CONTENIDO

1. Arquitectura software

El proponente deberá describir la arquitectura del software de la solución que está ofreciendo, el proceso de desarrollo asociado y las tecnologías utilizadas.

1.1 Tipo de software

El Banco desea una solución bajo un esquema SaaS, para esto se deberá documentar si ya se cuenta con una solución base con componentes ya implementados y de acuerdo con los requerimientos específicos del Banco es complementar las funcionalidades con desarrollos adicionales o si se va a hacer un desarrollo desde ceros para cumplir con los requerimientos solicitados por el Banco.

1.2 Arquitectura

Se deberá describir la arquitectura detallada de la solución ofrecida.

1.3 Diagrama de componentes

Se deberá presentar un diagrama de alto nivel donde se describan claramente cada una de las capas, componentes y/o módulos de cómo está construido o cómo se va a construir la solución. Se deben describir las tecnologías y lenguajes de desarrollo utilizados para la construcción de los componentes que conforman el sistema.

1.4 Diagrama de despliegue

Se deberá presentar un diagrama de despliegue donde se explique claramente la arquitectura de despliegue de la solución. El sistema debe tener mínimo 3 capas (Datos, Aplicación, Presentación), este diagrama debe dar una descripción clara de los actores del sistema, componentes de software, la infraestructura y comunicaciones que soportan la solución y donde está desplegada.

1.5 Proceso de desarrollo

Se deberá presentar la descripción del proceso de desarrollo que se implementará o se tiene implementado para la construcción de la solución.

1.6 Licenciamiento

El proponente deberá describir el esquema de licenciamiento de la plataforma, detallando los costos que se aplicará por el uso de esta. Todos los componentes de software requeridos por la plataforma para su funcionamiento deben estar debidamente licenciados o ser de propiedad del proponente.

2. Arquitectura infraestructura

2.1 Plataforma tecnológica

La propuesta deberá contener la especificación técnica de cada uno de los elementos y componentes que hacen parte de la solución. En esta descripción se deberá mencionar los servidores, sistemas operativos, sistemas manejadores de base de datos y demás componentes que apliquen. El proponente deberá garantizar que, por los próximos 3 años, las herramientas, componentes y demás que integran la solución presentada, estarán vigentes en el mercado con su debido nivel de soporte y de presentarse alguna novedad en este sentido, el proponente deberá comprometerse a realizar la correspondiente gestión para la actualización a la siguiente versión anunciada por el fabricante.

La solución propuesta como mínimo debe contar con 3 ambientes: desarrollo, pruebas y producción. El proponente deberá dar una descripción de como la solución implementa estos ambientes.

2.2 Alta disponibilidad

Se deberá explicar a nivel de la infraestructura tecnológica que soportará el sistema, si cuenta con esquemas de alta disponibilidad, o con esquemas que permitan extender esta característica. Lo anterior con el fin de garantizar que el sistema seguirá funcionando si alguno de sus componentes presenta una falla.

2.3 Disponibilidad

El proponente deberá especificar en su propuesta el acuerdo de nivel de servicio (SLA) de disponibilidad que se compromete a cumplir sobre la solución que ofrece, el cual debe ser igual o superior al **99.5%**. Se debe presentar un reporte mensual a Bancóldex de la disponibilidad de la solución, los motivos o causas de las indisponibilidades que se hayan presentado en el mes y la cantidad de operaciones realizadas por los clientes del Banco.

El incumplimiento de este SLA dará lugar a la penalización en los costos que el Banco pague por el servicio contratado. En los casos de indisponibilidad por mantenimientos programados, el proveedor deberá informar a Bancóldex el plan de trabajo establecido con mínimo quince (15) días hábiles de antelación para acordar y aprobar los horarios de los mantenimientos, esto con el fin de no afectar la operación y notificar con tiempo la indisponibilidad de la solución. El proponente debe describir cómo maneja el procedimiento de los mantenimientos programados sobre el sistema.

2.4 Contingencia

Se deberá explicar a nivel de la infraestructura si esta cuenta con esquemas de contingencia donde sus componentes se replican o pueden replicarse a centros de datos secundarios en

caso de una falla en el datacenter principal. El proponente debe especificar la ubicación de sus centros de cómputo y de operación alternos.

2.5 Escalabilidad

Se deberá explicar el detalle y la forma como la solución permite el escalamiento.

2.6 Monitoreo

El proponente deberá contar con monitoreo continuo de su plataforma tecnológica para identificar comportamientos inusuales o ciberataques, dicho monitoreo debe detectar operaciones o cambios no deseados y/o adelantar las acciones preventivas o correctivas cuando se requiera. El proponente debe informar al Banco -en su propuesta- como hace este monitoreo y establecer las estrategias de notificación y comunicación con el Banco en caso de interrupción.

3. Arquitectura de seguridad

3.1 Control de acceso

La solución propuesta debe contar con un módulo de seguridad que permita registrar, parametrizar usuarios, realizar asignación de roles y perfiles y generar reportes de trazabilidad de acciones de usuarios, bloqueo, eliminación, otros. En cualquier caso, el sistema debe manejar el control de acceso basado en roles y responsabilidades fundamentado en el principio de menor privilegio. Para los funcionarios del Banco la plataforma debe estar en la capacidad de hacer autenticación con el directorio activo de Windows. El proponente debe especificar cómo realizará esta integración y los requerimientos técnicos que el Banco debe proveer.

El sistema debe mantener el histórico de usuarios creados para efectos de la trazabilidad de las acciones realizadas en este, no se deben permitir la eliminación de los registros de usuarios.

3.2 Actualización del software

El proponente deberá garantizar la actualización del producto y/o de los componentes que integran la solución presentada, detallando la información de los componentes o productos que se van a actualizar. Dentro de la información presentada, se requiere mínimo:

- Versión del producto.
- Fecha de liberación de la versión.
- Mejoras o correcciones implementadas en la versión.
- Prerrequisitos para la actualización.

El proponente deberá contar con herramientas que permitan hacer el control de las versiones que se instalarán en los ambientes de producción, así mismo contar con procedimientos documentados para la instalación del software en producción, debe entregar al Banco como se hace este proceso.

El proponente deberá comunicar a los usuarios del Banco en la plataforma la indisponibilidad del servicio por labores programadas de mantenimiento que puedan generar indisponibilidad del sistema con 8 días previos al inicio de las actividades. Ante interrupciones mayores a una hora también debe mediar esta comunicación.

3.3 Estadísticas

El proponente deberá aportar al Banco de manera trimestral las estadísticas de disponibilidad y de uso con respecto a la prestación del servicio. Esta información debe ser conservada por 2 años. El proponente deberá indicar el detalle de la metodología utilizada para el cálculo de la disponibilidad.

4. Arquitectura de integración

4.1 Mecanismos de integración

El proponente deberá especificar qué mecanismos de integración ya tiene implementados o puede desarrollar para hacer la conexión con los sistemas del Banco y servicios de terceros (Archivos planos, Web Services, API’s, etc.), deberá especificar las características de estos y la recomendación a utilizar con base en su experiencia.

4.2 Integración de servicios

El proponente deberá especificar si la solución ya cuenta con integraciones de terceros para extender funcionalidades específicas de acuerdo con los requerimientos que el Banco pueda requerir. Se deberá describir si este esquema ya se encuentra implementado y que tipos de servicios se pueden utilizar para los requerimientos del Banco. Algunos servicios que se pueden necesitar es la conexión con entidades para servicios de autenticación fuerte.

5. Soporte técnico

El proponente deberá describir en la propuesta cómo se va a prestar el soporte técnico para la solución o para los componentes que presente en su propuesta (software base, aplicaciones, servicios, componentes, módulos, etc.). Presentar el esquema de atención, plan de comunicaciones y el equipo de soporte, si es subcontratado, describa el nombre del

subcontratista. Los tiempos de atención deben estar basados en Acuerdos de Niveles de servicio los cuales se deben especificar en la propuesta, el incumplimiento de estos dará lugar a la penalización en los costos que el Banco pague por el servicio contratado. Estos tiempos podrán ser sometidos a ajustes por las partes, según la criticidad y urgencia que se presente. Se deberá adjuntar el proceso de gestión de incidentes que se tiene implementado o que se implementará para la operación del sistema describiendo claramente los canales de atención, tiempos de respuesta y las actividades generales del proceso.

6. Certificaciones

El proveedor de servicios en la nube contar y mantener vigente, al menos, la certificación ISO 27001, y de observancia a los estándares o buenas prácticas, tales como ISO 27017 y 27018. El proveedor puede certificarse con estándares o mejores prácticas que reemplacen, sustituyan o modifiquen las anteriores.

El proponente debe entregar al Banco los informes y certificaciones que demuestren la calidad, desempeño y efectividad en la gestión de los servicios contratados. El proponente debe informar de qué manera entregará esta información al Banco.

6.1 Fuga de Información

El proponente debe especificar si la solución cuenta con mecanismos de control para la fuga de información. Se deben especificar cuáles son estos mecanismos.

6.2 Sincronización hora legal

El proponente debe comprometerse a que la hora de toda la infraestructura que soporta la solución está sincronizada con la hora legal colombiana. Se debe tener como referencia la hora oficial suministrada por la Superintendencia de Industria y Comercio.

6.3 Divulgación de la información

El proponente deberá mantener publicado sobre la solución que sea de uso del Banco las recomendaciones y medidas de seguridad y condiciones bajo las cuales se prestará el servicio, que deben conocer los clientes para el uso de la herramienta.

6.4 Privacidad de la Información

Toda la información del Banco que se encuentre almacenada en la solución propuesta es de propiedad del Banco y por tanto no podrá ser entregada a terceros. El proponente debe especificar en su propuesta como cumple con este requerimiento.

El proponente deberá garantizar que las jurisdicciones en donde se procesará la información para cualquiera de los ambientes de producción, pruebas o desarrollo 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. Se debe garantizar que esté en alguno de los países autorizados por la Superintendencia de Industria y Comercio.

7. Incidentes de seguridad de la Información, Ciberseguridad y Protección de datos personales

El proponente debe contar con mecanismos para la gestión de incidentes de ciberseguridad. Este deberá reportar al Banco de forma inmediata cualquier situación que afecte la confidencialidad, integridad o disponibilidad de la información de Bancóldex que se encuentre en la solución propuesta, o cuando se encuentre evidencia de alteración de los dispositivos usados para la solución ofrecida, así como cualquier incidente de seguridad en datos personales por violaciones de seguridad. El proponente deberá especificar en su propuesta como implementará este procedimiento en la operación del producto.

En consecuencia, con lo anterior el proponente se debe comprometer a efectuar el manejo del incidente de acuerdo con las instrucciones del Banco bajo previo acuerdo con el proponente, incluyendo la posibilidad de hacer el bloqueo del canal si es requerido. En caso de que el incidente de seguridad diera lugar a una investigación por parte de las autoridades, el proponente deberá facilitar la diligencia y aportar toda la documentación necesaria para la investigación.

8. Plan de Continuidad

El proponente debe contar con Planes de Continuidad y contingencia para los servicios ofrecidos, los mismos deben cubrir los riesgos a los que se encuentra expuesto el proponente y que pueden afectar la prestación del servicio al Banco.

Ante un evento de falla, se debe cumplir con el Tiempo Objetivo de Recuperación - (RTO) y el Punto Objetivo de Recuperación (RPO) definidos para el canal. Es importante que el proponente indique cómo da cumplimiento a este punto.

El proponente debe contar con un protocolo de comunicación con el objetivo de informar, en cuanto le sea posible, al Banco sobre cualquier evento o situación de interrupción que pudiera afectar significativamente la prestación del servicio.

El proponente debe permitir, en la medida de lo posible, vincular al Banco en la ejecución de sus pruebas / ejercicios que resulten necesarias para confirmar la efectividad de los procedimientos de contingencia para asegurar que funcionen en las condiciones requeridas.

El Banco podrá realizar, en cualquier, momento auditoria al cumplimiento de los requerimientos de continuidad de negocio para la prestación del servicio ofrecido.

El servicio debe contar con un diagrama homologado de la arquitectura de la infraestructura instalada en ambiente contingencia y producción.

La infraestructura instalada de producción y contingencia debe ser robusta y soportar adecuadamente la comunicación con plataformas transversales y debe tener la capacidad de redirigir automáticamente los servicios que consumen estas plataformas en el caso de que se presenten fallas.