CONTENIDO

[1. Observaciones Generales 3](#_Toc63694048)

[2. Arquitectura tecnológica 3](#_Toc63694049)

[2.1 Diagrama de despliegue 3](#_Toc63694050)

[2.2 Diagrama de componentes 3](#_Toc63694051)

[2.3 Plataforma tecnológica 4](#_Toc63694052)

[3. Ambientes 4](#_Toc63694053)

[3.1 Ambiente de desarrollo 4](#_Toc63694054)

[3.2 Ambiente de pruebas 4](#_Toc63694055)

[3.3 Ambiente de producción 5](#_Toc63694056)

[4. Disponibilidad 5](#_Toc63694057)

[5. Características del sistema 5](#_Toc63694058)

[5.1 Inicio de sesión 5](#_Toc63694059)

[5.2 Tiempo de sesión 5](#_Toc63694060)

[5.3 Tiempos de respuesta 5](#_Toc63694061)

[5.4 Licenciamiento 6](#_Toc63694062)

[5.5 Monitoreo 6](#_Toc63694063)

[6. Información 6](#_Toc63694064)

[6.1 Infraestructura y ubicación 6](#_Toc63694065)

[6.2 Independencia 7](#_Toc63694066)

[6.3 Backups 7](#_Toc63694067)

[6.4 Destrucción de Información 7](#_Toc63694068)

[7. Soporte técnico 7](#_Toc63694069)

[8. Requerimientos de Seguridad 8](#_Toc63694070)

[8.1 Aseguramiento de la Plataforma Tecnológica 8](#_Toc63694071)

[8.2 Desarrollo Seguro 8](#_Toc63694072)

[8.3 Incidentes de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales 8](#_Toc63694073)

[8.4 Gestión de Activos de Información 8](#_Toc63694074)

[8.5 Control de acceso 8](#_Toc63694075)

[8.6 Usuario Administrador 9](#_Toc63694076)

[8.7 Logs 9](#_Toc63694077)

[8.8 Análisis de vulnerabilidades 10](#_Toc63694078)

[8.9 Ciberseguridad 10](#_Toc63694079)

[8.10 Cadena de Suministro 10](#_Toc63694080)

[8.11 Certificaciones 11](#_Toc63694081)

[8.12 Cifrado 11](#_Toc63694082)

[9. Plan de Continuidad 11](#_Toc63694083)

[10. Referencias 12](#_Toc63694084)

# Observaciones Generales

Los requerimientos técnicos y de seguridad a los que hace referencia este documento se basan sobre el entendimiento de que el servicio a implementar para soportar la gestión de riesgo operacional y de auditoría de Bancóldex utilizará un esquema SaaS. En caso de que la propuesta de implementación sea en nube, el proveedor deberá garantizar el cumplimiento de la Circular Externa 005 de 2019 emitida por la Superintendencia Financiera de Colombia[[1]](#footnote-2) - Reglas relativas al uso de servicios de computación en la nube.

De igual forma, el proveedor del servicio debe garantizar el cumplimiento de lo que le corresponde según Circular Externa 042 de 2012 emitida por la Superintendencia Financiera de Colombia[[2]](#footnote-3).

# Arquitectura tecnológica

El proponente deberá especificar la arquitectura de los diferentes componentes; hardware, software, comunicaciones, datos y otros recursos de tecnología que tendrá la solución propuesta. Debe incluir los requerimientos mínimos y óptimos necesarios para la implementación de la solución y su correspondiente mantenimiento periódico.

## Diagrama de despliegue[[3]](#footnote-4)

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.

## Diagrama de componentes[[4]](#footnote-5)

Se deberá presentar un diagrama de alto nivel de los componentes de software que conforman el sistema. Este debe describir claramente las capas o módulos de cómo está construida la solución que se está ofreciendo.

## Plataforma tecnológica

La propuesta deberá contener la especificación técnica de cada uno de los elementos y componentes que hacen parte de la solución, los cuales son prerrequisitos para la implementación y funcionamiento de esta. En esta descripción se deberá mencionar los sistemas operativos, sistemas manejadores de base de datos, lenguajes de programación, software de terceros y demás elementos relacionados.

El proponente deberá garantizar que, por los próximos 3 años, las herramientas, componentes y demás piezas de software 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.

# Ambientes

El proponente debe contar con ambientes totalmente independientes para los procesos de desarrollo, pruebas y producción[[5]](#footnote-6). 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. El proponente debe garantizar la destrucción de estos una vez finalizada la prueba.

## 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.

# Disponibilidad

El proponente deberá especificar en su propuesta el acuerdo de nivel de servicio (SLA[[6]](#footnote-7)) 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. 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 usuario. El proponente debe describir cómo maneja el procedimiento de los mantenimientos programados sobre el sistema.

# Características del sistema

## Inicio de sesión

Es deseable que la aplicación informe al usuario la última fecha y hora de ingreso que este tuvo al sistema.

## 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.

## Tiempos de respuesta

El proponente deberá especificar en su propuesta los tiempos de respuesta que maneja el sistema para las diferentes transacciones que hacen los usuarios y a partir de cuantas sesiones concurrentes estos tiempos se empiezan a degradar. El Banco podrá exigir hacer pruebas de estrés con el fin de confirmar esta información.

## 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.

El proponente debe certificar que todo el licenciamiento dispuesto en la plataforma tecnológica y/o software utilizado en la prestación del servicio cumple con la ley de Derechos de Autor del país donde se encuentre la nube que aloja la información, si este fuera el caso.

## Monitoreo

El proponente deberá contar con monitoreo continuo de su plataforma tecnológica para identificar comportamientos inusuales o ciberataques y realizar el respectivo informe de acuerdo a lo estipulado en el punto [Incidentes de Seguridad de la Información, Ciberseguridad y Protección de Datos Personales](#_Incidentes_de_Seguridad). El proponente debe informar al banco en su propuesta cómo hace este monitoreo

# Información

## Infraestructura y ubicación

En caso de proponer un servicio en nube, el proponente deberá especificar el tipo de nube que ofrece incluyendo los sitios de procesamiento y almacenamiento de la información para el servicio.

El proponente debe garantizar que las jurisdicciones en donde se procesará la información, 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.

La infraestructura utilizada para la prestación del servicio debe convivir con el protocolo IPv4 / IPv6.

## Independencia

En caso de ofrecer un servicio en nube, el proponente debe garantizar una independencia de la información del Banco y sus *backups* con respecto a la información de otros clientes que utilicen el *software*, 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.

## Backups

En caso de ofrecer un servicio en nube, el proponente deberá establecer mecanismos que permitan contar con respaldo de la información que se procesa en la nube, la cual debe estar a disposición de la entidad cuando así lo requiera. 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.

## Destrucción de Información

Una vez finalizado el contrato el proponente o cuando el Banco lo requiera, deberá entregar toda la información al Banco en el formato acordado y certificar la destrucción segura de esta en sus sistemas o dispositivos de almacenamiento.

# 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.

# Requerimientos de Seguridad

## Aseguramiento de la Plataforma Tecnológica

El proponente deberá especificar como hace el aseguramiento de toda la plataforma tecnológica (Bases de datos, servicios web, servidores, sistemas operativos) que soportan el sistema ofrecido.

## Desarrollo Seguro

El proponente deberá garantizar que la plataforma ofrecida fue desarrollada con prácticas de desarrollo de software seguro, para esto deberá entregar un informe de análisis del código del sistema donde se evidencia que este no tiene fallas de seguridad.

## 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. El proponente deberá especificar en su propuesta cómo implementará este procedimiento en la operación del servicio.

En consecuencia, el proponente se debe comprometer a efectuar el manejo del incidente de acuerdo con las instrucciones del Banco bajo previo acuerdo con el proponente. 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.

## Gestión de Activos de 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. En caso de ofrecer el servicio en nube, y para efectos de la Ley 1581, el proponente tendrá el rol de encargado de los datos.

## 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. La plataforma debe estar en la capacidad de hacer autenticación con el directorio activo de Windows del Banco. 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 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.

Es un deseable que el sistema tenga habilitado doble factor de autenticación

El sistema debe contar con un certificado digital de sitio seguro.

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

## Usuario Administrador

El sistema deberá contar con un rol para administración centralizada de los usuarios del Banco que deberá permitir administrar los usuarios de los diferentes módulos (Riesgos, Auditoría, etc.).

## Logs

El proponente deberá especificar cómo el sistema administra los logs de auditoría, los cuales deben permitir la trazabilidad de todas las acciones que realizó un usuario en la aplicación. 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. En caso de que exista una investigación estos deben ser conservados hasta la finalización de la misma.

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
* Dirección IP desde donde el usuario hizo la operación

## Análisis de vulnerabilidades

El proponente deberá ejecutar análisis de vulnerabilidades a todos los elementos de infraestructura que soportan la solución ofrecida. De preferencia, esta actividad debe ser realizada mediante herramientas homologadas CVE - *Common Vunlnerabilities Exposures.* Una vez terminada su ejecución se deberá comprometer 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 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.

El proponente debe permitir a la entidad realizar análisis de vulnerabilidades y hacking ético sobre la plataforma WEB, con previo aviso.

## Ciberseguridad

El proponente deberá aceptar que el Banco implemente los mecanismos y procedimientos necesarios para verificar el cumplimiento normativo en relación con seguridad de la información, ciberseguridad, protección de datos y continuidad del negocio durante la vigencia del contrato. Este alcance incluye los proveedores de la cadena de suministro.

## Cadena de Suministro

El proponente deberá comunicar al Banco todos los proveedores que hacen parte de cadena de suministro de la solución propuesta. Como mínimo deberá ser una relación que contenga:

* Nombre del proveedor
* Servicio tecnológico que presta
* Año de vinculación con la empresa

## Certificaciones

Es deseable que el proponente cuente con certificación vigente ISO 27001 y observar los estándares 27017 y 27018 o puede anexar certificaciones que las reemplacen, las sustituyan o las modifiquen.

## Cifrado

En caso de ofrecer una solución en nube, el proponente debe garantizar que la información del Banco 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, RSA o 3DES.

El proveedor debe garantizar canales de comunicación para los servicios en la nube cifrados de extremo a extremo y que en lo posible usen rutas diferentes.

# 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) de mínimo 8 horas y el Punto Objetivo de Recuperación - RPO definidos para el proceso de 1 día. 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 hacer 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.

# Referencias

* Circular 042 de 2012 Superintendencia Financiera de Colombia
* Ley 1581 de 2012 protección de datos personales
* Circular 028 de 2016 Superintendencia Financiera de Colombia
* Circular 007 de 2018 Superintendencia Financiera de Colombia
* Circular 005 de 2019 Superintendencia Financiera de Colombia

1. https://www.superfinanciera.gov.co/descargas/institucional/pubFile1036287/ance005\_19.zip [↑](#footnote-ref-2)
2. https://www.superfinanciera.gov.co/descargas?com=institucional&name=pubFile1003495&downloadname=ance042\_12.doc [↑](#footnote-ref-3)
3. <https://en.wikipedia.org/wiki/Deployment_diagram> [↑](#footnote-ref-4)
4. <https://en.wikipedia.org/wiki/Component_diagram> [↑](#footnote-ref-5)
5. <https://en.wikipedia.org/wiki/Deployment_environment> [↑](#footnote-ref-6)
6. <https://en.wikipedia.org/wiki/Service-level_agreement> [↑](#footnote-ref-7)