuario deberá estar encriptada con un algoritmo conocido y seguro, y con la masterkey resguardada adecuadamente.

No deberá ser vulnerable a ninguno de los ataques incluidos en el Top 10 de OWASP y OWASP Top Ten mobile[6] más reciente.

[6] https://owasp.org/www-project-mobile-top-10/

Para el caso de implementación de interfaces SOAP deben considerarse, entre otros, aspectos relacionados a:

- Seguridad a nivel de mensaje
- Autenticación del Publicador y Consumidor
- Validación de Schema
- Validación de Contenido
- Protección contra Malware
- Limitación de Tamaño
- Protección contra XML DoS
- Ofuscación de WSDL

Para el caso de implementación de interfaces API REST deben considerarse, entre otros, aspectos relacionados a:

- Control de acceso del Consumidor
- Autorización del Consumidor
- restringir Verbos HTTP
- API Keys
- Validación de entrada de usuario
- Restricción de interfaces administrativas
- Uso de encabezados de seguridad
- Información sensible en pedidos HTTP
- Código de retorno HTTP

Sobre estos aspectos mencionados para ambos tipos de interfaces, se profundizará en la documentación que será entregada de acuerdo a lo indicado en el punto 10.1.8.

Tiene que ser viable la instalación de sistemas HIDS en por lo menos un componente del producto y firewall por software con filtrados restrictivos.

Debe contar con controles de seguridad en las sesiones de usuarios (ej timeout, cantidad de sesiones abiertas) siendo controles parametrizables a criterio del Banco.

La solución tecnológica deberá sincronizar la hora mediante protocolo NTP

La solución debe contemplar un Proxy Reverso o control similar, que publique y concentre el acceso evitando que los clientes se conecten directamente a los servidores de la aplicación

La solución debe contemplar un monitoreo completo del estado de salud, con métricas y alertas definidas que notifiquen de forma temprana ante desvíos. El monitoreo de los sistemas debe realizarse a través de protocolos seguros como por ejemplo SNMPv3.

Debe identificar el tráfico necesario para su funcionamiento y requerir únicamente la habilitación de los puertos para establecer las conexiones necesarias.

Deberá cumplir con estándares de la industria, normativa y regulaciones como BCU, PCI DSS y Habeas Data.

La aplicación deberá permitir la delegación de privilegios (inclusive asociados al superusuario) y la restricción de privilegios (inclusive los del superusuario).

Usuarios genéricos: La aplicación no debería utilizar usuarios genéricos y en caso de necesitarlos, deberá haber una relación única entre las acciones del usuario genérico y el usuario conectado a la aplicación que provocó la acción del usuario genérico. Deben soportar mecanismos de subrogación para cuentas genéricas de usuarios privilegiados

Usuarios hardcode: No deberá utilizarse usuarios o perfiles en forma de hardcode dentro de la aplicación (ejemplo: SA para definir la conexión del motor de base de datos).

A los efectos de garantizar la confidencialidad e integridad de la información de carácter privado, el sistema deberá garantizar que los tráficos de esos datos y los que el negocio entienda necesarios, por cualquier medio electrónico (web, e-mail, otros), sea de origen personalizado o automatizado, estén encriptados entre la aplicación y el cliente final.

#### 10.1.5. Auditoría

La aplicación deberá implementar un mecanismo propio de auditoría, que se utilizará de forma adicional a la auditoría de la base de datos. debiendo contemplar todas las transacciones e identificar unívocamente al usuario, las acciones realizadas y el momento de realizada.

Se deberán proporcionar funcionalidades para respaldo y depuración de los registros mencionados.

Debe permitir parametrizar las actividades a auditar y la información que es necesario registrar y almacenar de las mismas.

Deberá quedar identificado, en todos los casos, el usuario que realiza la transacción, fecha, hora y equipo.

La información registrada deberá permitir la trazabilidad de las actividades, lo que incluye, accesos exitosos o intentos fallidos, consultas, transacciones, tareas de administración de usuarios y parámetros o cambios sobre información, pero no necesariamente se limita a este detalle.

Deberá contar con un módulo amigable de consulta de la auditoría y con la información necesaria para entender las pistas allí registradas. Se deberán incluir funcionalidades de búsqueda por fecha, usuario y/o transacción (como mínimo) entre los datos del registro.

#### 10.1.6. Configuración relativa al ambiente

Toda configuración relativa al ambiente, a saber, conexiones a la base de datos, URL de web services, etc., deben estar externalizados a la aplicación y deben proveerse procedimientos de cambios de los mismos. En el caso de las conexiones a la base de datos, se valorará el uso de datasources del servidor de aplicaciones como forma de externalizar los orígenes de datos.

#### 10.1.7. Procesos agendados

De requerir mantener procesos o tareas (Jobs) de ejecución reiterada (agendada o manual) deberán implementarse con las herramientas de Gestión de Carga de trabajo estándar del Banco.

#### 10.1.8. Otros requisitos a contemplar

Una vez firmado el acuerdo de confidencialidad con el Banco, el solucionador ganador tendrá acceso al resto de la documentación y requisitos técnicos a tener presente en el desarrollo del proyecto.

Entre otros, se especificarán distintos lineamientos y la tecnología utilizada, como ser la referente a Sistemas operativos, LDAP, Servidores web y de aplicaciones, DBMS, Balanceo de carga, Intercambio de archivos, Middleware, Virtualización, Contenerización y Seguridad.

## 11. Contacto

Por dudas o consultas escribir al siguiente correo: desafiobrou@anii.org.uy