PREGUNTAS Y RESPUESTAS

LICITACIÓN N°90002663
SERVICIO DE ASESORÍA MODELO DE GOBIERNO Y GESTIÓN DE INCIDENTES TECNOLÓGICOS MAYORES

De acuerdo al calendario de las bases del proceso de Licitación N°90002663, se hace presente que se recibieron las siguientes consultas:

I. ACLARACIONES A LAS BASES:

No hay.

II. CONSULTAS Y RESPUESTAS TÉCNICAS:

1. ¿Dispone actualmente el Banco de un modelo de evaluación de madurez a aplicar en este servicio?

Respuesta: No, se espera como parte del servicio que se proporcione esta evaluación, según lo explicitado en el Anexo A 3.1.1, y en base al framework NIST según lo indicado en Anexo 3.1.2.

2. ¿Tiene el banco definido un proceso de gestión de incidentes al que sea necesario adherir o conectarse?

Respuesta: Se dispone de un proceso de gestión de escenarios de contingencia tecnológica, como también de gestión de incidentes de ciberseguridad, los cuales deben ser parte del Modelo de Gobierno y Gestión que se desarrollará.

3. Se acepta que, además del NIST CSF 1.1, se considere un referente de la familia de las normas ISO?

Respuesta: SI.

4. ¿Los entregables deben cumplir con alguna estructura u organización determinada? favor detallar

Respuesta: Si, los formatos de los entregables se entregarán durante el desarrollo del servicio. Los entregables deben contar con un hilo conductor, entre ellos abordando cada punto del Anexo A 3.1.-

5. ¿Es necesario considerar otras áreas fuera de las mencionadas en el alcance?

Respuesta: No, esta revisión solo considera la Gerencia de Tecnología del Banco, según lo indicado en el alcance del servicio, en Anexo A 3.- (descripción del requerimiento)

6. ¿Existen requerimientos normativos internos o externos que se deban cumplir?

Respuesta: No, solo se espera que el servicio sea basado en framework NIST y otros de apoyo propuestos por el proveedor.

7. ¿Se cuenta con evaluaciones anteriores o certificaciones relacionadas con Incidentes TI?

Respuesta: No.

8. ¿Es posible contemplar una instancia de revisión posterior al proyecto inicial como opcional, respecto del cumplimiento de las recomendaciones? (en 6 o 12 meses posterior al cierre del proyecto inicial)

Respuesta: No está requerido en el objetivo del servicio, Anexo A 1.-, ni en los requerimientos funcionales (Anexo 3.1), por lo anterior, no es parte de la evaluación en caso que sea adicionado como un opcional.

9. ¿El jefe de proyecto debe contar con certificación PMP?

Respuesta: No es solicitado en los requerimientos del servicio, ni evaluado específicamente en tabla N°1 Evaluación Técnica, del punto 8.3

10. ¿Se requiere alguna certificación específica en respuesta a Incidentes?

Respuesta: No.

11. Respecto al fondo del servicio. En el Anexo A, punto 3 se señala que alcance del requerimiento se orienta incidentes tecnológicos mayores para los 3 escenarios definidos.

    En el punto 3.1 se establecen los requisitos funcionales del servicio, focalizando en análisis sobre el marco NIST.

    En específico, cual es el marco NIST a considerar entendiendo que pueden ser compatible con el servicio los siguientes:
    - NIST CSF 1.1 como marco global de ciberseguridad en infraestructura crítica.
    - NIST 800-61 asociada al manejo de incidentes de seguridad
    - NIST 800-34 asociado a la planificación de contingencias en sistemas
    - NIST 800-184 guia de recuperación ante evento de ciberseguridad
    - NIST 800-160 ciberesiliencia

    Favor indicar en específico el marco a utilizar que será la base para el proyecto.

Respuesta: La ejecución del servicio debe utilizar el marco de referencia NIST CSF en conjunto con las NIST Special Publication (SP) que sean de valor para desarrollar el servicio.

12. Respecto al benchmark del mercado financiero al establecer el nivel de madurez objetivo. ¿Se espera hacer un estudio como parte del servicio para determinar ese benchmark o puede ser considerado estudios actuales sobre ello disponibles? Favor indicar curso de acción.

Respuesta: Se puede utilizar estudios actuales que se encuentren disponibles. No obstante, se deja libertad al proveedor de también poder utilizar metodologías propias para determinar ese benchmark.

13. Respecto a los KPI y KRI del modelo de ciberresiliencia a proponer. Indicar cual es la expectativa de dichos indicadores. Ej: monitorear el avance de la implementación o indicadores que regirán al modelo futuro, junto a la gobernanza de dichos indicadores. Favor indicar expectativas en este punto.

Respuesta: Es parte del servicio proponer y definir este tipo de indicadores

14. En un vector de 1 a 5 siendo 1 el más bajo y 5 el óptimo. A modo de autoevaluación rápida, en qué nivel se encuentra hoy BCCH respecto al servicio requerido. Favor indicar para dimensionar el esfuerzo requerido en las iniciativas.

Respuesta: 3

15. Respecto a la cláusula quinta y forma de pago. El servicio debiera ser considerado al menos en 2 hitos. Uno al cierre de la planificación del servicio correspondiente a un 30% del servicio y otro con la recepción conforme del servicio por el 70% restante.

Respuesta: **El Banco pagara el servicio de acuerdo con lo establecido en la cláusula quinta "Forma y lugar de pago del Servicio" del Modelo de contrato adjunto a las Bases; el cual establece un pago único.**

16. Respecto del nivel de detalle solicitado en el plan de implementación, en concreto hasta donde requieren que las iniciativas / recomendaciones se detallen.

Respuesta: **En anexo A 3.1.6 se mencionan algunos aspectos a considerar en las recomendaciones, por otro lado, deben ser abordables en etapas, priorizadas, con secuencia lógica en lo estratégico y táctico a implementar.**

III. CONSULTAS Y RESPUESTAS LEGALES:

NO HAY.

GERENCIA GESTIÓN CONTABLE Y PLANIFICACIÓN

Santiago, jueves 26 de mayo de 2022.