CONTENIDO

1. Arquitectura software

El proponente deberá proponer y describir en detalle la arquitectura del software que desarrollará para la solución requerida por el banco, el proceso de desarrollo asociado y las tecnologías utilizadas.

1.1 Tipo de software

El banco desea una solución bajo un esquema de desarrollo a la medida, donde la propiedad del software será del banco y la instalación con sus componentes se hará sobre la infraestructura On-Premise de la organización.

1.2 Arquitectura

Se deberá describir la arquitectura de solución a desarrollar con sus respectivas capas a nivel de software, esta debe ser desarrollada bajo un modelo orientado a servicios. El proponente debe presentar un blueprint de servicios del sistema donde describa como se van a desarrollar los servicios que van a soportar las necesidades funcionales hacia los clientes del banco.

1.3 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 se va a construir la solución.

1.4 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.

1.5 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 de cómo se debería montar la solución propuesta. Este diagrama deberá contemplar la implementación de la solución para el ambiente de contingencia.

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

1.6 Escalabilidad

Se deberá contemplar en el desarrollo de la arquitectura de la solución el esquema de escalabilidad del sistema a la nube de AWS, esto teniendo en cuenta que si el sistema tiene crecimiento a nivel de usuarios y con la plataforma On-Premise que cuenta el banco no es posible atender la demanda se debe migrar a la nube.

1.7 Proceso de desarrollo

Se deberá presentar la descripción del proceso de desarrollo que se implementará para la construcción de la solución. Este debe ser un esquema DevOps, se debe detallar 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. La herramienta en la cual debe estar soportado este proceso es Microsoft Azure DevOps.

1.8 Automatización de los procesos de pruebas

El proponente deberá especificar en su propuesta como se hace el proceso de automatización de las pruebas, como este se integra al proceso de desarrollo y cuáles son las herramientas utilizadas y deberá brindar acompañamiento al Banco para la ejecución de pruebas de contingencia y continuidad de negocio.

1.9 Licenciamiento

El proponente deberá describir el licenciamiento requerido para la implementación de la solución detallando claramente que componentes pueden tener costo o no para el banco.

2. Arquitectura de infraestructura

2.1 Infraestructura

El banco cuenta con tecnologías de base de datos ORACLE, servidor de aplicaciones WEBLOGIC – JBOSS EAP, servidor web JBOSS EAP. Los sistemas operativos sobre los cuales se despliegan la capa web se encuentran en sistemas operativos Linux Red Hat. El proponente podrá tomar esta arquitectura como referencia para el desarrollo de la solución, si se necesitan incorporar nuevas tecnologías el proponente las deberá especificar en su propuesta haciendo una descripción de esta y los motivos por los cuales se deberían incorporar en el desarrollo del sistema.

3. Arquitectura de seguridad

Cumplimiento Circular 042 SFC - Nuevo Canal

¿La solución informa al usuario la última fecha y hora de ingreso que este tuvo al sistema y restringe el inicio de sesiones simultaneas? **Descripción en *numeral 3.8 Inicio de Sesión***

¿La solución cuenta con tiempos de cierre de sesión por inactividad del usuario? **Descripción en *numeral 3.9 Tiempo de Sesión***

¿Cómo se realizan las verificaciones de manera constante a los enlaces del sitio web para identificar que no sean modificados ni suplantados y que la resolución de sus DNS no sea alterada?

¿Mencionar los mecanismos para incrementar la seguridad de la solución ofrecida, protegiéndola de ataques cibernéticos (denegación de servicio, inyección de código malicioso u objetos maliciosos)?

Desarrollo y Adquisición de Software

¿En el proceso de desarrollo de la solución se garantiza el desarrollo seguro de software con herramientas integradas al proceso y entrega de informes de ejecución? **Descripción en *numeral 3.1 Desarrollo Seguro***

¿Cuenta con procedimientos de control de cambios para las aplicaciones y sistemas operativos?

¿El sistema cuenta con funcionalidad para el control de versiones de software?

¿Cuenta con procedimientos y controles para el paso de programas a producción y el software en operación es catalogado?

¿La solución se somete periódicamente a un proceso de ejecución de análisis y remediación de vulnerabilidades y pruebas de penetración?

¿La información de los ambientes de producción, pruebas o desarrollo son ambientes independientes?

¿La solución permite el bloqueo (sesión o acceso) después de un número de intentos de accesos fallidos?

¿La solución cuenta con controles y alarmas (monitoreo) que informen sobre su estado, y además permitan identificar y corregir las fallas oportunamente?

¿El sistema cuenta con interfaces sencillas intuitivas y seguras para los usuarios?

¿El software utilizado por la organización cumple con los criterios de licenciamiento exigidos por el fabricante?, aplica solo si el proponente no es el dueño del software utilizado para el servicio.

¿Cuenta con procedimientos definidos para la planeación de capacidad de los sistemas de información objeto del servicio contratado?

¿La solución ofrecida permite la autenticación con el directorio activo del Banco?

¿La solución permite parametrizar las condiciones de las contraseñas como: vigencia, longitud, e impedir reutilización, ¿entre otros? **Descripción en *numeral 3.7 Contraseñas***

¿La solución proporciona un esquema de logs con los cuales se puede conocer la trazabilidad de las acciones que un usuario hizo en el sistema? **Descripción en *numeral 3.10 Logs***

¿Se garantiza la actualización del producto y de los componentes que integran la solución?

3.1 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 el software desarrollado no tiene fallas de seguridad.

3.2 Integración de herramientas

El proveedor deberá describir en su propuesta, si dentro del ciclo de vida de desarrollo integra herramientas de seguridad que permita hacer la detención de bugs, vulnerabilidades y temas de seguridad, para que estos sean corregidos en la etapa de codificación y garantizar que el software desde que se desarrolla incorpora mejoras prácticas de desarrollo seguro.

3.3 Ethical Hacking

El proveedor debe garantizar pruebas de Ethical Hacking sobre el desarrollo del sistema para lo cual deberá entregar los informes al banco, si se presentan hallazgos el proveedor debe emprender las acciones requeridas para hacer la remediación de estos. El banco podrá ejecutar pruebas adicionales de este tipo y si se presentan hallazgos estos también deben ser remediados por el proveedor.

3.4 Encripción de información

El sistema debe estar en capacidad de encriptar información para ser guardada en la Base de Datos con el fin de dotar de seguridad la información confidencial de los clientes. Durante la fase de análisis y diseño se deberá determinar qué información deberá ser guardada encriptada y cual no. Esta información puede estar definida como dato o tipo documental. El proveedor debe describir el proceso que utilizará para hacer la implementación de esta encripción de información a nivel de base de datos describiendo el tipo de algoritmos de cifrado que está en capacidad de utilizar.

3.5 Control de acceso

La solución ofrecida por el proponente debe contar con acceso de dos tipos de usuarios los cuales son funcionarios del Banco y los usuarios finales de las empresas. El desarrollo de la solución 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, 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 se debe 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 por parte del Banco y de sus clientes para efectos de la trazabilidad de las acciones realizadas en este, no se deben permitir la eliminación de los registros de usuarios. Adicionalmente se debe contar con un módulo que permita definir características de usuarios finales como por ejemplo características del dispositivo, dirección IP, entre otros.

3.6 Autenticación fuerte

El desarrollo de la solución debe estar en la capacidad de integrarse con mecanismos de autenticación fuerte que tenga el banco, esta comunicación se hace a través de servicios web.

3.7 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. Para esto se podrá implementar una solución de LDAP, actualmente el banco cuenta con Oracle Unified Directory para el registro de usuarios externos la cual puede ser tomada como referencia.

3.8 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.

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

3.9 Tiempo de sesión

La aplicación debe contar con tiempos de cierre de sesión por inactividad del usuario, el desarrollo de esta funcionalidad debe permitir la parametrización del tiempo en que la sesión estará activa cuando un usuario ingresa al sistema.

3.10 Logs

Dentro del desarrollo de la solución se debe incorporar la implementación de los logs de auditoría, los cuales deben permitir la trazabilidad de todas las acciones que realizó un usuario en el sistema.

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

El sistema debe llevar un registro de las consultas realizadas por los usuarios del Banco sobre la información confidencial de los clientes, que contenga al menos lo siguiente: identificación del usuario que realizó la consulta, fecha y hora.

4. Arquitectura de integración

4.1 Mecanismos de integración

El desarrollo del sistema debe contemplar esquemas de integración a través de archivos planos, Web Services o API's, el proponente deberá dar 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.

El Proponente deberá describir las estrategias, procesos, procedimientos y recursos que le permitirán sostener la disponibilidad y continuidad del servicio ofrecido, para cuando le ocurran eventos no previstos.