1. Requerimientos de seguridad de la información

1.1 Certificación ISO 27001

El proponente debe presentar al Banco certificación vigente de la ISO 27001 sobre el servicio que va a prestar, y de observancia a los estándares o buenas prácticas, tales como ISO 27017 y 27018, así como disponer de informes de controles de organización de servicios (SOC1, SOC2, SOC3) según lo establece la circular 005 de 2019 de la SFC

1.2 Disponibilidad

El proponente debe ofrecer una disponibilidad de al menos el 99.95% en los servicios prestados en la nube en los modelos IaaS y PaaS. Para aquellos proveedores del servicio de computación en la nube en el modelo SaaS, la disponibilidad debe ser de al menos el 99.5%. Esto en cumplimiento con la Circular Externa 005 de 2019 de la SFC

1.3 Procesamiento y almacenamiento de datos

El proponente debe informar el país o países donde se procesará y almacenará la información tanto en producción como en contingencia, y estos deben ser jurisdicciones que 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. Conforme a la circular 005 de la SFC y la Circular Externa 002 de 2018 de la SIC.

1.4 Análisis de vulnerabilidades

El proponente deberá ejecutar análisis de vulnerabilidades a todos los elementos de infraestructura que soportan la solución ofrecida, una vez terminada su ejecución se deberá compromete 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 con 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.

Se deberá dar una descripción si a la infraestructura del sistema ya se le aplica este proceso y en que periodicidad o si se debe implementar esto como un nuevo proceso.

A su vez el proveedor debe compartir los informes test y re-test de los análisis ejecutados con la finalidad de poder garantizar que efectivamente fueron realizados y los hallazgos remediados. Dichos informes serán soporte ante los entes regulatorios.

1.5 Ethical Hacking

El proponente debe ejecutar pruebas de Ethical Hacking y emprender las acciones requeridas para remediar los hallazgos identificados en dichas pruebas, como evidencia de las pruebas es requerido compartir los informes de las pruebas realizadas como soporte de las ejecuciones y remediaciones implementadas.

1.6 Cifrado

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 y que en lo posible usen rutas diferentes.

Cuando la información confidencial de los clientes se envíe como parte de, o adjunta a un correo electrónico, mensajería instantánea o cualquier otra modalidad de comunicación electrónica, ésta debe estar cifrada. El proponente debe garantizar que se implementan los algoritmos y protocolos necesarios para brindar una comunicación segura. Se debe especificar cómo se cumple con este requerimiento en la propuesta.

1.7 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. 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, 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 la plataforma debe estar en la capacidad de 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.

1.8 Autenticación fuerte

El sistema debe contar con un mecanismo fuerte de autenticación de usuarios de acuerdo con lo establecido en la Circular 042 de 2012 de la Superintendencia Financiera de Colombia. El proponente deberá especificar que esquemas de autenticación fuerte puede implementar para cumplir con este requerimiento, adicionalmente el sistema debe garantizar que la identificación y autenticación de los usuarios sea única y personalizada. De ser necesaria por la clasificación de la información.

1.9 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.

1.10 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

1.11 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.

1.12 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 al Banco la descripción de cómo se está realizando esta independencia. Como también es necesario compartir diagramas de arquitectura que permita soportar la independencia y de esta manera contar con dicha visualización.

1.13 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

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.

1.14 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.

1.16 Controles de Software Malicioso

El sistema debe verificar que la información enviada esté libre de software malicioso. Así mismo, se debe contar con una protección que valide que los archivos cargados por el usuario final a la plataforma estén libres de software malicioso. El proponente debe contar con mecanismos que fortalezcan la seguridad de la solución, para protegerla de los riesgos de denegación de servicio, inyección de código malicioso u objetos maliciosos. Así mismo, deberá verificar de manera constante que los

enlaces del sitio web no sean modificados ni suplantados y que la resolución de sus DNS no sea alterada.

1.17 Actualización del software

El proponente deberá garantizar la actualización del producto o de los componentes que integran la solución presentada, detallando la información de los componentes o productos que se van a actualizar. Dentro de la información presentada, se requiere mínimo:

- Versión del producto.
- Fecha de liberación de la versión.
- Mejoras o correcciones implementadas en la versión.
- Prerrequisitos para la actualización.

El proponente deberá contar con herramientas que permitan hacer el control de las versiones que se instalarán en los ambientes de producción, así mismo contar con procedimientos documentados para la instalación del software en producción, debe entregar al Banco como se hace este proceso.

1.18 Estadísticas

El proponente deberá aportar al Banco de manera trimestral las estadísticas de disponibilidad y de uso con respecto a la prestación del servicio. Esta información debe ser conservada por 2 años. El proponente deberá indicar el detalle de la metodología utilizada para el cálculo de la disponibilidad.