**BANCO DE COMERCIO EXTERIOR DE COLOMBIA S.A.**

# ANEXO TECNICO A LA INVITACIÓN PRIVADA PARA LA SELECCIÓN Y CONTRATACIÓN DE UNA PERSONA JURÍDICA QUE PRESTE EL SERVICIO DE SOFTWARE COMO SERVICIO (SAAS) PARA LOS PROCESOS DE GESTIÓN DE TALENTO HUMANO.

**Bogotá D.C., diciembre de 2025**

## CONTENIDO

## 1. Arquitectura de software

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

### 1.1 Diagrama de componentes

Se deberá presentar un diagrama de alto nivel donde se describan claramente cada una de las capas, componentes y/o módulos de cómo está construida la solución. (*https://en.wikipedia.org/wiki/Component_diagram)*

### 1.2 Proceso de desarrollo

Se deberá presentar la descripción del proceso de desarrollo de software que se tiene implementado para la construcción de la solución. Describir cómo aplican DevOps detallando como se hace todo el proceso y como se encuentran automatizadas las diferentes tareas.

### 1.3 Tecnologías

#### 1.3.1 Arquitectura

El proponente deberá describir las tecnologías de la solución, de tal manera que permita identificar elementos y características de la arquitectura del software tales como microservicios, uso de contenedores (Docker/Kubernetes), desacoplamiento y escalabilidad horizontal.

#### 1.3.2 Tecnología de Desarrollo

El proponente deberá describir las tecnologías en las cuales está construida la solución, de tal manera que permita identificar elementos y características del software tales como Frameworks y lenguajes usados.

### 1.3.3 Actualización y Mantenibilidad

El proponente deberá describir las tecnologías que apoyan la actualización y mantenimiento de la solución dentro del proceso del desarrollo del software, de tal manera que permita identificar los ciclos de actualización; el esquema, estrategia y periodicidad de liberación de versiones del software; la documentación que se maneja y el nivel de automatización de pruebas.

### 1.3.4 Experiencia de Usuario (UX/UI)

El proponente deberá describir las tecnologías en las cuales está construida la solución, de tal manera que permita identificar elementos y características de experiencia de usuario (UX/UI) tales como diseño responsive y accesibilidad (WCAG).

## 2. Arquitectura de infraestructura

### 2.1 Actualización tecnológica

El proponente deberá garantizar que 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.

Se deberá presentar las actualizaciones del producto de una forma clara y alineado con tendencias del sector.

### 2.2 Ambientes

La solución propuesta debe contar como mínimo con 3 ambientes: desarrollo, pruebas y producción. Se valorará adicionalmente un cuarto ambiente de preproducción para realizar validaciones finales antes del paso a producción. El proponente deberá dar una descripción de cómo tiene implementados estos ambientes.

El sistema debe contar con ambientes totalmente independientes para los procesos de pruebas y producción[1]. 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

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

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.

### 2.2.1 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.

### 2.2.2 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. Se deberá indicar si el esquema de alta disponibilidad cuenta con redundancia geográfica.

## 2.4 Disponibilidad

El proponente deberá especificar en su propuesta el acuerdo de nivel de servicio (SLA[2]) de disponibilidad que se compromete a cumplir sobre la solución que ofrece, el cual debe ser igual o superior al 99.5% en la prestación del servicio en la nube en modalidad SaaS. 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 usuarios del Banco. El incumplimiento de este acuerdo 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

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

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.

## 2.5 Contingencia y continuidad

El proponente debe disponer de un plan de contingencia y continuidad documentado y probado que permita mantener disponible la prestación del servicio contratado por el Banco, en el evento que se presenten situaciones de interrupción. Dicho plan se mantendrá documentado y disponible en el momento que EL BANCO lo requiera para verificar su adecuado funcionamiento. El plan de continuidad debe garantizar una respuesta a los RTO (8 horas) y RPO (1 día) establecidos por el Banco.

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 validación al cumplimiento de los requerimientos de continuidad de negocio para la prestación del servicio ofrecido.

## 2.6 Escalabilidad

Se deberá explicar si la solución cuenta con la capacidad de escalar vertical u horizontalmente cuando la demanda de peticiones aumente o cuando aumente la cantidad de usuarios, 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. Se debe describir y explicar en la propuesta como hace el monitoreo de eventos, las herramientas que usa, las tareas que realiza y los procedimientos que ejecuta para cumplir con este requerimiento, e indicar las estrategias de notificación y comunicación con el Banco en caso de interrupción.

## 2.8 Backups

El proponente deberá garantizar mecanismos automáticos y periódicos de respaldo (backups) de la información de EL BANCO y del software, así como procedimientos documentados para su restauración. De tal manera que estos se tomen de acuerdo con la periodicidad que el Banco le señale. Se debe indicar si los backups son cifrados y si se realizan pruebas periódicas de restauración. Para explicar todo lo anterior se debe incluir en la propuesta 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 utilicen la solución y procesan en la nube. La independencia se puede dar a nivel lógico o físico.

## 2.9 Actualizaciones

El proponente deberá indicar el modelo de despliegue que tiene implementado para su solución (multi-tenant, single-tenant, otro). Se deberá especificar cómo funciona el esquema de actualizaciones del software, las cuales deben ser automáticas y con un mínimo de tiempo de interrupciones. También se deberá explicar cómo se incorporan nuevos módulos o funcionalidades al sistema y qué tan flexible es este proceso.

## 2.10 Rendimiento del Sistema

El proponente deberá indicar el modelo de capacidad de la solución para procesar operaciones de manera eficiente bajo diferentes cargas de trabajo. Un buen rendimiento garantiza que los usuarios puedan acceder y utilizar el sistema sin demoras, incluso en momentos de alta demanda. Se debe indicar el throughput del sistema medido en el número de transacciones procesadas por unidad de tiempo, es decir, número de transacciones por segundo - TPS.

### 2.11 Latencia

El proponente deberá especificar la latencia promedio que maneja la solución en operaciones comunes, entendiendo la latencia como el tiempo que tarda una solicitud en viajar desde el cliente hasta el servidor y volver con una respuesta. Se debe indicar el tiempo en milisegundos. Una baja latencia es fundamental para una experiencia de usuario fluida y satisfactoria.

## 3. Arquitectura de integración

### 3.1 Capacidad de integración con sistemas existentes

Capacidad del sistema de software para interactuar, comunicarse y funcionar correctamente con otros sistemas, plataformas o servicios, independientemente de sus tecnologías, lenguajes o proveedores.

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 que llegaren a requerirse (Archivos planos, Web Services, API's, otros), deberá especificar las características de estos y la recomendación a utilizar con base en su experiencia.

### 3.2 Interoperabilidad

El proponente deberá indicar cuáles de las siguientes características de interoperabilidad posee el sistema y explicar brevemente cómo están implementados y para qué tipo de servicios y/o funcionalidades:

- APIs abiertas y documentadas (REST, GraphQL, otros)
- Conectores nativos con plataformas comunes (Microsoft 365, Oracle, otros)
- Soporte para estándares de intercambio de datos (JSON, XML, SAML, OAuth, otros).

## 4. Soporte técnico

### 4.1 Esquema de prestación del 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, el plan de comunicaciones, niveles de escalamiento y el equipo de soporte, si es subcontratado, describa el nombre del subcontratista.

### 4.2 ANSs

Los tiempos de atención deben estar basados en Acuerdos de Niveles de Servicio los cuales se deben especificar en la propuesta de acuerdo con su criticidad (alto, medio, bajo). 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. El proponente debe indicar qué estándares de métricas de satisfacción del servicio usa.

### 4.3 Proceso de gestión de incidentes

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 (chat, correo, teléfono, portal de autoservicio, otro), horarios de soporte, tiempos de respuesta y las actividades generales del proceso (incluir diagramas de proceso). Indicar qué herramienta ITSM maneja.

## 5. Arquitectura de seguridad

### 5.1 Remediación de vulnerabilidades

El proponente deberá remediar las vulnerabilidades encontradas en los análisis que realice el Banco a todos los elementos de la infraestructura que soportan la solución ofrecida. 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. El proponente debe informar en la propuesta los tiempos en que se compromete a remediar las vulnerabilidades encontradas según su clasificación. El proponente debe indicar qué estándares acoge para clasificación de vulnerabilidades.

El informe de remediaciones deberá ser presentado al Banco con la finalidad de poder garantizar que efectivamente los hallazgos fueron remediados. Si luego de las validaciones

al interior del Banco se detectan algunos aspectos que no fueron subsanados, se volverán a remitir al proveedor para que se hagan los ajustes respectivos.

Dichos informes serán soporte ante los entes regulatorios.

## 5.2 Desarrollo seguro

El proponente debe garantizar que cuenta con un proceso de desarrollo seguro y hacer la descripción de como hace su implementación. Debe detallar en la propuesta las herramientas que usa, las tareas que realiza y los procedimientos que ejecuta 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. Se deberá indicar si cuenta con certificación de prácticas seguras y bajo qué estándar.

El proponente debe permitir comprobaciones del código y realizar las respectivas pruebas de seguridad tomando como guía las mejores prácticas del mercado, en lo posible usando OWASP, para identificar fallas, vulnerabilidades o código malicioso. En caso de encontrar fallas el proveedor debe garantizar que estas sean corregidas, realizarse la respectiva reprueba y entregar los resultados donde se suministre evidencia de que se han hecho pruebas suficientes para la protección de la aplicación. Se debe informar en la propuesta de qué forma se cumplirá con este requerimiento.

El proponente deberá garantizar que el software no contiene ningún código que no se alinee a algún requerimiento del software y debilite la seguridad de la aplicación, incluyendo virus, gusanos, bombas de tiempo, puertas traseras, caballos de troya o cualquier otra forma de código malicioso. Adicionalmente, se deberá verificar que la aplicación no es susceptible a inyecciones, desbordamientos, manipulación y otros ataques ocasionados por entrada de datos corruptos.

## 5.3 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 solución debe utilizar la autenticación a través de Office 365 y contar con compatibilidad SSO (Single Sign-On) y con OAuth 2.0 / OpenID Connect. El proponente debe especificar cómo realizaría esta integración y los requerimientos técnicos que el Banco debe proveer.

La solución tecnológica deberá contar con autenticación de doble factor para los usuarios que accedan a la misma.

La solución deberá contemplar mecanismos y procedimientos de autenticación alternativos para los casos en que los usuarios estén inactivos en el Directorio Activo del Banco, pero se requiera que el usuario acceda a la solución (ej: funcionario en licencia o incapacidad). Deberán especificar en su propuesta cómo dan atención a este requerimiento.

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 proponente debe describir en la propuesta cómo funciona el módulo de seguridad para cumplir con estos requerimientos.

## 5.4 Contraseñas

Cuando la autenticación no está integrada con el directorio activo de Windows (Usuarios Bancóldex), el sistema debe contar con bloqueo por intentos fallidos y debe permitir parametrizar las condiciones de las contraseñas tales como: su longitud mínima, complejidad (uso de caracteres especiales y caracteres alfanuméricos, etc.), el tiempo con el cual los usuarios deben hacer el cambio de contraseña, llevar registro de estas e impedir su reúso. El proponente debe describir en la propuesta cómo es el manejo de contraseñas.

## 5.5 Inicio de sesión

La aplicación, en lo posible, deberá informar al usuario la última fecha y hora de ingreso que este tuvo al sistema.

Es necesario que el sistema restrinja 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

Según el esquema de licenciamiento, se debe indicar si la aplicación valida un número máximo de usuarios conectados concurrentemente o qué esquema de usuarios concurrentes maneja.

El proponente deberá describir en la propuesta cómo funciona el inicio de sesión para cumplir con estos requerimientos.

### 5.6 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. Indicar si contempla parametrización del tiempo de sesión por rol o tipo de usuario.

### 5.7 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

## 6. Protección de la información

### 6.1 Cifrado de datos

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, que cumplan con TLS 1.2 o superior y que en lo posible usen rutas diferentes. El sistema debe contar con un certificado digital de sitio seguro.

### 6.2 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 evidenciar la independencia y de esta manera contar con dicha visualización.

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

### 6.3 Ubicación de los datos

El proponente se compromete a que los datos almacenados o procesados en la nube permanecerán únicamente en ubicaciones autorizadas y dentro de jurisdicciones que garanticen niveles adecuados de protección de datos personales o confidenciales. El proveedor debe informar al banco en su propuesta estas ubicaciones. Los datos deben estar alojados en jurisdicciones que cumplan con la Ley 1581 de 2012 y, en particular atiendan lo establecido en la CE005 de 2017 de la SIC.

## 6.4 Seguridad de la información

El PROPONENTE deberá indicar cómo da observancia frente a que la plataforma propuesta Cloud cumpla con los estándares o buenas prácticas en seguridad de la información, tales como ISO27001, ISO/IEC 27018, SOC 2 Tipo II y/o CSA STAR.

## 6.5 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. Cuando se presente el evento de borrado seguro el proponente deberá presentar un certificado de borrado conforme a NIST 800-88.

## 6.6 Devolución de la información

El proponente deberá garantizar la devolución completa, segura y verificable de la información del Banco una vez finalice el contrato. El proponente debe describir y detallar en su propuesta, entre otros cómo cubrirá los siguientes aspectos:

**Formato de Entrega:** La información deberá ser entregada en formatos estructurados y abiertos que faciliten su reutilización y migración.

**Medios de entrega**: bien sea a través de medios físicos y/o medios de transferencia electrónicos, deben ser seguros y cifrados tanto en tránsito como en reposo.

**Plazo de Entrega:** el proponente deberá entregar la información en un plazo máximo de **treinta (30) días calendario** contados a partir de la finalización del contrato. Inclusive se podrán hacer entregas preliminares antes del vencimiento del contrato. El Banco podrá realizar validaciones de consistencia y completitud antes de dar por concluido el proceso.

**Documentación:** El proponente deberá entregar junto con la información, un manual técnico que describa la estructura de los datos, instrucciones para su importación o migración y un reporte de consistencia que evidencie la integridad de la información entregada.

**Destrucción de la Información:** El proponente deberá realizar el borrado seguro de toda la información del Banco que permanezca en sus sistemas, conforme a NIST 800-88. Además, deberá emitir una certificación de destrucción firmada y garantizar que no queda información residual en backups, logs o sistemas de terceros.

## 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