PREGUNTAS Y RESPUESTAS

LICITACIÓN N°90004433
SERVICIO DE ASESORÍA "EVALUACIÓN DE CIBERSEGURIDAD"

De acuerdo al calendario de las bases del proceso de Licitación N°90004433, se hace presente que se recibieron las siguientes consultas:

I. ACLARACIONES A LAS BASES:

1. **Se reemplaza numeral 3.1.8 del Anexo A por el siguiente:**

3.1.8. El servicio debe considerar entrevistas de trabajo focalizadas en los líderes de las unidades del alcance y el servicio completo deberá ser realizado en un máximo de **diecisiete (17)** semanas calendario para obtener el resultado, referencialmente distribuidas (no necesariamente de forma secuencial) en:

- Dos (2) semanas de planeación
- **Siete (7)** semanas para entrevistas y obtención de evidencia documental.
- Tres (3) semanas de análisis y revisión documental.
- Tres (3) semanas para generación de propuesta de resultados y obtener feedback del Banco.
- Dos (2) semanas para correcciones finales, obtención de informes y presentaciones de los resultados del servicio.

2. **En numeral 3.1.7 de las Bases, se reemplaza "benchmark con el mercado financiero" por "benchmark podrá ser realizado respecto al sector Bancario, Instituciones Financieras y/o Instituciones Públicas (nacional o internacional)". Ver pregunta técnica N°3.**

II. CONSULTAS Y RESPUESTAS TÉCNICAS:

1. En el punto 1. Objetivos del servicio del Anexo A especificaciones técnicas, la descripción del objetivo del servicio señala que se debe realizar una "Evaluación de la Ciberseguridad" basada en las definiciones contenidas en el Framework de Ciberseguridad de NIST versión 1.1 (en adelante "NIST CSF") señalando que se debe focalizar específicamente en la referencia informativa asociada a la publicación especial 800-53. Las Funciones, categorías y subcategorías del NIST CSF se basan en distintos estándares y marcos de referencia cómo son COBIT, ISO 27001 y los controles críticos CIS. Favor aclarar si este proceso de evaluación solo cubre medir e informar el nivel de adopción y madurez de la publicación 800-53 o se espera contar con una mirada completa de todos los controles y estándares que componen las subcategorías, categorías y funciones.

Respuesta: Los requerimientos se especifican detalladamente en el punto "3.1. Requerimientos Funcionales con los que deberá cumplir el servicio". En los requerimientos que correspondan deberá ser utilizada la referencia informativa de la NIST SP 800-53.

2. En el punto 3 Descripción del requerimiento del Anexo A especificaciones técnicas, se señala en el último párrafo de ese punto que "El servicio requerido en términos generales debe ser basado en entrevistas, revisión de documentación y verificación de evidencias".

Dentro de las definiciones incorporados en NIST CSF se señala que, para desarrollar un perfil, una organización puede revisar funciones, categorías y subcategorías, objetivos estratégicos y desarrollar una evaluación de riesgos para determinar correctamente el perfil tanto actual como objetivo. ¿Es posible incorporar actividades de evaluaciones técnicas de campo para desarrollar correctamente la evaluación de riesgo y tener toda la información requerida para determinar perfil actual y la definición del perfil objetivo?

Respuesta: La identificación del perfil actual y objetivo deberá esta basado en el análisis y evaluación de la gestión de riesgos asociadas a cada categoría y subcategoría, donde no necesariamente es requisito realizar actividades de evaluación técnicas de campo.

3. En el punto 3.1.7 del Anexo A especificaciones técnicas, se detalle la inclusión de un **benchmark con el mercado financiero** respecto de la evaluación realizada, ¿es obligatorio que sea con el mercado financiero? Esto pensando en que aún, en términos de mercado e industria, no se ha popularizado el uso de NIST CSF.

Respuesta: El benchmark podrá ser realizado respecto al sector Bancario, Instituciones Financieras y/o Instituciones Públicas (nacional o internacional). Se realiza aclaración respecto a este requerimiento. Ver aclaración N°2.

4. ¿Es posible que el oferente, al momento de declarar su experiencia en otras entidades del área financiera, anonimice el nombre de los clientes, para que en la fase de validación del Banco Central de estas referencias, el oferente pueda coordinar la sesión de validación con los respectivos clientes a los cuales ya ha prestado el servicio, salvaguardando así la solicitud de las entidades financieras de no proveer nombres y mediante nosotros, coordinar con el Banco Central la validación de las referencias?

Respuesta: El Banco se reserva el derecho de verificar la información con el contacto de referencia proporcionado, en atención a que es un requisito que forma parte de la pauta de evaluación, la no presentación de esta información implicaría obtener el puntaje mínimo de la pauta en ese factor.

5. Sobre el punto decimoctavo de las bases de la licitación N°90004433 ¿No será posible externalizar parte del servicio que se está proponiendo a una empresa partner?

Respuesta: No es posible de acuerdo con la cláusula decimoctava del modelo del contrato.

6. Anexo A numeral 6: ¿Dónde se prestará el servicio en caso de necesitar visita presencial? (Ubicación física)

Respuesta: En el caso que sea requerido tener reuniones presenciales (acordadas previamente entre ambas partes), estas se realizaran en las dependencias del Banco en Agustinas 1180 o Morandé 115, Santiago.

7. ¿Cómo se puede plasmar la experiencia en servicios similares respetando los NDA con clientes?

Respuesta: El Banco se reserva el derecho de verificar la información con el contacto de referencia proporcionado, en atención a que es un requisito que forma parte de la pauta de evaluación, la no presentación de esta información implicaría obtener el puntaje mínimo de la pauta en ese factor.

8. Considerando la tabla de pauta de evaluación inserta en el punto 8.3 Evaluación Técnica respecto al perfil Consultor, éstos deben ser perfiles diferentes para cada punto de evaluación o puede ser un solo perfil?

Respuesta: No necesariamente deben ser perfiles diferentes para cada punto de la evaluación, puede ser un consultor con todos los perfiles y/o varios consultores con perfiles distintos.

9. ¿Será posible coordinar reuniones con los contactos de referencias de proyectos anteriores para comprobar experiencia?

Respuesta: No es posible, ya que el Banco estima suficiente la información solicitada en las bases para evaluar. El Banco se reserva el derecho de verificar la información con el contacto proporcionado.

10. ¿La experiencia comprobable será válida sólo para aquellos proyectos en donde se hayan aplicado específicamente los controles de la NIST SP 800-53, o pueden servir como experiencia aquellos proyectos que en donde se hayan aplicado los controles regulares del CSF NIST para una organización completa?

Respuesta: Es válido como experiencia comprobable el uso de las otras referencias normativas de la NIST CSF

11. ¿Es excluyente proponer y/o utilizar un proceso de medición basado en el Modelo de Madurez de Capacidad (CMM) o similar? De ser así, ¿Qué puntuación tendría este apartado en la evaluación técnica?

Respuesta: No es excluyente.

12. ¿Es excluyente proponer y/o utilizar Project Management Body of Knowledge (PMBoK) del Project Management Institute (PMI) o similar, como metodología de proyecto ágil? De ser así, ¿Qué puntuación tendría este apartado en la evaluación técnica?

Respuesta: No es excluyente.

13. Respecto del Objetivo del servicio: En relación a lo requerido para el Departamento de Ciberseguridad, cual es el alcance de lo indicado en "Conocer el nivel de madurez de las capacidades/procesos de ciberseguridad del Departamento". ¿Están definidas formalmente las capacidades/procesos que se deben evaluar? ¿Es posible conocerlas?

Respuesta: Están definidas formalmente y corresponden a 4 subprocesos del Departamento. Serán conocidas durante las actividades de entrevistas, revisión de documentación y verificación de evidencias.

14. Respecto de las Condiciones preliminares: ¿Cuál es el alcance de la replanificación de actividades que se puede originar en necesidades del Banco?

Respuesta: Principalmente en el alcance de tiempos y secuencia de actividades.

15. ¿Están definidas las capacidades, procesos y actividades de ciberseguridad de la Gerencia de Tecnología? ¿Es posible saber cuáles son?

Respuesta: Están definidas formalmente y corresponden a 4 subprocesos del Departamento. Serán conocidas durante las actividades de entrevistas, revisión de documentación y verificación de evidencias.

16. (3.1.1.) Cuando se indica que se debe indicar gráfica y porcentualmente el cumplimiento para cada una de las componentes, ¿se refiere a cada subcategoría de NIST CSF o cada control de NIST 800-53?

Respuesta: Se refiere a las ciento ocho (108) Subcategorías.

17. (3.1.4) ¿Están formalmente definidos los objetivos y apetito de riesgo del Departamento de Ciberseguridad?

Respuesta: Los objetivos del Departamento de Ciberseguridad se encuentran definidos en base a las funciones definidas para éste, y el apetito de riesgo se encuentra alineado al apetito de riesgo del Banco, sin embargo, se espera que el servicio realice recomendaciones al respecto.

18. (3.1.7.) ¿Se deben considerar presentaciones diferentes para la Gerencia de Tecnología y para el Departamento de Ciberseguridad?

Respuesta: Si.

19. Entendemos que la coordinación de las entrevistas las haría el Encargado Técnico del Banco. ¿Es eso correcto?

Respuesta: Si.

20. Entendemos que no se consideran entrevistas fuera del ámbito de la Gerencia de Tecnología. ¿Esta condición se mantiene incluso para la evaluación de dimensión adicional de "Gobierno, cumplimiento y organización"?

Respuesta: Las entrevistas están consideras dentro del ámbito de la Gerencia de Tecnología y el Departamento de Ciberseguridad, pero en el caso que sea necesario recabar información fuera de estas áreas, esta será proporcionada por los encargados internamente.

III. CONSULTAS Y RESPUESTAS ADMINISTRATIVAS Y/O LEGALES:

1. Sobre numeral 5.1.1: ¿Los formularios F30 y F30.1 son suficientes para dar por cumplido lo solicitado respecto de Saldos Insolutos de Remuneraciones ni Cotizaciones de Seguridad Social?

Respuesta: Todo lo señalado en el numeral 5.1.1 son Formularios proporcionados por el Banco y que se encuentran como descargables en el Contenido del evento en Ariba. Solo deben descargarlos, completar, firmar y subirlos como parte de la presentación de su oferta.

2. Sobre numeral 12. ¿Pueden aclarar que solo se prohíbe la subcontratación para la prestación de servicios objeto de la licitación, y que en ningún caso se prohíbe a la empresa subcontratar servicios /o productos que le permitan prestar los servicios objeto de su giro de una manera más eficiente?

Respuesta: Así es, no se permite la subcontratación de los servicios a contratar.

3. Cláusula Quinta: ¿Se puede incluir el siguiente texto? "El no pago oportuno de los honorarios dará derecho a (EMPRESA) a cobrarle al Cliente un monto de penalización igual al menor de (i) un monto a ser determinado a discreción razonable de (EMPRESA), que no exceda el monto máximo de penalización permitido por la ley chilena o (ii) 8% anual, que se acumulará sobre los saldos impagos empezando de la fecha de vencimiento a la fecha de su pago completo."

Respuesta: No es posible incluirlo. El Banco honra sus compromisos contractuales y pagará en tiempo de acuerdo a lo señalado en la cláusula quinta del Modelo de Contrato adjunto a las bases.

4. Cláusula Séptima: ¿Se puede incluir las siguientes causales de término anticipado?:

   (i) Cualquiera de las partes podrá dar por terminada el contrato en cualquier momento dando aviso por escrito a la otra parte con al menos 30 (treinta) días de anticipación a la fecha efectiva de terminación.

   (ii) En adición, cualquiera de las partes podrá terminar el contrato en un plazo menor si (i) las leyes, normas, regulaciones o normas profesionales aplicables a una parte le impidieren seguir prestando o recibiendo los Servicios señalados en este instrumento, (ii) la seguridad física o la seguridad del personal de una parte se ve amenazada, o (iii) una parte incumple sus obligaciones conforme la Propuesta / Carta de Contratación o estos Términos y Condiciones, y el incumplimiento no es subsanado por la parte que haya incumplido dentro de los diez (10) días siguientes a la recepción de la notificación del incumplimiento respectivo hecha por la parte cumplidora. Cualquiera de las partes puede

ejercer sus derechos de terminación sin responsabilidad alguna por el ejercicio de los mismos.
¿Se puede incluir además? "En caso de terminación por cualquier motivo, el Banco se compromete a pagar a (EMPRESA) los honorarios y gastos devengados hasta el momento en que la terminación sea efectiva."

Respuesta: Se mantiene la cláusula sobre término anticipado del Modelo y las causales allí establecidas. En cuanto al término anticipado el Banco pagará los servicios prestados y recepcionados conforme hasta la fecha de término fijada.

5. Cláusula Octava: ¿Se puede limitar monto total de multas a 10% de los honorarios pactados?

Respuesta: No es posible aceptar su solicitud. El alcance en materia de responsabilidad es el establecido en la cláusula vigesimoprimera del Modelo de Contrato adjunto a las bases.

6. Cláusula Novena: ¿La propiedad del entregable sólo será del Banco una vez que este pague el total del honorario adeudado?

Respuesta: Los pagos están sujeto a la Recepción conforme de los servicios el que incluye el entregable.

7. Duodécimo: ¿Se puede incluir?:
   - la Información Confidencial no incluye aquella información que: (1) sea del conocimiento de la Parte Receptora al momento de divulgación de la Parte Reveladora; (2) sea o se convierta del dominio público, sin mediar incumplimiento de la Parte Receptora; (3) la Parte Receptora haya desarrollado de manera independiente, sin la Información Confidencial de la Parte Reveladora; (4) la Parte Receptora determine que está obligada a ser mantenida o divulgada por la Parte Receptora en virtud de las leyes o regulaciones tributarias aplicables a los Servicios o de disposiciones similares o análogas a la ley o regulación en otras jurisdicciones; (5) sea recibida por la Parte Receptora de terceros sin restricción y sin incurrir en incumplimiento de alguna obligación de confidencialidad.
   - La Parte Receptora devolverá a la Parte Reveladora o destruirá toda su Información Confidencial y todas las copias de la misma cuando así se lo requiera la Parte Reveladora, pudiendo conservar la Parte Receptora (i) copias que forman parte de los papeles de trabajo para sus archivos, (ii) información que los abogados de (EMPRESA) están obligados a conservar si aplica a los Servicios, información que se encontrará protegida por el secreto profesional entre cliente y abogado además de las disposiciones del presente documento, y (iii) cualquier información que pueda almacenarse en medios de respaldo u otros sistemas de almacenamiento de datos electrónicos, datos latentes y metadatos
   - En el caso de que (EMPRESA) sea solicitado o autorizado por el Banco, o sea requerido por la ley, las normas, la regulación o una solicitud legal en un procedimiento o una investigación en la que (EMPRESA) no sea una parte nombrada o demandada, para entregar los documentos o el personal de (EMPRESA) como testigos o para entrevistas, o de otra manera, para poner la información relacionada con los Servicios a disposición de un tercero, o al Banco por un motivo diferente a la prestación de los Servicios, el Banco reembolsará a (EMPRESA) por el tiempo empleado por sus profesionales, a sus tarifas por hora estándar vigentes en ese momento, y los gastos, incluyendo honorarios y gastos razonables de los abogados, incurridos en la respuesta a tales peticiones, autorizaciones o requisitos.

Respuesta: No es posible ajustar la cláusula de confidencialidad ya que es la estándar del Banco para sus proveedores.

8. Décimo quinto: ¿Se puede incluir?:
   En caso de que cualquiera de los Entregables (incluyendo la Propiedad de (EMPRESA) contenida en los mismos) o parte de los mismos se considere, o en opinión de (EMPRESA) pueda considerarse como que constituye una Infracción, (EMPRESA) podrá, a su elección,

dentro de un período razonable: (i) asegurar al Banco el derecho a continuar con el uso de esa parte que pudiera considerarse infractora; o (ii) sustituir, por su propia cuenta, esa parte por una esencialmente equivalente o modificarla de modo que ya no sea infractora. Si a juicio razonable de (EMPRESA) no se puede llevar a cabo cualquiera de las dos opciones que se describen en los incisos (i) o (ii), el Banco devolverá la parte considerada infractora de los Entregables a (EMPRESA) y la responsabilidad de (EMPRESA) consistirá exclusivamente en devolver al Banco el monto que hubiere pagado por la parte infractora.

Respuesta: No es posible modificar el texto solicitado.

9. Décimo Octavo: ¿Podrían aclarar si sólo se prohíbe la subcontratación para la prestación de servicios objeto de la licitación, y que en ningún caso se prohíbe a la empresa subcontratar servicios /o productos que le permitan prestar los servicios objeto de su giro de una manera más eficiente?

Respuesta: Véase respuesta 2

10. Vigésimo Primero: ¿Se puede limitar responsabilidad de (EMPRESA) al monto de los honorarios pactados, salvo caso de culpa grave o dolo atribuible a (EMPRESA), lo que en todo caso deberá constar en sentencia judicial o laudo arbitral ejecutoriado?

Respuesta: Véase respuesta 5

11. Vigésimo Segundo: ¿Se puede condicionar obligación de informar al Banco al cumplimiento de los procedimientos internos de (EMPRESA), asegurándonos que no se infrinja el deber de confidencialidad que (EMPRESA) mantiene con sus clientes o con sus stakeholders?
    ¿Se puede incluir?:
    El Banco reconoce que (EMPRESA) ha implementado un Modelo de Prevención de Delitos según lo disponen los Artículos 3 y 4 de la Ley Nº20.393 que establece la responsabilidad penal de las personas jurídicas (la "Ley N°20.393") por los delitos de lavado de activos, financiamiento del terrorismo, cohecho a funcionario público nacional o extranjero y receptación, y el resto de los delitos que en lo sucesivo se incorporen al catálogo contenido en el artículo 1º de la referida ley y sus modificaciones posteriores.
    El Banco no ejecutará actividades conducentes a los delitos estipulados en el Artículo 1° de la Ley N°20.393 y denunciará al Encargado de Prevención de Delitos de (EMPRESA) algún hecho destacado sobre el banco que pueda constituir un incumplimiento del Modelo de Prevención de Delitos de (EMPRESA) o un delito de la Ley N°20.393, a través del canal de denuncias mediante el siguiente correo electrónico: EPD-Ley-20393@(EMPRESA).com

Respuesta: Se mantiene la cláusula como está en el modelo.

12. Vigésimo Cuarto: ¿Se puede condicionar obligación de informar al Banco al cumplimiento de los procedimientos internos de (EMPRESA), asegurándonos que no se infrinja el deber de confidencialidad que (EMPRESA) mantiene con sus clientes o con sus stakeholders?

Respuesta: Se mantiene la cláusula como está en el modelo.

13. Trigésimo: ¿Se puede solicitar modificar el método de resolución de controversias a arbitraje frente a panel de 3 árbitros?

Respuesta: No es posible. Se mantiene la jurisdicción de los tribunales de justicia. Corresponde al estándar del Banco.

GERENCIA GESTIÓN CONTABLE Y PLANIFICACIÓN

Santiago, martes 25 de abril de 2023.