BANCO DE COMERCIO EXTERIOR DE COLOMBIA S.A. BANCÓLDEX

TÉRMINOS DE REFERENCIA PARA LA CONTRATACIÓN DE LOS SERVICIOS: SECURITY OPERATION CENTER – SOC, ANÁLISIS DE VULNERABILIDADES DEL SERVICIO, ETHICAL HACKING, MONITOREO DE MARCA Y GESTIÓN DE USUARIOS QUE PERMITAN FORTALECER LAS CAPACIDADES DE CIBERSEGURIDAD DEL BANCO

Bogotá D.C.

Enero de 2022

Contenido

BANCOLDEX
GRUPO BANCOLDEX

1. INTRODUCCIÓN

1.1. Acerca de Bancóldex

El Banco de Comercio Exterior de Colombia S.A. – Bancóldex, es una sociedad anónima de economía mixta del orden nacional creada por la Ley 7ª de 1991 y el Decreto 2505 de 1991, actualmente incorporado en el Decreto Ley 663 de 1993 (Estatuto Orgánico del Sistema Financiero), organizada como establecimiento de crédito bancario, sometida a la inspección, vigilancia y control de la Superintendencia Financiera de Colombia y vinculada al Ministerio de Comercio, Industria y Turismo no asimilada al régimen de las empresas industriales y comerciales del Estado.

Adicionalmente, y de conformidad con lo estipulado en sus estatutos sociales y en el numeral 3 del artículo 279 del mencionado Decreto Ley 663, Bancóldex tiene como objeto social la financiación, en forma principal pero no exclusiva, de las actividades relacionadas con la exportación y con la industria nacional, actuando para tal fin como banco de descuento o redescuento, antes que como intermediario directo.

Así las cosas, Bancóldex actúa como "banco de segundo piso", es decir, a través de intermediarios financieros sometidos a inspección, control y vigilancia de la Superintendencia Financiera de Colombia, tales como bancos, corporaciones financieras y compañías de financiamiento, y entidades orientadas a crédito microempresarial no sometidas a la vigilancia de dicho ente de control, como ONG micro crediticias, fundaciones financieras, cooperativas y cajas de compensación familiar.

1.2. Valores Institucionales de Bancóldex

El proponente deberá dar lectura al documento titulado "Valores Institucionales" y deberá diligenciar la carta sobre el conocimiento, aceptación y cumplimiento de dichos valores. Estos documentos se encuentran en el Anexo No. 3 – VALORES INSTITUCIONALES DE BANCOLDEX del presente documento.

1.3. Antecedentes y justificación de la convocatoria

Bancóldex conforme al cumplimiento regulatorio de las normas expedidas por la Superintendencia Financiera de Colombia requiere fortalecer sus capacidades para garantizar una adecuada gestión de la seguridad informática.

2. OBJETO DE LA INVITACIÓN

La presente convocatoria tiene por objeto la contratación de una persona jurídica que preste los servicios de: Security Operation Center – SOC[1], el análisis de vulnerabilidades, ethical hacking, monitoreo de marca y gestión de usuarios, que permitan fortalecer las capacidades para garantizar una adecuada gestión de la seguridad informática.

3. TÉRMINOS JURÍDICOS

3.1. Régimen jurídico aplicable

En atención al régimen de contratación del Banco de Comercio Exterior de Colombia S.A., por expresa disposición del artículo 285 del citado Decreto Ley 663 de 1993, así como del artículo 15 de la Ley 1150 de 2007, el presente proceso de selección y la contratación que se derive de la presente convocatoria, se encuentran sometidos a las normas del Derecho Privado Colombiano.

3.2. Cambio de Regulación

La normatividad aplicable, será la que se encuentra vigente a la fecha de la presente invitación, incluso si entre la fecha de ésta y el plazo máximo señalado para recibir las propuestas, se modifica o deroga alguna disposición normativa aplicable, salvo que por expresa disposición de la ley nueva, la misma deba ser aplicada a las invitaciones en curso.

La ley aplicable al contrato será la vigente al momento de su celebración.

3.3. Documentos y Prelación

Son documentos de la presente invitación todos sus anexos (si los hubiere), así como todas las Adendas que se generen con posterioridad a la fecha de envío de este documento. En caso de existir contradicciones entre los documentos mencionados se seguirán las siguientes reglas:

a) Si existe contradicción entre un Anexo y los Términos de Referencia, prevalecerá lo establecido en el respectivo Anexo.
b) Siempre prevalecerá la última Adenda publicada sobre cualquier otro documento.
c) En caso de contradicción en los Términos de Referencia, sus Adendas y el contrato, prevalecerá lo establecido en el contrato.

3.4. Veracidad de la información suministrada

[1] Centro de Operaciones de Seguridad o **SOC** por la siglas en ingles de Security Operations Center está compuesto por un equipo de analistas que emplean herramientas de ciberseguridad con el objetivo de detectar, registrar y responder a posibles ataques cibernéticos.

El Proponente está obligado a responder por la veracidad de la información entregada durante el proceso de selección de Proponentes. El Banco de Comercio Exterior de Colombia S.A., de conformidad con el artículo 83 de la Constitución Política, presume que toda la información que el Proponente presente para el desarrollo de esta invitación es veraz, y corresponde a la realidad. No obstante, el Banco de Comercio Exterior de Colombia S.A., se reserva el derecho de verificar toda la información suministrada por éste.

3.5. Confidencialidad de la información

El Proponente seleccionado acepta que la ejecución del contrato que se celebre será desarrollado bajo parámetros de absoluta reserva y no podrá utilizar total o parcialmente la información que reciba directa o indirectamente del Banco de Comercio Exterior de Colombia S.A. o aquella a la cual tenga acceso en cumplimiento de los servicios a contratar, para desarrollar actividades diferentes a las contempladas en el objeto, alcance y obligaciones que le correspondan de conformidad con el contrato que se celebre, adoptando las medidas necesarias para mantener la confidencialidad de los datos suministrados.

3.6. Propiedad de la información

El Proponente seleccionado acepta que la información entregada por Bancóldex en desarrollo de la presente invitación, así como la información que se genere como consecuencia de la prestación del servicio que se contrate es de propiedad exclusiva de Bancóldex.

3.7. Cláusula de Reserva

El Banco de Comercio Exterior de Colombia S.A. se reserva el derecho de cerrar anticipadamente la presente convocatoria, y de rechazar cualquiera o todas las propuestas que se presenten, si así conviene a sus intereses, sin necesidad de dar explicación alguna a los proponentes y sin indemnizar ningún tipo de perjuicio o asumir costo alguno que con tal cierre o rechazo se pudiera generar a alguno de las entidades que presentaron propuesta.

3.8. Garantía de seriedad de la Oferta

El Proponente deberá incluir una garantía de seriedad de la oferta con una suma asegurada equivalente al diez por ciento (10%) del valor de la oferta económica. La garantía de seriedad de la oferta podrá consistir en una garantía bancaria irrevocable a primer requerimiento (*on-demand*) o en una póliza de seguro expedida por una compañía de seguros vigilada por la Superintendencia Financiera de Colombia, que sea satisfactoria para el Banco de Comercio Exterior de Colombia S.A. La garantía deberá ajustarse a los presentes Términos de Referencia y a las disposiciones legales vigentes.

Las compañías de seguros que otorguen la póliza deberán estar legalmente establecidas en Colombia, los establecimientos bancarios que otorguen la garantía podrán ser nacionales o

extranjeros siempre que tengan límite de exposición crediticia con Bancóldex (cupo de crédito aprobado con Bancóldex).

La garantía deberá ser válida por un periodo de seis (6) meses calendario a partir de la fecha de cierre de la invitación.

La garantía de seriedad de la oferta deberá ser otorgada a favor del Banco de Comercio Exterior de Colombia S.A. – Bancóldex, NIT. 800.149.923-6, en formato para entidades particulares, la cual se hará efectiva si el proponente retira su propuesta dentro del período de validez estipulado, o si habiéndosele adjudicado el contrato no cumple con los requisitos establecidos para la firma del mismo o se niega a celebrar el contrato respectivo o no presenta las garantías del Contrato establecidas en estos Términos de Referencia o en el Contrato.

4. INSTRUCCIONES A LOS PROPONENTES

4.1. Estudios para participar en la convocatoria

Corresponde a todo Proponente efectuar los estudios y verificaciones que considere necesarios para la formulación de la Propuesta, incluyendo, pero sin limitarse a los estudios técnicos, contables, tributarios, entre otros; asumiendo todos los gastos, costos, impuestos y riesgos que ello implique, que no serán reembolsados en ningún caso y bajo ningún concepto.

La presentación de una Propuesta implicará que el Proponente realizó los estudios, análisis y valoraciones pertinentes para prepararla y, por lo mismo, no se reconocerá sobrecosto alguno derivado de deficiencias en ellos.

4.2. Impuestos y Deducciones:

Al formular la propuesta, el Proponente acepta que estarán a su cargo todos los impuestos, tasas y contribuciones establecidos por las diferentes autoridades Nacionales, Departamentales, Municipales o Ambientales, que afecten el contrato y las actividades que de él se deriven.

El proponente seleccionado pagará en su calidad de contratista todos los impuestos, derechos, tasas y contribuciones que se deriven de los contratos o sus modificaciones y, por lo tanto, su omisión en el pago será de su absoluta responsabilidad.

4.3. Instrucciones para participar en la Invitación

Las propuestas deben ser presentadas en español y todas sus páginas deben estar enumeradas en forma ascendente consecutiva, con el correspondiente índice o tabla de contenido que permita su fácil consulta.

Las propuestas remitidas que no cumplan los requisitos y no vengan acompañadas de la documentación exigida en estos Términos de Referencia, serán excluidas del proceso de evaluación. Lo anterior, sin perjuicio de lo establecido en los términos previstos en el numeral 5.11. de los Términos de Referencia.

La propuesta y sus anexos se recibirán únicamente a través del sistema de contratación dispuesto por el Banco para adelantar el presente proceso de contratación, realizando los siguientes pasos de conformidad con lo establecido en el ***Instructivo para el cargue de archivos y envío de propuestas***, remitido con el correo electrónico a través del cual se invitó a participar en la presente convocatoria:

- De apertura al correo electrónico remitido por el Banco con el link que permite acceder a la información de la invitación.
- Al ingresar al link encontrará los módulos que permiten llevar a cabo el proceso de la invitación.
- En el módulo A "Términos de Referencia" podrá consultar los términos y condiciones de la convocatoria. Asegúrese de agotar completamente su lectura para identificar los requisitos de participación y la documentación que debe reunir para presentar la propuesta.
- Ingrese al módulo B "Anexos de la invitación" para consultar los documentos que debe diligenciar y anexar a la propuesta.
- En el módulo C "Cronograma" encontrará la información correspondiente a las actividades y fechas en que se ejecutará el presente proceso de contratación. El Sistema habilitará o deshabilitará las actividades de acuerdo con las fechas allí parametrizadas.
- A través del módulo D "Preguntas" los proponentes podrán remitir las inquietudes acerca de la invitación. A través de este módulo se consultarán las respuestas.
- Ingrese al módulo E "Propuesta" para cargar la documentación y propuesta: En este módulo deberá ingresar toda la documentación requerida para presentar la propuesta. Los archivos a cargar deben ser formato PDF (creado como PDF, más no escaneado como PDF), a excepción de los documentos anexos que deben firmarse por el Proponente y la "matriz de capacidad financiera", la cual deberá adjuntarse en archivo Excel. El tamaño máximo por archivo debe ser de 10 megabites (10 MB).
- Para el correcto cargue de la información, tenga en cuenta los siguientes puntos:
  - Lea atentamente la etiqueta del nombre de cada documento que se encuentra en la parte izquierda de la pantalla. Asegúrese de cargar el archivo con la información correcta y actualizada según solicite la convocatoria, absténgase de cargar archivos en blanco, desactualizados o con errores, pues la falta de documentos puede invalidar la propuesta. Asegúrese de firmar los anexos que requieran firma del proponente antes de cargarlos.
  - Para cargar el archivo simplemente de clic en el botón con el "clip" y posteriormente a través del explorador de Windows, ubique el archivo a cargar y selecciónelo. Si requiere reemplazar el archivo, simplemente vuelva a ingresar por el "clip" y seleccione el nuevo archivo, el sistema reemplazará el cargado inicialmente.
  - Para consultar el archivo, de clic en botón con la lupa, y allí se visualizará el archivo cargado.

- A lado derecho de cada documento aparece un “Check Box” el cual, si está en color rojo indica que el documento es obligatorio y que por ende antes del envío final de la propuesta, este debe encontrarse cargado.
- Una vez finalizado el paso anterior deberá diligenciar la información, “Partes Relacionadas” en el módulo E “Propuesta” en su parte final, en el cual se deberán adicionar los datos de los cargos establecidos como “Partes Relacionadas” para el Banco.
- Envío de la propuesta: El proponente deberá asegurarse que toda la información se encuentra debidamente cargada, una vez cargada la completitud de los documentos con la información requerida en la invitación, dar clic en el botón “*Enviar Propuesta”* que se encuentra en la parte superior derecha del módulo E “Propuesta”.
- Una vez enviado, el sistema genera un mensaje en el cual indica que el proceso se realizó a satisfacción, al igual que un número de radicado, el cual también se evidencia en la parte superior derecha del módulo E “Propuesta”. El Sistema también enviará un correo electrónico con los datos del radicado de la propuesta: número de radicado, fecha y hora, al mismo correo en cual se recibió la invitación.

4.4. Requisitos para participar en la invitación

Los Proponentes deberán cumplir los siguientes requisitos:

i. Ser personas jurídicas nacionales extranjero con sucursal en Colombia, con mínimo cinco (5) años de existencia a la fecha de presentación de la propuesta, cuya actividad económica u objeto social sea servicios de ciberseguridad y seguridad informática.
ii. El Proponente deberá acreditar mínimo cinco (5) años de experiencia de conformidad con lo establecido en el numeral 5.9. del presente documento.
iii. La duración de la sociedad, contada a partir de la fecha de cierre del plazo de la presente invitación, no será inferior al plazo establecido para el contrato y tres (3) años más.
iv. Tener la capacidad financiera exigida en el numeral 5.3. de la presente convocatoria.
v. Aportar oportunamente toda la documentación exigida en estos Términos de Referencia o en sus documentos anexos.

4.5. Cronograma de la invitación

El desarrollo de esta convocatoria tendrá lugar de conformidad con el Cronograma publicado en el módulo C “Cronograma” del Sistema, el cual deberá consultarse por el proponente con el fin de conocer y hacer seguimiento a las actividades principales a través de las cuales se desarrollará el presente proceso de contratación.

El cronograma podrá ser modificado por Bancóldex sin restricción, mediante adenda a los presentes Términos de Referencia.

El Sistema deshabilitará las actividades descritas en el Cronograma de acuerdo con el vencimiento de las fechas informadas en este.

4.5.1. Formulación y respuesta de inquietudes

Las inquietudes o preguntas relacionadas con los presentes Términos de Referencia, que surjan por parte de los Proponentes, deberán ser presentadas en la fecha señalada en el módulo C "Cronograma" del Sistema.

Una vez realizada la lectura detallada de los Términos de Referencia, el Sistema le permitirá ingresar las preguntas a través del módulo D.

Al ingresar, el proponente deberá dar clic en el botón "Formular Pregunta" lo que habilita un espacio para ingresar el interrogante. Al terminar de ingresar la información, dar clic en el botón de envío. El proponente podrá registrar cuantas inquietudes tenga, en diferentes momentos, siempre y cuando no se encuentre fuera del plazo estipulado por el Banco dentro del Cronograma.

La información correspondiente a la respuesta de cada pregunta radicada por todos los proponentes podrá ser consultada a través del mismo módulo y en la página web del Banco, una vez hayan sido resueltas por el Banco y de acuerdo con la fecha registrada en la información del Cronograma.

4.5.2. Cierre y entrega de la Propuesta

Los Proponentes deberán presentar las Propuestas de conformidad con el numeral 6 de los presentes Términos de Referencia, a más tardar en la *Fecha de Cierre y entrega de la Propuesta*, informada en el Cronograma, a través del Sistema. La fecha de cierre no se modificará o aplazará, salvo que Bancóldex lo considere conveniente, lo cual será informado a todos los proponentes.

No serán tenidas en cuenta propuestas radicadas físicamente, ni enviadas por correo electrónico, fax o cualquier otro medio, ni las que sean radicadas con posterioridad a la fecha y hora de cierre, a menos que se presente una indisponibilidad en el Sistema que imposibilite la recepción de propuestas, caso en el cual las mismas deberán enviarse vía correo electrónico a: correspondenciasector@bancoldex.com con copia a gonzalo.fino@bancoldex.com, indicándose en el asunto del correo electrónico: Términos de Referencia Número – "**TÉRMINOS DE REFERENCIA PARA LA CONTRATACIÓN DE LOS SERVICIOS: SECURITY OPERATION CENTER – SOC, ANÁLISIS DE VULNERABILIDADES DEL SERVICIO, MONITOREO DE MARCA Y GESTIÓN DE USUARIOS QUE PERMITAN FORTALECER LAS CAPACIDADES DE CIBERSEGURIDAD DEL BANCO."** y en el contenido del mismo: nombre, dirección, teléfono, correo electrónico del proponente, número de folios de que consta la propuesta técnica y económica y la relación de los anexos enviados o radicarse físicamente en la ventanilla de correspondencia del Banco ubicada en la calle 28 N° 13 A 15 piso 39. Edificio Centro de Comercio Internacional para lo cual deberá enviarse en archivos separados la propuesta técnica y la propuesta económica con sus anexos.

En caso de que los archivos enviados a través del Sistema o por correo electrónico, en el evento de indisponibilidad del Sistema, presenten errores que no permitan que el Banco pueda acceder a ellos, la propuesta será rechazada sin que haya lugar a que el interesado la presente nuevamente, por lo que es responsabilidad de cada proponente asegurarse antes de su envío, que la misma es accesible y que se ha remitido en su integridad.

La fecha y hora de cierre no se modificará o aplazará, salvo que Bancóldex, considere conveniente. En tal caso, la ampliación del plazo se dará a conocer mediante adenda que publicará en la página Web del Banco antes de la fecha de cierre.

Una vez recibida la propuesta, Bancóldex enviará un correo electrónico al remitente de la propuesta, informando la fecha y hora de recepción de la misma.

4.6. Adendas

Bancóldex comunicará mediante adendas, las aclaraciones y modificaciones que encuentren conveniente hacer a estos Términos de Referencia. Todas las adendas deberán ser tenidas en cuenta por los oferentes para su Propuesta y formarán parte de estos Términos de Referencia. Las Adendas serán publicadas a través de la página web del Banco y podrán consultarse en el Sistema.

Nota. Para refrescar la información de la invitación y sus respectivos módulos, ingrese siempre a través del link que se adjuntó en el correo de invitación para presentar propuesta.

5. EVALUACIÓN

5.1. Criterios y proceso de evaluación

A toda propuesta que cumpla con la presentación de la documentación requerida en los presentes Términos de Referencia, se le realizará un análisis en donde se verifique y evalúen los siguientes criterios:

CRITERIOS DE EVALUACIÓN	PUNTAJE	PORCENTAJE
Capacidad jurídica, financiera, administrativa, declaratoria de seguridad y ciberseguridad y certificación ISO 27001 para los servicios de SOC	**Cumple / No Cumple**	
CRITERIOS TÉCNICOS		
Solución Técnica • **Security Operation Center** • **Análisis de Vulnerabilidades** • **Ethical Hacking** • **Monitoreo de Marca**	**70**	**80%**

• **Gestión de Usuarios** • **Aseguramiento de Linea Base**			
Equipo de trabajo		**15**	
Experiencia del proponente		**15**	
SUBTOTAL		**100**	
CRITERIOS ECONÓMICOS			
CRITERIO 3: EVALUACIÓN ECONÓMICA		**100**	**20 %**
TOTAL			**100 %**

Aquellas propuestas que resulten habilitadas por cumplir con la capacidad jurídica, financiera y administrativa, declaratoria de seguridad y ciberseguridad y certificación ISO 27001 para los servicios de SOC pasarán a ser evaluadas en su componente técnico.

Para que una propuesta sea considerada en la selección de la presente convocatoria, la evaluación de los criterios técnicos deberá alcanzar al menos el **ochenta por ciento** (80%) del puntaje total del respectivo criterio.

Las propuestas que cumplan con el umbral mínimo antes indicado pasarán a la evaluación de la propuesta económica en los términos indicados en el numeral 5.10. de la presente convocatoria.

La evaluación final será resultado de la sumatoria de la calificación obtenida en la evaluación técnica y económica de la propuesta. El Banco adjudicará la convocatoria a la propuesta que obtenga el mayor puntaje teniendo en cuenta la suma de los criterios técnicos y económicos. La adjudicación del contrato será comunicada al proponente seleccionado.

El resultado de la evaluación de las propuestas se consignará en el Formato de selección de proveedores suscrito por la instancia evaluadora.

NOTA 1: Bancóldex realizará consultas de control previo del proponente, de las personas o partes relacionadas con el proponente y vinculadas a la propuesta, según aplique, con el fin de analizar los riesgos relacionados con Lavado de Activos y Financiación del Terrorismo, y según con lo establecido en cada una de los Sistemas de Prevención del Lavado de Activos y Financiación del Terrorismo. En caso de encontrarse coincidencia en dichos reportes se rechazará la propuesta de forma inmediata.

Así mismo, en cumplimiento del artículo 60 de la Ley 610 de 1999, Bancóldex realizará consulta del proponente en el Boletín de Responsables Fiscales de la Contraloría General y en caso de que éste se encuentre reportado se rechazará la propuesta de forma inmediata.

Adicionalmente, Bancóldex realizará la consulta en centrales de riesgo al proponente y en caso de reporte negativo se llevarán a cabo los análisis correspondientes que permitan validar la capacidad de este para la celebración de la orden de servicio en una eventual adjudicación de la presente convocatoria.

Nota 2: Durante el proceso de evaluación, Bancóldex podrá solicitar a los proponentes las aclaraciones sobre la información contenida en las propuestas, por medio escrito y/o mediante sustentación virtual o presencial.

5.2. Capacidad Jurídica

La evaluación de la capacidad jurídica se llevará a cabo por parte de la Oficina de Gestión de Contratos del Banco y corresponde a las actividades tendientes a validar la capacidad del proponente para presentar la propuesta y celebrar el respectivo contrato en el evento que resulte adjudicado en el proceso de selección.

Para el efecto la Oficina de Gestión de Contratos del Banco verificará contra el certificado de existencia y representación legal de los proponentes y demás documentos los siguientes aspectos, (i) Que el objeto social principal del proponente se relacione con el servicio de ciberseguridad y seguridad informática, (ii) la duración de la sociedad de acuerdo con lo exigido en el numeral 4.4. de los presente Términos de Referencia, (iii) facultades del representante legal para presentar la propuesta y/o contraer obligaciones en nombre de la misma.

5.3. Capacidad Financiera

El proponente deberá tener la capacidad financiera suficiente para el cumplimiento de sus obligaciones contractuales. Para la evaluación de la capacidad financiera el proponente deberá diligenciar la “matriz de capacidad financiera” Anexo No. 6 con los datos de los estados financieros de los dos últimos años certificados o dictaminados con corte al 31 de diciembre del respectivo año. Para la validación de esta información, el proponente deberá adjuntar la totalidad documentación solicitada de acuerdo con el numeral 6.3. (documentación de la propuesta) de la presente invitación.

Validada la información contenida en la matriz, El Banco realizará una evaluación financiera de los proponentes revisando entre otros aspectos, liquidez, endeudamiento y rentabilidad, indicadores que se compararan con el promedio del sector. Así mismo, se revisará el endeudamiento del proponente en Centrales de riesgo y la calificación respectiva.

En caso de que se considere necesario explicar un posible reporte negativo por parte de los proponentes se deberá enviar toda la documentación que permita aclarar tal situación, tales como cartas aclaratorias y certificados de pagos a las entidades financieras.

5.4. Capacidad Administrativa

En la evaluación de la capacidad administrativa se tendrán en cuenta los aspectos informados por el Proponente en su propuesta respecto de la estructura organizacional, infraestructura física ofrecida y equipo de trabajo por este para la prestación del servicio objeto de la presente convocatoria.

Adicionalmente, los Proponentes que cuenten con políticas de Responsabilidad Social Empresarial deberán informarlo en su propuesta, como el desarrollo de su equipo humano de trabajo bajo condiciones laborales dignas, compensación justa, adecuadas condiciones de bienestar, seguridad y salubridad en el trabajo; el respeto y cuidado por el medio ambiente y el compromiso con el desarrollo de las comunidades en las que operan.

5.5. Declaratoria de seguridad, ciberseguridad y nube

El Proponente debe dar respuesta puntual a cada items del Anexo N° 8“Declaraciones de seguridad y ciberseguridad”, indicando si su propuesta cumple con los mismos, explicando y argumentando técnicamente cómo cumplirá con lo solicitado y en qué página de su propuesta se desarrolla el respectivo requerimiento. El documento deberá remitirse diligenciado y firmado por el representante legal del proponente.

5.6. Certificación ISO 27001

Los Proponentes deben presentar copia de la certificación ISO 27001 particularmente en los procesos de prestación de servicios de SOC. Esta certificación deberá contener la información del ente certificador para verificar la vigencia y autenticidad de la misma. En caso de no contar con las certificaciones ISO 27001 su calificación en este criterio será de “No Cumple”

5.7. Solución Técnica

Los Proponentes deben dar respuesta puntual a cada uno de los numerales relacionados en el Anexo N° 1. Especificaciones Técnicas, argumentando técnicamente cómo cumplirá con lo solicitado. Aquel proponente que cumpla con lo definido previamente obtendrá como calificación el porcentaje definido en la matriz de calificación.

En caso de que la propuesta presentada no exprese con claridad la forma en que se cumplirán los numerales relacionados el puntaje que se obtendrá en este criterio es cero.

5.7.1. Security Operation Center – SOC

Cumplir con los requerimientos planteados en el Anexo Técnico pestaña "SOC". para lo cual el proponente deberá justificar cada una de las respuestas, el mayor puntaje será asignado a quien cumpla y argumente correctamente todos los requisitos, para los que no cumplan con esta

condición se revisara uno a uno los requisitos contestados y se asignará un puntaje de acuerdo a la importancia de cada requisito, su cumplimiento y su argumentación.

5.7.2. Análisis de Vulnerabilidades del Servicio

Cumplir con los requerimientos planteados en el Anexo Técnico pestaña "Análisis de vulnerabilidades", para lo cual el proponente deberá justificar cada una de las respuestas, el mayor puntaje será asignado a quien cumpla y argumente correctamente todos los requisitos, o, su cumplimiento y su argumentación.

5.7.3. Ethical Hacking

Cumplir con los requerimientos planteados en el Anexo Técnico pestaña "Ethical Hacking", para lo cual el proponente deberá justificar cada una de las respuestas, el mayor puntaje será asignado a quien cumpla y argumente correctamente todos los requisitos, , su cumplimiento y su argumentación.

5.7.4. Monitoreo de Marca

Cumplir con los requerimientos planteados en el Anexo Técnico pestaña "Monitoreo de marca", para lo cual el proponente deberá justificar cada una de las respuestas, el mayor puntaje será asignado a quien cumpla y argumente correctamente todos los requisitos, su cumplimiento y su argumentación.

5.7.5. Gestión de Usuarios

Cumplir con los requerimientos planteados en el Anexo Técnico pestaña "Monitoreo y gestión de usuarios", para lo cual el proponente deberá justificar cada una de las respuestas, el mayor puntaje será asignado a quien cumpla y argumente correctamente todos los requisitos, , su cumplimiento y su argumentación.

5.7.6. Aseguramiento Linea base

Cumplir con los requerimientos planteados en el Anexo Técnico pestaña "Aseguramiento líneas base", para lo cual el proponente deberá justificar cada una de las respuestas, el mayor puntaje será asignado a quien cumpla y argumente correctamente todos los requisitos, , su cumplimiento y su argumentación.

5.8. Equipo de trabajo

El Equipo de Trabajo deberá ser suficiente e idóneo para cumplir con el objeto de la presente invitación, debe incluir como mínimo los siguientes miembros que cumplan con las siguientes características:

1. Gerente del proyecto (Obligatorio) - Descripción del cargo: Un (1) director responsable del cumplimiento del objeto de la presente convocatoria con todos sus componentes. - Experiencia: Por lo menos tres (3) años de experiencia, en la prestación de proyectos de servicios de ciberseguridad.
2. Equipo de implementación: - Roles: se sugiere que se cuente como mínimo con un equipo de trabajo que este integrado por: un (1) ingeniero de sistemas y un (1) analista técnico que también debe ser ingeniero de sistemas o ingeniero con experiencia en implementación de soluciones de ciberseguridad.
3. Equipo de soporte: Personal de soporte deberá contar con experiencia en ciberseguridad y apoyará los requerimientos de servicio objeto de este contrato.

El máximo puntaje asignado en este criterio es quince (15) puntos. El Proponente para relacionar el equipo de trabajo propuesto deberá diligenciar el Anexo No.9 “Formato resumen del Equipo de Trabajo”, en el cual deberá indicar para cada experto del Equipo de Trabajo:

(i) El nivel de formación (profesional, técnico o tecnólogo, posgrado) (ii) La experiencia específica relacionada (años, meses y días). El Proponente deberá adjuntar las cartas de intención de cada uno de los integrantes del Equipo de Trabajo, mediante las cuales se manifieste el compromiso de trabajar en el objeto de la presente convocatoria.

(ii) El puntaje de este criterio se otorgará de la siguiente forma:

A) Experiencia del Gerente del proyecto: - Cinco (5) puntos se le otorgará en este subcriterio al proponente que cuente con un gerente de proyecto que demuestre experiencia en soluciones similares mayores a 5 años. - Tres (3) puntos se le otorgará en este subcriterio al proponente que cuente con un gerente de proyecto que demuestre experiencia en soluciones similares entre tres (3) y cinco (5) años.

B) Número de integrantes del equipo de implementación. El equipo de trabajo base se define como el equipo mínimo sugerido de dos ingenieros. Si presentan más integrantes en el equipo, los miembros del equipo deben ser plenamente identificados en la propuesta. El puntaje de este criterio se otorgará de la siguiente forma: • Cinco (5)

puntos se le otorgará si el equipo de trabajo base está conformado por un número mayor al mínimo integrantes requerido con los perfiles indicados
• Tres (3) puntos se le otorgará si el equipo de trabajo base está conformado por el número mínimo de integrantes requerido. En caso de que los proponentes no cumplan con la experiencia mínima requerida en proyectos similares y/o el equipo no está conformado por el número mínimo de personas requerido por esta convocatoria recibirán un puntaje de cero (0) en la evaluación de este criterio.

C) Número de integrantes del equipo de soporte. El equipo de trabajo base se define como el equipo mínimo sugerido de tres ingenieros. Si presentan más integrantes en el equipo, los miembros del equipo deben ser plenamente identificados en la propuesta. El puntaje de este criterio se otorgará de la siguiente forma: • Cinco (5) puntos se le otorgará si el equipo de trabajo base está conformado por un número mayor al mínimo integrantes requerido con los perfiles indicados • Tres (3) puntos se le otorgará si el equipo de trabajo base está conformado por el número mínimo de integrantes requerido. En caso de que los proponentes no cumplan con la experiencia mínima requerida en proyectos similares y/o el equipo no está conformado por el número mínimo de personas requerido por esta convocatoria recibirán un puntaje de cero (0) en la evaluación de este criterio.

Los ingenieros de implementación y/o soporte deberán contar con certificaciones vigentes para la utilización de herramientas que soporten los servicios objeto de la contratación, en caso de que el personal dispuesto para la prestación del servicio no cuente con las certificaciones, se aceptarán profesionales de Ingeniería de sistemas o carreras afines que cuenten con estudios de postgrado tipo especialización y/o maestría, en seguridad informática, ciberseguridad o temas afines. Lo solicitado anteriormente deberá documentarse debidamente en la propuesta, con las hojas de vida del personal relacionado que deberá incluir cartas de compromiso con una duración igual a la del plazo del contrato.

El perfil o los perfiles solicitados por el Banco para soportar la operación del servicio deben contar con los siguientes títulos:

1. Magister en Seguridad de la Información o Equivalente
2. Certificación CEH
3. Certificación OSCP
4. Certificación ISO 27001 Implementador o auditor

5.9. Experiencia del proponente

Los Proponentes deberán acreditar y contar con mínimo tres (3) años de experiencia en la prestación de los servicios de SOC, análisis de vulnerabilidades, ethical hacking, aseguramiento de líneas base, monitoreo de marca y gestión de usuarios.

Para acreditar la experiencia exigida, cada Proponente deberá aportar certificaciones, o contratos con sus respectivas actas de liquidación y/o terminaciones expedidas por sus clientes, correspondientes a empresas que operen en Colombia, en las cuales se hayan prestado servicios de ciberseguridad y seguridad informática.

Las certificaciones o contratos con sus respectivas actas de liquidación y/o terminación deberán contener como mínimo la siguiente información:

- Nombre o razón social del Contratante
- Nombre o razón social del Contratista
- Objeto del servicio o contrato
- Datos de contacto del Contratante

No se entenderá como acreditación de experiencia una lista donde se relacione la experiencia, sin que se aporten las respectivas certificaciones, contratos con sus respectivas actas de liquidación o terminación.

La asignación del puntaje para este criterio se hará con base en la calificación de “Cumple o No cumple” donde mínimo el proponente deberá presentar una certificación de experiencia de los siguientes servicios: Servicios de SOC, análisis de vulnerabilidades y ethical hacking. El puntaje si cumple serán quince (15) puntos y en su defecto cero (0).

Para el Banco es obligatorio que la experiencia reportada sea emitida por una entidad vigilada por la Superintendencia Financiera de Colombia.

Nota: La certificación puede ser remplazada por la copia del contrato, siempre y cuando también se anexe la respectiva acta de terminación y/o acta de liquidación, debidamente suscrita por la entidad contratante, que en conjunto cumplan con los contenidos y requisitos establecidos anteriormente, de lo contrario no será tenida en cuenta. El acta de liquidación debidamente suscrita por las partes servirá para acreditar la experiencia del proponente, siempre que en ella conste la información de nombre del contratante, objeto, vigencia y valor del contrato.

5.10. Oferta económica

El Proponente deberá presentar su oferta económica de acuerdo con el alcance y condiciones del servicio descritos en el numeral 7 de estos términos de referencia.

El proponente deberá incluir en su oferta económica el IVA de los servicios ofertados, discriminando los valores para la prestación de los servicios de SOC, análisis de vulnerabilidades, ethical hacking, aseguramiento de líneas base, monitoreo de marca y gestión de usuarios, informado todos los impuestos a que haya lugar conforme a las normas tributarias vigentes. Si el Proponente no discrimina el impuesto al valor agregado (IVA) u otro impuesto y el servicio causa dicho impuesto, Bancóldex lo considerará INCLUIDO en el valor total de la oferta y así lo acepta el Proponente.

La Propuesta económica deberá cubrir todos los gastos en los que incurra el Proponente, incluyendo aquellos correspondientes a la prestación de los servicios y cualquier otro gasto.

En ningún caso Bancóldex reembolsará o cubrirá gastos adicionales que superen el valor de la propuesta presentada.

Todo error u omisión en la oferta económica, indebida interpretación del alcance del objeto de la presente invitación y condiciones previstas en estos Términos de Referencia, así como de las normas tributarias aplicables, será responsabilidad del Proponente y no se le permitirá ajustar sus precios.

El proponente que presente la oferta más económica obtendrá el mayor puntaje, es decir 100 puntos y a los demás oferentes se les asignará un puntaje proporcional.

Bancóldex revisará las operaciones aritméticas de la propuesta económica y en caso de error se le solicitará las respectivas aclaraciones al proponente de acuerdo con lo establecido en el numeral 5.11. de la presente convocatoria.

Si el proponente no da repuesta en el término que para el efecto le haya establecido Bancóldex, los errores en las operaciones aritméticas serán corregidos de la siguiente manera:

- Cuando se presente divergencias entre el valor expresado en números y en letras, prevalecerá la cantidad expresada en letras.
- Los valores corregidos se tendrán en cuenta en la evaluación de las propuestas, en la adjudicación y suscripción de la orden de servicio, por lo que los errores u omisiones en que se incurra en la propuesta económica serán de la exclusiva responsabilidad del proponente, debiendo asumir los mayores costos y/o pérdidas que se deriven de dichos errores u omisiones.

Los proponentes responderán cuando formulen propuestas en las cuales se fijen condiciones económicas y de contratación artificialmente bajas con el propósito de obtener la adjudicación de la presente convocatoria.

5.11. Solicitud de aclaración o complementación o subsanibilidad

De considerarlo necesario, Bancóldex podrá solicitar aclaraciones o complementaciones a la propuesta hasta antes de la adjudicación de la presente Convocatoria, respecto de cualquiera de los requisitos y documentación relacionada con aspectos que no otorguen puntaje, ya sea porque no encuentran claridad en algún tema o para subsanar la ausencia de algún documento. En la solicitud concederá un plazo para las respuestas y si fuere necesario podrá aplazarse la adjudicación, previa información a todos los proponentes. En ningún caso la aclaración o complementación podrá dar lugar a modificar el alcance inicial de la propuesta, mejorarla, ni acreditar requisitos o condiciones adquiridas con posterioridad al cierre del proceso de selección.

Igualmente podrá solicitar aclaraciones en aspectos de la propuesta económica, pero únicamente para la corrección de errores de trascripción, numéricos, matemáticos o formales. En ningún caso la aclaración podrá dar lugar a modificar el alcance inicial de la propuesta económica, mejorarla, ni acreditar requisitos o condiciones adquiridas con posterioridad al cierre del proceso de selección.

En caso de que el proponente no presente la aclaración o complementación en el plazo establecido, Bancóldex podrá descartar la propuesta y no tenerla en cuenta para ser evaluada.

5.12. Criterios de desempate

Cuando entre dos o más propuestas se presente un empate en la calificación total obtenida, se tendrán en cuenta los siguientes criterios de desempate en su orden:

- Mayor puntaje en el criterio de Anexo Técnico capítulo SOC.
- El proponente que acredite que por lo menos el 10% de su nómina la conforman empleados en las condiciones de discapacidad enunciadas en la Ley 361 de 1997 debidamente certificadas por la oficina de trabajo de la respectiva zona y contratados por lo menos con anterioridad de un año a la presentación de la propuesta. Si la propuesta es presentada por un Consorcio o Unión Temporal, el integrante del proponente que acredite que el diez por ciento (10%) de su nómina está en condición de discapacidad, debe tener una participación de por lo menos el veinticinco por ciento (25%) en el Consorcio o la Unión Temporal y aportar mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la propuesta. En todo caso; en el evento que la propuesta seleccionada sea aquella que acredite cumplir con esta condición, los empleados deberán mantenerse vinculados por un lapso igual al plazo del contrato que se celebre como consecuencia de la adjudicación de la presente convocatoria.

5.13. Rechazo de Propuestas

Se rechazarán de plano las Propuestas en las que:

- El Proponente no cumpliere con los requisitos establecidos en estos Términos de Referencia.

- No se aporte toda la documentación requerida en los presentes Términos de Referencia y/o sus anexos o aquella documentación que requiera el Banco antes de finalizado el proceso de adjudicación de la presente convocatoria y que no se aporte por el proponente durante el plazo definido para ello por El Banco.
- Se hubiere presentado la Propuesta en forma subordinada al cumplimiento de cualquier condición.
- Se incluya información que no sea veraz.
- Se incluyan disposiciones contrarias a la ley colombiana.
- La propuesta se hubiere presentado de forma extemporánea.
- Cuando se presenten propuestas parciales, es decir, propuestas que no oferten por la totalidad del objeto de conformidad en lo establecido en los presentes Términos de Referencia
- Cuando existan varias propuestas presentadas por el mismo proponente en el mismo proceso de selección de manera directa o por interpuesta persona.

5.14. Declaratoria de desierta

La convocatoria se declarará desierta en los siguientes casos:

- Cuando ninguna de las propuestas evaluadas cumpla con los requisitos exigidos en los términos de referencia.
- Por motivos o causas que impidan la escogencia objetiva.
- Cuando se hubiere violado la reserva de las propuestas presentadas.
- Cuando no se presente ninguna propuesta.
- Cuando ninguna de las propuestas hubiese obtenido la calificación mínima exigida para los aspectos técnicos.

6. CONTENIDO Y ESTRUCTURA DE LA PROPUESTA

6.1. Presentación de la Propuesta

El Proponente presentará una sola propuesta en idioma español a través del Sistema, al que puede acceder a través del enlace remitido por correo electrónico por medio del cual recibió acceso a la invitación, previa inscripción inicial en la página web de Bancoldex.

La propuesta se deberá presentar debidamente foliada y presentarse dentro del plazo fijado.

Cualquier información adicional que el proponente considere necesario presentar, debe incluirla o adjuntarla a la Propuesta que entregue de acuerdo con la fecha establecida para el cierre de convocatoria.

Para los efectos de este proceso se advierte a los proponentes que la fecha y hora válida, es la indicada por el Sistema, la cual se notificará a través de correo electrónico en el momento de realizar la radicación de la propuesta.

6.2. Periodo de validez de la propuesta

La Propuesta tendrá un periodo de validez de seis (6) meses, contados a partir de la fecha de cierre y entrega de la propuesta señalada en el numeral 4.5. de estos Términos de Referencia.

6.3. Documentación de la Propuesta

La Propuesta deberá incluir los siguientes documentos:

1. Anexo No 1 Carta sobre las políticas de Seguridad de la Información y Ciberseguridad para Proponentes y Proveedores de Bancóldex S.A.
2. Anexo No. 2 – Carta de presentación de la propuesta. Se debe diligenciar en su totalidad esta carta, en la que, entre otros aspectos, se debe indicar el nombre del Proponente, así como el nombre, cargo e información de contacto del responsable a quien se contactará para cualquier asunto relacionado con la Propuesta. Esta carta deberá estar firmada por el representante legal del Proponente o por el apoderado constituido para el efecto.
3. Anexo No. 3 Carta de conocimiento-Aceptación de los Valores institucionales
4. Anexo No. 4 confidencialidad y tratamiento de datos personales
5. Anexo No. 5 requisitos de seguridad y salud en el trabajo.
6. Anexo No. 6 “Matriz Capacidad financiera”
7. Anexo No 7 Anexo Especificaciones Técnicas”
8. Anexo No 8 “Declaraciones de seguridad y ciberseguridad”
9. Anexo No 9 “Anexo Técnico”
10. Documentación soporte que acredite la experiencia del proponente de conformidad con lo establecido en el numeral 5.9.
11. Documentación que acredite los aspectos considerados en la Capacidad Administrativa de conformidad con el numeral 5.4. de la presente convocatoria.
12. En el evento que aplique, acta del órgano social respectivo autorizando al Representante Legal de la persona jurídica para presentar la presente propuesta y celebrar el contrato con Bancóldex en caso de que resulte seleccionado.
13. Poder debidamente otorgado y reconocido en texto y firma ante notario y/o apostillado según sea el caso, cuando se actúe por representación.
14. Garantía de seriedad de la oferta en formato de entidades particulares, de conformidad con lo establecido en el numeral 3.8. En el caso de pólizas de seguro se deberá anexar adicionalmente el respectivo recibo de pago.
15. Estados Financieros certificados o dictaminados de los dos últimos años, con notas aclaratorias.
16. Certificado de existencia y representación legal con una vigencia no mayor a sesenta (60) días.
17. Copia del Registro Único Tributario (RUT) del proponente.
18. Certificado de pago de seguridad social y parafiscales.

19. Certificación bancaria indicando la cuenta a la que debe hacerse la transferencia electrónica de fondos.
20. Propuesta Técnica.

7. TÉRMINOS DE LA CONTRATACIÓN

7.1. Alcance del servicio

Para la prestación del servicio se requiere fortalecer las capacidades de ciberseguridad en modalidad de servicio de:

1. Security Operation Center – SOC
2. Análisis de vulnerabilidades
3. Ethical hacking
4. Aseguramiento de líneas base
5. Monitoreo de marca
6. Gestión de usuarios.

7.2. Condiciones para el servicio de Security Operation Center – SOC

1. Prestar el servicio de SOC que permita identificar, contener, mitigar y solventar los riesgos de seguridad que puedan comprometer la confiabilidad, integridad o disponibilidad en la infraestructura del Banco, en una modalidad de 7 X 24 X 365.
2. Contar con sus centros de servicios dentro de la geografía nacional o fuera de ella, siempre alineándose con la normativa vigente de la Superintendencia Financiera de Colombia – SFC.
3. Prestar el servicio de acuerdo con estándares de calidad o cumpliendo con sus prácticas equivalentes.
4. Garantizar la migración de la información de la operación del anterior proveedor para empalmar el conocimiento de la correlación de eventos y casos de negocio ya aprendidos por el Banco.
5. Atender un plan de transición entre al anterior prestador del servicio que garantice la correcta prestación del servicio de SOC y correlación de eventos. De igual forma se deberá llevar el histórico de información que suministre el anterior proveedor del servicio.
6. Garantizar la colección de los últimos tres meses de la información del Banco durante la ejecución del contrato, para la consulta en línea. Para tal fin el contratista dispondrá de los medios requeridos, lo cuales podrán incluir la instalación de colectores de información en el Datacenter del Banco que se comuniquen con la infraestructura del contratista. Será

responsabilidad del contratista garantizar la disponibilidad de la infraestructura necesaria para cumplir este propósito en la volumetría, tiempos históricos y los niveles de servicio solicitados.

7. Ofrecer al Banco para su consulta un portal WEB con acceso a los requerimientos e incidentes del servicio, donde se pueda contar con toda la trazabilidad de los casos y demás información relevante del servicio. De igual manera en dicho portal se deberá disponer de reportes periódicos del servicio con el nivel de detalle que la operación del Banco demande. Esto implicará un mínimo de 10 plantillas de reportes que serán acordadas dentro de la operación.
8. Detectar de manera temprana amenazas o evidencias de compromiso de la infraestructura del Banco, basado en la recolección de información pública de entidades dedicadas a la ciberseguridad de Internet o de grupos o foros de comunicación formales e informales. Lo anterior con el propósito de establecer acciones preventivas en la infraestructura y en los procesos de gestión de seguridad de la información o seguridad informática del Banco.
9. Monitorear la información del Banco en redes sociales con el propósito de detectar y contener posibles riesgos de abuso de marca o imagen del Banco.
10. Detectar el uso del nombre del Banco en técnicas de malware como phishing, aplicaciones tipo rogue o credenciales para fines maliciosos que busquen el robo de identidades o demás actividades mal intencionadas en Internet.
11. La operación de los servicios de monitoreo de ciberseguridad deberá basarse en el cumplimiento de unos ANS, los cuales se proponen a continuación. En todos los escenarios, el tiempo máximo de registro será de 15 minutos y de solución de:

Criticidad	Tiempo Requerido de Solución
Crítica	2 horas
Alta	8 horas
Moderada	16 horas
Baja	48 horas

12. El Banco requiere conocer suficientemente la infraestructura que soportará el servicio a contratar tanto a nivel de software como de hardware. Para tal fin el proponente deberá entregar la información de la arquitectura del servicio en bajo nivel. Será valorado por el Banco la utilización de herramientas líderes de sus respectivos segmentos.

7.3. Condiciones para el servicio de Análisis de vulnerabilidades

1. Realizar un ejercicio de análisis de vulnerabilidades con periodicidad semestral, para un total de 2 pruebas en al año. Cada análisis de vulnerabilidades deberá contar con una metodología diferencial, basada en el ejercicio inmediatamente anterior, todos a excepción del primer análisis donde se definirá la línea base. En todo escenario los análisis se harán sobre la totalidad de los CI´s y direcciones IP que determine el Banco.

2. Cada ejercicio de análisis de vulnerabilidades deberá contar con hasta con 2 re test, para corroborar la correcta aplicación de las remediaciones sugeridas. Estos ejercicios de re test no requieren la presentación de informes personalizados.
3. El análisis de vulnerabilidades se debe realizar sobre un rango de 800 a 1000 direcciones IP, las cuales corresponden a servidores, equipos de infraestructura y telecomunicaciones y estaciones de cómputo de clientes. El número de IP puede variar en un 20% sin que esto implique variación en el costo del servicio.
4. Los informes de cada análisis de vulnerabilidades deberán ser sustentados y explicados por el proponente a los administradores de los CI´s que el Banco delegue. Los informes de las herramientas de análisis de vulnerabilidades deberán ser acompañados de los análisis detallados por parte del proponente.
5. La remediación de las vulnerabilidades encontradas en cada uno de los ejercicios, serán acompañadas por el proponente hasta su implementación, que implica una tarea consultiva para asesorar al Banco en el cómo se realizan estas remediaciones.
6. El Banco requiere conocer suficientemente la infraestructura que soportará el servicio a contratar tanto a nivel de software como de hardware. Para tal fin el proponente deberá entregar la información de la arquitectura del servicio en bajo nivel. Será valorado por el Banco la utilización de herramientas líderes de sus respectivos segmentos.
7. Las herramientas usadas en el análisis de vulnerabilidades deberán estar homologadas por el CVE (Common vulnerabilitis and Exposures) y las actualizaciones de la fecha de utilización. Para los informes solicitados se deberán tomar como referencia la lista de nombre de vulnerabilidades CVE publicada por la corporación Mitre (www.mitre.org)

7.4. Ethical hacking

1. Realizar (2) dos ejercicios de Ethical Hacking durante el año. El primero de ellos se debe realizar durante el primer semestre de operación del servicio y el segundo en el segundo semestre del año de servicio correspondiente. Estos ejercicios deben contemplar la posibilidad de hacer mínimo dos retest para verificar las correcciones posteriores por parte del Banco. Las pruebas podrán ser tipo caja gris, caja blanca o caja negra, de acuerdo a lo solicitado por el Banco.
2. Realizar el Ethical Hacking basado en buenas prácticas y metodologías como PTES, OWASP, NIST, MITRE, entre otros y NO deberá basarse en el uso de herramientas de análisis de vulnerabilidades. El proponente debe sustentar con claridad la estructura del servicio para la validación del Banco.
3. Realizar un ejercicio de pruebas tipo red team con una duración mínima de 4 semanas de ejecución y informes.

7.5. Monitoreo de marca

1. Tener capacidad de realizar detección de registro de dominios similares al de la marca del Banco y mostrar esta información a través de un portal web con la siguiente información como mínimo: 1. Fecha de alerta. 2. Dominio Similar. 3. Registro MX (indicar si tiene registro MX activo).
2. Informar los datos sobre ejecutivos y colaboradores. (Emails, contraseñas, fechas de nacimiento, información personal identificable, etc.). El Proponente deberá informar sobre falsas campañas (de contratación, comerciales, de servicios financieros, o similares relacionados con el negocio).
3. El Proponente realizara el descubrimiento y reporte de amenazas en la Deep Web (Internet profundo), y Dark Web (Internet oscuro) enfocadas al sistema financiero o dirigidas hacia el Banco.
4. Prestar el servicio de takedown para al menos 12 dominios/app's anuales. En promedio una acción por mes, durante el periodo total del servicio.

7.6. Gestión de usuarios

1. Realizar un monitoreo y correlación de hasta 30 repositorios de usuarios (Incluyendo tablas de bases de datos, motores de bases de datos, sistemas operativos windows y linux, LDAP, AD, archivos planos, entre otros)
2. El software deberá recolectar y correlacionar información de los repositorios de usuarios con una periodicidad mínima de 1 semana.
3. El software deberá correlacionar los usuarios de los sistemas con las identidades definidas en la línea base

7.7. Forma de pago

Se pagará de forma mensual vencida previa presentación de la factura y aprobación del supervisor del contrato del informe mensual presentado.

NOTA 1: Previo a la presentación de la factura, las partes validarán el cumplimiento durante el mes respectivo de los niveles de servicio ofrecidos, con el fin de establecer si hay lugar a aplicar los descuentos en la facturación mensual de acuerdo con las penalidades previamente establecidas.

NOTA 2. Si el Contratista que resulte seleccionado se encuentra obligado a expedir factura electrónica de venta bajo la normatividad colombiana aplicable, el contratista deberá enviar una representación gráfica de la factura al correo electrónico correspondenciasector@bancoldex.com habilitado por el Banco garantizando que la misma se pueda leer, copiar, descargar e imprimir de

formar gratuita sin tener que acudir a otras fuentes para proveerse de las aplicaciones necesarias para ello.

7.8. Entregables

- Entregables de la prestación del servicio (ejecución).
- Informes mensuales de la prestación del servicio de monitoreo de marca y gestión de usuarios privilegiados y el servicio de SOC.
- Informes trimestrales con respecto al seguimiento de análisis de vulnerabilidades y pruebas de ethical hacking

8. EL CONTRATO

8.1. Suscripción del contrato

Una vez se adjudique el Contrato por parte de Bancóldex se informará por escrito de dicha decisión al Proponente favorecido, quien procederá a la firma y devolución del mismo, junto con los demás documentos requeridos para su legalización, dentro de los diez (10) días hábiles siguientes a la fecha de envío del documento.

En caso de negativa u omisión del adjudicatario a suscribir el Contrato en el plazo previsto, o en el evento de presentarse cualquier otra circunstancia por la cual el adjudicatario no esté en condiciones de firmar conforme a estos Términos de Referencia, Bancóldex podrá contratar con el Proponente siguiente en el orden de calificación mayor a menor y así sucesivamente.

En este caso, Bancóldex podrá hacer efectiva la garantía de seriedad de la Propuesta sin menoscabo de las acciones legales conducentes al reconocimiento de perjuicios causados y no cubiertos por el valor de la garantía.

8.2. Obligaciones de Bancóldex

En el desarrollo del Contrato suscrito en virtud de estos Términos de Referencia, Bancóldex, tendrá las siguientes obligaciones:

(i) Pagar al Contratista la suma debida según los términos del Contrato.
(ii) Cooperar con el Contratista para el normal desarrollo del Contrato.
(iv) Entregar al Contratista información con la que cuente y sea susceptible de entregar para efectos del desarrollo del objeto del Contrato.

8.3. Obligaciones del Contratista

En el desarrollo del Contrato suscrito en virtud de estos Términos de Referencia, el Contratista tendrá, entre otras, las siguientes obligaciones:

(i) Desarrollar las actividades contratadas, de conformidad con lo establecido en el Contrato y en sus documentos anexos, los cuales será controlados por el banco mediante la aplicación de acuerdos de niveles de servicio e informes mensuales que consolidarán los resultados de la prestación del servicio.

(ii) Diseñar conjuntamente con EL BANCO el cronograma de actividades en donde se relacionen las diferentes tareas a cargo del personal designado para ejecutar el objeto del presente contrato.

(iii) Designar un Gerente de Proyecto, quien será el interlocutor válido para EL BANCO, así como coordinar las labores y funciones con el interlocutor que EL BANCO designe para el desarrollo del presente contrato.

(iv) Garantizar los recursos técnicos y físicos para la ejecución del contrato.

(v) Contar con una mesa de ayuda, para la atención de los requerimientos e incidentes, con la disponibilidad de 7x24x365 para la atención.

(vi) Realizar la detección y correlación de múltiples vectores de ataque, como por ejemplo eventos e incidentes de seguridad, registros de auditoria – logs, análisis de tráfico, filtrado de red, vulnerabilidades, registros de fuga de información.

(vii) Generar reglas de monitoreo que permitan fortalecer la seguridad digital al interior de BANCOLDEX, las cuales deben estar alineadas con las buenas prácticas de seguridad de la información y Ciberseguridad.

(viii) Elaborar en conjunto con el Banco un perfil de amenazas alineadas con el modelo de operación de la infraestructura tecnológica de EL BANCO y determinar el esquema de monitoreo y respuesta a las mismas.

(ix) Diseñar y construir en conjunto con EL BANCO indicadores que permitan identificar la eficiencia, eficacia y efectividad del servicio contratado, específicamente en lo que respecta a la gestión de la ciberseguridad

(x) En coordinación con los administradores de los dispositivos y/o aplicaciones correlacionadas, actualizar las reglas pre-configuradas, las cuales deberán basarse en los ataques, riesgos y fallas más comunes.

(xi) Contar con el registro de todos los eventos e incidentes de seguridad que se detecten, los cuales tendrán la asignación de un número único de identificación con el fin de realizar un seguimiento de las acciones tomadas sobre las respuestas ante los incidentes reportados, así como la generación de las estadísticas e indicadores con base en estos registros.

(xii) Generar alertas de otras amenazas que puedan impactar a EL BANCO

(xiii) Administrar el ciclo de vida de los eventos e incidentes reportados desde su apertura hasta su cierre.

(xiv) Adelantar las actividades del servicio de SOC y del servicio de Análisis de Vulnerabilidades, de acuerdo con lo descrito en el anexo de especificaciones técnicas.

(xv) Contar con procedimientos controlados para la entrega de información por parte del Banco durante la vigencia del contrato y para la destrucción de la misma por parte de EL CONTRATISTA una vez finalizado el contrato. Dicho procedimiento deberá ser informado al Banco antes de que inicie la ejecución del presente contrato.

(xvi) Dar cumplimiento en todo momento a las normas que sobre seguridad de información y ciberseguridad sean expedidas por cualquier autoridad nacional.

(xvii) Permitir las visitas que EL BANCO deba realizar para verificar el cumplimiento de las obligaciones señaladas en el presente numeral.

(xviii) Cumplir con las disposiciones contenidas en el Decreto 1072 de 2015 y demás normas que regulen la seguridad y salud en el trabajo, respecto del personal que designe para la prestación de los servicios objeto del presente contrato.

(xix) Guardar absoluta reserva y no utilizar total o parcialmente la información de carácter confidencial que reciba directa o indirectamente de EL CONTRATANTE para propósitos diferentes al cumplimiento del presente contrato. De acuerdo con lo anterior, el Proponente se obliga a informar y a hacer cumplir estrictamente la presente obligación al personal que destine para la ejecución del servicio requerido.

(xx) Diligenciar anualmente la Lista de Verificación de Cumplimiento en seguridad de la información, con el fin de validar el cumplimiento por parte de EL CONTRATISTA de los requerimientos normativos en seguridad de la información, ciberseguridad, protección de datos, continuidad del negocios y soluciones en la nube.

(xxi) En cumplimiento de la Circulares de la Superfinanciera se debe :

• Cumplir todo lo relacionado con los niveles de servicio y operación,

• Hacer uso de los Sistemas de Información del Contratante a los que tenga acceso con la ejecución del contrato, única y exclusivamente para lo estipulado en el objeto del mismo.

• Prestar toda la colaboración que se requiera por el Contratante y las autoridades competentes, en el evento de presentarse cualquier situación que constituya sospecha o evidencia de alteración o manipulación de equipos o información relacionada con el cumplimiento de su objeto. En especial el Contratista se compromete a dar aviso inmediato al Contratante acerca de tal situación, a facilitar de manera inmediata la custodia de los equipos y elementos que se consideren necesarios para ser puestos a disposición del Contratante o de las autoridades competentes y a entregar de manera inmediata la información que le sea requerida por el Contratante o por las autoridades competentes dentro del proceso de investigación.

• Cumplir con las políticas corporativas de seguridad de la información para proponentes y proveedores definidas por EL BANCO, como también con los procedimientos definidos por la oficina de seguridad de la información para el manejo de los recursos tecnológicos, los cuales fueron conocidos y aceptados por EL CONTRATISTA previamente a la ejecución del presente contrato.

• Cumplir con las normas de seguridad física definidas por el Contratante, como con los procedimientos definidos por el Banco para el acceso, permanencia y retiro de las instalaciones de Contratante del personal del Contratista y sus equipos, conocidas y aceptadas por el Contratista. Para el efecto, el Contratista suministrará los elementos que permitan identificar plenamente al personal designado para la ejecución del presente contrato, así como instruir a este personal para que permanentemente porten los elementos de identificación.

• El Contratista, de ser aplicable, se obliga a contar con procedimientos controlados para la entrega de información por parte del Contratante durante la vigencia del contrato y para la destrucción de la misma por parte del Contratista una vez finalizado el contrato. Dicho procedimiento deberá ser informado al Contratante antes de que inicie la ejecución del presente contrato.

• Permitir las visitas que el Contratante deba realizar para verificar el cumplimiento de las obligaciones señaladas en el presente numeral.

• Dar cumplimiento a las demás obligaciones inherentes al objeto del contrato que se encuentren señaladas en el mism

Informar de los planes de continuidad y contingencia para la prestación del servicio.

El cual debe cubrir por lo menos los siguientes aspectos:

- Identificación de los riesgos que pueden afectar la operación,
- análisis de impacto especificando RTO y RPO,
- actividades a realizar cuando se presentan fallas,
- Operación en situaciones contingentes.
- alternativas de operación y regreso a la actividad normal.
- Planes de Contingencia tecnológica: Específicamente sobre la infraestructura tecnológica que apoya los servicios contratados.

El plan debe garantizar la continuidad ante fallas que puedan afectar la prestación del servicio durante la ejecución del contrato.

Nota: el Contratista acepta que la información entregada por el Contratante en desarrollo del contrato, así como la información que se genere como consecuencia de la prestación del servicio contratado, es de propiedad exclusiva del Contratante.

8.4. Duración del Contrato

La duración del contrato para su ejecución será de doce (12) meses, contados a partir de su legalización.

8.5. Supervisión

Sin perjuicio del control y supervisión interno que deberá establecer el adjudicatario de la presente invitación para supervisar sus actividades, Bancóldex supervisará la ejecución del Contrato, verificando las actividades relacionadas con el mismo.

El supervisor del Contrato por parte de Bancóldex será, para todos los efectos, el que se designe en el Contrato.

8.6. Garantía del contrato

Para la ejecución del Contrato, el adjudicatario deberá constituir a favor de Bancóldex NIT No. 800.149.923-6 una garantía bancaria o un seguro de cumplimiento, en formato de entidades particulares, expedido por una compañía de seguros o establecimiento bancario, debidamente autorizado por las autoridades colombianas, el cual deberá contener los amparos que se mencionan a continuación:

(i) Cumplimiento de las obligaciones derivadas del contrato con una suma asegurada equivalente al veinte (20%) por ciento del precio del Contrato y con una vigencia igual a la del Contrato y tres (3) meses más.
(ii) Pago de salarios, prestaciones sociales, indemnizaciones laborales y demás prestaciones de índole laboral del personal dedicado por el contratista para la ejecución del contrato, con una suma asegurada equivalente al treinta por ciento (30%) del precio del Contrato y con una vigencia igual a la del contrato y tres (3) años y tres (3) meses más.
(iii) Calidad de los servicios prestados con una suma asegurada equivalente al veinte por ciento (20%) del precio del contrato y con una vigencia igual a la del contrato tres (3) meses más.

CON EL FIN DE QUE LA VIGENCIA DEL SEGURO SEA CONGRUENTE CON EL INICIO DE VIGENCIA DEL CONTRATO, LA CUAL INICIA CUANDO SE PRODUCE LA LEGALIZACIÓN DEL MISMO, EL SEGURO DEBERÁ PRESENTARSE CON UNA VIGENCIA ADICIONAL DE UN (1) MES RESPECTO DE LAS VIGENCIAS INDICADAS EN LOS ANTERIORES NUMERALES.

Las compañías de seguros que otorguen la garantía deberán estar legalmente establecidas en Colombia, los establecimientos bancarios que otorguen la garantía podrán ser nacionales o extranjeros siempre que tengan límite de exposición crediticia con Bancóldex (cupo de crédito aprobado con Bancóldex).

8.7. Subcontratos

El adjudicatario de los recursos podrá subcontratar a su propia conveniencia las labores que requiera para la ejecución del contrato, siempre y cuando por este conducto no se deleguen sus propias responsabilidades. En todo caso, ante Bancóldex, el Contratista será el responsable del cumplimiento de todas las obligaciones contractuales.

8.8. Autorizaciones sobre uso de información, habeas data y tratamiento de datos personales

En caso de que los servicios a contratar impliquen el levantamiento y entrega de bases de datos personales, el Contratista se obliga a obtener de parte de los titulares de la información, las autorizaciones respectivas, de tal forma que el Banco de Comercio Exterior de Colombia S.A. y el Ministerio de Comercio, Industria y Turismo puedan hacer uso de los datos personales y la información, atendiendo lo preceptuado en la ley 1581 de 2012 y el Decreto 1377 de 2013.

8.9. Prevención de Lavado de Activos y Financiación del Terrorismo

El Contratista declara que sus recursos no provienen de ninguna actividad ilícita contemplada en el Código Penal Colombiano o en cualquier otra norma que lo modifique o adicione. Para el efecto, Bancóldex realizará consultas de control previo del proponente de las personas o partes relacionadas con el proponente y vinculadas a la propuesta, según aplique, con el fin de analizar los riesgos relacionados con Lavado de Activos y Financiación del Terrorismo.