



CONSULTAS–ACLARACIONES–RESPUESTAS COTIZACIÓN N°90000113

A continuación, se presentan las aclaraciones y respuestas a las consultas, realizadas por las Empresas que participan del proceso de Cotización N°90000113, para los servicios de evaluación nivel de madurez de los procesos de ciberseguridad y entrega de un plan de implementación de mejora continua.

I. ACLARACIONES A LAS BASES:

NO HAY

II. CONSULTAS Y RESPUESTAS TÉCNICAS:

1. VI. ENTREGABLES DEL SERVICIO: ¿El Benchmark solicitado es nacional y regional (América Latina)?

Respuesta: El Benchmark es con respecto al mercado financiero, no se condiciona o especifica si es nacional y/o regional.

2. IV. DESCRIPCIÓN DE LOS SERVICIOS, A) REQUERIMIENTOS FUNCIONALES: ¿Se deben identificar las joyas de la corona?; ¿Se deberán realizar pruebas técnicas o solo madurez basado en los Tier 1 – 4 de NIST?; ¿Se prevé durante el proyecto la identificación y evaluación de riesgos solo con madurez?; ¿Requieren identificar y presentar el perfil de riesgo de industria?

Respuesta:

- La identificación se basa en las componentes Core del Framework NIST CSF (Funciones Categorías y subcategorías) a los procesos de ciberseguridad establecidos, no necesariamente a activos específicos como Joyas de la Corona.
 - No es necesario realizar pruebas técnicas, sino que el servicio se basa en Entrevistas y Recopilación de Evidencia Documental.
 - Lo observado con brecha identificada (sección A.iv.a) se desprende de la identificación de una mejora observada del Core, lo que implica una detección de posible riesgo de desviación del Framework.
 - Presentar un Perfil de riesgo de industria no aplica. Lo solicitado corresponde la definición en conjunto de un Perfil de Adopción del Framework (PROFILE).
3. En el Anexo A. Título III. Condiciones generales para la prestación del servicio, segundo párrafo, se indica: "La Empresa se obliga a que todo material gráfico y/o de texto que sea parte de la ejecución del Servicio que el Banco contrate, debe ser aprobado por escrito por el Jefe de Departamento de Ciberseguridad o su representante, antes de su ejecución". Entendemos que esta indicación se refiere a los elementos que constituyan resultados parciales y finales del trabajo, pero que no incluyen las herramientas o elementos que se utilicen en el trabajo de levantamiento o análisis de los antecedentes. ¿Es esta interpretación correcta?

Respuesta: Si, la interpretación es correcta.



4. En el Anexo A, Título III. Condiciones generales para la prestación del servicio, quinto párrafo se indica “El Banco se obliga a otorgar flexibilidad al Servicio, y podrá durante su ejecución solicitar a la Empresa la replanificación de las actividades asociadas a la materia objeto de la presente Solicitud. Asimismo, permitir ajustes permanentes de la estrategia del servicio, enfocado a cumplir con los objetivos propuestos.” Entendemos que ambas partes, el Banco y la Empresa, podrán solicitar replanificación de actividades o ajustes en la estrategia del servicio, en la medida que éstas modificaciones aporten a la conclusión exitosa del servicio. ¿Es esta interpretación correcta?

Respuesta: Si, la interpretación es correcta.

5. ¿Ha definido el Banco su apetito de riesgo respecto de Ciberseguridad?

Respuesta: Si está definido

6. En el Anexo A, Título IV, “REQUERIMIENTOS NO FUNCIONALES”, se menciona que el equipo de trabajo deberá tener “dedicación exclusiva para el Banco”. Quisiéramos entender la flexibilidad de este punto considerando escenarios como los siguientes: Es usual que un jefe de proyecto, en un rol estricto de PM, tenga una dedicación menor a la de el/los consultor/es especialistas que este lidera. Si decidimos ampliar el equipo del proyecto a 2 o más consultores (para paralelizar reuniones en las etapas iniciales, por ejemplo), se podrían cubrir más tareas en menos tiempo. Por lo tanto, la dedicación a tiempo completo de esos mismos recursos durante todo el proyecto, podría ya no ser necesaria. Un tercer escenario, podría resultar al momento de existir espacios de tiempos entre reuniones, debido a retrasos del cliente. En estos casos, ¿es posible flexibilizar esta restricción con sentido común, siempre que no se afecte la disponibilidad de los consultes hacia el proyecto?

Respuesta:

La Empresa se obliga a cumplir con los Servicios, conforme a lo solicitado por el Banco y en los tiempos establecidos para tales fines. Por tanto, el Banco espera que, en los tiempos planificados de común acuerdo entre las partes, para la ejecución de los Servicios, el Oferente tenga una dedicación exclusiva para el Banco, con el propósito de cumplir con los objetivos requeridos y en el plazo definido para tales fines.



7. En el Anexo A, Título IV. Descripción de los Servicios, letra A), párrafo vii, se indica como actividad: "Coordinar las entrevistas de trabajo con los líderes de los Departamentos de la Gerencia de Tecnología y de las Unidades Usuarias que tengan asociadas a sus funciones temas de ciberseguridad.". Entendemos que esta coordinación queda asignada al interlocutor definido por el Banco para la coordinación del servicio. Es esto correcto?

Respuesta: El Interlocutor Banco será el nexo responsable para establecer con los líderes de cada una de las Unidades del Banco el compromiso para su participación en este estudio, como así también los miembros de los equipos de trabajo en cada una de dichas unidades. Una vez resuelto este nexo por parte del Interlocutor Banco, el Interlocutor de la Empresa podrá, previo acuerdo con el Interlocutor Banco, coordinar directamente con los líderes de cada unidad las entrevistas de trabajo. Si eventualmente se presentarán reiterados atrasos en las entrevistas, atribuibles a replanificaciones solicitadas por los miembros de los equipos Banco, el Interlocutor Banco deberá velar por el cumplimiento de los plazos acordados para los fines pertinentes.

8. Pag. 3 En la sección de factores a evaluar 1.5.2.1 parte A) Empresa, para los numerales 1.2, 1.3, 1.4 y 1.5 se solicita contar con al menos 2 servicios en los últimos 3 años. Por favor indicar si los servicios deben ser excluyente para cada uno de los numerales 1.2, 1.3, 1.4 y 1.5

Respuesta: No son excluyentes. Es posible evidenciar un servicio para numeral 1.2 y el mismo servicio evidenciarlo en el numeral 1.3 u otro, si y solo si, cumple con el requisito del numeral respectivo.

9. Pag. 4. En la sección de factores a evaluar 1.5.2.1 parte B) Equipo de Trabajo, para los numerales 2.1, 2.2, 2.3 y 2.4 se solicita contar con al menos 2 servicios como jefe de proyecto en los últimos 3 años. Por favor indicar si los servicios deben ser diferentes para cada uno de los numerales 2.1, 2.2, 2.3 y 2.4

Respuesta: Podrá evidenciarse distintos numerales con el mismo servicio, si y solo si, cumple con el requisito del numeral respectivo.

10. Pag. 4. En la sección de factores a evaluar 1.5.2.1 parte B) Equipo de Trabajo, para los numerales 2.5, 2.6, 2.7 y 2.8 se solicita contar con al menos 2 servicios como consultor especialista en los últimos 3 años. Por favor indicar si los servicios deben ser diferentes para cada uno de los numerales 2.5, 2.6, 2.7 y 2.8

Respuesta: Podrá evidenciarse distintos numerales con el mismo servicio, si y solo si, cumple con el requisito del numeral respectivo.

11. Pag. 19. Es posible utilizar la escala especificada por CMMI como estándar de medición sobre el nivel de madurez del Banco? (Independiente del nivel Tier en que se encuentre)

Respuesta: El Servicio solicita utilizar específicamente el Framework NIST CSF, en lo que respecta a evaluación, adherencia y profile.



12. Pag. 19. Se puede utilizar un Framework propietario que posee el mapeo al Framework NIST?

Respuesta: El Servicio solicita utilizar específicamente el Framework NIST CSF, en lo que respecta a evaluación, adherencia y profile, independiente de la metodología en particular para desarrollar el servicio.

13. Pag. 20. En el caso de que sea necesario escalar asuntos que queden sin un acuerdo entre el jefe de proyecto y el interlocutor del banco, cuál será el procedimiento y cómo afectará al proyecto?. En términos del proveedor, como deberá proceder para que no lo afecte?

Respuesta: Las partes se obligan a cumplir con la ejecución de los Servicios, conforme a los términos y condiciones establecidos para tales fines en la Solicitud de Cotización y sus Anexos. Si eventualmente se presentaran desacuerdos entre las partes, por falta de cumplimiento en la ejecución de los Servicios, conforme a lo establecido en la Solicitud de Cotización y sus Anexos, será obligación del Interlocutor del Banco informar a la Encargada del Proceso de Compras del Departamento de Adquisiciones del Banco acerca de los desacuerdos. La Encargada de Adquisiciones, informará y escalará el incidente a la instancia pertinente.

14. Pag. 21. Tiene el banco sus procesos actuales de ciberseguridad documentados? Esto permitirá entender el grado de granularidad a la hora de solicitar información.

Respuesta: El Banco cuenta con material documentado en lo que se refiere a sus Políticas, Normas, procedimientos y estructuras de Ciberseguridad.

15. Pag. 21-iv. Será requerido entregar una asignación o evaluación económica por las recomendaciones entregadas, sea frente a equipamiento, software o iniciativas propuestas?

Respuesta: No será requerido.

16. Pag. 21-vi. 1. Se entiende que serán 4 áreas para entrevistar en la Gerencia de Tecnología, donde se podrían incluir áreas usuarias del banco. En ese sentido, se podrán coordinar con antelación al inicio del proyecto todas las reuniones que requieran entrevistas? Esto para evitar posibles atrasos en lo acotado del tiempo.

Respuesta: Si, podrá ser posible. Sin embargo, se hace presente que los plazos estarán supeditados a la disponibilidad de los líderes, y previo acuerdo escrito con el Interlocutor Banco.

17. Pag. 21-vi. 2. Se entiende que serán 4 áreas para entrevistar en la Gerencia de Tecnología, donde se podrían incluir áreas usuarias del banco. Adicionalmente, se podrán incluir otras gerencias como Riesgo, recursos humanos o fiscalía para entender mejor la cultura, estructura, coordinación, entre otros ámbitos? Esto permite un análisis más exhaustivo y recomendaciones más certeras

Respuesta: Si, podrá ser posible. Sin embargo, se hace presente que los tiempos de otras áreas que no están en el programa establecido por el área de tecnología para este estudio, estará supeditado a la disponibilidad que comprometan los líderes de las unidades adicionales propuestas por la Empresa adjudicataria, y previo acuerdo escrito con el Interlocutor Banco.



18. Pag. 23-vi. Cuáles son las expectativas para el plan de implementación de mejora continua a 3 años: a) Un Roadmap de iniciativas que especifique las actividades a realizar a un alto nivel, b) Agregar la estrategia e iniciativas estratégicas, adicional un Roadmap de iniciativas de alto nivel, c) Estrategia, iniciativas estratégicas alineadas con la estrategia banco, Roadmap y actividades a un alto nivel de detalle (FTE, actividades por equipo, criticidad), d) otro, especificar por favor

Respuesta: Las recomendaciones técnicas y/o administrativas esperadas del numeral iv, deben considerar al menos los aspectos descritos en letras a,b,c,d,e,f , de forma de estructurar un plan de implementación (roadmap) de mejoras, a 3 años, donde se documenten las actividades a desarrollar (iniciativas) de forma secuenciales según estratégica y táctica.

19. Pag. 23-vi. La solicitud del Benchmark con mercado financiero debe ser acotado a una región específica o a nivel global?.

Respuesta: El Benchmark es con respecto al mercado financiero, no se condiciona o especifica si es nacional y/o regional.

20. Pag. 5. En la sección de factores a evaluar 1.5.2.1, Propuesta técnica en el numeral 3.6, ¿Es suficiente con establecer descripción y estructura de entregable, o es requerido ejemplo gráfico anexo de cada entregable?

Respuesta: la evaluación de este numeral considerará todos aquellos antecedentes que se presenten como parte de la Estructura y Contenido de cada entregable del servicio (cumplimiento de Core del framework, identificación de TIER, definición de Profile, recomendaciones a través de un Plan de Implementación a 3 años), de forma de poder evaluarlos en criterios de si son inapropiados, adecuados, coherentes y/o ampliamente innovadores.

21. ¿Se requiere que los servicios se realicen de manera presencial o dada la contingencia actual se pueden realizar de manera remota?

Respuesta: El servicio puede ser realizado de manera presencial y/o remota según las condiciones de la contingencia sanitaria actual lo dicten

III. CONSULTAS Y RESPUESTAS ADMINISTRATIVAS:

NO HAY

IV. CONSULTAS Y RESPUESTAS LEGALES:

NO HAY

Santiago, jueves 23 de julio 2020.