**INDICE**

[REQUERIMIENTOS ESPECIFICOS 3](#_Toc456970352)

[1. SOLUCIÓN REQUERIDA 3](#_Toc456970353)

[2. CARACTERÍSTICAS TÉCNICAS AUTENTICACIÓN 4](#_Toc456970354)

[2.1 RECONOCIMIENTO DE LAS CARACTERÍSTICAS DEL EQUIPO O EQUIPOS MOVILES 4](#_Toc456970355)

[2.2 BIOMETRÍA 4](#_Toc456970356)

[2.3 OTP (ONE TIME PASSWORD) 4](#_Toc456970357)

[2.3.1 DISPOSITIVOS FÍSICOS OTP 4](#_Toc456970358)

[2.3.2 OTP VIRTUALES 4](#_Toc456970359)

[2.4 AUTENTICACIÓN FUERA DE BANDA 5](#_Toc456970360)

[2.5 VERIFICACIÓN Y FIRMA DE LA TRANSACCIÓN 5](#_Toc456970361)

[2.6 APLICACIÓN PARA DISPOSITIVOS MÓVILES 5](#_Toc456970362)

[2.7 SDK (Software Development Kit) 5](#_Toc456970363)

[2.8 SOLUCIÓN MULTICANAL 5](#_Toc456970364)

[2.9 INTEGRACIÓN 6](#_Toc456970365)

[2.10 EXPERIENCIA 6](#_Toc456970366)

[2.11 CUMPLIMIENTO REGULATORIO 6](#_Toc456970367)

[2.11.1 CONTINUIDAD DEL NEGOCIO 6](#_Toc456970368)

[2.11.2 CONSULTAS Y LOGS 6](#_Toc456970369)

[2.12 ACOMPAÑAMIENTO EN LA IMPLEMENTACIÓN DE LA SOLUCIÓN 6](#_Toc456970370)

[2.13 PLAN DE TRABAJO 7](#_Toc456970371)

[3. REQUERIMIENTOS TECNICOS 8](#_Toc456970372)

[3.1 LICENCIAMIENTO 8](#_Toc456970373)

[3.2 DEFINICIÓN DE CONCEPTOS Y TÉRMINOS DE LA SOLUCIÓN OFRECIDA 8](#_Toc456970374)

[3.3 ARQUITECTURA TECNÓLOGICA 8](#_Toc456970375)

[3.4 PLATAFORMA TECNOLOGICA QUE SOPORTARÁ LA SOLUCIÓN 8](#_Toc456970376)

[4. ENTREGA Y PUESTA EN MARCHA DE LA SOLUCIÓN OFRECIDA 9](#_Toc456970377)

[4.1 ESQUEMA DE IMPLANTACIÓN Y ADECUACIÓN 9](#_Toc456970378)

[4.2 PRUEBAS DE LA SOLUCIÓN OFRECIDA 9](#_Toc456970379)

[4.3 DOCUMENTACIÓN TÉCNICA Y DE USUARIO 9](#_Toc456970380)

[4.4 RECIBO Y ENTREGA DEFINITIVA 10](#_Toc456970381)

[4.5 CAPACITACIÓN QUE BRINDARÁ A LA SOLUCIÓN OFRECIDA 10](#_Toc456970382)

[4.6 GARANTÍA 10](#_Toc456970383)

[5. SOPORTE DEL SERVICIO A LA SOLUCION OFRECIDA 10](#_Toc456970384)

[5.1 MANTENIMIENTO A LA SOLUCIÓN OFRECIDA 10](#_Toc456970385)

[5.2 SOPORTE TÉCNICO A LOS COMPONENTES EXPUESTOS EN LA SOLUCIÓN OFRECIDA 11](#_Toc456970386)

# REQUERIMIENTOS ESPECIFICOS

# SOLUCIÓN REQUERIDA

El Banco está interesado en contratar una solución de seguridad informática en modalidad de licenciamiento a perpetuidad para el Banco o suscripción de uso del licenciamiento a 3 años, que provea un esquema de autenticación fuerte y que permita a sus clientes realizar transacciones seguras, garantizando la autenticidad del origen, integridad y el no repudio en todos los movimientos que se realicen a través de un portal Web para cuentas de ahorro. Este servicio en principio estará dirigido al sector empresarial para un estimado de 1.000 usuarios, dicha solución deberá ser escalable en todos sus componentes de Software y Hardware con el fin de soportar autenticación en nuevos canales que el Banco desee implementar a futuro,

Esta plataforma debe entregarse con un esquema para pruebas, producción en alta disponibilidad y contingencia.



# CARACTERÍSTICAS TÉCNICAS AUTENTICACIÓN

El Banco requiere una solución de autenticación de fuerte que permita verificar la identidad de sus clientes en las transacciones que éstos realizan en un portal web transaccional utilizando métodos cómo:

## RECONOCIMIENTO DE LAS CARACTERÍSTICAS DEL EQUIPO O EQUIPOS MOVILES

Característica que le permitirá al Banco identificar los equipos donde sus clientes realizan las transacciones, con el fin de poder analizar en tiempo real que el cliente se está conectando desde una estación o un dispositivo móvil autorizado. El proponente deberá especificar en su propuesta qué características puede recolectar de la estación final del cliente, del dispositivo móvil y cómo se realiza éste proceso. Describiendo si se requiere el uso de agentes instalados localmente en las estaciones de los clientes o aplicaciones móviles.

## BIOMETRÍA

Característica que permitirá identificar los clientes del Banco a través de algunos de sus rasgos físicos. El proponente deberá especificar en su propuesta qué características biométricas del cliente puede validar y cómo se realiza éste proceso. También deberá describir que tipos de dispositivos se requieren para éste proceso y si éstos tienen costos adicionales se deberán especificar en la propuesta económica.

## OTP (ONE TIME PASSWORD)

### DISPOSITIVOS FÍSICOS OTP

Mecanismo que permita al Banco entregar a sus clientes dispositivos físicos con un segundo factor de autenticación que genere en tiempo real contraseñas de tiempos no mayores a 60 segundos que cuente con códigos de preguntas de desafío y firma de transacciones basado en lo que se ve es lo que se firma. Estos tokens deben tener PIN de seguridad para el ingreso por parte del usuario el cual se debe bloquear por intentos fallidos. El proponente deberá especificar en su propuesta los tipos de tokens físicos que ofrece y las características de éstos especificando claramente la fecha de vencimiento o vida útil del dispositivo. Se deberán detallar los costos de éstos por cada usuario que tenga el Banco y costos de personalización si el Banco decide optar por ésta opción.

### OTP VIRTUALES

Mecanismo que permita al Banco entregar a sus clientes contraseñas en tiempo real de tiempos no mayores a 30 segundos, a través de la instalación de aplicaciones móviles, envío de SMS, mensajes push, correo electrónico o aplicaciones en las estaciones de los equipos de los usuarios. Deseable que cuente con códigos de preguntas de desafío y firma de transacciones basado en lo que se ve es lo que se firma.

## AUTENTICACIÓN FUERA DE BANDA

Mecanismo que permita al Banco confirmar transacciones de los clientes en tiempo real a través de un canal diferente a aquel utilizado para realizar la transacción, mediante la instalación de aplicaciones móviles, IVR, o aplicaciones en las estaciones de los equipos de los usuarios.

## VERIFICACIÓN Y FIRMA DE LA TRANSACCIÓN

Mecanismo que permita al Banco firmar las transacciones que realice el cliente en el portal web transaccional bajo el principio lo que veo es lo que firmo. Este permitirá conocer las características de la transacción previamente, con el fin de que el cliente pueda hacer la aprobación o el rechazo. La firma que se genere solo puede ser utilizada para las características de la transacción que el cliente está haciendo, utilizando datos como cuentas de origen, cuentas destino y montos. Esto con el fin de que la transacción no pueda sufrir ataques de hombre en el medio (man-in-the-middle), si esta firma es utilizada para realizar otras transacciones el sistema de autenticación fuerte debe denegar la transacción.

## APLICACIÓN PARA DISPOSITIVOS MÓVILES

Característica de la solución de autenticación fuerte, que permita a los clientes del Banco tener una aplicación instalada en sus teléfonos inteligentes para generar diferentes mecanismos de autenticación ante en el portal web transaccional del Banco. Entre estas características se encuentra el envío de notificaciones push, envío de OTP, biometría, firma de transacción, autenticación a través de códigos QR o pictogramas, etc. El proponente deberá especificar en su propuesta todas las características que la aplicación móvil que ofrece, si ésta puede ser personalizada a la imagen institucional del Banco y en que plataformas se puede instalar (Android, IOS, Windows, etc.).

## SDK (Software Development Kit)

El sistema de autenticación fuerte debe contar un SDK para que el Banco pueda integrar otros desarrollos que involucren procesos de autenticación fuerte. Este SDK debe ser multiplataforma.

## SOLUCIÓN MULTICANAL

La solución que presente el proponente debe estar en la capacidad de soportar la autenticación fuerte de nuevos canales que el Banco desee implementar en un futuro. El proveedor deberá especificar en su propuesta con qué canales es compatible la solución a parte de portales web transaccionales.

## INTEGRACIÓN

La solución debe contar como mínimo con la integración a través de servicios web entre los diferentes canales y el sistema de autenticación fuerte. Si la solución permite otros esquemas de integración como por ejemplo el uso de APIs se debe especificar en la propuesta haciendo una descripción.

## EXPERIENCIA

El proponente deberá contar con la implementación de la solución ofertada en portales web transaccionales de entidades vigiladas por la Superintendencia Financiera de Colombia, en los cuales se cumpla los requerimientos de autenticación fuerte requeridos por la circular 042.

El proponente podrá presentar experiencia en portales web de entidades no vigiladas por la Superintendencia Financiera de Colombia.

Para acreditar la experiencia exigida, el proponente deberá aportar la certificación emitida por cada entidad en la cual haya prestado servicios de implementación de la solución.

## CUMPLIMIENTO REGULATORIO

La solución de autenticación fuerte debe cumplir con las características exigidas por la Circular Externa 042 de la Superintendencia Financiera de Colombia para el tema de autenticación fuerte.

### CONTINUIDAD DEL NEGOCIO

El proponente deber adjuntar su plan de continuidad del negocio el cual permita al Banco identificar estrategias en los casos de reemplazo del personal asignado al proyecto garantizando la transferencia de conocimiento y continuidad en la prestación del servicio contratado.

### CONSULTAS Y LOGS

La solución debe contar con un módulo de consultas, logs y permitir la parametrización de usuarios administradores de la herramienta los cuales deben ser sincronizados con el Directorio de Windows.

##  ACOMPAÑAMIENTO EN LA IMPLEMENTACIÓN DE LA SOLUCIÓN

El proponente seleccionado deberá acompañar al Banco en sitio durante la integración de la solución de autenticación fuerte con el portal web transaccional. Este acompañamiento debe ser con consultores especializados y certificados, implementando mejores prácticas que ya tenga establecidas con base en los proyectos previamente realizados.

El proponente deberá mantener éste equipo asignado al proyecto durante toda la ejecución del contrato o en su defecto deberá garantizar la transferencia de conocimiento cuando el equipo de trabajo sufra alguna modificación.

## PLAN DE TRABAJO

El Proponente deberá presentar con la propuesta un cronograma o plan de trabajo que en tiempo no sea mayor a 3 meses utilizando describiendo la metodología de desarrollo de proyectos, en el que describa los procesos/actividades requeridos para la instalación, implementación e integración de la solución de autenticación fuerte con el portal Web transaccional del Banco. Este cronograma debe detallar el número de días de cada actividad y los profesionales y su dedicación asociados a cada actividad.

El cronograma debe cumplir con las siguientes condiciones:

1. Explicar la relación entre las distintas actividades, e identificar rutas críticas si las hay.
2. Indicar los productos específicos a ser presentados y la fecha de entrega (por ejemplo: informes, reportes, manuales, etc.).
3. Para cada actividad relacionar el personal empleado y su dedicación.

Si la propuesta llegara a ser seleccionada, al momento de la firma del acta de inicio, la empresa deberá entregar a Bancóldex el cronograma actualizado teniendo en cuenta la fecha de inicio del proyecto.

Bancóldex a través del Supervisor del contrato verificará el desarrollo del cronograma presentado, la dedicación del personal ofrecido, los resultados esperados y en general el cumplimiento de los compromisos adquiridos.

El proponente deberá como mínimo incluir las siguientes actividades en su plan de trabajo:

1. **Planificación del proyecto:** Etapa en la que proveedor y el Banco acordarán el desarrollo del plan de la gestión del proyecto. En ésta etapa el proveedor deberá entregar: cronograma de trabajo, plan de alcance, plan de gestión de riesgos y demás documentos que se acuerden con el Banco.

1. **Instalación de la solución:** En esta etapa el proveedor describirá todas las actividades requeridas para realizar la instalación del esquema de autenticación fuerte con el fin de que éste quede operando para iniciar la integración con el portal transaccional del Banco.
2. **Integración:** En esta etapa el proveedor describirá todas las actividades requeridas para realizar la integración con el portal transaccional del Banco.

1. **Documentación:** En ésta etapa el proveedor entregará al Banco la documentación final del proyecto como manuales de usuario, arquitectura implementada, manuales de instalación, manuales técnicos y demás documentos que se acuerden con el Banco.
2. **Capacitación:** En esta etapa el proveedor realizará toda la transferencia de conocimiento de la implementación de la solución de autenticación fuerte. En ésta el proveedor deberá entregar: plan de capacitación para usuarios finales y técnicos, documentación con el contenido temático de cada una de las capacitaciones a realizar ya se funcionales o técnicas, registros de asistencia a las sesiones de capacitación y demás documentos que se acuerden con el Banco.

Se tendrá en cuanta en la calificación al proponente que optimice los tiempos propuestos para la implementación.

# REQUERIMIENTOS TECNICOS

## LICENCIAMIENTO

El proponente deberá tener en cuenta en su propuesta que el licenciamiento requerido por el Banco contempla los ambientes de pruebas, producción en alta disponibilidad y contingencia.

## DEFINICIÓN DE CONCEPTOS Y TÉRMINOS DE LA SOLUCIÓN OFRECIDA

El proponente deberá detallar los conceptos y términos que son particulares de su propuesta, con el fin de tener un mejor entendimiento por parte del Banco para fines de la calificación de la propuesta.

## ARQUITECTURA TECNÓLOGICA

El proponente deberá presentar un diagrama donde se muestre claramente la arquitectura de la solución de autenticación fuerte a implementar en el proyecto. En ésta se deberá hacer una descripción de todos los componentes requeridos en las diferentes capas.

## PLATAFORMA TECNOLOGICA QUE SOPORTARÁ LA SOLUCIÓN

El proponente deberá describir todos los requerimientos técnicos necesarios para la implementación del esquema de autenticación fuerte como servidores de aplicaciones, bases de datos, etc. La solución debe correr sobre plataforma Vmware 6.1, servidores Linux Red Hat, servidor de aplicaciones JBOSS EAP 6 y Base de Datos ORACLE 12 Release 1 o en esquema de appliance para instalar en el Banco. La solución debe integrarse con servidores LDAP.

# ENTREGA Y PUESTA EN MARCHA DE LA SOLUCIÓN OFRECIDA

## ESQUEMA DE IMPLANTACIÓN Y ADECUACIÓN

El proponente deberá describir la metodología que será utilizada durante la adecuación e implantación de la solución ofrecida. Así mismo deberán especificarse los tiempos, recursos del Banco requeridos y recursos del proveedor ofrecidos para la implantación exitosa de su solución de acuerdo con el cronograma de actividades propuesto. De igual manera, el proponente deberá comprometerse a realizar las adecuaciones o extensiones necesarias para que la solución ofrecida cumpla totalmente con los requerimientos definidos en esta nota técnica.

La metodología de implantación del servicio debe incluir como mínimo:

* Planeación detallada del proceso de instalación y pruebas.
* Tiempo de desarrollo y adecuación para los requerimientos funcionales que se comprometen a realizar si se requieren.
* Pruebas: Técnicas y de usuario.
* Esquema de funcionamiento.
* Capacitación.
* Implantación.
* Equipo de trabajo (Banco y proveedor).
* Resultados/productos de cada fase.
* Cronograma de trabajo general del proyecto.

## PRUEBAS DE LA SOLUCIÓN OFRECIDA

El proponente se debe comprometer a realizar las pruebas de la solución ofrecida, antes de iniciar las pruebas del Banco e implementación, las cuales pueden incluir:

* Pruebas modulares para verificar que la solución ofrecida funciona correctamente.
* Pruebas integrales orientadas a verificar la integridad de operación de los procesos y de los datos después de la ejecución de diferentes funcionalidades que los comparten.
* Pruebas de las interfaces requeridas.
* Pruebas de funcionamiento de la solución sobre la infraestructura de TI propuesta.
* Pruebas de conectividad a través de los diferentes dispositivos propuestos.
* Pruebas para verificar que el servicio ofrecido funciona como se espera.
* Pruebas de rendimiento (stress) orientada al acceso WEB.
* Pruebas de usuarios finales para detección de errores, fallas funcionales, tiempos de respuesta, entre otros.

## DOCUMENTACIÓN TÉCNICA Y DE USUARIO

El proponente deberá entregar la documentación técnica y de usuario en español incluyendo los siguientes elementos: Documentación del proyecto o servicio ofrecido, documentación de usuario, documentación técnica, manual de instalación y manual para el mantenimiento técnico.

## RECIBO Y ENTREGA DEFINITIVA

El recibo definitivo de la solución estará sujeto a que se realicen las respectivas pruebas funcionales y revisiones técnicas de la arquitectura de TI propuesta y que las mismas hayan finalizado con resultados a satisfacción del Banco. BANCÓLDEX, considerará implementada la solución cuando se hayan cumplido los siguientes eventos:

* Recibo de la solución contratada funcionando correctamente en producción.
* Las pruebas hayan finalizado con resultados a satisfacción del Banco.
* Se hayan realizado todos los cursos de capacitación para el personal definido por el Banco.
* Se hayan entregado y aprobado los manuales y documentos solicitados por el Banco.
* Se haya firmado un acta de terminación y aceptación por parte de los responsables autorizados por el Banco, de aceptar la solución ofrecida, y por el proveedor, el representante autorizado.

## CAPACITACIÓN QUE BRINDARÁ A LA SOLUCIÓN OFRECIDA

El proponente deberá presentar las condiciones bajo las cuales brindará la capacitación respectiva en todos los componentes de su propuesta: Tipo de capacitación (técnica, administración y usuario), contenido de cada curso; duración, intensidad horaria, grupo objetivo del curso, requisitos de grupo, recursos necesarios u otras condiciones necesarias.

## GARANTÍA

El proponente deberá entregar una garantía sobre la implementación de la solución realizada por un período mínimo de 6 meses, contados a partir de la fecha de la firma del acta de entrega a satisfacción del producto. Esta garantía cubre defectos en el software instalado en el Banco y defectos en las personalizaciones realizadas por el proveedor.

# SOPORTE DEL SERVICIO A LA SOLUCION OFRECIDA

## MANTENIMIENTO A LA SOLUCIÓN OFRECIDA

Adjuntar por separado la propuesta de soporte para el primer año, prorrogable según la evaluación requerida para su renovación, incluyendo el acompañamiento en la instalación de nuevas versiones liberadas. En el caso de la modalidad de suscripción el valor del soporte a nuevas versiones debe estar inmerso dentro del canon del contrato y todas las actualizaciones, mantenimiento y soporte estarán a cargo del proveedor. El tiempo del soporte se contará a partir del vencimiento del período de garantía de la solución de autenticación fuerte. Se pide detallar el esquema de atención, los costos y los acuerdos de servicio que el proponente tenga establecido con sus clientes. En esta propuesta se deberán especificar como mínimo los siguientes puntos:

* Esquema de las diferentes líneas de soporte (teléfono, mail, online, presencial, entre otros).
* Acuerdos de servicio (SLA).
* Horarios de soporte sobre la funcionalidad.

El proponente debe indicar los ajustes según incremento anual para los servicios de mantenimiento y actualizaciones, en todo caso, éste no podrá superar el IPC vigente para el año en curso.

El proponente deberá especificar en su propuesta los acuerdos de niveles de servicio para la entrega de tokens físicos.

## SOPORTE TÉCNICO A LOS COMPONENTES EXPUESTOS EN LA SOLUCIÓN OFRECIDA

El proponente debe describir cómo va a prestar el soporte técnico para los componentes que presente en su propuesta (hardware, software de base, aplicaciones, servicios). Este soporte debe estar disponible 7 x 24 y a cargo de profesionales capacitados. El tiempo máximo de atención de la solicitud crítica no deberá exceder de 2 horas y su solución dependiendo la gravedad no deberá exceder de 48 horas.