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

Se deberá describir el esquema bajo el cual se hará la implementación del sistema. 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 Diagrama de componentes[1]

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.

1.3 Tecnologías

Se deberá presentar un diagrama donde se mapean las tecnologías de software y de infraestructura a cada una de las capas del sistema a implementar.

1.4 Diagrama de despliegue[2]

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. Describir si este es un esquema DevOps detallando como se hace todo el proceso y como se encuentran automatizadas las diferentes tareas. Importante mencionar cuales son los mecanismos que garantizan el desarrollo de software seguro desde el proceso de construcción y evolución del sistema.

---

[1] https://en.wikipedia.org/wiki/Component_diagram
[2] https://en.wikipedia.org/wiki/Deployment_diagram

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 el de desarrollo, pruebas y producción. El proponente deberá dar una descripción de como la solución implementa estos ambientes.

2.2 Ambientes

El sistema debe contar con ambientes totalmente independientes para los procesos de desarrollo, pruebas y producción[3]. Se deberá presentar una descripción de cómo se tienen implementados estos ambientes para la solución que se está ofreciendo.

Para los ambientes de pruebas y desarrollo solo debe permanecer el software que está siendo probado o desarrollado. Si el Banco no se encuentra en alguna de estas fases, en los servidores no debe permanecer instalación del software ni información del Banco. El proponente debe garantizar la destrucción de estos una vez finalizada la prueba.

Los ambientes mínimos que se esperan sean entregados al Banco son Pruebas y Producción.

[3] https://en.wikipedia.org/wiki/Deployment_environment

2.2.1 Ambiente de desarrollo

Es un ambiente que es instalado por los grupos de desarrollo y que tiene como propósito soportar los procesos de codificación de software para el desarrollo de nuevas funcionalidades solicitadas por un usuario.

2.2.2 Ambiente de pruebas

Es un ambiente donde se instalan las funcionalidades solicitadas por los usuarios con el propósito de que grupos de pruebas o usuarios finales puedan validar y verificar que las funcionalidades implementadas cumplen con los requisitos solicitados.

2.2.3 Ambiente de producción

Es el ambiente donde los usuarios finales interactúan con el sistema, en este se encuentran todas las funcionalidades que fueron certificadas y que cumplen con las necesidades del usuario.

2.3 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 incorporar esta característica esto con el fin de garantizar que el sistema seguirá funcionando si alguno de sus componentes presenta una falla.

2.4 Disponibilidad

El proponente deberá especificar en su propuesta el acuerdo de nivel de servicio (SLA[4]) 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 al cliente. El proponente debe describir cómo maneja el procedimiento de los mantenimientos programados sobre el sistema.

[4] https://en.wikipedia.org/wiki/Service-level_agreement

2.5 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. A su vez es necesario garantizar que el proponente cuenta con un plan de continuidad que permite responder a los RTO (8h) y RPO (1d) establecidos por el Banco.

2.6 Escalabilidad

Se deberá explicar si la solución cuenta con la capacidad de escalar vertical u horizontalmente cuando se la demanda de peticiones aumente, detallar si este escalamiento se hace de forma automática o manual y como se hace.

2.7 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. Este 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.

2.8 Backups

El proponente deberá tomar los backups de la información y del software de acuerdo con la periodicidad que el Banco le señale, para esto se deberá hacer una descripción general del esquema de backup que se tiene implementando. Adicionalmente, deberá entregar de manera periódica previo acuerdo entre las partes, medios removibles en el formato que se establezca la información respaldada para almacenamiento del Banco.

El respaldo de la información debe estar a disposición del Banco cuando la requiera. Las copias de respaldo de la información deben contar con independencia de las de otras entidades que procesan en la nube. La independencia se puede dar a nivel lógico o físico

3. Arquitectura de seguridad

3.1 Análisis de vulnerabilidades

El proponente deberá ejecutar análisis de vulnerabilidades a todos los elementos de infraestructura que soportan la solución ofrecida, una vez terminada su ejecución se deberá compromete a realizar el plan de remediación en plazo máximo de 30 días para las

clasificadas en críticas, 60 días las moderadas y 90 días las bajas. Estos informes con sus respectivos planes de remediación deberán ser entregados al Banco junto con el análisis diferencial comparando con el informe actual y el inmediatamente anterior para su revisión y conservación.

La periodicidad de ejecución de esta actividad deberá ser como mínimo 2 veces al año o cuando haya cambios importantes en la infraestructura y con los lineamientos que establece la Circular 042 de 2012 de la Superintendencia Financiera de Colombia en su numeral 7.

Se deberá dar una descripción si a la infraestructura del sistema ya se le aplica este proceso y con qué periodicidad se realiza, o si se debe implementar esto como un nuevo proceso.

A su vez el proveedor debe compartir los informes test y re-test de los análisis ejecutados con la finalidad de poder garantizar que efectivamente fueron realizados y los hallazgos remediados. Dichos informes serán soporte ante los entes regulatorios.

De preferencia, esta actividad debe ser realizada mediante herramientas homologadas CVE - Common Vunlnerabilities Exposures.

3.2 Ethical Hacking

El proponente debe ejecutar pruebas de Ethical Hacking y emprender las acciones requeridas para remediar los hallazgos identificados en dichas pruebas, como evidencia de las pruebas es requerido compartir los informes de las pruebas realizadas como soporte de las ejecuciones y remediaciones implementadas.

3.3 Desarrollo seguro

El proponente debe confirmar si cuenta con un proceso de desarrollo seguro y hacer la descripción de como hace la implementación de este detallando las herramientas o tareas que realiza para cumplir con este requerimiento. Así mismo deberá entregar un informe de la ejecución de pruebas de desarrollo seguro donde se evidencie que este no tiene fallas de seguridad, al igual que las pruebas de vulnerabilidad se requiere que los resultados de los informes sean suministrados para los entes que los soliciten.

3.4 Cifrado

El proponente debe garantizar que la información de las operaciones en tránsito o reposo debe estar cifrada, la encripción debe estar basada en estándares y algoritmos reconocidos internacionalmente que brinden al menos la seguridad ofrecida por AES o RSA. Para esto se **deberá hacer una descripción de los diferentes esquemas de cifrado que se utilizan o se pueden implementar en la solución para cifrar la información a nivel de bases de datos, repositorios de archivos, comunicaciones y demás capas del sistema**.

Se debe contar con canales de comunicación cifrados de extremo a extremo y que en lo posible usen rutas diferentes. El sistema debe contar con un certificado digital de sitio seguro.

3.5 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. La solución debe facilitar la aplicación del principio de menor privilegio para los roles y perfiles configurados. Es deseable que la plataforma realice la autenticación a través del directorio activo de Windows para los usuarios del banco. El proponente debe especificar cómo realizaría esta integración y los requerimientos técnicos que el Banco debe proveer.

El sistema debe mantener el histórico de usuarios creados por parte del Banco y para efectos de la trazabilidad de las acciones realizadas en este, no se deben permitir la eliminación y/o reutilización de los usuarios. Sin embargo, se debe permitir el bloqueo permanente de los mismos en la aplicación.

3.6 Contraseñas

Cuando la autenticación no está integrada con el directorio activo de Windows (Usuarios Bancóldex), el sistema debe permitir parametrizar las condiciones de las contraseñas tales como: su longitud mínima, el tiempo con el cual los usuarios deben hacer el cambio de contraseña, llevar registro de estas e impedir su reúso.

3.7 Inicio de sesión

La aplicación deberá informar al usuario la última fecha y hora de ingreso que este tuvo al sistema. Como también es necesario que se restringa el inicio de sesiones simultaneas desde los usuarios que se creen en el sistema de información.

El sistema deberá contar con procedimientos de ingreso (log-on) seguro entre ellos:

- Proteger contra intentos de ingreso (*Log-On*) mediante fuerza bruta
- Llevar un registro (Log) con los intentos exitosos y fallidos
- Declarar un evento de seguridad si se detecta un intento potencial o una violación exitosa de los controles de ingreso (Log-On) seguro
- No visualizar una contraseña que se esté ingresando

3.8 Tiempo de sesión

La aplicación debe contar con tiempos de cierre de sesión por inactividad del usuario, el proponente deberá especificar como es el manejo de esta sesión en el sistema, si este es parametrizable o tiene un tiempo fijo, en caso de ser así se debe informar cuanto es este tiempo.

3.9 Independencia de la información

El proponente debe garantizar una independencia de la información del Banco y sus backups con respecto a la información de otros clientes que utilice el software y procesen en la nube, esta independencia se puede hacer a nivel lógico o físico. Se deberá entregar a el Banco la descripción de cómo se está realizando esta independencia. Como también es necesario compartir diagramas de arquitectura que permita soportar la independencia y de esta manera contar con dicha visualización.

El proponente debe garantizar la entrega de información para almacenamiento del Banco.

3.10 Logs

El proponente deberá especificar como el sistema administra los logs de auditoría, los cuales deben permitir la trazabilidad de todas las acciones que realizó un usuario en el sistema. Adicionalmente, deberá garantizar que los logs de todos los componentes de infraestructura que soportan el sistema se encuentran habilitados de manera permanente con el fin de que estos se encuentran disponibles cuando el Banco requiera hacer una investigación. Se debe garantizar la copia de seguridad de estos logs por dos años, en caso de que exista una investigación estos deben ser conservados hasta la finalización de esta.

Sin modificación de la información grabada inicialmente

Los logs en la aplicación deben contener como mínimos la siguiente información:

- ✓ Identificación del funcionario que realiza la acción
- ✓ Fecha y hora en que se realizó la acción en el sistema
- ✓ Identificación de la operación realizada en el sistema y costo de esta para el cliente o usuario (si aplica).
- ✓ Dirección IP desde donde el usuario hizo la operación

3.11 Destrucción de la información

El proponente debe contar con mecanismos de borrado seguro de los datos existentes en los medios de almacenamiento, cuando lo solicite el Banco o cuando el proveedor de servicios en la nube elimine y/o reemplace dichos medios y debe certificar la destrucción de esta al Banco. Este debe informar al banco en su propuesta como hace este procedimiento.

3.11 Actualización del software

El proponente deberá garantizar la actualización del producto 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 lasversiones que se instalarán en los ambientes de producción, así mismo contar con procedimientos documentados para la instalación del software en producción, debe entregaral Banco como se hace este proceso.

El proponente deberá comunicar a los clientes 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.

3.12 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.

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. Tiempos de Respuesta

El proponente deberá describir los tiempos de respuesta promedio en los diferentes tipos de transacciones del sistema. Por ejem; Consulta, registro de facturas, cargue de soportes, etc.

REFERENCIAS

- ✓ Capítulo I del Título II de la Parte I de la Circular Básica Jurídica de la Superintendencia Financiera “CANALES, MEDIOS, SEGURIDAD Y CALIDAD EN EL MANEJO DE INFORMACIÓN EN LA PRESTACIÓN DE SERVICIOS FINANCIEROS”
- ✓ Capítulo VI del Título I de la Parte I de la Circular Básica Jurídica de la Superintendencia Financiera “REGLAS RELATIVAS AL USO DE SERVICIOS DE COMPUTACIÓN EN LA NUBE”
- ✓ Capítulo V del Título IV de la Parte I de la Circular Básica Jurídica de la Superintendencia Financiera “REQUERIMIENTOS MÍNIMOS PARA LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN Y LA CIBERSEGURIDAD”
- ✓ Ley 1581 de 2012 protección de datos personales
- ✓ Circular 028 de 2016 Superintendencia Financiera de Colombia