CONSULTAS LICITACIÓN 90006990
SERVICIOS RED TEAM, ACOMPAÑAMIENTO, Y APOYO A DESARROLLO SEGURO Y PENTEST

De acuerdo al calendario del proceso de Licitación 90006990, a continuación, se presentan las consultas recibidas con sus respectivas respuestas.

1. ¿Se acepta alguna otra certificación equivalente a la del Customer Security Programme (CSP) de SWIFT?
Respuesta: No, considerar que se debe cumplir con el 80% de los requerimientos.

2. ¿Cuánto tiempo debe haber sido válida la certificación de SWIFT para cumplir con este requisito?
Respuesta: Debe estar vigente.

3. ¿Se requiere algún tipo de documentación o informe de auditoría que demuestre el uso de OWASP top 10 en evaluaciones de desarrollo seguro?
Respuesta: Por ejemplo, con una declaración simple firmada por los representantes legales, explicando como la implementan dentro del servicio.

4. ¿Existe algún nivel mínimo de adherencia o cumplimiento que deba demostrarse para OSSTMM?
Respuesta: Por ejemplo, con una declaración simple firmada por los representantes legales, indicando nivel de adherencia y como lo implementan dentro del servicio.

5. ¿Se aceptan certificaciones alternativas o equivalentes a las mencionadas (p. ej., otras certificaciones de seguridad ofensiva, Red Team, ingeniería social, Ethical Hacking)?
Respuesta: No, considerar que se debe cumplir con el 80% de los requerimientos.

6. ¿Hay un número mínimo de ingenieros certificados que se requiere para cada tipo de certificación?
Respuesta: Si, debe existir al menos 1 por cada ítem.

7. ¿Es necesario que las certificaciones estén actualizadas a una versión específica?
Respuesta: Que estén vigentes.

8. ¿Cómo se validará el número de ingenieros certificados en caso de empate?
Respuesta: Deberán adjuntar los certificados de los ingenieros correspondientes.

9. ¿Existe un formato o procedimiento específico para reportar y comprobar las certificaciones del personal?
Respuesta: ver respuesta 8.

10. ¿Cómo se debe documentar la antigüedad de la empresa en la prestación de servicios similares? ¿Qué tipos de pruebas o documentos se aceptarán?
Respuesta: Por ejemplo, con declaración simple firmada por los representantes legales o Inicio de actividades en SII.

11. ¿Cuál es el procedimiento específico para la reevaluación técnica en caso de que se soliciten mayores antecedentes durante la evaluación económica?
Respuesta: En el entendido que se refiere al párrafo final de la Bases. Le informamos que el Banco podrá solicitar mayores antecedentes al Oferente que presente la oferta o re oferta económica más económica, pudiendo reevaluarla cuando el precio esté bajo un porcentaje respecto del promedio ofertado por de las demás oferentes.
Cursando las autorizaciones correspondientes, el Jefe del área técnica encargada del proceso será quien resolverá solicitar mayores antecedentes a uno o más Oferentes, que se instruya una reevaluación técnica de la Oferta y/o, se la declare como no elegible técnicamente, previa validación del Comité de Compras del Banco, cuando como resultado de la reevaluación se concluya que el Precio Total deriva de algún incumplimiento de las Especificaciones Técnicas de las Bases de Licitación.

12. ¿Qué criterios adicionales se aplicarán durante esta reevaluación técnica para determinar si una oferta es "Técnicamente No Elegible"?
Respuesta: No se aplican criterios adicionales. La propuesta debe cumplir con la totalidad de los requerimientos técnicos establecidos en las bases. Ver respuesta a pregunta anterior.

13. ¿Habrá algún tipo de feedback proporcionado a los proveedores que no sean seleccionados sobre las áreas de mejora en sus ofertas?
Respuesta: Sí, a los proveedores no seleccionados se les comunicará los motivos específicos por los cuales no fueron considerados técnicamente elegibles.

14. ¿Se publicará el Informe Final o se compartirá exclusivamente con los proveedores participantes?
Respuesta: El Informe Final no se publica, no obstante, puede hacer una solicitud formal para obtenerlo.

15. En la lista de ítems técnicos, no se mencionan requerimientos técnicos específicos de SWIFT. ¿Por qué no se han incluido estos requerimientos técnicos específicos, considerando que se solicitan certificaciones excluyentes en esta materia?
Respuesta: Serán entregados a la empresa adjudicada, por ser información confidencial.

16. Con respecto a las certificaciones requeridas (OSCP, OSWE, CRTO, etc.) ¿Se considerarán equivalencias o certificaciones alternativas para asegurar una competencia más amplia?
Respuesta: No.

17. ¿Podría proporcionar más detalles sobre cómo se alinean las certificaciones requeridas con los objetivos específicos del proyecto, especialmente en lo que respecta a la seguridad y el uso de SWIFT?
Respuesta: Serán entregados a la empresa adjudicada, por ser información confidencial.

18. ¿Qué medidas se han tomado para asegurar que el proceso de evaluación sea justo y no excluya a proveedores potencialmente calificados, pero con diferentes certificaciones o enfoques técnicos?
Respuesta: La Evaluación de las ofertas está regulada en el numeral 9 de las Bases de Licitación, y consta de diversas etapas, todas las que son ejecutadas acorde a dicho texto, incluida la evaluación técnica, que señala los requisitos para calificar técnicamente (véase pauta y párrafos segundo y tercero del numeral 9.3 de la Bases). Solo las ofertas técnicamente elegibles podrás pueden ser evaluadas económicamente.

19. ¿Podrían proporcionar una justificación detallada de la importancia de cada certificación mencionada en los ítems 5 a 10 en relación con los objetivos del proyecto?
Respuesta: Es información confidencial. Se entiende que el oferente debe poseer conocimientos en las materias objeto de esta licitación.

20. En caso de empate, se menciona que la adjudicación se basará en el número de ingenieros certificados. ¿Cómo se asegura que este criterio no favorezca desproporcionadamente a empresas con más recursos para obtener múltiples certificaciones y que quizás no cuenten con la experiencia técnica requerida?
Respuesta: Los criterios de desempate definidos por el Banco para este proceso son los señalados en el numeral 9.5 de la Bases.

21. ¿Qué consideración se ha dado a la calidad y relevancia de las certificaciones frente a la cantidad, especialmente en contextos específicos de SWIFT?
Respuesta: Considerar que se debe cumplir con el 80% de los requerimientos para que la oferta sea considerada técnicamente elegible.

22. La ingeniería social se menciona como un aspecto opcional en los ítems técnicos, sin embargo, se requieren certificaciones específicas en este campo para poder ofertar. ¿Por qué se considera opcional, pero al mismo tiempo se exigen certificaciones que podrían excluir a proveedores que no las tengan?
Respuesta: No se menciona en el documento como opcional, se indica que puede ser utilizada, sin embargo, el equipo del Banco debe saber que se cuenta con el conocimiento necesario para este fin.

23. ¿Podrían clarificar cómo se evaluará el ítem de ingeniería social si se menciona como opcional, pero se requiere para ser técnicamente elegible?
Respuesta: Ver respuesta 22.

24. ¿Cómo se alinean estas certificaciones de ingeniería social con los objetivos específicos del proyecto, especialmente cuando no se detallan requerimientos técnicos específicos relacionados con este campo?
Respuesta: Ver respuesta 22.

25. ¿Se aceptarán certificaciones alternativas o experiencia equivalente en ingeniería social para asegurar una competencia más amplia y no excluir a proveedores potencialmente calificados?
Respuesta: No

26. ¿Qué criterios se usarán para evaluar la relevancia y validez de las certificaciones de ingeniería social en relación con los otros aspectos del proyecto?
Respuesta: Considerar que se debe cumplir con el 80% de los requerimientos para que la oferta sea considerada técnicamente elegible.

27. ¿Por qué se ha optado por un enfoque que parece más centrado en las certificaciones del personal que en los requisitos técnicos específicos del proyecto?
Respuesta: Debido a que se necesita que los servicios sean prestados por personal calificado puesto que se trata de un servicio sensible para el Banco.

28. En la evaluación técnica, ¿qué peso relativo se asigna a la experiencia práctica del proveedor en proyectos similares frente a la posesión de las certificaciones específicas mencionadas? ¿Podrían proporcionar una clarificación sobre cómo se balancearán estos dos factores en la evaluación final?
Respuesta: No hay ponderación. Favor remitirse al numeral 9.3 evaluación técnica de las Bases.

29. ¿Es posible que Banco Central reconsidere la cantidad y o la calidad de los 10 requisitos técnicos para la postulación? Por ejemplo: Reduciendo de 8 a 6 los requisitos de postulación; Englobando el requisito de swift en uno solo y el de red team con ingeniería social en otro; Suprimir requisitos como certificaciones Swift y/o ingeniería social; Agregando que se pueda justificar experiencia en Swift y/o Ingeniería social, en servicios que los postulantes ya hayan prestado al banco; o una mezcla de algunos de los anteriores.
Respuesta: No es posible.

30. ¿Cuántas horas están consideradas para el servicio de asesoría y acompañamiento?
Respuesta: La empresa deberá estimar la cantidad necesaria, según lo que estime de acuerdo a los requerimientos señalados en las Bases y lo explicado en la reunión informativa.

31. Requisitos (pags 19-20) ¿en qué formato mostremos las acreditaciones?
Respuesta: Declaración simple firmada por los representantes legales.

32. ¿El precio para cada uno de los servicios debe ser mensual, anual o por hora/hombre?
Respuesta: Debe ser anual por cada uno de los tres servicios individuales. Favor revisar nueva versión de Formulario de presentación de oferta económica.

33. ¿La adjudicación se hará a un solo proveedor o podrían adjudicar a varios proveedores para los distintos servicios?
Respuesta: Los servicios se adjudicarán a un solo proveedor.

34. ¿Cuántos proyectos necesitan ser revisados anualmente para el servicio de desarrollo seguro?
Respuesta: Aproximadamente 40.

35. Mencionan tres servicios: Red Team, Acompañamiento y Asesoría, y Desarrollo Seguro y Pentest. ¿Podrían aclarar a qué se refieren con el servicio de Acompañamiento y Asesoría? ¿Es en relación a la mitigación de hallazgos del servicio de Red Team o se refiere a algo diferente?
Respuesta: Por favor referirse al numeral 3.1.4. Acompañamiento y asesoría durante la mitigación de hallazgos, del Anexo A.

36. En el Anexo A, punto 5, incisos ii y iii, ¿cuál es el modelo de acreditación que requieren? ¿Es posible para ambos puntos acreditar con una carta simple firmada por nuestro representante legal?
Respuesta: Declaración simple firmada por los representantes legales.

37. Respecto a la evaluación técnica donde se habla de certificaciones, ¿deben ser exactamente las certificaciones nombradas en la descripción de cada punto o puede ser algunas similares al tema solicitado?
Respuesta: SI, deben ser las nombradas en las Bases.

38. ¿Se requieren todas las certificaciones mencionadas en cada una de las descripciones de cada referencia o basta con algunas de ellas?
Respuesta: Se requieren las de cada ítem sin embargo, puede ser una por ítem.

39. ¿Los tiempos definidos para cada ejercicio son establecidos por ustedes o los proponemos nosotros? Ej: para el ejercicio de Red Team.
Respuesta: Se revisan en conjunto por ambas partes.

40. Legal Pág. 26// Anexo N° 1: Especificaciones Técnicas- Octavo: Multas. Por todos los años de vigencia NO pueden superar el 20% de la sumatoria del valor del contrato ¿Está de acuerdo con limitar el importe acumulado de las multas a dicho porcentaje?
Respuesta: Se mantiene el límite de multa en los términos señalados en la cláusula Octava del Contrato: "….. el monto total de las deducciones que efectúe el Banco respecto de incumplimientos acaecidos no excederá del 10% del precio o tarifa total bruta anual que el Banco deba pagar a la Empresa…"

41. Legal Pág. 30// Anexo N° 1: Especificaciones Técnicas- Décimo cuarto: Responsabilidad de la Empresa por Infracciones Legales y Reglamentarias. Las modificaciones de ley que afectaran al alcance de los servicios debe ser evaluada e común acuerdo entre las partes ¿Está de acuerdo en que se proceda de común acuerdo?
Respuesta: La Empresa está obligada a cumplir las leyes y reglamentos en los términos señalados en la cláusula décimo cuarta del Modelo de Contrato. En caso de modificaciones la empresa estará obligada a cumplirlas. En caso contrario debe hacerlo presente al Banco para que este se pronuncie al respecto. Tenga en cuenta que el Banco Central de Chile solo puede contratar con proveedores cumplan con las normas y regulaciones vigentes.

42. Legal Pág. 34// Anexo N° 1: Especificaciones Técnicas- Vigésimo tercero: Prevención de Delitos. El Proveedor responderá únicamente hasta el 100% del valor del servicio contratado, y responderá sólo por daños directos y previsibles. El Proveedor no será responsable por lucro cesante, daño

emergente y daños indirectos, salvo en caso de dolo o fraude. ¿Está de acuerdo con la modificación mencionada?
Respuesta: La responsabilidad de la Empresa está regulada en la cláusula vigésimo segundo del Modelo de Contrato, sin perjuicio de las acciones o sanciones penales u otras que correspondan a los delitos se refiere la cláusula vigesimotercera relativos a la ley N° 20.393.

43. Técnico ¿Qué se espera con el ítem Ofrecer resultados que faciliten al Banco revisar el análisis, comprensión y efectividad de su inversión en Ciberseguridad?
Respuesta: Ver la efectividad de las plataformas con las que cuenta el Banco.

44. Técnico ¿Qué se espera con el ítem Realizar un análisis de riesgo basado en hechos, lo cual facilitará poder desarrollar un plan de mitigación y que se adapte a la metodología del Banco?
Respuesta: Obtener las brechas que el Banco pueda tener y con las cuales mediante planes dispuestos por el banco se puedan adoptar o mitigar.

45. Técnico ¿Requieren de una evaluación de riesgos?
Respuesta: No.

46. Técnico ¿Requieren hacer una evaluación de ciberseguridad a su plan director?
Respuesta: No.

47. Técnico ¿Requieren de un servicio de arquitectura IT de ciberseguridad?
Respuesta: No.

48. Técnico ¿Con cuántos usuarios cuenta la compañía?
Respuesta: Esta información no es requerida para el Servicio.

49. Técnico ¿Cuántos procesos posee la compañía?
Respuesta: Esta información no es requerida para el Servicio.

50. Técnico. En caso de requerirse una evaluación ¿La evaluación es para toda la compañía o un área en específico?
Respuesta: La única evaluación necesaria es para el servicio de Desarrollo Seguro.

51. Técnico ¿El análisis de riesgos es para toda la compañía o un área en específico?
Respuesta: Esta información no es requerida para el Servicio.

52. Técnico ¿Cuántas personas participarían en la capacitación de Blue Team? ¿Se daría por una única vez? ¿O más de una?
Respuesta: No es posible responder la primera pregunta. Respecto de las preguntas siguientes considerar que puede ser más de una vez.

53. Técnico ¿Requieren apoyo en la mitigación de vulnerabilidad, o se necesita de un proceso para la gestión de vulnerabilidades? es decir, este proceso implica:

- Establecer un procedimiento
- Establecer programa:

  Frecuencia de pruebas
  Alcance de test
  Herramientas
  Responsables
- Establecer norma de parchado considerando

  Criterios
  Ambientes de prueba
  Priorizacion
  Responsables

Respuesta: Algunos puntos podrían ser contemplados para el Servicio de desarrollo seguro.

10 de junio de 2024
Departamento de Adquisiciones