CONSULTAS LICITACIÓN 90002728
"MANAGED SECURITY SERVICE PROVIDER (MSSP)"

De acuerdo al calendario de las bases del proceso de Licitación 90002728, a continuación se presentan las consultas recibidas con sus respectivas respuestas.

1 Página 9 - Evaluación Técnica. Tabla N1 Factores a evaluar. El servicio entregado será ejecutado desde el mismo sitio evaluado en alguno de los ranking indicado en el numeral anterior. Estos reportes al momento de su confección fueron consideradas las prácticas y presencia global, como se distinguirá de lo global al país que donde se debería entregar el servicio?
Respuesta: Los servicios deberán ser entregados desde sus oficinas centrales.

2 Página 13 - Situación Actual. Punto 3.3 ¿El Banco es dueño de la solución de IBM Qradar con su correspondiente licenciamiento?
Respuesta: Si.

3 Página 13 - Situación Actual. Punto 3.3 ¿El Banco está solicitando al proveedor reemplazar esa solución de IBM Qradar con una de su preferencia?
Respuesta: No, es un complemento con lo que dispongan como servicio.

4 Página 13 - Situación Actual. Punto 3.3 ¿El Banco está solicitando que adicionalmente a la solución de IBM Qradar que posee el Banco, el proveedor ofrezca otra adicional por sobre esa o remplazarla?
Respuesta: No, es un complemento con lo que dispongan como servicio.

5 Página 13 - Situación Actual. Punto 3.4 Por favor confirmar que cantidad de licenciamiento está solicitando el Banco ¿600 EPS? ¿4000 EPS o 6500 EPS?
Respuesta: 6500 EPS.

6 Página 13 - Situación Actual. Punto 3.3 En caso de remplazar la tecnología actual del Banco y nueva infraestructura sea necesaria en los 4 sitios de procesamiento. El Banco entregará infraestructura local (virtual o física) para montar la solución?
Respuesta: No hay reemplazo. Es un complemento con lo que dispongan como servicio.

7 Página 13 - Situación Actual. Punto 3.3 ¿El Banco permite que los registros/Logs sean llevados a una nube privada del oferente? ¿Alguna condición que deba cumplir esta nube privada?
Respuesta: Si, pero el repositorio debe ser reservado solo para los datos del Banco y no compartido con otros clientes, deberá además estar ubicada en Estados Unidos y cumplir con el Acuerdo de confidencialidad de la información.

8 Página 13 - Situación Actual. Punto 3.3 ¿El Banco mantendrá su solución de IBM Qradar? ¿Por cuánto tiempo?
Respuesta: Si lo mantendrá, por el tiempo que el Banco estime conveniente.

9 Página 14 - Especificaciones de los servicios requeridos 4.1.4 ¿Cuántos casos de uso el Banco quiere implementar? Esta información es necesaria para dimensionar la cantidad de esfuerzos en el monitoreo 24/7.
Respuesta: Deben informar catálogo de casos de uso que disponen para acordar su implementación.

10 Página 14 - Especificaciones de los servicios requeridos 4.1.4 ¿Cuál es el crecimiento esperado año a año en casos de uso?
Respuesta: 5 al año.

11 Página 14 - Especificaciones de los servicios requeridos 4.1.7 ¿El SIEM actual del Banco IBM Qradar cumple con lo necesario para este almacenamiento?
Respuesta: No.

12 Página 14 - Especificaciones de los servicios requeridos 4.1.7 En caso que el Banco continue con su IBM Qradar licenciado, ¿el oferente es el que debe entregar storage para almacenar la información mencionada?
Respuesta: Si.

13 Página 14 - Especificaciones de los servicios requeridos 4.1.7 ¿Qué condiciones (tipo storage, locacion) debe cumplir el storage en caso que se solicite?
Respuesta: El repositorio debe ser reservado solo para los datos del Banco y no compartido con otros clientes, deberá además estar ubicada en Estados Unidos y cumplir con el Acuerdo de confidencialidad de la información.

14 Página 14 - Especificaciones de los servicios requeridos 4.1.7 ¿Se pueden almacenar los logs en una nube privada y certificada por el oferente?
Respuesta: Si, pero el repositorio debe ser reservado solo para los datos del Banco y no compartido con otros clientes, deberá además estar ubicada en Estados Unidos y cumplir con el Acuerdo de confidencialidad de la información.

15 Página 15 - 4.2 servicios de respuesta a incidentes de ciberseguridad 4.2.3 ¿Cuántos playbooks el Banco está pensando en desarrollar en conjunto con el oferente?
Respuesta: Deben informar catálogo de playbooks que disponen para acordar su implementación.

16 Página 15 - 4.2 servicios de respuesta a incidentes de ciberseguridad Se entiende en este servicio que la respuesta a incidentes es cuando un evento de seguridad (alerta) fue declarado un incidente y se requiere responder al mismo ¿es correcto?

Respuesta: Sí.

17 Página 15 - 4.2 servicios de respuesta a incidentes de ciberseguridad ¿El Banco está dispuesto a tomar este servicio como un servicio tipo retainer?
Respuesta: No.

18 Página 15 - 4.3 Servicio de Threat Hunting Favor confirmar con que periodicidad o cantidad de ejercicios de hunting se requieren, ya que indica que no deben ser ejecutados on demand o con alguna periodicidad. Tener una visibilidad acertada de la cantidad de estos ejercicios ayuda a dimensionar correctamente el servicio.
Respuesta: Threat Hunting continuo que día a día este analizando y entregando información.

19 Página 15 - 4.4 Gestión y/o integración con plataforma EDR/XDR del Banco Favor confirmar si se está solicitando la administración de estos módulos de Defender o solo su integración al SIEM.
Respuesta: El XDR actual es Microsoft Defender, por lo que se necesita que se gestione o integren con él.

20 Página 16 - 5 configuración inicial del servicio ¿Se está esperando que se integren las 900 fuentes dentro de los 60 días solicitados en caso de ser un SIEM nuevo?
Respuesta: No, solo se deben integrar las fuentes necesarias para los casos de uso.

21 Página 16 - 5 configuración inicial del servicio ¿Cuándo se espera que el proveedor entregue su biblioteca de casos de uso?
Respuesta: Después de la adjudicación se debe entregar el catálogo.

22 Página 16 - 5 configuración inicial del servicio ¿Se puede proponer una configuración inicial para abordar las 900 fuentes a integrar y dejar sprints a lo largo del tiempo?
Respuesta: No, solo se deben integrar las fuentes necesarias para los casos de uso.

23 Página 16 - 6 CONDICIONES GENERALES DE LOS SERVICIOS - 6.2 Todos los servicios indicados en estas bases pueden otorgarse desde cualquier parte del mundo y en idioma español y/o inglés, y garantizando la resiliencia del servicio entregado. Se observa un conflicto con la tabla de condiciones a cumplir inicial que el servicio debe entregarse desde donde aparecen las compañías nombradas en MSSP Alert, Gartner y Forrester. Favor aclarar.
Respuesta: El servicio puede ser entregado desde cualquier parte del mundo, siempre y cuando sea en la oficina certificada en los reportes, usando lenguaje español o inglés.

24 Administrativas 1) ¿Cómo será el proceso para redactar de mutuo acuerdo el contrato en el caso de ser adjudicados, y en qué momento podrán discutirse modificaciones a las cláusulas señaladas en estas bases de licitación?

Respuesta: El momento para hacer presente sus solicitudes es esta instancia o bien una vez adjudicado, siempre respetando las cláusulas mínimas de las Bases. En todo caso y en cualquier instancia como se señala en las bases el Banco se reserva el derecho de efectuar ajustes de acuerdo a sus políticas y normativa interna de contratación.

25 Administrativas 2) ¿Cuál será el límite de responsabilidad hasta el que responderá el Oferente en el caso de ser adjudicado? Proponemos que se limite al monto de los honorarios efectivamente pagados.
Respuesta: No es posible limitar la responsabilidad en los términos señalados. La cláusula sexta mínima del Anexo B de las Bases establece el alcance de la responsabilidad, la cual está conforme a las normas generales de derecho.

26 Administrativas 3) En el punto 11 de las Bases Administrativas se señala: "En este Proceso de Licitación, los Proveedores podrán, si ello es factible y técnicamente conveniente, subcontratar el cumplimiento de algunas de las obligaciones, siempre que haya sido aceptado por el Banco. En todo caso, los servicios subcontratados no podrán corresponder a servicios propios de la esencia y naturaleza de las obligaciones que asume en virtud de esta contratación." ¿Qué se entenderá como servicios propios de la esencia y naturaleza de las obligaciones que se asumen?
Respuesta: Son los propios de un Servicio de Managed Security Provider. y que lo hacen ser este y no otro. No serán de la esencia ni naturaleza, aquellos que por ejemplo apoyen alguna gestión puntual para poder realizar el Servicio, siempre y cuando no hayan sido elevados a la categoría de esencial por el Banco o así se desprenda de las bases o sus anexos.

27 Administrativas 4) ¿Existe un límite en cuanto al porcentaje de los servicios que pueden ser subcontratados?
Respuesta: Véase respuesta a pregunta 26.

28 Administrativas 5) En caso de término anticipado del contrato por cualquier causa ¿Se pagarán los honorarios devengados a la fecha de término efectivo del servicio?
Respuesta: Efectivamente, siempre y cuando estos hayan sido recibidos conformes por el Banco.

29 Administrativas 6) ¿Se podrá guardar la documentación necesaria para cumplir con requerimientos judiciales, regulatorios, estándares profesionales y/o políticas internas del Receptor?
Respuesta: Véase lo señalado al respecto en la cláusula mínima: Confidencialidad, del anexo de las bases.

30 Administrativas 7) ¿Podrá someterse la resolución de conflictos, que no pueda ser resuelta por las partes, a un árbitro mixto regido por el reglamento del CAM Santiago vigente al momento de la suscripción del contrato?
Respuesta: No es posible, los conflictos se someterán a los tribunales ordinarios de justicia de Santiago.

31 Administrativas 8) ¿Bajo qué criterio la información entregada por el Banco será catalogada como “altamente sensible”?
Respuesta: El Banco es quien efectúa esta calificación acorde sus regulaciones internas e informará a la empresa qué información es altamente sensible. Véase cláusula mínima sobre confidencialidad.

32 Administrativas 9) Por temas de certeza jurídica y políticas de la firma no podemos suscribir obligaciones con vigencia indefinida; en el caso de información “altamente sensible” ¿podrá establecerse de común acuerdo un plazo cierto para la vigencia de la obligación de confidencialidad? Solo podemos aceptar un plazo de hasta 5 años contados desde el término de la relación contractual.
Respuesta: No es posible acceder a lo solicitado, respecto de ese tipo de información. Véase lo señalado en la cláusula mínima de Confidencialidad.

33 Administrativas 10) En el formulario Declaración de confidencialidad se señala: “El Proveedor declara tener conocimiento que “Información Reservada o Altamente Sensible” del Banco Central de Chile, significa cualquier documento, material de trabajo, iniciativas, datos o cualquier otro antecedente o información que diga relación, ya sea con las operaciones, actos, contratos, negocios, investigaciones o proyectos del Banco y, en general, con todas aquellas materias a que se refiere la presente contratación.”.
¿Cuándo se entiende que estamos ante información reservada y cuando ante información Altamente Sensible?
¿Se podrá modificar la redacción para acotar la información que se entenderá como “reservada o Altamente Sensible” a solo aquella que se entrega dentro del marco de la licitación y eventual servicio?
Respuesta: No es posible modificar el formulario. El Banco señalará cual es la información que tiene tal calificación.

34 Administrativas 11) En el formulario Declaración de confidencialidad se señala: “El Banco se reserva el derecho de solicitar al Proveedor la destrucción de la documentación que tenga el carácter de “Reservada o Altamente Sensible”, lo que deberá ser certificado por un apoderado del Proveedor con facultades suficientes para ello.” ¿Podremos modificar redacción incorporando lo siguiente: “Lo anterior no aplicará en caso que dicha destrucción contravenga requerimientos judiciales, regulatorios, estándares profesionales o políticas internas del Receptor.”? Necesitamos guardar cierta documentación.
Respuesta: No es posible. Tenga en cuenta que tal calificación la da el Banco y no toda la que se maneja en el servicio tiene esa calidad.

35 Administrativas 12) En el formulario Declaración de confidencialidad se señala: “Esta obligación subsistirá entre las partes, aún después de finalizada la prestación o provisión de los productos y/o servicios y por un plazo de 3 años contado desde dicha fecha, salvo que tal información haya sido calificada, catalogada y entregada al Proveedor por el Banco como “Información Altamente Sensible”, en cuyo caso la obligación de

confidencialidad subsistirá de manera indefinida.” ¿Podrá establecerse de común acuerdo un plazo cierto para la vigencia de la obligación de confidencialidad? Solo podemos aceptar un plazo de hasta 5 años contados desde el término de la relación contractual, no podemos aceptar obligaciones indefinidas.
Respuesta: Véase respuesta a pregunta 32.

36 Por favor confirmar el número de endpoints.
Respuesta:2000 endpoints aproximadamente.

37 Por favor confirmar si mantendrán su SIEM actual
Respuesta: Si, se confirma.

38 Por favor confirmar si los ítems del 6.1 están reportando al SIEM de QRADAR
Respuesta: Si, se confirma.

39 Bases Solicitamos indicar si la propuesta debe ser presentada por el proveedor de servicios MSSP en forma directa o si puede ser presentada por un representante y/o partner local.
Respuesta: Puede ser presentada por Partner local.

40 Bases Solicitamos indicar si un oferente puede presentar oferta de más de un proveedor de servicio MSSP y en caso de ser así, indicar el mecanismo.
Respuesta: Sólo se acepta una oferta por proveedor.

41 Bases 4.1 Antecedentes Administrativos Solicitamos confirmar que la información administrativa a presentar es la del representante local del proveedor de servicios MSSP
Respuesta: Esta debe ser la del participante de la licitación.

42 Bases 4.1.2. Antecedentes Legales Solicitamos confirmar que la información administrativa a presentar es la del representante local del proveedor de servicios MSSP
Respuesta: Véase respuesta a pregunta 41.

43 Bases 4.1.3. Antecedentes financieros Solicitamos confirmar que la información administrativa a presentar es la del representante local del proveedor de servicios MSSP
Respuesta: Véase respuesta a pregunta 41.

44 Bases 4.3. Oferta Económica Solicitamos indicar en que moneda se debe presentar la propuesta.
Respuesta: En la que sea más conveniente para el proveedor.

45 Bases Solicitamos indicar si el contrato se firmará con el representante local o con el proveedor de servicios MSSP.
Respuesta: El contrato se suscribirá con el proveedor adjudicatario que participó en la licitación.

46 Solicitamos indicar si el Banco acepta que el servicio sea facturado directamente por el proveedor de servicios MSSP desde el extranjero.
Respuesta: La facturación y pagos son a la compañía con la que se suscriba el contrato.

47 Bases 7.3 Evaluación Técnica En el Punto Certificaciones Técnicas MSSP: La empresa MSSP se encuentra en alguno de los siguientes rankings:
•TOP 100 Best MSSP 2021, según MSSP Alert.
•Pertenecer al cuadrante mágico de Gartner MSSP 2019.
•Pertenecer al Forrester Wave MSSP 2020.
¿Se aceptará una de estas o calificaciones equivalentes que cumplan con los mismos puntos?
Respuesta: Solo una de las indicadas.

48 Bases 7.3 Evaluación Técnica Los servicios deberán ser entregados desde las mismas oficinas, localidad o centro en las que obtuvieron su calificación en el TOP MSSP, Gartner o Forrester.
¿El licitante aceptará que los servicios sean provistos por el fabricante desde su sitio certificado y representados en el país por partners autorizados para distribuir estos servicios?
Respuesta: Si, siempre y cuando haya sido la oficina a la cual midieron para obtener la certificación.

49 Anexo A "Especificaciones Técnicas" 3 Situación Actual Si la respuesta anterior fue afirmativa favor de brindar las localidades.
Respuesta: No hay localidades de preferencia.

50 Anexo A "Especificaciones Técnicas" 3 Situación Actual ¿Los 900 usuarios en los edificios contiguos pertenecen a alguna de las localidades mencionadas en la pregunta anterior?
Respuesta: No se entiende la pregunta.

51 Anexo A "Especificaciones Técnicas" 3 Situación Actual ¿El QRadar seguirá operando?, si es así favor de detallar arquitectura pensada.
Respuesta: Si, su servicio es un complemento con lo que dispongan como servicio de forma paralela.

52 Anexo A "Especificaciones Técnicas" 3 Situación Actual ¿Aceptaría el licitante que se presente una propuesta de reemplazo para Qradar en forma total o parcial? De ser así ¿estarían abiertos a analizar una propuesta con un SIEM basado en cloud utilizando su licenciamiento actual de Microsoft?
Respuesta: No.

53 Anexo A “Especificaciones Técnicas” 3 Situación Actual ¿Cuántos son los GBPD consumidos en promedio de los últimos 3 meses?
Respuesta: No aplica la pregunta.

54 Anexo A “Especificaciones Técnicas” 3 Situación Actual De los 10 FW cluster que menciona, ¿qué configuración tienen, Activo Pasivo o Activo Activo?, favor de dar detalles.
Respuesta: No aplica la pregunta.

55 Anexo A “Especificaciones Técnicas” 3 Situación Actual Los 10 FW cluster,4 FW standalone y 2 FW Paloalto ¿son DMZ o Trust FW?, favor de especificar.
Respuesta: Esta información será entregada al adjudicatario.

56 Anexo A “Especificaciones Técnicas” 3 Situación Actual Actualmente, ¿utilizan Active Directory OnPrem, Azure, o hibrido?, ¿A dónde apunta su DNS actualmente?
Respuesta: Active Directory Hibrido y DNS Cloud.

57 Anexo A “Especificaciones Técnicas” 3 Situación Actual Si utilizan Azure Active Directory, ¿Ya está populado con cuentas de usuarios?
Respuesta: Si.

58 Anexo A “Especificaciones Técnicas” 3 Situación Actual Si utilizan Azure Active Directory, ¿Ya está configurado AAD Connect?
Respuesta: Si.

59 Anexo A “Especificaciones Técnicas” 3 Situación Actual ¿Hay alguna necesidad de conectar un dominio On Prem con AAD?
Respuesta: No.

60 Anexo A “Especificaciones Técnicas” 3 Situación Actual ¿Su Correo electrónico esta hospedado en M365?
Respuesta: Si.

61 Anexo A “Especificaciones Técnicas” 3 Situación Actual ¿Utilizan McAfee como AV y MDE (Microsoft Defender for EndPoint) en todos los EndPoints y Servidores?, favor de brindar detalle.
Respuesta: Si, el Banco cuenta con McAfee Endpoint Security como antivirus primario y Defender for Endpoint como secundario.

62 Anexo A “Especificaciones Técnicas” 3 Situación Actual Actualmente, ¿cómo gestionan los EndPoints (Intune, SCCM, RADIA)?
Respuesta: No aplica la pregunta.

63 Anexo A “Especificaciones Técnicas” 3 Situación Actual ¿Cuantos servidores de los 800 mencionados son Windows y cuantos Linux?, ¿Son OnPrem o Cloud?, favor de especificar con detalle incluyendo que Cloud hosting están utilizando.
Respuesta: No aplica la pregunta.

64 Anexo A “Especificaciones Técnicas” 3 Situación Actual De los 900 usuarios O365 mencionados, ¿Que licenciamiento tienen E3 o E5?, Favor de especificar por nivel de licenciamiento número de usuarios si tienen una mezcla de ambos niveles.
Respuesta: E5.

65 Anexo A “Especificaciones Técnicas” 3 Situación Actual ¿Requieren la implementación de Microsoft defender con todas sus herramientas?
Respuesta: No.

66 Anexo A “Especificaciones Técnicas” 3 Situación Actual Para Defender for Cloud Apps, ¿qué aplicaciones/servicios integran?
Respuesta: O365.

67 Anexo A “Especificaciones Técnicas” 4 Especificaciones de los Servicios Requeridos Cuando hablan de 3 meses en línea y 12 meses de históricos son: ¿9 meses con logs históricos y los 3 meses actuales al final del año de contrato?
Respuesta: No, 3 meses de logs cargados en disco, para consulta rápida y los 12 meses de histórico en respaldo.

68 Anexo A “Especificaciones Técnicas” 4 Especificaciones de los Servicios Requeridos ¿Nos puede mencionar si se tiene que cumplir algún un compliance, marco de trabajo y/o estándar?
Respuesta Para el servicio solicitado no.

69 Anexo A “Especificaciones Técnicas” 3 Situación Actual ¿Requieren la implementación de Microsoft defender con todas sus herramientas?, Si ya está implementado dar detalle de estatus de dicha implementación.
Respuesta: Se encuentra implementado.

70 Anexo A “Especificaciones Técnicas” 3 Situación Actual Para Defender for Cloud Apps, ¿qué aplicaciones/servicios integran?
Respuesta: O365.

71 Técnica Anexo A - 1 Introducción Respecto al sistema interno de monitoreo de ciberseguridad que ya cuenta Banco Central:
- ¿cuál es su cobertura en cuanto a monitoreo y notificaciones: 5x8 ó 7x24?
- ¿Es administrado por un tercero o por el mismo Banco?

Respuesta: 7x24 para monitoreo y notificaciones. Administrado por un tercero.

72 Técnica Anexo A - 1 Introducción Favor aclarar según lo indicado: "El Banco Central de Chile ha iniciado un proceso de licitación para contratar los servicios de un Managed Security Service Provider (MSSP), para complementar su sistema interno de monitoreo de ciberseguridad con un servicio de monitoreo externo 24x7":
- ¿se espera que el oferente realice la toma de control del actual SIEM y posterior administración como parte del servicio?, o
- ¿se espera la implementación de una nueva plataforma que reemplace este monitoreo interno?

Respuesta: No hay reemplazo. Es un complemento con lo que dispongan como servicio.

73 Técnica Anexo A - 3 Situación Actual ¿Los 4 sitios poseen conectividad entre sí o son redes completamente aisladas?
Respuesta: Poseen conectividad entre sí.

74 Técnica Anexo A - 3 Situación Actual ¿Los 4 sitios se encuentran integrados con el SIEM o se espera que se implementen durante la configuración inicial del servicio?
Respuesta: Todos están integrados con el SIEM del Banco.

75 Técnica Anexo A - 3 Situación Actual Respecto al actual SIEM Qradar y en caso se requiera realizar la toma de control de esta plataforma, favor indicar la vigencia respectiva del licenciamiento (y el mayor detalle posible).
Respuesta: No se requiere que tomen administración del SIEM del Banco.

76 Técnica Anexo A - 3 Situación Actual Favor compartir arquitectura de plataforma SIEM actual
Respuesta: 2 Event Collector y 2 Event Procesor y 1 Consola.

77 Técnica Anexo A - 3 Situación Actual Respecto a la plataforma SIEM actual, favor indicar número/tipo/distribución de dispositivos que son parte de la solución.
Respuesta: 2 Event Collector y 2 Event Procesor y 1 Consola.

78 Técnica Anexo A - 3 Situación Actual Respecto a la plataforma SIEM actual, favor indicar si los dispositivos parte de la solución son físicos y/o virtuales, on premise/cloud.
Respuesta: Virtuales On-premise.

79 Técnica Anexo A - 3 Situación Actual ¿Los dispositivos actuales de la plataforma SIEM son de propiedad del Banco o de un tercero?
Respuesta: Son propiedad del Banco.

80 Técnica Anexo A - 3 Situación Actual ¿Cuántos casos de uso tienen desplegados en el actual SIEM?
Respuesta: Esta información se entregará al adjudicatario.

81 Técnica Anexo A - 3 Situación Actual ¿Cuántas reglas de correlación tienen desplegadas en el actual SIEM?
Respuesta: Esta información se entregará al adjudicatario.

82 Técnica Anexo A - 3 Situación Actual Favor indicar el número de incidentes de seguridad en promedio generados de forma mensual, y su proporción de acuerdo a prioridad.
Respuesta: Esta información se entregará al adjudicatario.

83 Técnica Anexo A - 3 Situación Actual Favor indicar el número de ofensas por mes generadas por la plataforma actual.
Respuesta: Esta información se entregará al adjudicatario.

84 Técnica Anexo A - 3 Situación Actual Favor indicar cuántos tickets de incidentes de seguridad son escalados a un segundo nivel, para ser analizados mensualmente por el Banco, luego de que un primer nivel de monitoreo haya realizado un primer análisis de descarte de falsos positivos monitoreando el SIEM.
Respuesta: Esta información se entregará al adjudicatario.

85 Técnica Anexo A - 3 Situación Actual Favor indicar el número de servidores por tipo (Windows, Unix, Linux), según el número total existente (800).
Respuesta: Esta información se entregará al adjudicatario.

86 Técnica Anexo A - 3 Situación Actual Favor indicar si Banco cuenta con un equipo de analistas de seguridad local para atención de alertas generadas por el actual SIEM.
Respuesta: Si.

87 Técnica Anexo A - 3 Situación Actual ¿Hoy en día se monitorean los flujos de red a través del SIEM?
Respuesta: No.

88 Técnica Anexo A - 3 Situación Actual ¿Hoy en día se monitorea y analiza el comportamiento de usuarios a través del SIEM?
Respuesta: Si.

89 Técnica Anexo A - 4 Especificaciones de los servicios requeridos - 4.1 Servicio de Monitoreo ¿Se requiere que el servicio de SOC se integre directo al portal ITSM (sistema de tickets) del Banco, para la creación automática de tickets y seguimiento de los mismos?
Respuesta: No.

90 Técnica Anexo A - 4 Especificaciones de los servicios requeridos - 4.1 Servicio de Monitoreo En caso de requerir la integración de la pregunta anterior, favor indicar qué solución de ITSM posee el Banco.
Respuesta: No aplica la pregunta.

91 Técnica Anexo A - 4 Especificaciones de los servicios requeridos - 4.1 Servicio de Monitoreo ¿Cuál es la proyección de crecimiento del número de fuentes que reportan eventos al SIEM?, ¿está considerado en el número de EPS actualmente licenciado: 6500?
Respuesta: No aplica la pregunta.

92 Técnica Anexo A - 4 Especificaciones de los servicios requeridos - 4.1 Servicio de Monitoreo Favor de confirmar que el proveedor del servicio de SOC, deberá brindar un servicio de análisis, contextualización y orquestación inicial, de las alertas generadas por el monitoreo de SOC, siendo este rol un punto focal operativo entre el SOC y el cliente. En caso contrario, indicar si el Banco tiene un rol interno para gestión de incidentes de seguridad.
Respuesta: Si, se confirma.

93 Técnica Anexo A - 4 Especificaciones de los servicios requeridos - 4.1 Servicio de Monitoreo ¿Se cuenta con subscripción a fuentes de ciberinteligencia premium?
Respuesta: Esta información se entregará al adjudicatario..

94 Técnica Anexo A - 4 Especificaciones de los servicios requeridos - 4.4 Plataforma EDR/XDR Al indicar "4.4 Gestión y/o integración con plataforma EDR/XDR del Banco", ¿Se espera que el oferente tome el control completo de la solución EDR?, ¿o solo la integración como fuente y la gestión de la plataforma seguirá siendo de Banco?
Respuesta: No, la gestión de la plataforma seguirá siendo del Banco.

95 Técnica Anexo A - 4 Especificaciones de los servicios requeridos - 4.4 Plataforma EDR/XDR Si la respuesta a la pregunta anterior es afirmativa, favor entregar detalles de la plataforma actual:
- Diagrama de arquitectura
- Tipo de licenciamiento existente
- Tipo de soporte actual

Respuesta: No aplica la pregunta.

96 Técnica Anexo A - 4.2 Servicio de respuesta a incidentes de ciberseguridad Favor indicar si el servicio de respuesta debe ser 24x7 continuo o puede ser 8x5 con guardia.
Respuesta: Puede ser 24x7 o 8x5 con guardia.

97 Técnica Anexo A - 4.3.1 Servicio de Threat Hunting Favor confirmar si la única herramienta de EDR Microsoft Defender for Endpoint.
Respuesta: Si.

98 Técnica Anexo A - 5.2 CONFIGURACIÓN INICIAL DEL SERVICIO Favor indicar la cantidad de casos de uso que se espera implementar durante los 60 días.
Respuesta: Deben informar catálogo de casos de uso que disponen para acordar su implementación.

99 Técnica Anexo A - 5.3 CONFIGURACIÓN INICIAL DEL SERVICIO Favor indicar si se cuenta con una herramienta tipo SOAR.
Respuesta: Si.

100 PreciosFormulario Presentación Oferta Económica Favor confirmar si es posible ofertar por un período de 14 meses de contrato considerando una toma de control de 2 meses y la operación por 12 meses?
Respuesta: Está considerado para el primer año de vigencia un pago por una única vez por la configuración inicial, y posteriormente los pagos mensuales vencidos por la operación.

101 Precios Formulario Presentación Oferta Económica¿es posible ofertar desde ya un contrato por 5 años?
Respuesta: No es posible.

102 Calendario Fecha de Presentación de PropuestasConsiderando que las respuestas llegarán una semana antes del plazo de envío de propuestas, ¿es posible que puedan extender el plazo por lo menos por 7 días adicionales?
Respuesta: No se extenderá el calendario, no obstante se ajusta según la nueva fecha de publicación de respuestas a consultas..

103 Este oferente participará mediante la presentación de una contrapropuesta, que en ningún caso implica la aceptación de los términos y condiciones de las bases de licitación y sus anexos. Este oferente está disponible para revisar dichos términos y condiciones, en el marco del proceso de licitación, de manera de acordar el texto del eventual contrato a ser firmado por Banco Central y este oferente, en caso de ser adjudicada nuestra propuesta.
Respuesta: Para participar debe ajustarse a los términos de las Bases de licitación y sus anexos. Esto está de conformidad con los requerimientos de los procesos de compras regulados por el Banco Central de Chile.

4 de agosto de 2022
Departamento de Adquisiciones