CONTENIDO

[1. Arquitectura software 3](#_Toc92379252)

[1.1 Tipo de software 3](#_Toc92379253)

[1.2 Administrador de contenido 3](#_Toc92379254)

[1.3 Diagrama de componentes 3](#_Toc92379256)

[1.4 Tecnologías 3](#_Toc92379257)

[1.5 Diagrama de despliegue 3](#_Toc92379260)

[1.6 Proceso de desarrollo 4](#_Toc92379261)

[1.7 Herramientas de Gestión y Desarrollo 4](#_Toc92379263)

[1.8 Licenciamiento 4](#_Toc92379264)

[2. Arquitectura infraestructura 4](#_Toc92379265)

[2.1 Plataforma tecnológica 4](#_Toc92379266)

[2.2 Ambientes 5](#_Toc92379267)

[2.2.1 Ambiente de desarrollo 5](#_Toc92379268)

[2.2.2 Ambiente de pruebas 5](#_Toc92379269)

[2.2.3 Ambiente de producción 5](#_Toc92379270)

[2.3 Alta disponibilidad 5](#_Toc92379271)

[2.4 Contingencia 6](#_Toc92379273)

[2.5 Escalabilidad 6](#_Toc92379275)

[2.6 Monitoreo 6](#_Toc92379276)

[2.7 Backups 6](#_Toc92379277)

[3. Arquitectura de seguridad 6](#_Toc92379280)

[3.1 Ethical Hacking 6](#_Toc92379287)

[3.2 Desarrollo seguro 6](#_Toc92379288)

[3.3 Control de acceso 6](#_Toc92379289)

[3.4 Contraseñas 7](#_Toc92379295)

[3.5 Inicio de sesión 7](#_Toc92379296)

[3.6 Tiempo de sesión 7](#_Toc92379297)

[3.7 Logs 8](#_Toc92379298)

[4. Arquitectura de integración 8](#_Toc92379299)

[4.1 Mecanismos de integración 8](#_Toc92379300)

[5. Soporte técnico 8](#_Toc92379315)

[6. Experiencia 9](#_Toc92379316)

[REFERENCIAS 9](#_Toc92379317)

# Arquitectura software

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

## Tipo de software

El banco requiere contratar el desarrollo de una solución a la medida, adaptando el uso de un CMS para cumplir con los requerimientos funcionales especificados por el banco, esta solución debe poder ser desplegada en la nube de AWS .

## Administrador de contenido

La solución debe incorporar la utilización de un CMS que permita al usuario administrar la información del sistema de forma dinámica de acuerdo con los roles que se tengan creados. El proponente deberá especificar que administrador de contenido se usará en el sistema, tecnología sobre las que este se soportará y las principales características que este incorpora.

## Diagrama de componentes[[1]](#footnote-2)

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.

## 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.

## Diagrama de despliegue[[2]](#footnote-3)

Se deberá presentar un diagrama de la solución donde se explique claramente la arquitectura de despliegue de la misma. 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.

## Proceso de desarrollo

Se deberá presentar la descripción del proceso de desarrollo el cual debe estar basado en un esquema de DevOps, el proponente debe detallar en su propuesta como implementará este proceso realizando la descripción de cómo se realizaría la automatización de las diferentes tareas desde su fase de planeación hasta la fase de despliegue. A su vez es necesario mencionar cuales son los mecanismos que garantizan el desarrollo de software seguro desde el proceso de construcción y evolución del sistema.

## Herramientas de Gestión y Desarrollo

El banco utiliza para el proceso de gestión y desarrollo la herramienta de Azure DevOps de Microsoft. Para el desarrollo de esta solución el proponente debe adaptar su proceso de gestión y desarrollo con el uso de esta herramienta, según lo mencionado en el punto anterior.

## Licenciamiento

El proponente debe detallar los costos adicionales de componentes que se requieran y que el banco deba contemplar para la implementación de esta solución.

# Arquitectura infraestructura

## 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, los cuales deberán están ubicados en la nube de AWS. El proponente deberá dar una descripción de como la solución implementa estos ambientes.

## Ambientes

El sistema debe contar con ambientes totalmente independientes para los procesos de desarrollo, pruebas y producción[[3]](#footnote-4). 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.

### 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.

### 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.

### 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. Automática

## Alta disponibilidad

El diseño de la solución debe contar con esquemas de alta disponibilidad que permitan garantizar que el sistema seguirá funcionando si alguno de sus componentes presenta una falla.

## Contingencia

El proponente debe contemplar como el banco puede implementar un esquema de contingencia de la solución.

## Escalabilidad

El proponente debe contemplar en el diseño de despliegue de la solución que esta pueda contar con la capacidad de escalar vertical u horizontalmente, teniendo en cuenta la demanda de peticiones aumente, detallar si este escalamiento se hace de forma automática o manual y como se hace.

## Monitoreo

El proponente deberá contemplar en el diseño de la solución el inventario de componentes e infraestructura critica para que el banco la pueda parametrizar en su esquema de monitoreo.

## Backups

El proponente deberá especificar los componentes y datos críticos del sistema a los cuales el banco deberá tomar los backups de la información y del software.

# Arquitectura de seguridad

## Ethical Hacking

El proponente debe emprender las acciones requeridas para remediar los hallazgos identificados en las pruebas realizadas por el banco, se debe compartir el informe de las remediaciones implementadas.

## Desarrollo seguro

El proponente debe implementar un proceso de desarrollo seguro. Así mismo deberá entregar un informe de la ejecución de pruebas de desarrollo seguro donde se evidencie que este no tiene fallas de seguridad.

## 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 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.

El Banco debe 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.

## 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. Así mismo deberá contar con un timeout para el método de recuperación de contraseña.

## 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

## 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.

## Logs

La solución deberá implementar la función de logs de auditoría, 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.

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 (sincronizado con la hora legal Colombia http://horalegal.inm.gov.co/)
* 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

Así mismo se debe generar un log que cuente con la información de la autorización del tratamiento de datos personales, en este es requerido conocer nombre del usuario, número de identificación y Fecha y hora en la que autorizo el tratamiento de datos.

# Arquitectura de integración

## Mecanismos de integración

Para la integración del sistema se deben contemplar para el desarrollo de la solución mecanismos de integración 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.

# 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.

# Experiencia

La empresa deberá demostrar experiencia en desarrollo de proyectos similares del objeto que plantea este documento (desarrollo a la medida sobre el CMS propuesto para la implementación del sistema) para verificar este cumplimiento se deben adjuntar las referencias de las empresas con los datos del contacto y fechas en la que se desarrollaron los proyectos.

# 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 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

1. <https://en.wikipedia.org/wiki/Component_diagram> [↑](#footnote-ref-2)
2. <https://en.wikipedia.org/wiki/Deployment_diagram> [↑](#footnote-ref-3)
3. <https://en.wikipedia.org/wiki/Deployment_environment> [↑](#footnote-ref-4)