Subdirección de Administración
Depto. Adquisiciones
SMR
RAB N°

Santiago, 07 de noviembre de 2023

RESOLUCIÓN SII N° 27

VISTOS: Lo dispuesto en el Artículo 7° letra o), de la Ley Orgánica del Servicio de Impuestos Internos, contenida en el Artículo 1° del DFL N°7 de 1980 del Ministerio de Hacienda; Ley N° 21.516 sobre Presupuesto del Sector Público para el año 2023; la Ley N° 19.880 que establece Bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado; la Ley N°19.886 de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios y su Reglamento; la Resolución Exenta N° 1055, de 2010, sobre procedimientos para adquisiciones, y la Resolución Exenta N° 96, de 2013, que la modifica; la Resolución Exenta N° 146, de 2020, sobre delegación de facultades y la Resolución Exenta N°63, de 2021, que la complementa; todas de la Dirección Nacional del Servicio de Impuestos Internos; la Resolución N° 7, de 2019, la Resolución N°5 de 2020 y la Resolución N°14, de 2022, todas de la Contraloría General de la República; las necesidades del Servicio; y

CONSIDERANDO:

1° Que, el Servicio de **Impuestos** Internos necesita contratar "**Servicios Integrales de Ciberseguridad"**, asociado a la Solicitud Interna de Compra (SIC) **N° 830,** dando origen al proceso código interno **LR-1138**, solicitado por el Departamento Informática Aseguramiento de Estándares Tecnológicos de la Subdirección de Informática.

2° Que, revisado el catálogo electrónico de Convenio Marco que dispone la Dirección de Compras en el portal Mercado Público, no se encontró disponible el servicio requerido en la modalidad de Convenio Marco, según consta en certificado emitido por la Jefe de Departamento de Adquisiciones, de fecha 16 de agosto de 2023.

3° Que, para llevar a cabo dicho propósito, es necesario efectuar un llamado a Licitación Pública, para lo cual fueron preparadas las Bases Administrativas y Técnicas que regularán el proceso mencionado.

4° Que, el llamado a Licitación será publicado en Internet a través del portal Mercado Público (www.mercadopublico.cl).

5° Que, para el referido proceso de licitación, el Servicio realizó un proceso de consultas al mercado (RFI), a través del portal Mercado Público, identificado con el ID 2601-22-RF22, emitiéndose como resultado el informe de análisis técnico económico de fecha 13 de abril de 2023, esto en relación con lo solicitado en el artículo 13 ter del Reglamento de la Ley 19.886, incorporado por el Decreto N° 1.410, de 2015.

RESUELVO:

I. LLÁMASE a Licitación Pública **N° LR-1138**, denominada **Servicios Integrales de Ciberseguridad.**

II. APRUÉBANSE las respectivas Bases Administrativas, Técnicas y Anexos, que a la letra expresan:

FICHA EJECUTIVA

NOMBRE DE LA LICITACIÓN	**SERVICIOS INTEGRALES DE CIBERSEGURIDAD**
N° de la Licitación	**LR-1138**
Tipo	**PÚBLICA**
Información y Obtención de Bases	En el portal de Mercado Público, **www.mercadopublico.cl**, desde la Fecha de Publicación y hasta la Fecha de Cierre del proceso en el portal.
Recepción de Consultas	A través de la opción de foro del portal de Mercado Público, y dentro del plazo máximo de 5 días hábiles contados desde las cero horas del día siguiente al de la fecha de publicación del llamado a licitación.
Publicación de Respuestas	Las respuestas se publicarán como documento adjunto en el portal de Mercado Público, dentro del plazo máximo de 7 días hábiles contados desde la Fecha Final de Recepción de Consultas.
Recepción de la "Garantía de Seriedad de la Oferta"	En Agustinas N°1269, segundo piso (Subdirección de Administración del Servicio de Impuestos Internos), **hasta el día de cierre del proceso a las 16:00 horas.** Para el caso de las garantías otorgadas electrónicamente, de conformidad con la Ley N° 19.799 sobre Documentos electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma, deberán ser adjuntadas a los documentos de la licitación. **Nota: En el evento que se encuentre cerrado tal acceso, favor entrar por Agustinas N°1253 (Dirección del Trabajo)**
Recepción Electrónica de las Ofertas Técnicas y Económicas	La presentación de las ofertas técnicas y económicas se realizará, exclusivamente, en forma electrónica a través del portal de Mercado Público y hasta las 16:00 horas del día de la fecha de cierre del proceso, lo que ocurrirá luego de **30 días corridos**, o al día hábil siguiente en caso de que dicho día sea inhábil, contados desde las cero horas del día siguiente al de la fecha de publicación del llamado a licitación. La apertura electrónica de las ofertas técnicas y económicas se efectuará a las 16:15 horas del día de cierre.
Plazo de Evaluación	La evaluación de las ofertas se realizará en el plazo máximo de 70 días hábiles, a contar del término del plazo del cierre de recepción electrónica de las ofertas.
Plazo de Adjudicación	La adjudicación de la licitación se realizará en el plazo máximo de 90 días hábiles, a contar del término del plazo del cierre de recepción electrónica de las ofertas.
Documento de Garantía por Seriedad de la Oferta **(**A la vista e irrevocable**)**	**Monto: $2.000.000.- (Dos millones de pesos).** **A Favor:** Del Servicio de Impuestos Internos. RUT 60.803.000-K **Glosa:** Para garantizar la seriedad de la oferta en licitación pública **N° LR-1138** del SII. **Vigencia:** Deberá extenderse a lo menos 120 días corridos, contados a partir del día siguiente de la fecha de cierre de la recepción electrónica de las ofertas.
Documento de Garantía de Cumplimiento Contrato (A la vista e irrevocable**)**	**El oferente podrá garantizar el contrato por medio de alguna de las siguientes opciones:** **Opción N°1: Un solo documento de garantía por toda la vigencia del contrato.** **Monto**: UF _____5% del valor total del contrato (IVA incluido), en unidades de fomento. **A Favor:** Del Servicio de Impuestos Internos

	Glosa: Para garantizar el fiel cumplimiento del contrato (N° interno a asignar) con el SII. **Vigencia mínima:** Por toda la vigencia del contrato más 60 días hábiles. **<u>Opción N°2: Documentos de garantía asociada a hitos anuales (Cada hito anual, corresponderá a 12 meses consecutivos).</u>** **Monto:** - **Garantía 1: UF _____ 5** % del precio total del contrato (IVA incluido) en unidades de fomento. - **Garantía 2: UF _____ 5** % del saldo insoluto del contrato (IVA incluido) en unidades de fomento. - **Garantía 3: UF _____ 5** % del saldo insoluto del contrato (IVA incluido) en unidades de fomento. **A Favor:** Del Servicio de Impuestos Internos. **Glosa:** Para garantizar el fiel cumplimiento del contrato (N° interno a asignar) con el SII. **Vigencia:** - **Garantía 1:** Desde la firma del contrato y por toda la vigencia del contrato más 60 días hábiles. - **Garantía 2:** Presentar una nueva garantía de cumplimiento de contrato 30 días corridos antes del vencimiento del primer hito anual y por toda la vigencia restante del contrato más 60 días hábiles. - **Garantía 3:** Presentar una nueva garantía de cumplimiento de contrato 30 días corridos antes del vencimiento del segundo hito anual y por toda la vigencia restante del contrato más 60 días hábiles. Esta segunda opción puede ser ejercida en cualquiera de los 2 hitos anuales del contrato. El documento de garantía puede ser otorgado de forma física o electrónica, en este caso debe ajustarse a lo dispuesto en la Ley N° 19.799 sobre Documentos electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma.

BASES DE LA LICITACIÓN

Í N D I C E

I) BASES ADMINISTRATIVAS - TÉRMINOS PARTICULARES

1 OBJETO DE LA LICITACIÓN

El objetivo de la presente licitación es la contratación de servicios de seguridad informática con el fin de asegurar la protección de los sistemas informáticos del Servicio de Impuestos Internos (SII) en ambientes Internet e Intranet, por un periodo de 36 meses. Los servicios corresponden a las componentes descritas a continuación:

COMPONENTES REQUERIDOS	
Componente 1	ITEM 1: Servicio de centro de operación de seguridad (SOC)
	ITEM 2: Servicio Gestionado de Detección y Prevención de Intrusos (IPS).
	ITEM 3: Servicio Gestionado de protección contra ataques de denegación de servicios (Anti DDOS).
	ITEM 4: Servicio Gestionado de análisis de vulnerabilidades.
	ITEM 5: Servicio Gestionado de firewall para aplicaciones Web y APIS (WAAP).
	ITEM 6: Servicio Gestionado de detección y respuesta de amenazas en red de datos interna (NDR, Network Detección and Response).
Componente 2	Horas Hombre para servicios profesionales avanzados en seguridad de la información y ciberseguridad

Las dos componentes serán adjudicadas a un solo oferente.

2. ASPECTOS RELEVANTES DE LOS PROPONENTES Y SUS OFERTAS

2.1. Quiénes pueden participar

Pueden participar en la presente licitación todas las personas naturales, jurídicas y/o uniones temporales de proveedores que tengan interés en ello y no se encuentren inhabilitadas conforme a lo establecido en el artículo 4° de la Ley N° 19.886, de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios y otros cuerpos legales, según se indica en el siguiente punto.

2.2 Requisitos de admisibilidad

La oferta deberá cumplir necesariamente con lo siguiente:

a. Presentación del documento de garantía de seriedad de la oferta, según lo estipulado en la Ficha Ejecutiva. Para el caso de boletas electrónicas, éstas deberán ajustarse a lo dispuesto en la Ley N° 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma.
b. Los requerimientos mínimos solicitados en el anexo N° 5, verificable con la información entregada en la oferta.
c. El oferente haya ofertado por las dos componentes, y la totalidad de los ítems solicitados.

Además, se procederá a revisar que el oferente no haya sido condenado por prácticas antisindicales e infracción a los derechos fundamentales del trabajador, ni por los delitos concursales del Código Penal, en el transcurso de los dos años anteriores a la presentación de la oferta. Lo anterior será validado con la información obtenida a través del portal Mercado Público. De igual forma, en el mismo sitio, se verificará que los oferentes no hayan sido condenados por delitos contra la libre competencia, de acuerdo con lo prescrito en el DL N° 211, ni se encuentren afectos a la pena de

prohibición de celebrar actos y contratos con los organismos del Estado, en conformidad a la Ley N° 20.393 y la Ley 21.595 que establece nuevos delitos económicos.
Para lo anterior, los oferentes deberán completar las declaraciones juradas referidas a inhabilidades que despliega el portal Mercado Publico al momento de ingresar su oferta.

Se debe considerar que:

- ✓ **Si no cumple con alguno de estos requisitos, la oferta será declarada inadmisible.**
- ✓ Es responsabilidad del oferente proveer todos los elementos necesarios para el adecuado cumplimiento del objeto de la presente licitación.
- ✓ Se deja expresa constancia que cualquier estipulación en las ofertas que limiten, condicionen y/o restrinjan los términos y condiciones solicitados en las bases, se tendrán por no escritas.

2.3. Subcontrataciones

El SII puede aceptar subcontrataciones dentro de las ofertas. En el caso que, para el cumplimiento de la prestación licitada, el oferente requiera subcontratar a otra empresa, junto con indicarlo claramente en su oferta, deberá proporcionar los antecedentes que la identifique, incluyendo aquellos que acreditan que no se encuentran afectados por ninguna de las inhabilidades señaladas en la legislación nacional. Asimismo, deberá indicar qué parte del trabajo será realizada por la empresa subcontratada, en el anexo N° 1. **El SII permitirá la subcontratación sólo para los servicios de instalación y puesta en marcha del equipamiento, en caso de que fuese necesario.**

El monto total de los servicios subcontratados en su conjunto no debe exceder del 30% del monto total del contrato celebrado con el adjudicatario.

El adjudicatario será el único responsable ante el SII del cumplimiento de los servicios de la presente licitación.

En todo caso, el adjudicatario no podrá pretender modificaciones de especificaciones, de precios o de plazos. El SII se reserva el derecho de objetar fundadamente a un subcontratista.
Si durante la vigencia del contrato, fuere necesario efectuar subcontrataciones, el adjudicatario deberá informar previamente al Servicio, cumpliendo con los mismos requisitos y limitaciones señaladas en los párrafos 1 y 2 de este numeral.

3. PROCESO DE LICITACIÓN

3.1 Forma de Presentación de las Propuestas

a) **DOCUMENTO DE GARANTÍA DE SERIEDAD DE LA OFERTA:** Deberá presentarse en un sobre denominado **"Garantía de Seriedad de la Oferta de la Licitación N° LR-1138"** en el lugar, la fecha y hora señaladas en la Ficha Ejecutiva, y en el caso de garantía electrónica deberá ajustarse a la Ley N° 19.799 sobre Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de dicha firma, y ser adjuntada a los documentos de la licitación.

Nota: Dada la contingencia actual, se les solicita a los oferentes privilegiar el uso de documentos de garantía electrónicos, para mayor certeza y seguridad en la presentación en tiempo y forma de la garantía solicitada.

b) **OFERTA TÉCNICA,** deberá ser presentada a través del sitio web www.mercadopublico.cl, en el campo destinado a recibir la oferta técnica, como documento adjunto, en formato compatible con MS-Office o archivo .pdf con los siguientes documentos:

- La **PROPUESTA TÉCNICA**, la cual debe ajustarse a los requerimientos exigidos en las presentes Bases de Licitación.
- **Anexo N° 1, ANTECEDENTES DEL OFERENTE Y SUBCONTRATISTA**

- **Anexo N°3**, **FICHA EXPERIENCIA DE LA EMPRESA.**
- **Anexo N° 4, FICHA CURRICULUM VITAE.**
- **Anexo N° 5, REQUISITOS MÍNIMOS DE LOS PRODUCTOS Y/O SERVICIOS OFERTADOS**
- **Anexo N° 6, CARACTERÍSTICAS TÉCNICAS OFERTADAS DE LOS SERVICIOS OFERTADOS**.
- **Anexo N°7, PACTOS DE INTEGRIDAD; MODELO DE PREVENCION DE DELITOS; CAPACITACIONES.**

c) La **OFERTA ECONÓMICA** deberá ser presentada en Unidades de Fomento (UF), a través del sitio web www.mercadopublico.cl. Además, se debe adjuntar el **ANEXO N° 2: Propuesta Económica** en el mismo formato, en el campo destinado a recibir la oferta económica.

En caso de existir discrepancia entre la oferta económica presentada en el sitio web www.mercadopublico.cl y la propuesta económica indicada en el Anexo N° 2, se considerará como válido el valor indicado en el Anexo N° 2. En caso de discrepancia en los valores unitarios y totales, se considerarán los valores más beneficiosos para el SII.

3.2 Vigencia de la Oferta

Las ofertas que presenten los oferentes deberán tener una vigencia de 120 días corridos contados a partir del día siguiente de la fecha de cierre de la recepción electrónica de las ofertas.

En circunstancias excepcionales, el SII podrá solicitar a los oferentes que extiendan el período de validez de sus ofertas. Tanto la solicitud como las respuestas deberán ser hechas por medio del portal www.mercadopublico.cl , y en caso de aceptación, el oferente, dentro del plazo de cuatro días hábiles siguientes a la recepción de la solicitud de extensión de la oferta, deberá extender la vigencia del documento de garantía de seriedad de la oferta o adjuntar uno nuevo, idéntico al anterior, por el lapso equivalente al de la extensión del periodo de validez de la oferta. Por la sola presentación del nuevo documento de garantía de seriedad de la oferta se entiende que el oferente extiende el periodo de validez de esta.

En caso de que no se extienda la vigencia del documento de garantía, en el plazo antes señalado, la oferta será declarada inadmisible.

3.3 Evaluación de las Ofertas

En forma previa a la evaluación técnica se verificará que los oferentes cumplan con lo solicitado en el N° 2.2 de las Bases Administrativas-Parte I.

La apertura de las ofertas se realizará en una etapa.

3.3.1 Comisión evaluadora:

La evaluación técnica y económica de las ofertas estará a cargo de una comisión evaluadora y se extenderá por el lapso señalado en la Ficha Ejecutiva de la licitación.

La comisión evaluará de acuerdo con los criterios establecidos en las presentes Bases y podrá requerir las asesorías y los antecedentes que estime pertinentes para su adecuado funcionamiento, como así también corroborar los datos presentados por los oferentes.

La comisión evaluadora estará integrada por tres profesionales del SII y será designada por el Subdirector de Informática, por medio de un Memorándum.

La evaluación de las ofertas recibidas se efectuará de acuerdo con el procedimiento que se detalla a continuación.

3.3.2 Evaluación técnica (70%)

De las ofertas que no hayan sido declaradas inadmisibles, se elaborará un ranking de oferentes, de acuerdo a la suma de puntajes de los ítems, calificando técnicamente todos aquellos que logren un puntaje ponderado mayor o igual a **60 puntos**, sobre la base de los parámetros y ponderaciones detalladas en la siguiente tabla:

Si la oferta, en alguno de los componentes, no obtiene un puntaje en la evaluación técnica de 60 puntos o más, **la oferta de la empresa será declarada inadmisible.**

Dado que la evaluación técnica comprende dos componentes, la componente 1 considera el 80% y la componente 2 considera el 20% en el total de la evaluación técnica.

3.3.2.1 COMPONENTE 1

	Criterio Por Evaluar	Ponderación
Evaluación Técnica (70%)	A. EVALUACIÓN DEL OFERENTE	30%
	B. EVALUACIÓN DE LA SOLUCIÓN Ítems 1, 2, 3, 4, 5 y 6	65%
	C. CUMPLIMIENTO DE LOS REQUISITOS DE PRESENTACIÓN DE LAS OFERTAS Y PACTO DE INTEGRIDAD.	5%

A continuación, se detalla la ponderación de cada criterio a evaluar:

A. EVALUACIÓN DEL OFERENTE (30%)			
Criterios		**Subcriterio**	
Ítems	**Ponderación**	**Característica**	**Puntaje**
Cantidad de clientes en la prestación de servicios SOC (componente 1, ítem 1)	35%	5 o más clientes	100
		Entre 3 y 4 clientes	70
		Entre 1 y 2 clientes	30
		No tiene clientes de la solución o no provee información	0
Experiencia general del oferente en el mercado de servicios de seguridad de la información y ciberseguridad (servicios gestionados, consultorías en seguridad, prestación de horas hombre en la materia).	30%	Más de 6 años	100
		Más de 4 años y hasta 6 años.	70
		Más de 2 años y hasta 4 años	30
		2 años o menos	0
Experiencia especifica del oferente en el mercado de servicios gestionados de seguridad de componente 1 (referidos a todos o al menos 3 de los ítems 2,3,4,5,6 del componente 1) debe especificar en cuales de los ítems tiene la experiencia referida.	35%	Más de 6 años	100
		Más de 4 años y hasta 6 años.	70
		Más de 2 años y hasta 4 años	30
		2 años o menos	0
NOTAS: **Cantidad de clientes de solución (SOC) en el mercado**: El oferente deberá proporcionar antecedentes sobre su experiencia en prestación de servicios integrales de ciberseguridad, para la componente 1, ítem 1. Adjuntar antecedentes según formato de Anexo N°3 Ficha de experiencia de la empresa.			

Experiencia general del oferente en el mercado de servicios de seguridad de la información: se considera como criterio de evaluación la cantidad de años a la fecha de publicación de la licitación en Mercado Público, que lleva prestando servicios de seguridad informática (servicios gestionados, consultorías en seguridad, prestación de horas hombre en la materia, etcétera). Para esto se tomará en cuenta la fecha de inicio de proyecto más antiguo especificado en el Anexo N°3. Solo serán consideradas las fichas debidamente acreditadas.

Experiencia especifica del oferente en el mercado de servicios de seguridad de la información: se considera como criterio de evaluación la cantidad de años a la fecha de publicación de la licitación en Mercado Público, que lleva prestando servicios de seguridad informática (referidos a todos o alguno de los ítems 2,3,4,5 y 6 del componente 1). Para esto se tomará en cuenta la fecha de inicio de proyecto más antiguo especificado en el Anexo N°3. Solo serán consideradas las fichas debidamente acreditadas.

Los criterios evaluados en años consideran años cumplidos a la fecha de publicación de la presente licitación

B. EVALUACIÓN DE LA SOLUCIÓN (65%)				
Ítem	**Criterios**	**Ponderación**	**Subcriterio**	
			Característica	**Puntaje**
Ítem 1 **Servicio SOC** **20%**	La Infraestructura del servicio SOC ofertado cuenta con certificaciones actualizadas de nivel internacional en el ámbito de seguridad informática (como ejemplo ISO 27001, ISO 20000 o certificación CERT), lo cual debe ser acreditado.*	20%	2 o más Certificaciones del SOC	100
			1 Certificación del SOC	70
			Sin Certificación	Inadmisible
	Cobertura del Servicio. Cantidad de SOC certificados que posee el oferente.	20%	3 SOC o más	100
			2 SOC	70
			1 SOC (el ofertado)	0
	Analistas de seguridad con certificaciones nivel 1, en las herramientas con las que entregará el servicio SOC ** (Nivel 1: Herramienta de correlación de eventos Security Information Event Management (SIEM) o similar)	20%	Más de 5 analistas de seguridad informática de nivel 1 certificados en herramienta ofertada.	100
			5 analistas de seguridad informática de nivel 1 certificados en herramienta ofertada.	70
			Entre 1 y 4 analistas de seguridad informática de nivel 1 certificados en herramienta ofertada	50
			No cuenta con analistas de seguridad informática de nivel 1 certificados en la herramienta ofertada	Inadmisible
	Analistas de seguridad con certificaciones para nivel 2, que forman parte del servicio SOC *** (Nivel 2: CCNA Security, Ethical Hacking, pentesting, etc.)	20%	Más de 3 analistas de seguridad con certificaciones nivel 2	100
			2 o 3 analistas de seguridad con certificaciones nivel 2	70
			1 analista de seguridad con certificaciones nivel 2	50
			No cuenta con analistas de seguridad con certificaciones nivel 2	Inadmisible

	Indicar zona de Cuadrante Gartner para SIEM o similar donde se encuentra el Sistema de correlación de eventos a utilizar en el servicio ofertado, en la versión vigente a la fecha de publicación de la licitación.	20%	Cuadrante líder	100
			Cuadrantes Challengers y Visionaries	70
			Cuadrante Niche Players	50
			No se encuentra	Inadmisible

NOTAS:

*Las certificaciones asociadas a la infraestructura SOC deben encontrarse vigentes a la fecha de publicación de la licitación en el portal mercado público, y mantenerse en esta condición durante toda la vigencia del contrato, en caso contrario, se aplicará la multa indicada en el punto 4.2.17 de las Bases Administrativas de Licitación Parte I.

** Se entiende por analistas nivel 1, a aquellos que monitorean y evalúan continuamente las alertas del SOC, para alertarlas y escalarlas al nivel 2, si corresponde.

*** Los analistas nivel 2 determinan si los sistemas se han visto afectados y entregan las recomendaciones de mitigación.

Ítem 2 **Servicio de Prevención y Detección de Intrusos (IPS)** **15%**	Servicio se basa en tecnología con presencia en cuadrante Gartner, categoría “Magic Quadrant for Intrusion Detection and Prevention Systems (IDPS)”, en la versión vigente a la fecha de publicación de la licitación.	30%	Cuadrante Líder	100
			Otro cuadrante	70
			No se encuentra	Inadmisible
	Cantidad de especialistas con certificaciones técnicas en la tecnología IPS con la que entregará el servicio.	40%	Cuenta con más de 1 especialista	100
			Cuenta con 1 especialista	70
			No cuenta con especialista certificado	Inadmisible
	Tecnología efectúa Bypass físico interno ante falla catastrófica del mismo.	30%	Sí	100
			No	0

Ítem 3 **Protección contra ataques de denegación de servicios** **15%**	Cantidad de especialistas con certificaciones técnicas en la solución de servicios de protección contra ataques DDoS con la que entregará el servicio	40%	Cuenta con más de 1 especialista	100
			Cuenta con 1 especialista	70
			No cuenta con especialista certificado	Inadmisible
	Tecnología efectúa Bypass Físico interno ante falla catastrófica del mismo.	20%	Sí	100
			No	0
	Servicio se basa en tecnología con presencia en estudio “DDoS Mitigation Solutions report" de Forrester, en la versión vigente a la fecha de publicación de la licitación.	40%	Zona “Leaders”	100
			Zona “Strong Performers”	60
			Zonas “Contenders” o “Challengers”	30
			No se encuentra	Inadmisible

Ítem 4 **Análisis de vulnerabilidades** **15%**	Cumplimiento de estándares de controles técnicos de seguridad	40%	Entrega cumplimiento de los siguientes estándares: CIS, ISO27001/27002 y NIST	100
			Entrega cumplimiento de alguno de los siguientes estándares: CIS o ISO 27001/27002 o NIST (cumple 1 o 2)	50
			No entrega cumplimiento de estándares CIS o ISO27001/27002 o NIST (0)	Inadmisible
	Opciones de escaneo de vulnerabilidades.	30%	Permite escaneo en modo caja gris (greybox) y caja negra (blackbox)	100
			Sólo permite escaneo en modo Caja negra (blackbox)	0
	Cantidad de aplicaciones de negocio a analizar (Pentest)	30%	Más de 3	100
			2 o 3	70
			1	50
			Ninguna	Inadmisible

Ítem 5 **Servicio de firewall aplicativo WAAP** **15%**	Servicio se basa en tecnología con presencia algún cuadrante de “Gartner Magic Quadrant for WAAP”, en la versión vigente a la fecha de publicación de la licitación,	55%	Cuadrante Líder	100
			Cuadrantes Challengers o Visionaries	70
			Cuadrante Niche Players	50
			No se encuentra	Inadmisible
	Número de especialistas con certificaciones técnicas en las soluciones WAAP con las cuales se entregarán los servicios.	45%	Cuenta con más de 1 especialista certificado	100
			Cuenta con 1 especialista certificado	50
			No cuenta con especialista certificado	0
NOTAS: **Cantidad de especialistas con certificaciones técnicas en la solución WAAP:** Se considera lo indicado por el oferente en el Anexo N° 4 Ficha Curriculum Vitae, con copia de sus certificaciones, para evaluar la cantidad de especialistas con certificaciones en las herramientas asociadas.				

Ítem 6 **Servicio de detección y respuesta de amenazas en red de datos interna (NDR)** **20%**	Servicio se basa en tecnología con presencia algún cuadrante de Gartner o estudio Forrester, en el cual se realice una evaluación y benchmarking de la tecnología del tipo NDR (Network Detect and Response), comparando con otras alternativas de mercado, vigente a la fecha de publicación de la licitación.	50%	Líder	100
			Challengers o Visionaries	70
			Players	50
			No se encuentra	Inadmisible
	Modalidad de inspección del tráfico de datos en la red del SII	20%	Mediante mecanismo no intrusivo, no afectando el flujo normal de los datos en ninguna circunstancia	100
			interviene el flujo de datos, afectando eventualmente dicho flujo en caso de falla	0
	Cantidad de especialistas con certificaciones técnicas en la solución con la que entregará el servicio	30%	Cuenta con más de 1 especialista certificado	100
			Cuenta con 1 especialista certificado	50
			No cuenta con especialista certificado	Inadmisible

NOTA APLICABLE A TODOS LOS CRITERIOS:

Toda certificación asociada al personal presentada como parte de la oferta debe encontrarse vigente a la fecha de publicación de la licitación en el portal mercado público, y mantenerse en esta condición durante toda la vigencia del contrato, en caso contrario, se aplicará la multa indicada en el punto 4.2.17 de las Bases Administrativas de Licitación Parte I.

C. CUMPLIMIENTO DE LOS REQUISITOS DE PRESENTACIÓN DE LAS OFERTAS Y PACTO DE INTEGRIDAD(5%)			
Criterio	**Ponderación**	**Característica**	**Puntaje**
Cumplimiento de los requisitos de presentación de las ofertas	50%	El oferente cumple con todos los requisitos de presentación de la oferta dentro del plazo establecido.	100
		El oferente cumple con todos los requisitos de presentación de la oferta en el plazo adicional otorgado por el SII de acuerdo con lo establecido en el N°3.8 del punto II Bases Administrativas –Parte II.	30
		El oferente no presenta antecedentes o certificaciones que se solicitaren para acreditar una situación no mutable entre el periodo de vencimiento del plazo para presentar ofertas y el periodo de evaluación, o presenta una certificación o antecedente producido con posterioridad al vencimiento del plazo inicial de presentación de las ofertas, en el plazo adicional otorgado por el SII de acuerdo a lo establecido en el N°3.8 del punto II Bases Administrativas –Parte II.	0

Cuenta con Pactos de Integridad compliance; entre otros, para prevenir la corrupción. Indicar en Anexo N°7	50%	El oferente cuenta con planes de integridad; modelo de prevención de delito; programas de compliance; código de ética y son conocidos por su personal.	**100**
		El oferente no cuenta con planes de integridad; modelo de prevención de delito; programas de compliance y solo acredita capacitaciones a su personal en materias relacionadas a cumplimientos normativos; trasparencia, probidad; ética, entre otras materias.	**30**
		El oferente no cuenta o no acredita planes de integridad; modelo de prevención de delito; programas de compliance o de ética, ni tiene capacitaciones en esta materia a sus trabajadores.	**0**

3.3.2.2 Componente 2

	Criterio A Evaluar	Ponderación
Evaluación Técnica (70%)	A. EVALUACIÓN DEL OFERENTE	30%
	B. EVALUACIÓN DE LA SOLUCIÓN	65%
	C. CUMPLIMIENTO DE LOS REQUISITOS DE PRESENTACIÓN DE LAS OFERTAS	5%

A continuación, se detalla la ponderación de cada criterio a evaluar:

A. EVALUACIÓN DEL OFERENTE (30%)			
Criterios		**Subcriterio**	
Ítems	**Ponderación**	**Característica**	**Puntaje**
Cantidad de clientes para los cuales presta servicios de asesoría de seguridad de la información y ciberseguridad	60%	7 o más Clientes	100
		5 o 6 Clientes	70
		2 a 4 Clientes	50
		Menos de 2 Clientes	0
Experiencia del oferente en el mercado en el rubro de servicios de consultoría avanzados en seguridad de la información y ciberseguridad	40%	Más de 6 años	100
		Más de 4 años y hasta 6 años.	70
		Más de 2 años y hasta 4 años	30
		2 años o menos	0

NOTAS:
Cantidad de clientes para los cuales presta servicios de asesoría de seguridad de la información y ciberseguridad: El oferente deberá proporcionar antecedentes sobre su experiencia en prestación de servicios integrales de ciberseguridad, para la componente 2. Adjuntar antecedentes según formato de Anexo N°3 Ficha de experiencia de la empresa.
Experiencia del oferente en el mercado de servicios de seguridad de la información: se considera como criterio de evaluación la cantidad de años a la fecha de publicación de la licitación en Mercado Público, que lleva prestando servicios de consultoría avanzados en seguridad de la información. Para esto se tomará en cuenta la fecha de inicio de proyecto más antiguo asociado a esta componente y que se encuentra especificada en el Anexo N°3, solo serán consideradas las fichas debidamente acreditadas.

Los criterios evaluados en años consideran años cumplidos a la fecha de publicación de la presente licitación.

B. EVALUACIÓN DE LA SOLUCIÓN (65%)			
Servicios Profesionales			
Criterios		**Subcriterio**	
Ítems	**Ponderación**	**Característica**	**Puntaje**
Disponibilidad del Servicio.	30%	7x24x365	100
		7x24 (1)	70
		5x9 (2)	50
		5x8 (2)	30
Certificaciones de reconocimiento internacional del o los **consultores senior en seguridad** de la información tales como, CISSP, CISM, CISA o similar.	40%	Más de 2 certificaciones	100
		1 o 2 certificaciones	50
		Sin certificaciones	Inadmisible
Certificaciones de reconocimiento internacional del o los **consultores senior en ciberseguridad** tales como, CISSP, CISM, CISA o similar.	20%	Más de 2 certificaciones	100
		1 o 2 certificaciones	50
		Sin certificaciones	Inadmisible
Certificaciones del o los **consultores junior en seguridad TI,** tales como, Diplomados, cursos de especialización, certificaciones internacionales u otros asociados a seguridad TI.	10%	Más de 2 certificaciones	100
		1 o 2 certificaciones	50
		Sin certificaciones	Inadmisible

(1) Se consideran días de lunes a domingo, exceptuando días festivos.
(2) Se consideran los horarios, los días hábiles de lunes a viernes, de 09:00 a 18:00 horas para el horario de 5x8 y de 08:30 a 18:30 horas para el horario de 5x9, considerando 1 hora de almuerzo.

NOTAS:

Para los criterios de certificación de personal, se considera lo indicado por el oferente en el Anexo N° 4 Ficha Curriculum vitae, con copia de sus certificaciones, se evalúa la cantidad total de certificaciones presentadas y vigentes, según corresponda.

Toda certificación asociada al personal presentada como parte de la oferta debe encontrarse vigente a la fecha de publicación de la licitación en el portal mercado público, y mantenerse en esta condición durante toda la vigencia del contrato, en caso contrario, se aplicará la multa indicada en el punto 4.2.17 de las Bases Administrativas de Licitación Parte I.

C. CUMPLIMIENTO DE LOS REQUISITOS DE PRESENTACIÓN DE LAS OFERTAS Y PACTO DE INTEGRIDAD (5%)			
Criterio	**Ponderación**	**Característica**	**Puntaje**
Cumplimiento de los	50%	El oferente cumple con todos los requisitos de presentación de la oferta dentro del plazo establecido.	100

requisitos de presentación de las ofertas		El oferente cumple con todos los requisitos de presentación de la oferta en el plazo adicional otorgado por el SII de acuerdo con lo establecido en el N°3.8 del punto II Bases Administrativas –Parte II.	30
		El oferente no presenta antecedentes o certificaciones que se solicitaren para acreditar una situación no mutable entre el periodo de vencimiento del plazo para presentar ofertas y el periodo de evaluación, o presenta una certificación o antecedente producido con posterioridad al vencimiento del plazo inicial de presentación de las ofertas, en el plazo adicional otorgado por el SII de acuerdo a lo establecido en el N°3.8 del punto II Bases Administrativas –Parte II.	0
Cuenta con Pactos de Integridad compliance; entre otros, para prevenir la corrupción. Indicar en Anexo N°7	50%	El oferente cuenta con planes de integridad; modelo de prevención de delito; programas de compliance; código de ética y son conocidos por su personal.	**100**
		El oferente no cuenta con planes de integridad; modelo de prevención de delito; programas de compliance y solo acredita capacitaciones a su personal en materias relacionadas a cumplimientos normativos; trasparencia, probidad; ética, entre otras materias.	**30**
		El oferente no cuenta o no acredita planes de integridad; modelo de prevención de delito; programas de compliance o de ética, ni tiene capacitaciones en esta materia a sus trabajadores.	**0**

3.3.3 Evaluación económica (30%)

Para efectos de la evaluación económica, ésta se realizará teniendo en cuenta lo siguiente:

- Se evaluará solo las ofertas admisibles técnicamente.
- Cada oferente contará con 3 propuestas económicas, las cuales corresponderán a lo siguiente:

  Oferta tipo A: {Valor Componente 1} + {Valor Componente 2 opción 1404 UT}

  Oferta tipo B: {Valor Componente 1} + {Valor Componente 2 opción 1224 UT}

  Oferta tipo C: {Valor Componente 1} + {Valor Componente 2 opción 1008 UT}

El puntaje de cada tipo de oferta económica (A, B, y C) se calculará de acuerdo con la siguiente fórmula:

$Puntaje\ oferta\ económica$ tipo A i = ($Oferta\ mínima$ tipo A / $Oferta\ económica$ tipo A "i") x 100
$Puntaje\ oferta\ económica$ tipo B i = ($Oferta\ mínima$ tipo B / $Oferta\ económica$ tipo B "i") x 100
$Puntaje\ oferta\ económica$ tipo C i = ($Oferta\ mínima$ tipo C / $Oferta\ económica$ tipo C "i") x 100

Dónde:
Puntaje oferta económica tipo X i: *Puntaje asociado a la oferta económica tipo X* ***"i"***
Oferta mínima tipo X*: Precio de la oferta más económica entre todas las ofertas tipo X*
Oferta económica tipo X *i: Precio de la oferta económica tipo X del oferente* ***"i"***

3.3.4 Puntaje final de la evaluación técnico-económica

El puntaje final de las ofertas presentadas por las empresas corresponde al resultado de la aplicación de los criterios de evaluación técnicos y económicos antes enunciados, según las siguientes ponderaciones:

Teniendo en cuenta que para el componente 2 se evalúan tres alternativas diferentes, se obtendrá un total de 3 evaluaciones finales por cada oferente, las que corresponden a lo siguiente:

Evaluación Final Oferta Tipo A = 70%(Evaluación técnica) + 30%(Evaluación Económica Oferta tipo A)

Evaluación Final Oferta Tipo B = 70%(Evaluación técnica) + 30%(Evaluación Económica Oferta tipo B)

Evaluación Final Oferta Tipo C = 70%(Evaluación técnica) + 30%(Evaluación Económica Oferta tipo C)

3.4 Adjudicación

El SII adjudicará, a un solo oferente, los ítems 1, 2, 3, 4, 5 y 6 del componente 1 y una de las alternativas del componente 2,

La opción adjudicada (Oferta tipo A, B o C) será la que mejor se ajuste de manera inferior y más cercana al presupuesto disponible (**$2.100.000.000**, incluyendo los impuestos respectivos) en la presente licitación, y de acuerdo al siguiente orden de prelación:

Oferta tipo A: Componente 1 + Componente 2 opción 1404 UT

Oferta tipo B: Componente 1 + Componente 2 opción 1224 UT

Oferta tipo C: Componente 1 + Componente 2 opción 1008 UT

Considerando que la oferta se debe ingresar en Unidades de Fomento, para efectos de la comparación y adjudicación respecto del presupuesto máximo, el valor de la oferta de cada proponente se convertirá a pesos chilenos tomando como referencia el valor de la UF al día de publicación de la presente licitación pública.

De esta manera, el Servicio adjudicará la licitación a la oferta mejor evaluada, que se encuentre dentro del presupuesto máximo disponible, y de acuerdo con las opciones señaladas anteriormente.

Criterio de desempate por componente: En caso de que dos o más empresas obtengan el mismo puntaje final, se privilegiará la oferta de la empresa con un mayor puntaje final en la componente 1; si en este caso, hay igualdad, se optará por la oferta que presente mayor puntaje en el criterio técnico “Evaluación de la Solución” de la componente 1. De mantenerse el empate, se adjudicará el componente a la oferta con un mayor puntaje en el criterio técnico “Evaluación del Oferente” de la componente 1.

En caso de aún persistir el empate, el Servicio adjudicará a la oferta que primero se haya presentado por medio del portal Mercado Público

4. DISPOSICIONES CONTRACTUALES

4.1 Precio y Forma de Pago

4.1.1 Precio:

El precio total del contrato será igual al precio mensual adjudicado para todos los componentes e ítems por un plazo 36 meses, el cual estará expresado en Unidades de Fomento.

El Servicio pagará los precios convenidos en el contrato, en su equivalente en pesos con impuestos incluidos, al valor de la Unidad de Fomento publicado por el Banco Central el día de emisión de las facturas respectivas.

4.1.2 Forma de Pago:

Los pagos se realizarán **mensualmente por períodos vencidos**, de acuerdo con el valor mensual ofertado por el adjudicatario en el Anexo N° 2 "Propuesta Económica".

El procedimiento de pago se regirá de acuerdo con lo siguiente:

1. La recepción conforme de los servicios se realizará en el portal Mercado Público.

2. **Para lo anterior, el Administrador del Contrato del SII notificará al Depto. de Adquisiciones, mediante el "*Formulario de Recepción Conforme*", de la prestación satisfactoria de los servicios, procediendo este último a realizarla en el portal Mercado Público**. Cabe señalar, que la recepción conforme del bien y/o servicio implica la entrega por parte de la empresa de todos los documentos contractuales exigidos en las bases de licitación como parte de su ejecución.
3. Posterior a la recepción conforme de la Orden de Compra en el portal Mercado Público, la EMPRESA podrá emitir la factura respectiva.

La factura electrónica debe indicar claramente:

1. El número del contrato (N° interno del SII) o el N° de la Orden de Compra, en la sección "E.- INFORMACIÓN DE REFERENCIA", específicamente en el campo "Folio de Referencia" del XML de facturación electrónica.
2. El hito al cual corresponde el pago y una breve glosa descriptiva del pago correspondiente, en la sección "A.- ENCABEZADO.", específicamente en el campo "Glosa descripción Pago" del XML de facturación electrónica.

La ausencia de esta información será motivo de rechazo del documento.

Recepcionado el Documento Tributario en los servidores del Servicio de Impuestos Internos, el Depto. de Finanzas verificará aspectos formales, tales como, nombre o razón social, Rut, dirección, comuna, ciudad y fecha. De existir error en ellos, se procederá a rechazar el documento mediante el portal del SII. Caso contrario, se enviará la factura a la contraparte técnica del SII para revisión de requisitos de pago y validación, quien verificará que los valores y productos o servicios se encuentren de acuerdo con lo contratado y de toda la documentación exigida contractualmente para procesar el pago.

Si se cumplen los requisitos de pago, y la factura se encuentra conforme, el Administrador del Contrato del SII enviará al Depto. de Finanzas el documento tributario visado, junto con el o los respaldos que acrediten la recepción conforme de la OC en el portal Mercado Público.

Por su parte, para proceder al pago, el Depto. de Finanzas verificará que:

1. La orden de compra enviada se encuentre en estado Recepción Conforme en el portal Mercado Público para cada mensualidad.

2. La factura esté expresada en pesos chilenos, de acuerdo al valor de la Unidad de Fomento al día de emisión de las facturas respectivas.
3. La factura cuente con el visto bueno del Jefe de Departamento Informática Aseguramiento Estándares Tecnológicos de la Subdirección de Informática.

En caso de atraso o no pago de las obligaciones laborales con los trabajadores, el Servicio estará facultado para retener los montos adeudados, y pagar directamente las cotizaciones pendientes a cuenta del empleador. Lo anterior en virtud de lo dispuesto en los Artículos 183-A, 183-B y 183-C del Código del Trabajo.

El pago será efectuado dentro del plazo de 30 días corridos a contar de la fecha de recepción del Documento Tributario en los servidores del Servicio de Impuestos Internos y se efectuará a la EMPRESA por medio de transferencia electrónica a la cuenta corriente informada por el adjudicatario al momento de la suscripción del contrato. En caso de que, durante la ejecución del contrato el medio de transferencia electrónica cambie, es obligación de la EMPRESA indicar una nueva cuenta bancaria enviando un correo electrónico a tesoreria@sii.cl

No obstante, a lo señalado, el Servicio podrá objetar o reclamar respecto al contenido de la factura, mediante los procedimientos señalados en el artículo 3° de la Ley N° 19.983, dentro de los 8 días corridos siguientes de la recepción del Documento Tributario, entendiéndose que después de ese plazo la factura se tendrá por irrevocablemente aceptada, siendo responsabilidad del adjudicatario validar el estado de aceptación o reclamo de sus documentos en el portal del SII.

4.2 Multas

Las multas presentadas a continuación no son excluyentes entre sí. Para el pago de las multas se considerará el valor de la UF del día del pago.

Las multas que se apliquen no podrán superar el 30% del monto total del contrato. En caso de superarse dicho porcentaje, se considerará un incumplimiento grave de las obligaciones del contrato, de conformidad al punto 4.8.1 de las Bases Administrativas – Parte II.

4.2.1 Multas por atraso en la reposición de servicios de la componente 1 ítem 1 (SOC).

El servicio para la componente 1 contempla un máximo para la **reposición de servicios** de **3 horas**, contadas desde el aviso del SII, respaldado por correo en donde quede constancia de la fecha y hora del aviso.

En caso de no cumplir con el plazo señalado, se aplicará una multa de 3 UF cumplida la primera hora y el mismo monto por cada fracción de hora sucesiva.

En caso de que el atraso exceda de 24 horas completas, el valor de la hora de atraso se aumentará a 5 UF.

Ejemplo: para el caso de 25 horas de atraso la multa aplicada corresponderá a 125 UF.

4.2.2 Multas por atraso en la entrega de reportes establecidos en la componente 1 ítem 1 (SOC).

En caso de que el adjudicatario no cumpla con los plazos de entrega de reportes indicados en la letra j) del punto 2.1 Bases Técnicas (reporte semanal y mensual), le será aplicada una multa equivalente al 3 UF por cada día corrido de atraso.

El plazo de entrega para el reporte semanal es hasta las 18:30 hrs., del segundo día hábil de la semana siguiente.

Ejemplo: Si el adjudicatario entrega el reporte semanal el segundo día hábil de la semana siguiente en un horario de 19:00 hrs, se computará como un día de atraso.

El plazo de entrega para el reporte mensual es: hasta el quinto día corrido del mes siguiente.

4.2.3 Multas por no informar incidentes de seguridad según lo establecido en la componente 1 ítem 1 (SOC).

En caso de que el adjudicatario no informase al Servicio de Impuestos Internos de un incidente de seguridad en el plazo establecido para ello (20 minutos desde ocurrido) o no lo reportó, y el SII detectare su existencia se le aplicará una multa equivalente al 5% del valor mensual establecido para la componente 1 ítem 1, por cada ocasión en que suceda la situación descrita.

4.2.4 Multas de indisponibilidad del servicio SOC de la componente 1 ítem 1 (SOC)

En caso de que el servicio de SOC presente una disponibilidad anual inferior a 99,9% (uptime), se aplicará una multa de acuerdo con el siguiente cuadro:

Porcentaje de uptime anual	Multa
99,9% o superior	Sin multa.
95,9% e inferior a 99,9%	0,5 % del valor anual del contrato.
90,1% e inferior a 95,9%	1 % del valor anual del contrato.
Inferior 90,1%	2 % del valor anual del contrato.

El uptime anual será verificado por el SII cada 12 meses corridos de contrato, contados desde la recepción conforme de la instalación.

4.2.5 Multa por atraso en la entrega de registros LOGS establecidos para la componente 1 ítem 1 (SOC)

En caso de que el adjudicatario no cumpla con los plazos para la entrega de los registros LOGS, se aplicará una multa de acuerdo con lo siguiente:

Para LOGS de almacenamiento online, el plazo de entrega es de 1 día corrido desde la hora y fecha de realizada la solicitud. En caso de atraso, se aplicará una multa de 1 UF por día corrido.

Para LOGS almacenados, el plazo de entrega es máximo de 5 días corridos desde la hora y fecha realizada la solicitud. En caso de atraso, se aplicará una multa de 2 UF por día corrido.

Ejemplo: Para LOGS de almacenamiento online; si la solicitud fue realizada el lunes a las 08:00 hrs, y el registro LOGS es entregado el martes a las 10:00 hrs, se aplicará la multa correspondiente por un día de atraso.

Para el caso de LOGS almacenados se aplica el mismo criterio, considerando el plazo de entrega contemplado para éste.

4.2.6 Multa por atraso en la presentación del reporte por correo electrónico según lo establecido en la componente 1 ítem 1 (SOC)

En caso de que el adjudicatario no cumpla con la presentación del reporte por correo electrónico al SII (punto 2.1.1 de las bases técnicas, apartado “incidentes), dentro del plazo máximo de 40 minutos desde detectado el incidente, se aplicará una multa de 0,2 UF, por cada 20 minutos de atraso y/o fracción de este tiempo.

4.2.7 Multas por atraso en la atención especializada mediante soporte telefónico, según lo establecido en la componente 1 ítems 2,3,4,5 y 6

En caso de que el adjudicatario no cumpla con la atención del soporte telefónico especializado dentro de un periodo máximo de 20 minutos contados desde el requerimiento, se aplicará una multa de acuerdo con lo siguiente. Al minuto 21 corresponde aplicar una multa de 1 UF, luego se aplicará una multa equivalente a 1 UF por fracción de 10 minutos adicional de atraso.

4.2.8 Multas por atraso en el escalamiento para la atención de problemas críticos según lo establecido en la componente 1 ítems 2,3,4,5 y 6

En caso de que el adjudicatario no cumpla con el escalamiento de problemas críticos (involucramiento del centro de soporte del fabricante), dentro de un plazo máximo de 2 horas desde el requerimiento, se aplicará una multa de 2 UF cumplida la primera hora y el mismo monto por cada fracción de hora sucesiva .

4.2.9 Multas por atraso en la asistencia onsite según lo establecido en la componente 1 ítems 2,3,4,5 y 6

En caso de que el adjudicatario no cumpla con la asistencia onsite de personal especializado dentro de un plazo máximo de 2 horas corridas desde el requerimiento, se aplicará una multa de 2 UF cumplida la primera hora y el mismo monto por cada fracción de hora sucesiva.

4.2.10 Multas por atraso en la reposición de servicios según lo establecido en la componente 1 ítems 2,3,4,5 y 6

La componente 1 ítems 2, 3, 4, 5 y 6, contempla un máximo para la **reposición de servicios** de **5 horas**, contados desde el aviso del SII, respaldado por correo electrónico, u otro medio escrito en donde quede constancia de la fecha y hora del aviso

En caso de no cumplir con el plazo señalado, se aplicará una multa de 3 UF cumplida la primera hora y el mismo monto por cada fracción de hora sucesiva.

En caso de que el atraso exceda de 24 horas completas, el valor de la hora de atraso se aumentará a 5 UF.

Ejemplo: para el caso de 25 horas de atraso la multa aplicada corresponderá a 125 UF (5UF*25 horas).

4.2.11 Multas por atraso en alerta de vulnerabilidades según lo establecido en componente 1, ítem 4

En caso de que el adjudicatario no informase al Servicio de Impuestos Internos la detección de una vulnerabilidad, dentro del plazo máximo de 1 hora desde su detección y el SII descubriera su existencia, se aplicará una multa por cada ocasión en que esto suceda correspondiente al 2 % del valor mensual de la componente 1, ítem 4.

4.2.12 Multa por atraso en la entrega de reporte de análisis de vulnerabilidad en el perímetro según lo establecido en la componente 1, ítem 4

En caso de que el adjudicatario no realice la entrega del reporte de vulnerabilidades en el plazo solicitado para ello, se le aplicará una multa correspondiente al 1 % del valor mensual del componente 1, ítem 4 por cada día corrido de atraso.

El plazo de entrega máximo para el reporte del análisis de vulnerabilidad es al día siguiente de la realización del análisis, hasta las 18:30 hrs.

Ejemplo: Si el análisis de vulnerabilidad en el perímetro ocurre un sábado a las 13:00 hrs, y el adjudicatario entrega el reporte un día domingo a las 19:00 hrs, se computará como atraso en la entrega del reporte, correspondiendo aplicar la multa.

4.2.13 Multa por atraso en la entrega del reporte de análisis de vulnerabilidad en activos internos según lo establecido en la componente 1, ítem 4

En caso de que el adjudicatario no realice la entrega del reporte de vulnerabilidades en un plazo máximo de 5 días corridos desde ejecutado el análisis hasta las 18:30 del quinto día corrido, le será aplicada una multa equivalente a 2 UF por cada día corrido de atraso.

4.2.14 Multas de indisponibilidad del servicio de la componente 1, ítems 2, 3, 5 y 6

En caso de que el servicio presente una disponibilidad anual inferior a 99,6% (uptime), se aplicará una multa de acuerdo con el siguiente cuadro:

Porcentaje de uptime anual	Multa
99,6% o superior	Sin multa.
95,9% e inferior a 99,6%	0,5 % del valor anual del contrato.

90,1% e inferior a 95,9%	1 % del valor anual del contrato.
Inferior 90,1%	3 % del valor anual del contrato.

El uptime anual será verificado por el SII cada 12 meses corridos de contrato, contados desde la recepción conforme de la instalación

4.2.15 Multas por atraso en la instalación y puesta en marcha de los servicios componente 1

En caso de que el adjudicatario no cumpla con el plazo propuesto para la correcta puesta en marcha de los servicios suministrados por la componente 1, por causas imputables a este, se aplicará una multa 15 UF por cada día corrido de atraso.

En caso de que el atraso exceda de 10 días corridos completos, se incrementará la multa a 20 UF por día.

Por ejemplo, para 12 días de atraso el valor de la multa aplicada será de 240 UF (20UF*12 días).

4.2.16 Multas por iteración de informes de la componente 2

Al pasar de la tercera iteración de un informe generado por la solicitud de servicios profesionales se aplicará una multa de 0,5 % del valor mensual establecido para la componente 2 por cada iteración adicional. Por ejemplo, si un informe fue iterado por correcciones 5 veces, corresponderá (5-3)*0,5%=1% de valor mensual del contrato. El medio de verificación de las iteraciones por este motivo corresponde a correos electrónicos enviados al adjudicatario solicitando alguna corrección en el informe.

4.2.17 Multas por incumplimiento en la obligación de mantener vigentes las certificaciones asociadas al servicio

Constatado el vencimiento de alguna de las certificaciones asociadas al personal, o alguna certificación asociada a la infraestructura del SOC ofertado, y sin que el adjudicatario haya revalidado dichas certificaciones, se aplicará por cada evento una multa equivalente al 5% del valor mensual del ítem o componente que corresponda, hasta que obtenga la nueva certificación.

La aplicación de esta multa no eximirá al adjudicatario de la obligación de mantener vigente las certificaciones informadas en la oferta, para lo cual tendrá un plazo de 4 meses desde el término de la vigencia de éstas para revalidarlas, plazo en el cual no se aplicará la presente multa. Dicho plazo podrá ser extendido, en la medida que al adjudicatario alegue que el tiempo de revalidación es más amplio, lo cual deberá ser acreditado por la empresa certificadora.
En caso de no revalidar la certificación en el plazo señalado se aplicará la multa indicada en el párrafo primero.

4.3 Vigencia del contrato

El contrato regirá desde la total tramitación del acto administrativo que lo aprueba y su vigencia se extenderá hasta los 36 meses posteriores a la recepción conforme de la instalación y puesta en marcha de todos los servicios contratados.

4.4 Plazo de puesta en marcha de los servicios contratados

El plazo máximo para la puesta en marcha de los servicios contratados es de 60 días corridos contados desde la **primera reunión de coordinación entre el Servicio y el adjudicatario la que se realizará en un plazo máximo de 10 días hábiles contados desde la total tramitación de la resolución que aprueba el contrato**. La fecha de la reunión de coordinación constara en acta emitida por el SII y firmada por los administradores del contrato.

Al momento de la primera reunión de coordinación el adjudicatario deberá hacer entrega de una **carta gantt y un plan de instalación y puesta en marcha**, en el que se incluya un protocolo de pruebas, considerando todas las que éste estime necesarias. El plazo de puesta en marcha indicado en la carta Gantt debe ser coincidente con el plazo máximo solicitado.

En caso de que la puesta en marcha de los servicios coincida con los periodos de freezing[1] del Servicio de Impuestos Internos, los plazos contemplados previamente, se suspenderán por la cantidad de días que correspondan al evento, de lo que se dejará constancia en un Acta de Suspensión firmada por los administradores de contrato de ambas partes.

4.5 Confidencialidad

El adjudicatario, sus consultores, profesionales, y personal que se encuentre ligado al proyecto objeto de la presente contratación, deberá guardar estricta reserva y confidencialidad de los antecedentes, resultados e informes que conozcan o se obtengan con motivo de la ejecución del contrato, tanto del SII como de los contribuyentes.

Toda información relativa al SII o a contribuyentes, que con motivo de la ejecución de la presente contratación conociere y/o procesare el adjudicatario a través de su personal, revestirá para todos los efectos legales del contrato, el carácter de confidencial y no podrá ser divulgada por el adjudicatario, sus asociados y demás personas relacionadas de ninguna forma durante la vigencia de la contratación y una vez terminada ésta, de acuerdo a lo señalado en los artículos 30 y 206 del Código Tributario.

A tal efecto, el adjudicatario deberá adoptar las medidas necesarias para garantizar la confidencialidad y reserva de la información a que acceda él y/o las personas señaladas anteriormente, por cuanto responde por el hecho o culpa de sus empleados, cualquiera sea el vínculo que los una, que infringieren las obligaciones de confidencialidad.

En caso alguno, y con motivo de la información confidencial a que accede el adjudicatario, podrá ejercer funciones administradoras y fiscalizadoras del cumplimiento del sistema tributario. En tal sentido, no podrá asumir labores propias de la fiscalización de los contribuyentes, tener acceso a los procesos de fiscalización, adoptar decisiones para la aplicación del sistema tributario ni en la resolución de conflictos que surjan con la Administración Tributaria respecto de dicho cumplimiento ni otras funciones análogas a las mencionadas.

El adjudicatario debe comunicar inmediatamente y por escrito al SII, acerca de la ocurrencia de cualquier acto, hecho u omisión que constituya una infracción a la obligación asumida precedentemente, sea por acciones u omisiones propias, de sus dependientes o de tercero. Asimismo, el adjudicatario deberá impetrar todas las medidas que fueren necesarias y cooperar en todo lo necesario para que, en el evento que todo o parte de la Información Confidencial hubiere sido divulgada, el daño sea reparado.

En caso de infracción al deber de confidencialidad, el SII se reserva el derecho de ejercer las acciones legales que correspondan, de acuerdo a las normas legales vigentes, persiguiendo las responsabilidades que procedan (Civil – Penal u otra), de acuerdo la normativa vigente. En este sentido, se deja constancia que, respecto del acceso y procesamiento de declaraciones, la infracción a esta obligación será sancionada con reclusión menor en su grado medio y multa de 5 a 100 UTM, de acuerdo a lo dispuesto en el inciso quinto del artículo 30 del Código Tributario.

El adjudicatario siempre deberá garantizar el pago de esta sanción a través de una boleta bancaria u otra garantía suficiente.

---

1 Freezing: Hace referencia a congelamiento de intervenciones físicas en los Datacenter del SII durante periodos críticos para el negocio. Las fechas definidas como periodo de freezing corresponden al Periodo de Renta, desde el 15 de febrero al 15 de mayo de cada año, ambas fechas inclusive. Además, se considera el Vencimiento de IVA, correspondiente al día 12 y 20 de cada mes. En caso de que dicho día sea sábado, domingo o festivo, se traslada automáticamente para el día hábil siguiente.

De igual forma, en casos calificados, el SII podrá exigir al adjudicatario la suscripción de un Acuerdo Confidencial que regule de forma más detallada esta materia, el cual contendrá - entre otros puntos – el acceso a la información que se habilitará, la definición de confidencialidad; documentos e información que reviste tal carácter; alcances de las prohibiciones; sanciones ante incumplimientos; deber de restitución de la información.

Como parte de las obligaciones de la contratación, el adjudicatario deberá restituir al SII, sin más trámite y a más tardar en el último día de vigencia del contrato, toda la documentación e información que le haya sido entregada, junto con todas las copias escritas o registradas por cualquier medio magnético u otro, que se encuentre en su poder y/o colaboradores. Cuando por motivos razonables y fundados, la devolución de la información fuese impracticable, el adjudicatario cumplirá con esta obligación, destruyendo la información, de lo cual debe dejarse constancia y emitirse un certificado a nombre del SII.

Se entenderá por incumplimiento grave de las obligaciones del contrato, la infracción al deber de confidencialidad y la no restitución o destrucción de la información, lo que habilita al SII para poner término anticipado al contrato y hacer efectiva la garantía de fiel cumplimiento del contrato, sin perjuicio de ejercer las demás acciones que estime convenientes en resguardo del interés fiscal.

4.6 Administración de Contrato

El Jefe del Departamento Informática Aseguramiento de Estándares Tecnológicos de la Subdirección de Informática, designará un Administrador del Contrato, el cual actuará como contraparte técnica y como encargado de la ejecución del contrato, conjuntamente con el Administrador del Contrato que designe el adjudicatario. Estos administradores no podrán modificar el contrato, y en conjunto, les corresponderá ejercer las siguientes funciones principales:

- Representar a las partes en la discusión de las materias relacionadas con la ejecución del contrato.
- Supervisar el cumplimiento de los procedimientos establecidos por el SII en las presentes Bases de Licitación, para la oportuna entrega de los productos contratados.
- Fiscalizar el estricto cumplimiento del contrato respectivo.

Los administradores del contrato del adjudicatario y del SII, actuarán como representantes, sólo para los efectos de la administración del desarrollo y ejecución del proyecto, a partir de la fecha de inicio de los trabajos y su designación deberá contar con la aprobación del Servicio. En caso de ausencia o cambio del encargado de la Administración del Contrato de alguna de las partes, dicha circunstancia deberá ser comunicada a la contraparte con la debida antelación mediante correo electrónico. Lo anterior, sin perjuicio de la participación de los representantes legales cuando ella se requiera.

4.7 Servicios adicionales.

El SII podrá contratar servicios profesionales no incluidos en la componente 2. En este caso, el adjudicatario deberá mantener los precios y características ofrecidas en el Anexo N° 2. Las condiciones económicas con relación a los precios sólo podrán ser modificadas a favor del Servicio y con consentimiento de éste.
Los servicios adicionales serán originados por la necesidad de realizar mejoras que el SII estime convenientes para la operación de los servicios contratados. Para estos efectos, el adjudicatario deberá elaborar y presentar un presupuesto detallado de los servicios adicionales, el cual podrá ser aceptado o rechazado por el SII, mediante el administrador designado para este contrato.

Los servicios adicionales serán proporcionados a solicitud del Servicio, y su precio no podrá superar el 30% del valor total del contrato. Los servicios serán formalizados mediante una modificación del contrato.

4.8 Revisión del estado de las certificaciones

El SII realizará un proceso de revisión de certificaciones, con el fin de validar que el servicio contratado mantenga en estado vigente las certificaciones de la infraestructura de SOC ofertado, como también, las del personal asociado a la prestación del servicio.

Esta revisión corresponderá a un proceso formal, en el cual el SII solicitará con al menos 30 días de anticipación al vencimiento de una certificación la presentación de algún documento que acredite la revalidación de esta. La solicitud se realizará mediante correo electrónico y el oferente tendrá 10 días corridos para presentar la documentación solicitada.
El plazo estándar para obtener la revalidación de las certificaciones será de 4 meses, contados desde su vencimiento, a menos que el adjudicatario solicite su ampliación y acredite que el tiempo extra tiene relación con la empresa certificadora. Para ello, deberá presentar documentos que acrediten dicha circunstancia.
El incumplimiento de esta obligación se encuentra sujeta a la multa establecida en el punto 4.2.17 de las presentas bases de licitación.

4.9 Reporte de Incidentes

En virtud de lo dispuesto en el artículo 3 del Decreto 273, de 2022 del Ministerio del Interior y Seguridad Pública, el adjudicatario deberá informar al administrador del contrato del SII, de forma inmediata de cualquier actividad o hecho que **amenace, vulnere y/o afecte a las redes**, **plataformas y sistemas informáticos a los cuales tenga acceso, le pertenezcan o no al SII.** De igual manera, deben indicar las medidas de mitigación aplicadas a éstas, así como las políticas y prácticas de seguridad de la información incorporadas en los servicios prestados. Dicha acción es una obligación contractual que se encuentra sujeta a término anticipado en caso de incumplimiento.

4.10 Propiedad de la información

El SII será la titular de todos los datos de transacciones, bitácoras (logs), parámetros, documentos, documentos electrónicos y archivos adjuntos y, en general, de las bases de datos y de toda información contenida en la infraestructura física y tecnológica que le suministre el adjudicatario y que se genere en virtud de la ejecución de los servicios objeto de la contratación.

La EMPRESA no podrá utilizar la información indicada en el párrafo anterior, durante la ejecución del contrato ni con posterioridad al término de su vigencia, sin autorización escrita del SII. Por tal motivo, una vez que el adjudicatario entregue dicha información a la entidad o al finalizar la relación contractual, deberá borrarla de sus registros lógicos y físicos.

Asimismo, la EMPRESA deberá consignar la destrucción de la información en un documento, que deberá ser entregado dentro los últimos 10 días corridos de contrato, en caso de que sea solicitado por el SII.

4.11 Protección de datos personales

El adjudicatario se compromete a tratar los datos con la finalidad exclusiva de la realización del servicio. Una vez realizada la prestación del servicio, se compromete a destruir los datos proporcionados por el SII, así como el resultado de cualquier elaboración de los mismos y los soportes o documentos en que se halle recogida la información.

El adjudicatario se obliga a utilizar los datos a los que le dé acceso el SII única y exclusivamente para los fines del presente contrato y a guardar secreto profesional respecto a todos los datos de carácter personal que conozca y a los que tenga acceso durante la realización del contrato de prestación de servicios. Igualmente, se obliga a custodiar e impedir el acceso a los datos de carácter personal a cualquier tercero ajeno al presente contrato. Las anteriores obligaciones se extienden a toda persona que pudiera intervenir en cualquier fase del tratamiento por cuenta de la empresa y subsistirán aun después de terminados los tratamientos efectuados en el marco del presente contrato.

El adjudicatario, además, se compromete a comunicar y hacer cumplir a sus empleados, asignados al proyecto, las obligaciones establecidas en esta cláusula. Cualquier uso de los datos que no se ajuste a lo dispuesto en la presente cláusula, será responsabilidad exclusiva de la empresa frente a terceros y frente al SII, ante la que responderá por los daños y perjuicios que le hubiere podido causar, siendo considerado también responsable del tratamiento a estos efectos.

4.12 Normas laborales

El adjudicatario, en su calidad de empleador, será responsable exclusivo del cumplimiento íntegro y oportuno de las normas del Código del Trabajo y leyes complementarias, leyes sociales, de previsión, de seguros, de enfermedades profesionales, de accidentes del trabajo y demás pertinentes respecto de sus trabajadores y/o integrantes de sus respectivos equipos de trabajo. En consecuencia, el adjudicatario será responsable, en forma exclusiva, y sin que la enumeración sea taxativa, del pago oportuno de las remuneraciones, honorarios, indemnizaciones, desahucios, gratificaciones, gastos de movilización, beneficios y, en general, de toda suma de dinero que, por cualquier concepto, deba pagarse a sus trabajadores y/o integrantes de sus respectivos equipos de trabajo.

El SII se reserva el derecho a exigir al contratista, a simple requerimiento de la contraparte técnica, y sin perjuicio de lo dispuesto en el artículo 4° de la Ley de Compras y el artículo 183-C del Código del Trabajo, un certificado que acredite el monto y estado de cumplimiento de las obligaciones laborales y previsionales emitido por la Dirección del Trabajo respectiva, o bien, por medios idóneos que garanticen la veracidad de dicho monto y estado de cumplimiento, respecto de sus trabajadores. Ello, con el propósito de hacer efectivo por parte del órgano comprador, su derecho a ser informado y el derecho de retención, consagrados en los incisos segundo y tercero del artículo 183-C del Código del Trabajo, en el marco de la responsabilidad subsidiaria derivada de dichas obligaciones laborales y previsionales, a la que alude el artículo 183-D del mismo Código.

Por otra parte, se deja expresa constancia que la suscripción del contrato respectivo no significará en caso alguno que el adjudicatario, sus trabajadores o integrantes de los equipos presentados por éstos, adquieran la calidad de funcionarios públicos, no existiendo vínculo alguno de subordinación o dependencia de ellos con el SII.

4.13 Gestión de Proveedores del SII

Respecto al Sistema de Gestión de Igualdad de Género y Conciliación de la vida laboral, familiar y personal (SGIGC) existente en el SII, frente a eventuales situaciones de maltrato, acoso laboral, acoso sexual o prácticas discriminatorias que involucren a Proveedores/as o personal contratado o subcontratado por estos, deberán remitirse a lo indicado en el punto 6.3 del Procedimiento de Gestión de Proveedores. Este procedimiento quedará disponible en el portal Mercado Público una vez haya finalizado el proceso de esta contratación y que adicionalmente el Administrador de Contrato del SII se encargará de remarcar o recordar en la reunión de inicio o en el desarrollo de la presente contratación.

II. BASES ADMINISTRATIVAS – PARTE II

1. ANTECEDENTES Y CONDICIONES GENERALES

1.1. De las bases de la licitación

Las presentes bases de licitación contienen las disposiciones generales que regirán las relaciones entre el "Servicio de Impuestos Internos", en adelante el "Servicio" o indistintamente el "SII", y los proveedores a que se refiere la presente licitación, en adelante "proponentes", "oferentes", "consultores", "contratistas", "participantes" o "empresa", durante el proceso y en todas las materias relacionadas con esta licitación.

Para que una oferta o postulación se considere válida, deberá cumplir con las disposiciones de las presentes bases administrativas y de las bases técnicas, en lo sucesivo "bases".

La presentación de una propuesta, implica para la persona natural o jurídica que haga una oferta, la aceptación de las presentes bases.

Los plazos que se establecen en las bases son de días hábiles a menos que expresamente se señale lo contrario. Se entenderán inhábiles, en conformidad a lo dispuesto en el Artículo 25 de la Ley 19.880, los días sábado, domingo y festivo. Cuando los plazos fijados para el cumplimiento del contrato, se expresen en días corridos y finalicen en días sábados, domingos o festivos, se entenderán prorrogados para el primer día hábil siguiente.

1.2. Normas generales

Esta licitación y la realización de su objeto, se regirá por los siguientes documentos:

a. Las bases administrativas y su Ficha Ejecutiva
b. Las bases técnicas
c. Los anexos de las bases de licitación
d. Las consultas, respuestas y las aclaraciones derivadas del procedimiento estipulado en las bases administrativas
e. Las modificaciones de las bases, si las hubiere
f. La oferta técnica
g. La oferta económica
h. La resolución de adjudicación
i. El contrato respectivo y/u orden de compra respectivo.

También regirá en lo no previsto en el contrato y estos documentos, las normas del Derecho Común Chileno que rigen o en adelante rijan sobre la materia, en especial las normas del Código Civil y sus leyes complementarias, que puedan tener vigencia en relación con el suministro a que se refiere la presente licitación. De igual manera, será aplicable toda normativa técnica que rija la materia y que se encuentre vigente al momento de este proceso de licitación, como sus eventuales modificaciones. Los documentos antes mencionados forman un todo integrado y se complementan recíprocamente, en forma tal que se considerará parte del contrato toda obligación y/o derecho, que conste en cualquiera de los documentos señalados.

Se deja constancia que se considerará el principio de preeminencia de las bases, como marco básico, sin perjuicio del valor del contrato pertinente.

NOTA: Los precedentes documentos son de carácter **PÚBLICO** en atención a la naturaleza de esta Licitación.

1.3. Cumplimiento de plazos

Los plazos que se establecen en estas bases, para las distintas etapas del proceso de la licitación son fatales y el no cumplimiento de los mismos por algún participante implicará su exclusión del proceso a partir de esa fecha.

1.4. Modificación de las bases

El Servicio podrá modificar o complementar los requerimientos técnicos y plazos de la licitación, hasta antes del cierre de recepción de las ofertas, informando de ello a través del portal del mercado público (www.mercadopublico.cl). En el mismo acto, establecerá un plazo prudencial para que los proveedores interesados puedan conocer y adecuar sus ofertas a tales modificaciones.

Estas modificaciones o complementaciones deberán ser aprobadas por un acto administrativo totalmente tramitado.

2. CONDICIONES Y PROHIBICIONES DE LOS PROPONENTES

2.1. Condiciones

Los Participantes deberán ceñirse a las siguientes condiciones generales de licitación:

a) Tribunales competentes:
Para todos los efectos legales derivados de la licitación y del contrato, la persona natural o jurídica que participe en la licitación aceptará expresamente la competencia de los Tribunales de Justicia de la comuna y ciudad de Santiago.
b) Financiamiento de la preparación de la oferta:
Los costos derivados de la formulación de la oferta en que incurra el proponente, serán de su cargo, no originando derecho a reembolso ni indemnización alguna en caso de rechazarse o no adjudicarse la oferta.

2.2. Prohibiciones que afectan a los oferentes durante su participación en la Licitación

Ejecutar cualquiera de las siguientes conductas:

a) Ofrecer, prometer, entregar, recibir o solicitar bienes o valores con el fin de influir la actuación de un funcionario o asesor del Servicio en relación con la presente licitación.
b) Tergiversación de los hechos con el fin de influenciar el proceso de licitación; ejecución de prácticas colusorias entre oferentes (antes o después de la presentación de las ofertas) con el fin de establecer precios de ofertas a niveles artificiales, no competitivos.

El Servicio se entenderá facultado para declarar inadmisible la oferta, dejar sin efecto la adjudicación o poner término anticipado al contrato, según corresponda, en caso que se acredite alguna de las prácticas señaladas anteriormente.
Asimismo, el Servicio podrá ejercer las acciones o gestiones tendientes a verificar las circunstancias previamente expuestas, dentro del marco jurídico y con pleno respeto a los derechos de los oferentes.

3. PROCESO DE LICITACIÓN

3.1. Obtención de bases de licitación

El llamado a Licitación será publicado en el Sitio Web de Mercado Público, www.mercadopublico.cl y las bases de licitación sólo se obtendrán a través de dicho Sitio Web, de acuerdo a lo especificado en la Ficha Ejecutiva de la licitación. La publicación se hará después de la total tramitación del acto administrativo que aprueba las presentes bases.

3.2. Inhabilidades para contratar

El Servicio de Impuestos Internos **no suscribirá contratos administrativos** con:

a. Funcionarios directivos del Servicio, o personas unidas a ellos por vínculos de parentesco descritos en la letra b) del artículo 54 de la ley 18.575, Ley Orgánica Constitucional de Bases Generales de la Administración del Estado (cónyuge, hijos, adoptados o parientes hasta el tercer grado de consanguinidad y segundo de afinidad inclusive).
b. Sociedades de personas de las que aquéllos o éstas, formen parte.
c. Sociedades en comanditas por acciones o anónimas cerradas en que aquéllos o éstas sean accionistas.

d. Sociedades anónimas abiertas en que aquéllos o éstas sean dueños de acciones que representen el 10% o más del capital.

e. Gerentes, administradores, representantes o directores de cualquiera de las sociedades antedichas.

f. Quienes hayan sido condenados por prácticas antisindicales o infracción a los derechos fundamentales del trabajador, dentro de los dos años anteriores a la presentación de la oferta.

g. Quienes hayan sido condenados por delitos concursales establecidos en el Código Penal, dentro de los 2 años anteriores a la presentación de la oferta.

h. Las personas jurídicas que se encuentren afectas a la inhabilitación para contratar con el Estado y con los organismos del Estado, en conformidad a la Ley N° 21.595, que establece delitos económicos.

i. Se encuentra prohibido contratar con personas jurídicas cuyo socio o socios directos o indirectos, accionista, miembro o partícipe con poder de influir en la administración, hayan sido condenados con la pena de inhabilitación para contratar con el Estado.

j. Las demás que determine la Ley, entre ellas, la indicada en el DL N°211.

Los subcontratos no podrán ejecutarse por personas afectas a las inhabilidades anteriores ni a las establecidas en el artículo 76 del Reglamento de la Ley N° 19.886 contenido en el Decreto Supremo N° 250 de 2004, del Ministerio de Hacienda.

Asimismo, el Servicio podrá ejercer las acciones o gestiones tendientes a verificar las circunstancias previamente expuestas, dentro del marco jurídico y con pleno respeto a los derechos de los oferentes.

3.3. Recepción de consultas

Todas las consultas, tanto las de carácter técnico como las de índole administrativo, que los Oferentes deseen formular en relación con la materia de esta licitación, deberán ser realizadas a través del sitio Web www.mercadopublico.cl, de acuerdo a lo especificado en la Ficha Ejecutiva de la licitación.

3.4. Entrega de respuestas

El Servicio procederá a analizar y responder todas las consultas formuladas. Las respuestas se pondrán a disposición de los proponentes en el Sitio Web del portal de Mercado Público (www.mercadopublico.cl), por el ID de la licitación y de acuerdo a lo especificado en la Ficha Ejecutiva de la licitación.

3.5. Recepción de las propuestas

3.5.1 Recepción electrónica:

Las ofertas técnicas y económicas se deberán entregar electrónicamente a través del portal de Mercado Público, el día y hora señalados en el Ítem de etapas y Plazos de la Ficha respectiva del portal y en la Ficha Ejecutiva de las bases de licitación.

El soporte papel sólo podrá ser utilizado en los casos de excepción establecidos en la Ley N° 19.886 y su Reglamento, contenido en el Decreto Supremo N° 250 de 2004, del Ministerio de Hacienda.

En el caso de producirse un problema de indisponibilidad técnica del Sistema de Información, circunstancia que deberá ser ratificada por la Dirección mediante el correspondiente certificado, el proveedor afectado deberá:

- Solicitar el certificado de indisponibilidad a la Dirección de compras dentro de las 24 horas siguientes al cierre de la recepción de las ofertas.

- En tal caso, los oferentes afectados tendrán un plazo de 2 días hábiles contados desde la fecha del envío del certificado de indisponibilidad, para la presentación de sus ofertas fuera del Sistema de Información.

Las propuestas que se presenten en formato papel se entregarán en Agustinas 1269, segundo piso, comuna de Santiago, en tres sobres cerrados caratulados respectivamente de la siguiente forma:

1.- Sobre N° 1: “Oferta Técnica Licitación ID (Señalar la ID asignada en el portal mercadopublico), nombre o razón social, domicilio, teléfono y correo electrónico del proponente”.

2.- Sobre N° 2 “Oferta Económica Licitación ID (Señalar la ID asignada en el portal mercadopublico), nombre o razón social, domicilio, teléfono y correo electrónico del proponente”.

3.- Sobre N° 3 “Código de Reclamo”, nombre o razón social, domicilio, teléfono y correo electrónico del proponente”.

El sobre N° 1 contendrá todos aquellos antecedentes que se deben presentar como documento adjunto en el campo dispuesto por el portal Mercado Público para presentar la Oferta Técnica. El sobre N° 2 contendrá los documentos que se deben adjuntar en el campo destinado a presentar la Oferta Económica en el portal Mercado Público. El sobre N° 3 contendrá el código de reclamo efectuado en el Sistema de Información de Compras y Contratación Pública.

El Servicio informará por medio del Portal Mercado Público la presentación de una oferta en formato papel.

Los sobres se abrirán en una o en dos etapas, de acuerdo a lo dispuesto en la ficha técnica de la presente Licitación.

Corresponderá al Secretario General del Servicio de Impuestos Internos o quien esté designado como su subrogante o suplente custodiar las ofertas presentadas en formato papel.

3.5.2 Recepción de sobre:

La garantía de seriedad de la oferta, se deberá entregar en un sobre denominado “**GARANTÍA DE SERIEDAD DE LA OFERTA LICITACIÓN**” indicando el N° de licitación al que se refiere, en el lugar, día y hora, de acuerdo a lo especificado en la Ficha Ejecutiva de la Licitación.

Asimismo, podrá ser otorgada de forma electrónica, debiendo ajustarse a lo dispuesto en la ley N° 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma. En este caso, para su presentación válida, sólo se debe considerar día y hora, de acuerdo a la Ficha Ejecutiva de la Licitación, por cuanto al ser documento electrónico, solo basta que sea adjuntado a la correspondiente licitación.

En el caso que un oferente entregue un sobre o una garantía que tenga un error u omisión de carácter menor o meramente formal y su rectificación no altere el tratamiento igualitario a todos los oferentes ni vulnere aspectos esenciales de la licitación, el Servicio podrá solicitar que el error sea enmendado.

La presentación y contenidos tanto de la oferta económica como de la oferta técnica serán de responsabilidad del representante legal del oferente, en el caso de personas jurídicas, y del propio oferente tratándose de personas naturales.

Si encontrándose próxima la fecha de vencimiento del documento de garantía de seriedad de la oferta, aún estuviera en curso el proceso de firma del contrato con el adjudicatario, o bien, en caso que se amplíe el plazo de vigencia de la oferta de acuerdo al N° 3.12, letra a) párrafo segundo de estas bases, se deberá prorrogar la vigencia del documento o reemplazarlo por uno nuevo en las mismas condiciones del documento primitivo, abarcando el periodo faltante para la firma del contrato y/o de la prórroga del plazo de vigencia de la oferta.

IMPORTANTE:
Se deja constancia que el SII es un usuario más del portal Mercado Público, por lo que no se responsabiliza por los defectos operativos de sus aplicaciones.

3.6. Apertura y revisión del sobre que contenga la garantía de seriedad de la oferta.

Después de cerrado el plazo de recepción del sobre de garantía de seriedad de la oferta, se procederá públicamente a abrirlo, levantándose un acta de ello. Este acto se realizará a partir de los 15 minutos posteriores al cierre del proceso, en la sala de reuniones del Departamento de Adquisiciones, Agustinas 1269, 2° piso, Santiago.

En la apertura de dichos sobres participará como ministro de fe el Presidente de la comisión evaluadora o quien esté designado como su subrogante o suplente y el encargado del proceso licitatorio.

En este acto se revisará el documento de garantía de seriedad de la oferta. Si se omitiera dicha garantía, la oferta del proveedor será declarada inadmisible.

3.7. Apertura electrónica de las ofertas

Salvo la situación excepcional señalada en el 3.5.1 de las Bases Administrativas -Parte II, las ofertas técnicas y económicas se abrirán electrónicamente a través del portal de Mercado Público, el día y hora señalados en el Ítem de etapas y Plazos de la Ficha respectiva del portal y en la Ficha Ejecutiva de las bases de licitación.

En el caso que se presenten dificultades técnicas en la plataforma electrónica que impidan el desarrollo de la apertura electrónica, el Servicio podrá interrumpir la continuidad administrativa del proceso y disponer su continuación el día hábil siguiente en que esté disponible la plataforma.

3.8. Errores u omisiones en las ofertas

Serán declaradas inadmisibles las ofertas que no cumplan con los requisitos establecidos en las Bases, o con las especificaciones técnicas contenidas en el punto III) Bases Técnicas. Asimismo, aquellas ofertas que presenten errores u omisiones cuya solicitud posterior al plazo de presentación de la oferta altera el tratamiento igualitario a todos los oferentes.

Sin perjuicio de lo anterior, el Servicio se reserva el derecho de admitir ofertas que presenten defectos de forma, omisiones o errores menores, siempre que éstos no alteren el tratamiento igualitario a todos los oferentes y el principio de estricta sujeción a las bases. Asimismo, el SII podrá permitir la presentación de certificaciones o antecedentes que los oferentes hayan omitido presentar al momento de efectuar la oferta, siempre que dichas certificaciones o antecedentes se hayan producido u obtenido con anterioridad al vencimiento del plazo para presentar ofertas o se refiera a situaciones no mutables entre el vencimiento del plazo para presentar ofertas y el periodo de evaluación. Dichas omisiones deberán ser corregidas en un plazo no superior a las 48 horas contadas desde el requerimiento del SII al oferente que haya omitido certificaciones o antecedentes, el que se informará a través del Sistema de Información de Compras y Contratación Pública.

No se consideran errores y, por lo tanto, no se pedirá aclaración ni será considerados como un incumplimiento de requisitos formales: a) los errores ortográficos o gramaticales o la contracción o resumen de palabras, si de ello no puede derivarse dudas en cuanto al sentido de la palabra. Esta regla se aplicará aun cuando se trate de expresiones que constituyan una formalidad legal; b) errores u omisiones cometidos en la individualización de personas, clientes, trabajadores o representantes, si de ello no puede derivarse dudas en cuanto a la identidad de la persona de que se trata; c) los errores numéricos o de cifras o porcentajes, que manifiestamente no sean de carácter sustancial y; d) en general, las disconformidades no esenciales que existan entre los distintos documentos de la oferta, siempre que no pudiere derivarse dudas del aspecto al que se refieren.

3.9. Completitud de la oferta

Los oferentes podrán presentar una única oferta, acompañando un documento de seriedad de la oferta, en las condiciones señaladas en la Ficha Ejecutiva. En caso que el oferente presente más de una oferta, se considerará la última oferta publicada en el portal Mercado Público como oferta válida para efectos de evaluación, desestimándose las anteriormente presentadas.

Es responsabilidad del oferente proveer todos los elementos necesarios para el adecuado cumplimiento del objeto de la presente licitación.

Se deja expresa constancia que las ofertas que contengan cláusulas que limiten, condicionen y/o restrinjan la oferta en los términos y condiciones solicitadas en las bases, dichas cláusulas se tendrán por no escritas.

3.10. Aclaración de las ofertas y consultas a los oferentes

Será responsabilidad de los proponentes proporcionar toda la información que permita al Servicio efectuar la evaluación de sus ofertas.

De considerarlo necesario, el Servicio podrá requerir –por escrito y a través del portal Mercado Público - aclaraciones a algún proponente sobre aspectos de su propuesta que no resulten suficientemente claros. Estas aclaraciones no podrán modificar la oferta ni referirse a elementos

esenciales o que afecten el tratamiento igualitario de los oferentes. Las respuestas deberán ser entregadas por medio del portal www.mercadopublico.cl, dentro del plazo de 48 horas, contados desde la solicitud efectuada.

Tanto las aclaraciones solicitadas a los oferentes como sus respuestas serán publicadas en el portal Mercado Público (www.mercadopublico.cl), y pasarán a formar parte integrante de los antecedentes del contrato, en caso de serle adjudicado.

3.11. Evaluación de las ofertas

El Servicio evaluará las ofertas entregadas por los proponentes, procediendo a adjudicar la licitación, fundadamente, a aquella oferta que de acuerdo a los criterios de evaluación sea la más conveniente para los intereses y necesidades del Servicio.

Asimismo, la Comisión Evaluadora podrá ejercer las acciones o gestiones tendientes a verificar las condiciones, circunstancias, hechos, y requerimientos, presentados por los oferentes en la propuesta técnica, a través de asesorías, consultas a expertos, fabricantes, entre otros, siempre respetando los principios de estricta sujeción a las bases e igualdad de los oferentes.

3.12. Adjudicación de la licitación

La adjudicación de la licitación y la notificación al adjudicatario y a los no adjudicados se realizará de la siguiente forma:

a) Adjudicación:

Una vez que se haya adjudicado la licitación, se dejará constancia de la decisión del Servicio mediante acto administrativo de adjudicación, según lo dispuesto en el art. 41 del Reglamento de la Ley N° 19.886, contenido en el Decreto Supremo N° 250 de 2004, del Ministerio de Hacienda, el que será notificado mediante su publicación en el portal Mercado Público. La notificación de la resolución de adjudicación se entiende realizada luego de 24 horas transcurridas desde que el Servicio efectúe su publicación en el Sistema de Información de Compras y Contratación Pública.

Cuando la adjudicación no se realice dentro del plazo señalado en las presentes bases de licitación, el Servicio informará en el Sistema de Información de Compras y Contratación Pública las razones que justifican la ampliación del plazo para adjudicar e indicará un nuevo plazo.

En caso de que los proveedores requieran hacer consultas sobre el acto de adjudicación, estas deberán ser remitidas al correo electrónico adquisiciones@sii.cl.

Las obligaciones entre ambos sólo serán exigibles a partir de la total tramitación del acto administrativo que aprueba el contrato, salvo que, por razones de buen servicio, se indique un plazo distinto. Sin perjuicio de ello, todo pago se realizará previa tramitación del acto administrativo aprobatorio.

El Servicio declarará inadmisibles las ofertas cuando éstas no cumplieren los requisitos establecidos en las bases. Declarará desierta una licitación cuando no se presenten ofertas, o bien, cuando éstas no resulten convenientes a sus intereses. En ambos casos la declaración deberá ser por resolución fundada.

b) Devolución del documento de garantía de seriedad de la oferta:

Las cauciones de seriedad de la oferta se devolverán a los oferentes a su sola solicitud, dentro de los 10 días hábiles siguientes a la fecha de publicación del resultado de la licitación en el portal Mercado Público, indicada en la letra a) precedente o en la fecha de vencimiento de las cauciones, según lo que ocurra primero. Lo anterior, no será aplicable al adjudicatario y a los dos siguientes oferentes mejor evaluados a quienes se le devolverá dicho documento luego de la total tramitación de la resolución que aprueba el contrato respectivo.

Respecto de los oferentes cuyas ofertas hubiesen sido declaradas inadmisibles se les devolverá la garantía de seriedad de la oferta una vez que se encuentre totalmente tramitada la respectiva resolución que declara la inadmisibilidad.

En caso que la licitación sea declarada desierta, se devolverán las garantías de seriedad de la oferta una vez que se encuentre totalmente tramitada la respectiva resolución que declara desierta la licitación.

Dichas garantías podrán ser retiradas en el Departamento de Adquisiciones, Agustinas 1269, 2° piso, comuna de Santiago.

La garantía será devuelta sin reajustes, ni intereses y sin costo alguno para el Servicio.

3.13. Revisión de los saldos insolutos de remuneraciones y cotizaciones previsionales

Con anterioridad a la suscripción del contrato materia de la presente licitación, el SII revisará en el certificado de antecedentes laborales y previsionales emitido por la Dirección del Trabajo, si el adjudicatario registra o no saldos insolutos de remuneraciones o cotizaciones, de seguridad social con sus actuales trabajadores o con trabajadores contratados en los últimos dos años.

Si existen montos pendientes de pago, los primeros estados de pago producto del contrato deberán ser destinados al pago de dichas obligaciones, debiendo la empresa acreditar que la totalidad de las obligaciones se encuentren liquidadas al cumplirse la mitad del período de ejecución del contrato, con un máximo de 6 meses.

El incumplimiento de esta obligación por parte del adjudicatario dará derecho a poner término al contrato respectivo, sin que genere la obligación de indemnizar, pudiendo el Servicio llamar a una nueva licitación.

Si el contratista subcontratare parcialmente algunas labores del contrato, el Servicio revisará igualmente el estado de cumplimiento de las obligaciones laborales y previsionales. El subcontratista estará sujeto a los mismos requisitos señalados en este punto.

3.14. Dejación sin efecto de la adjudicación

La adjudicación podrá ser dejada sin efecto en los siguientes casos:

a) Si dentro del plazo establecido en el párrafo primero del N° 4.1 de las Bases Administrativas -Parte II, el adjudicatario no acompaña la documentación requerida para la formalización del contrato.
b) Si el adjudicatario incurre en alguna de las inhabilidades para contratar con el SII, señaladas en el N° 3.2 del punto II Bases Administrativas Parte II.
c) Si el adjudicatario no se inscribe en el registro electrónico oficial de contratistas de la administración, Registro de Proveedores, en el plazo establecido en el párrafo segundo del N° 4.1 del punto II) Bases Administrativas -Parte II.
d) Si el adjudicatario no firma el contrato que ejecuta la presente licitación en el plazo establecido en el párrafo tercero del N° 4.1 de las Bases Administrativas -Parte II.
e) Si se comprueba que cualquiera de los antecedentes presentados por el adjudicatario son falsos.
f) Si el adjudicatario se desiste de su propuesta o la retira unilateralmente.

En todos estos casos el SII hará efectiva la garantía de seriedad de la oferta.

El SII declarará desierta la licitación en caso que la siguiente oferta no resulte conveniente a sus intereses, en caso contrario podrá adjudicar la licitación a la oferta que siga en el orden de prelación de acuerdo con el puntaje obtenido. Lo anterior se podrá efectuar hasta el tercer oferente mejor calificado.

4. DISPOSICIONES CONTRACTUALES

4.1. Preparación del contrato

El adjudicatario deberá proporcionar, dentro de los 15 días hábiles siguientes a la fecha de notificación de la adjudicación, los antecedentes pertinentes para redactar el contrato y el **documento de garantía de Cumplimiento** de éste.

El adjudicatario debe estar inscrito en el registro electrónico oficial de contratistas de la administración, Registro de Proveedores, para suscribir el contrato respectivo. En caso contrario, estará obligado a inscribirse dentro del plazo de 15 días hábiles, contados desde la notificación de la adjudicación respectiva. El SII no suscribirá contrato con un oferente no inscrito en el registro mencionado.

El plazo para suscribir el contrato será de 10 días hábiles, contados desde la fecha de la notificación del SII para suscribir éste, la que se realizará mediante correo electrónico. Este plazo podrá ser ampliado por razones de caso fortuito o fuerza mayor, lo que será formalizado mediante resolución fundada.

Para todos los efectos legales y, atendido a que el contrato será suscrito con firma electrónica, la fecha del contrato será de acuerdo al último firmante. Sin perjuicio de lo anterior, la contratación comenzará a regir de acuerdo a lo establecido en el numeral 4.3, de las BASES ADMINISTRATIVAS – PARTE I.

4.2. Documentación requerida para la formalización del contrato

Para la firma y tramitación del contrato, el adjudicatario, si es persona jurídica, deberá proporcionar copia legalizada u original de:

a) Declaración jurada de **inhabilidades para contratar**
b) Extracto de escritura de constitución inscrito en el Registro de Comercio respectivo o certificado de vigencia de la sociedad, extendido con no más de 30 días corridos de anticipación a la fecha de la firma del contrato.
c) Escritura en que conste la personería del representante legal del oferente con vigencia y su respectivo certificado de vigencia del Registro de Comercio, extendido con no más de 30 días corridos de anticipación a la fecha de la firma del contrato.
d) Garantía de fiel cumplimiento del contrato.
e) Certificado de antecedentes laborales y previsionales.
f) Declaración jurada indicando si registra o no saldos insolutos de remuneraciones y/o cotizaciones de seguridad social con sus actuales trabajadores o con trabajadores contratados en los últimos dos años.

En el caso de las personas jurídicas acogidas al régimen simplificado de la Ley 20.659 se deberá acompañar: Certificado de migración (si corresponde); Certificado de vigencia; Certificado de estatuto actualizado; y Certificado de anotaciones.

En caso de adjudicatarios extranjeros:

a) Deberán acreditar su existencia legal y vigencia, mediante documentos que demuestren dichas circunstancias, los que deben ser legalizados en Chile, tanto en el consulado del país de origen como en el Ministerio de Relaciones Exteriores.
b) Deberán acreditar la existencia de un representante legal en Chile, acompañando para ello escritura pública donde conste el mandato y representación, y los documentos que acrediten la existencia, vigencia y representación legal de ese mandatario, legalizados si hubiesen sido otorgados en el extranjero; o escritura pública de constitución de sociedad chilena, documentos en el que conste la personería del representante legal, RUT de la sociedad chilena y cédula de identidad del representante legal; o escritura pública de constitución de la agencia de la sociedad extranjera, documento donde conste la personería del presentante legal, RUT de la agencia y cédula de identidad del representante legal, cuyo objeto debe comprender la ejecución del contrato materia de las presentes bases.
c) Designar domicilio en la ciudad y comuna de Santiago de Chile.
d) Si se trata de una sociedad anónima extranjera, acreditar su existencia de acuerdo a lo dispuesto en el artículo 121 de la Ley N° 18.046.
e) Declaración jurada indicando si registra o no saldos insolutos de remuneraciones o cotizaciones de seguridad social con sus actuales trabajadores o con trabajadores contratados en los últimos dos años.

Tratándose de personas naturales, deberán proporcionar los siguientes antecedentes, en copia legalizada u original:

a) Cédula de identidad
b) Declaración jurada de **inhabilidades para contratar**
c) Garantía de fiel cumplimiento del contrato.
d) Certificado de antecedentes laborales y previsionales vigente.
e) Declaración jurada indicando si registra o no saldos insolutos de remuneraciones o cotizaciones de seguridad social con sus actuales trabajadores o con trabajadores contratados en los últimos dos años.

En el caso de Corporaciones, fundaciones y otras entidades sin fines de lucro:

a) RUT.
b) Declaración jurada de inhabilidades para contratar
c) Deberán acreditar su existencia legal mediante original o copia legalizada de Decreto Supremo de concesión de personalidad jurídica emitido por el Ministerio de Justicia, o mediante certificado emitido por Registro Civil en que conste su inscripción según corresponda.
d) En los casos que corresponda, deberán acompañar certificado de vigencia emitido por Registro Civil, emitido con una antigüedad no superior a 30 días corridos contados desde su presentación ante el SII.
e) Certificado de composición de los órganos de dirección y administración de las personas jurídicas, emitido por el Registro Civil en que conste la personería del representante legal, con una antigüedad no superior a 30 días corridos contados desde su presentación ante el SII.
f) Garantía de fiel cumplimiento del contrato.
g) Certificado de antecedentes laborales y previsionales.
h) Declaración jurada indicando si registra o no saldos insolutos de remuneraciones o cotizaciones de seguridad social con sus actuales trabajadores o con trabajadores contratados en los últimos dos años.

Todos los documentos señalados anteriormente deben enviarse al correo electrónico que notificará la respectiva adjudicación.

4.3. Documento de garantía de fiel cumplimiento del contrato

Se procederá a la firma del contrato previa entrega, según lo señalado en el 4.2 anterior, por parte del adjudicatario, de un documento de garantía por el fiel cumplimiento del contrato, según las condiciones estipuladas en la Ficha Ejecutiva de la licitación, el que deberá ser pagadero a la vista y tener el carácter de irrevocable. Dicho documento, en el caso de la prestación de servicios, asegurará además el pago de las obligaciones laborales y sociales de los trabajadores del contratante, acorde al art. 22 N°6 del Reglamento de la Ley N° 19.886, contenido en el Decreto Supremo N° 250 de 2004, del Ministerio de Hacienda. El documento será devuelto al adjudicatario a partir de la fecha de vencimiento del mismo, a su sola solicitud, si correspondiese.

El adjudicatario deberá mantener vigente la garantía de fiel cumplimiento por el período señalado en la Ficha Ejecutiva, siendo de su cargo los gastos que le irrogue tal obligación.

La garantía de fiel cumplimiento tiene por objeto caucionar el cumplimiento en tiempo y forma, por el adjudicatario, de las obligaciones que impone el contrato.

El Servicio podrá hacer efectiva la garantía de fiel cumplimiento, en cualquier momento, una vez producida alguna de las siguientes circunstancias:

a) Cuando por causa imputable al proveedor se ponga término anticipado al contrato.
b) Término anticipado en caso que el adjudicatario registre saldos insolutos de remuneraciones o cotizaciones de seguridad social con sus actuales trabajadores o con trabajadores contratados

en los últimos 2 años, a la mitad del periodo de ejecución del contrato, con un máximo de 6 meses.

c) Cuando no existieren saldos pendientes de pago al contratista que fueren suficientes para pagar íntegramente las multas impuestas y, a falta de dichos saldos, el contratista no accediere a pagar la multa en efectivo.
d) Por incumplimiento de las obligaciones impuestas en el contrato.

En caso de hacerse efectivo el documento de garantía de fiel cumplimiento de acuerdo a la letra c), el adjudicatario estará obligado a reponer dicha garantía manteniendo su monto y vigencia original en el plazo de cinco días hábiles contados desde la fecha de notificación de cobro del documento.

4.4. Procedimiento de aplicación de multas.

El proceso de aplicación de multas se ceñirá al procedimiento que se contiene en este numeral, se efectuará por vía administrativa.

Si los hechos que dan lugar a la aplicación de multas se producen por hechos de caso fortuito o fuerza mayor, u otras causas que fueren atribuibles al Servicio, no procederá la aplicación de multas al contratista.

Las notificaciones que se señalan en este numeral se efectuarán mediante carta certificada, y se entenderán practicadas a contar del tercer día hábil siguiente a su ingreso para despacho en oficina de correos.

Los antecedentes que pudieran justificar la aplicación de una multa, serán remitidos en un informe, por el usuario interno requirente, al Jefe del Departamento de Adquisiciones. Dicho informe contendrá el detalle de los incumplimientos que dan origen al procedimiento precisando la normativa de las bases de licitación y contrato que se transgrede. El informe y los antecedentes serán notificados mediante carta certificada al domicilio indicado en el contrato. El contratista dispondrá de un plazo fatal de 5 días hábiles completos, contados desde la notificación, para presentar sus descargos, ante el Jefe del Departamento de Adquisiciones, domiciliado en calle Agustinas 1269, 2° piso, en la ciudad de Santiago, quien remitirá copia de los descargos realizados al usuario interno requirente.

Transcurrido este plazo, y en caso de existir descargos por parte del contratista, estos serán sometidos ante el órgano que elaboró el informe de incumplimiento respectivo a efecto que los pondere e informe si ellos motivan variar las conclusiones del informe anterior.

Posteriormente, con los antecedentes que el Servicio disponga y los que el contratista haya aportado, el Subdirector Jurídico resolverá sobre los hechos, determinando en su caso la procedencia de la sanción y su cuantía.

La resolución fundada que se emita al efecto será notificada al contratista.

La resolución será impugnable mediante los recursos establecidos en la Ley 19.880, dentro de los 5 días hábiles siguientes contados desde la fecha de notificación de aquella.

En general, las multas antes mencionadas se aplicarán sin perjuicio de las medidas tendientes a mantener la continuidad de servicio que deba efectuar el SII, por cuenta, costo y riesgo del contratista, previa notificación al mismo. Para estos efectos, a modo ejemplar, se entenderán como medidas correctivas, el tener que recurrir para la ejecución de las obligaciones contractuales del contratista a la contratación de terceros.

Sin perjuicio de lo señalado precedentemente, el Servicio podrá ejercer las acciones legales que correspondan para el debido resguardo del interés fiscal.

Las multas podrán hacerse efectivas en cualquier pago pendiente que el Servicio deba efectuar al contratista con motivo del contrato respectivo o, en su defecto, en la garantía de fiel cumplimiento, sin perjuicio de la facultad del contratista de pagar la multa impuesta en efectivo, con cualquier otro medio legal de pago, o vale vista a nombre del Servicio de Impuestos Internos.

Para el cálculo de la equivalencia en pesos chilenos de la multa cobrada en Unidades de Fomento, se tomará el valor de la unidad al día del pago de la respectiva multa.

4.5. Unión Temporal de Proveedores

El servicio podrá ser provisto por una Unión Temporal de Proveedores, conformada por personas naturales y/o jurídicas. Para tal efecto, los integrantes deberán autorizar a una representante común para que ejerza en su nombre todos los derechos y cumpla todas las obligaciones de la Unión Temporal de Proveedores a que se refieren las presentes Bases de Licitación.

Las causales de inhabilidad contempladas en las presentes Bases, y en la legislación vigente, para la presentación de las ofertas, formulación de las propuestas o para la suscripción del contrato, afectarán a cada uno de los integrantes de la Unión Temporal, individualmente considerados. De detectarse por el Servicio, la concurrencia de alguna inhabilidad que afecte a alguno de los participantes, se notificará de tal concurrencia a través del Portal Mercado Público. En dicho caso, la Unión deberá decidir si continuará con el respectivo procedimiento de contratación con los restantes integrantes no inhábiles de la misma (que no pueden ser menor a 2 proveedores) o si se desistirá de su participación en el proceso, dentro del plazo de 48 horas, contadas desde la publicación de la aclaración en el portal.

Para la presentación de las ofertas la Unión Temporal de Proveedores deberá presentar un documento, en el que todos y cada uno de los oferentes integrantes de la Unión Temporal de Proveedores, deberán designar de entre sus miembros, un representante común, con facultades suficientes para actuar en el proceso licitatorio en representación de todos ellos.

En caso de serle adjudicada la presente licitación a una Unión Temporal de Proveedores, se deberá cumplir con las siguientes reglas especiales:

1.- La formalización de la Unión Temporal de Proveedores deberá realizarse mediante escritura pública, la que deberá acompañarse para la firma del contrato.

2. La Unión Temporal de Proveedores comprometerá de manera solidaria a sus integrantes, como consecuencia de lo cual, el Servicio podrá exigir a cualquiera de sus miembros, indistintamente, el cumplimiento total de las obligaciones contraídas, cualquiera sea su naturaleza. De igual forma, el pago efectuado por el Servicio a cualquiera de sus integrantes será válido y extinguirá la deuda con respecto a los otros en la parte en que hubiere sido satisfecha, sin perjuicio de la representación que los miembros de la Unión establezcan para los efectos del proceso de licitación. Serán aplicables al referido pacto de solidaridad, las disposiciones que al respecto establece el Título IX del Libro IV del Código Civil.

3.- Todos los miembros de la Unión Temporal de Proveedores deberán encontrarse inscritos en el Registro de Proveedores, en el plazo indicado en el N° 4.1 del punto II) Bases Administrativas - Parte II.

4.- La Vigencia de la Unión Temporal deberá ser, a lo menos, equivalente a la vigencia del contrato derivado de la presente licitación.

4.6. Gastos e impuestos

Los eventuales gastos e impuestos que se generen o produzcan por causa o con ocasión del contrato, tales como los gastos notariales de celebración de contrato, y/o cualesquiera otros que se originen en el cumplimiento de obligaciones que, según el contrato o las bases, ha contraído el adjudicatario, serán de cargo exclusivo de éste.

4.7. Cesibilidad del contrato

El adjudicatario no podrá, ceder, transferir o traspasar en forma alguna, parcial o totalmente, a cualquier título, el contrato que suscriba con el Servicio o los derechos y obligaciones emanados de él, sin perjuicio de lo señalado en el punto relativo a subcontratación. La infracción a esta estipulación se entenderá como incumplimiento grave de las obligaciones de la empresa y será causal suficiente para que el Servicio, ponga término anticipado al contrato y sin derecho a indemnización de ninguna especie para el adjudicatario.

No obstante, el adjudicatario queda facultado para efectuar operaciones de cesiones de crédito y/o factoring en el marco de los artículos 1901 y siguientes del Código Civil.

La cesión de la o las facturas a terceros no liberará al adjudicatario de ninguna de las obligaciones que se establezcan en el contrato suscrito con el Servicio.

Toda operación de factoring y/o cesión de crédito debe ser informada al Servicio en calle Agustinas 1269, 2° piso, comuna de Santiago, en la forma señalada en el artículo 7° de la Ley N° 19.983 que "Regula la Transferencia y Otorga Merito Ejecutivo a Copia de la Factura". Deberá constar en el anverso de la copia cedible de la factura la firma del cedente, agregando el nombre completo, rol único tributario y domicilio del cesionario. En caso de no cumplimiento de esta indicación, el Servicio, pagará lo que corresponda al adjudicatario titular del contrato.

4.8. Causales de modificación y término anticipado del contrato

4.8.1. Causales de término del contrato

Son causales de término del contrato las siguientes:

a) Resciliación o mutuo acuerdo de las partes.

b) Incumplimiento grave de las obligaciones contraídas por el contratante.

c) Estado de notoria insolvencia del contratante, a menos que se mejoren las cauciones entregadas o las existentes sean suficientes para garantizar el cumplimiento del contrato.

d) Por exigirlo el interés público o la seguridad nacional.

e) Si el adjudicatario a la mitad del período de ejecución del contrato, con un máximo de 6 meses, registra saldos insolutos de remuneraciones o cotizaciones de seguridad social con sus actuales trabajadores o con trabajadores contratados en los últimos dos años.

   Si así correspondiere y a fin de verificar la ocurrencia de esta causal, la empresa podrá presentar los antecedentes que estime necesarios, tales como, contratos de trabajo, copias firmadas de las respectivas liquidaciones de remuneraciones del personal empleado en la ejecución del contrato, planillas de declaración y pago de imposiciones previsionales, de salud y seguro de cesantía del personal, empleado en la ejecución del contrato, registros de asistencia y control de jornada de trabajo, certificado extendido por la Dirección del Trabajo correspondiente al lugar donde se ejecuta el contrato en que conste que no tiene reclamos pendientes con dicho personal por incumplimiento de leyes laborales o previsionales o por incumplimiento de los contratos de trabajo, que acrediten el pago de remuneraciones y cotizaciones previsionales. Ahora bien, sin perjuicio de lo expuesto, el SII podrá requerir mayores antecedentes en el caso de constatar incumplimientos o inconsistencia en la documentación brindada.

f) Haber sido condenado, mediante sentencia ejecutoriada, por los delitos señalados en la Ley 21.595 sobre delitos económicos.

Se entenderá por incumplimiento grave de las obligaciones del adjudicatario, las siguientes acciones:

i. Incumplimiento de estándares técnicos de calidad ofrecidos por el adjudicatario en la oferta, tales como, problemas de configuraciones, no seguir recomendaciones del fabricante que luego tienen impacto en el servicio, entre otros.

ii. En caso que el adjudicatario transgreda la prohibición de ceder, transferir o traspasar en forma alguna, parcial o totalmente, a cualquier título, el contrato que suscriba con el Servicio o los derechos y obligaciones emanados de él.

iii. Cuando se hiciere efectivo el documento que garantiza el fiel cumplimiento del contrato y el adjudicatario no repusiere la garantía dentro de plazo.

iv. El incumplimiento de los límites establecidos para la subcontratación.

v. La ejecución por parte del contratista de las conductas señaladas en el N° 2.2 del punto II) Bases Administrativas-Parte II.

vi. La aplicación de multas alcance % máximo establecido.

vii. Se verifica incumplimiento a la cláusula de confidencialidad señalada en el N° 4.5 del punto I) Bases Administrativas-Parte I.

viii. Incumplimiento del deber de reportar incidentes de seguridad informática, de acuerdo al punto 4.9 de las Bases Administrativas Parte I.

ix. Paralización intempestiva de los servicios por 5 días consecutivos o manifiesto abandono de funciones por parte de la empresa y sus trabajadores.

x. Incumplimiento de las obligaciones establecidas en el contrato y/o bases de licitación que generen un potencial peligro o causen daño o perjuicio a las personas o bienes del Servicio.

El Servicio terminará el contrato unilateralmente si acaece cualquiera de las causales establecidas en la letra b) hasta la f) de este número.

4.8.2. **Causales de modificación del contrato**

Son causales de modificación del contrato las siguientes:

a) Mutuo acuerdo de las partes.

b) Por exigirlo el interés público o la seguridad nacional.

Las modificaciones podrán efectuarse con el fin de lograr un mejor cumplimiento de los objetivos del contrato o de hacerse cargo de situaciones imprevistas, ocurridas durante la ejecución del contrato, y que incidan en su normal desarrollo.

En el caso de requerirse una modificación del contrato, se formalizará un anexo al contrato original, el que será aprobado mediante resolución. La modificación del contrato regirá a contar de la total tramitación del acto administrativo que la aprueba. El conjunto de modificaciones efectuadas no podrá superar el 30% del valor del contrato.

El adjudicatario deberá constituir un nuevo documento de garantía de fiel cumplimiento a favor del Servicio, de iguales características al señalado en la ficha ejecutiva, por todo el plazo de vigencia de la modificación más 60 días hábiles, la glosa de dicho documento señalará: “Garantizar el Fiel Cumplimiento de la Modificación N° __del Contrato N° (número interno a asignar)”. Dicha garantía será devuelta al contratante al término de la vigencia de la garantía, si correspondiere.

4.9. Procedimiento y normas aplicables al término contractual anticipado y a la ejecución de la garantía de fiel cumplimiento de contrato

El procedimiento y las normas aplicables al término contractual anticipado y/o a la ejecución del documento que garantiza el fiel cumplimiento del contrato, corresponde al descrito en el presente numeral.

Las notificaciones que se señalan en este numeral se efectuarán mediante carta certificada, y se entenderán practicadas a contar del tercer día hábil siguiente a su ingreso para despacho en oficina de correos.

Los antecedentes que pudieran justificar la aplicación de una (o ambas) de estas medidas, serán remitidos en un informe, por el usuario interno requirente, al Jefe del Departamento de Adquisiciones. Dicho informe contendrá el detalle de los incumplimientos que dan origen al procedimiento precisando la normativa de las bases de licitación y contrato que se transgrede. El informe y los antecedentes serán notificados mediante carta certificada al domicilio indicado en el contrato. El proveedor dispondrá de un plazo fatal de 5 días hábiles, contados desde la notificación, para presentar sus descargos, ante el Jefe del Departamento de Adquisiciones domiciliado en calle Agustinas 1269, 2° piso, en la ciudad de Santiago. Transcurrido este plazo, y con los antecedentes que el Servicio disponga y los que el proveedor haya aportado, la autoridad competente resolverá sobre los hechos, determinando en su caso la procedencia de éstas.

La resolución fundada que se emita al efecto será notificada al proveedor.

La resolución será impugnable mediante los recursos establecidos en la Ley 19.880, dentro de los 5 días hábiles siguientes contados desde la fecha de notificación de aquella.

La resolución que disponga el término anticipado del contrato o la ejecución del documento que garantice el fiel cumplimiento del contrato, deberá ser fundada y publicarse en el sistema de información de Mercado Público, a más tardar dentro de las 24 horas de dictada. Además, deberá notificarse a la empresa mediante carta certificada, enviada al domicilio registrado en el contrato, con diez (10) días hábiles de antelación a la fecha en que se desea terminar el contrato.

Puesto término anticipado a un contrato por cualquiera de las causas señaladas, salvo la estipulada en las letras a) y d) del N°4.8.1 del punto II) Bases Administrativas – Parte II, se cobrará la garantía de fiel cumplimiento. Adicionalmente, el adjudicatario deberá responder de las multas que correspondan por el atraso que se produzca o cualquier otro perjuicio que resultare para el Servicio con motivo de esta terminación.

Todo, sin perjuicio de las acciones que el Servicio pueda ejercer para exigir el cumplimiento forzado de lo pactado o la resolución del contrato, en ambos casos, con la correspondiente indemnización de perjuicios.
El término anticipado del contrato, no dará lugar al pago de indemnizaciones a favor del contratista.

BASES TÉCNICAS – PARTE III

1. INTRODUCCIÓN

En este apartado se encuentran indicadas las especificaciones técnicas para la contratación de servicios en el ámbito de seguridad informática con el fin de garantizar la protección de los sistemas informáticos del Servicio de Impuestos Internos (SII), tanto en ambientes Internet como Intranet.

Los servicios por contratar deben proporcionar un conjunto de recomendaciones y acciones en el ámbito de la seguridad informática, las cuales producto del análisis de vulnerabilidades y pruebas de estudios, deben llevar a los sistemas informáticos del SII (considerando elementos físicos y lógicos) al máximo nivel de seguridad posible, tanto en sus ambientes Internet como de Intranet.

Los servicios por contratar refieren a los 2 componentes, las cuales se indican a continuación.

COMPONENTES REQUERIDOS	
Componente 1	ITEM 1: Servicio de centro de operación de seguridad (SOC)
	TEM 2: Servicio Gestionado de Detección y Prevención de Intrusos (IPS).
	ITEM 3: Servicio Gestionado de Protección contra ataques de denegación de servicios (Anti DDOS).
	ITEM 4: Servicio Gestionado de Análisis de vulnerabilidades.
	ITEM 5: Servicio Gestionado de Firewall para aplicaciones Web y APIS (WAAP).
	ITEM 6: Servicio Gestionado de detección y respuesta de amenazas en red de datos interna (Network Detección and Response NDR).
Componente 2	Horas Hombre para servicios profesionales avanzados en seguridad de la información y ciberseguridad.

Es de responsabilidad de los oferentes proveer todos aquellos materiales, herramientas o equipos necesarios para el buen funcionamiento de los productos y servicios objeto de la presente licitación. Los componentes prestarán servicios sobre los dos data center en los cuales el SII posee sistemas de negocio On Premise, los cuales se encuentran ubicados en la Región Metropolitana y también en los ambientes de nube pública en los cuales el SII posea servicios instalados, los cuales corresponden actualmente a los ambientes MICROSOFT AZURE y Amazon AWS.

Cada Centro de datos cuenta con 4 enlaces de distintos proveedores de servicios, que entregan el servicio internet con tráfico nacional e internacional. Se debe considerar un peak de 2.000.000 (dos millones) conexiones concurrentes por Centro de datos. Actualmente el SII cuenta con un servicio de monitoreo de plataforma de seguridad perimetral, el cual será reemplazado por la propuesta adjudicada en este proceso de licitación.

Los oferentes deberán analizar la factibilidad técnica de su equipamiento y realizar todas las indicaciones pertinentes que permitan el buen funcionamiento de este durante la implementación.

El equipamiento necesario para el funcionamiento de los servicios contratados a través de las componentes adjudicadas por el Servicio de Impuestos Internos debe contar con soporte 7 días, 24 horas, los 365 días del año, por el fabricante.

Ante la eventualidad de que el fabricante deje de brindar soporte técnico de algún equipo asociado a los módulos adjudicados durante la vigencia del contrato, el adjudicatario deberá reemplazarlo por un modelo con soporte vigente y de igual o superiores características, sin costo adicional para el Servicio de Impuestos Internos.

2. ESPECIFICACIONES DE LAS COMPONENTES

2.1. COMPONENTE 1

Los servicios por contratar de los ítems 1, 2, 3, 4, 5 y 6, deben considerar los elementos de hardware (si aplica), software, configuración, puesta en marcha, administración, soporte, actualización, mantenimiento y acciones necesarias para hacer efectiva la protección de los activos del SII, tanto en los ambientes Onpremise del Servicio, así como en los ambientes de nube pública Amazon AWS y Microsoft Azure, en los cuales el SII disponibiliza los sistemas de negocio para usuarios internos/externos y contribuyentes en general.

En el caso On premise, la protección comprende los sistemas alojados en los dos Centro de datos del SII: uno primario que corresponde a infraestructura propia y otro secundario que corresponde a infraestructura de Centro de datos subcontratada. Los dos Centros de datos operan en modalidad activo/activo.

En el caso Nube Pública, la protección debe comprender los sistemas de negocio alojados tanto ambientes de nube Amazon AWS, así como en ambientes de nube Microsoft Azure. En ambos casos, los sistemas de negocio se basan en arquitectura de microservicios y contenedores con repositorios de datos encriptados. Los usuarios (contribuyentes) acceden directamente a estos sistemas en nube desde internet, los cuales están conectados y debidamente sincronizados con los sistemas CORE del SII alojados en la plataforma Onpremise.

Para los ítems 2, 3, 4, 5 y 6, se debe considerar un especialista de nivel técnico onsite en modalidad 5x9, quien debe colaborar en el servicio de administración de dichas plataformas y canalizar los requerimientos que realice el SII al oferente. La modalidad 5x9 considera un horario de 08:30 a 18:30 horas, los días hábiles de lunes a viernes.

El perfil requerido para cumplir esta labor debe considerar un Técnico de seguridad TI, para las labores de administrador Nivel 1 (administración y gestión de mejora continua del proceso de entrega del servicio), quien debe acreditar experiencia de al menos 2 años en la administración de plataformas de seguridad (IPS, AntiDDos, WAAP y NDR, principalmente).

2.1.1. ÍTEM 1: SERVICIO DE CENTRO DE OPERACIÓN DE SEGURIDAD (SOC)

El servicio requerido consiste en el monitoreo, detección, gestión, contención y respuestade las incidencias de seguridad de la información y ciberseguridad que ocurran en las plataformas tecnológicas del SII.

Servicio de SOC ofertado debe contar con certificaciones vigente de nivel internacional en el ámbito de seguridad informática, tales como, ISO 27001, ISO 20000 o certificación CERT. Estas certificaciones deben ser acreditadas para ser consideradas válidas, y deberán mantenerse en esta condición durante toda la vigencia del contrato.

El servicio SOC se alimentará de los registros LOGs o eventos generados a partir de los servicios IPS, WAAP,AntiDDos y NDR asociados a la componente 1, tanto en ambientes on-premise como de nube pública del SII, así como también de los equipos de seguridad que son parte de la infraestructura perimetral del SII (firewalls perimetrales, principalmente).

El servicio de SOC debe entregar permanentemente una mirada global de la situación y estado de la plataforma de seguridad, tanto a nivel on premise como a nivel de nube pública del SII, tomando y ejerciendo el rol de auditor. Debe gestionar e informar al SII sobre cualquier hallazgo o incidente

que vaya dirigido a afectar o dañar algún recurso del SII o que sea utilizado por éste para la entrega de los servicios a la ciudadanía u otras entidades externas con las cuales debe intercambiar información.

Dicho servicio deberá ser integral, es decir, debe contemplar todas las herramientas de hardware y software necesarios que se requieran, como así mismo, interfaces que permitan visualizar resultados, patrones y gráficos interactivos que permitan tener una visión global de los eventos.

El servicio ofertado debe estar basado en la operación de un SOC (Security Operation Center) por parte del adjudicatario, el cual debe cumplir, al menos, los siguientes requisitos:

a) El servicio SOC debe contemplar los registros LOGs de las plataformas de seguridad perimetral presentes en los centros de datos que utiliza el SII para la entrega de sus servicios. Actualmente el SII entrega sus servicios de intercambio de información en 2 centros de datos que operan en modalidad activo-activo.

b) También debe contemplar los registros LOGs de las plataformas de seguridad perimetral presentes en los ambientes de nube pública del SII.Actualmente el SII cuenta con servicios de intercambio de información en las nubes públicas de Amazon AWS y Microsoft Azure.

c) Debe contar con operadores-analistas de seguridad que posean certificaciones en la herramienta de correlación avanzada de eventos ofertada. Se evaluará la cantidad de analistas con las certificaciones indicadas, las que deben encontrarse en estado de vigente, a la fecha de publicación de la licitación y mantenerse en dicha condición durante toda la vigencia del contrato.

d) Debe contar con analistas de seguridad que cumplan la función de especialistas de seguridad nivel 2, quienes deben apoyar las labores de corrección y remediación ante incidentes detectados. Los especialistas deben poseer certificaciones del tipo CCNA Security, Ethical Hacking o similares, que permitan cumplir con este rol. Se evaluará la cantidad de analistas de seguridad con las certificaciones para nivel 2, las que deben encontrarse en estado vigente, a la fecha de publicación de la licitación y mantenerse en dicha condición durante toda la vigencia del contrato

e) Debe contar con soporte telefónico con disponibilidad 7 días, 24 horas, los 365 días del año, con atención de operador-analista en idioma español.

f) Debe considerar el tratamiento y manejo de incidentes, de manera que al detectar actividad anómala que vaya dirigida a afectar o dañar cualquier recurso utilizado por el SII, se deban ejecutar las actividades necesarias para contenerlos, minimizar el impacto y recuperar el normal funcionamientode las plataformas, Se deberá coordinar con el SII, a fin de realizar las actividades tendientes a restaurar la operación normal de los servicios.

g) Debe ejecutar análisis y generar respuestas ante incidentes, identificar comportamientos sospechosos y/o anómalos, como también, ataques externos e internos. Debe proveer un servicio de vigilancia tecnológica y evaluación de la seguridad de la plataforma que el SII dispone para la entrega de servicio, que apoye la identificación de nuevas amenazas.

h) Proporcionar visibilidad de los incidentes más significativos no resueltos (TOP 10) al SII

i) Debe contemplar procedimientos para respuesta y resolución de alarmas de seguridad generadas a partir de los servicios correspondientes de los ítems 2, 3, 5 y 6 de la componente 1 de la presente licitación, cuyo origen pudieran estar en los siguientes ámbitos:

- Las tecnologías y soluciones de seguridad que son administradas por el adjudicatario.
- Los equipos de seguridad perimetral que son administrados por el SII.
- La herramientas, productos y soluciones de seguridad utilizados por el SII en sus ambientes de nube pública.

Dichos procedimientos deben considerar el registro del evento reportado y las gestiones realizadas para la recuperación o mitigación del evento.

j) El servicio debe contemplar la entrega semanal y mensual de reportes en formato pdf., resumen ejecutivo y detallado a nivel técnico, respecto de los eventos relevantes ocurridos durante el período.

El reporte semanal deberá contener al menos, el comportamiento del servicio indicando los incidentes, requerimientos, consultas y reclamos del período.

El plazo de entrega para el reporte semanal es hasta el segundo día hábil de la semana siguiente, en horario hábil, entendiéndose horario hábil entre las 09:00 y las 18:30 hrs.

El reporte mensual deberá contener al menos, un resumen del estado de los incidentes y comentarios u observaciones respecto a las tendencias entregadas en las gráficas mensuales del servicio.

El plazo de entrega para el reporte mensual es hasta el quinto día corrido del mes siguiente.

k) Cuando el SII lo solicite, el adjudicatario deberá elaborar un informe de la gestión realizada de un determinado incidente de seguridad.

l) El servicio ofertado debe considerar un sistema de correlación de eventos que se encuentra en Cuadrante Gartner para SIEM o similar, en la versión vigente a la fecha de publicación de la licitación.

m) El servicio ofertado, a partir del uso de la herramienta SIEM o similar incluida en la propuesta, debe realizar el registro y correlación de eventos de tal forma que permita la detección de amenazas, eventos y/o incidentes que no necesariamente se identifiquen individualmente a partir de las fuentes de información del SOC indicadas:

- Las tecnologías y soluciones de seguridad que son administradas por el adjudicatario (ítems 2, 3, 5 y 6 de la Componente 1).
- Los equipos de seguridad perimetral que son administrados por el SII.
- La herramientas, productos y soluciones de seguridad utilizados por el SII en sus ambientes de nube pública.

En este caso, el servicio ofertado debe proveer al SII una herramienta, vista o Dashboard, mediante el cual se tenga acceso a la verificación de las acciones de correlación realizadas por el SIEM o similar, con el fin de efectuar sus propias consultas y descargar informes resultantes.

n) Se debe considerar el almacenamiento histórico de información de 30 días corridos en la plataforma (almacenamiento online) y un tiempo de retención de 6 meses (LOGS almacenadas), los cuales pueden ser solicitados por el SII en cualquier momento y que deben ser proporcionados en un archivo Excel, en los tiempos de respuestas de acuerdo a la ventana de tiempo requerida.

o) Cada incidente registrado debe contemplar la fecha y horario de inicio, actualización y termino, estado de escalamiento y criticidad, impacto y acciones realizadas para su mitigación.

p) El servicio debe considerar todos los recursos físicos y lógicos requeridos para la recolección de LOGS, de manera de garantizar la recepción de los eventos de los dispositivos de seguridad de la componente 1 y los equipos de seguridad que el SII requiera integrar.

q) Las instalaciones del SOC ofertado no necesariamente deben hallarse en territorio nacional (Chile). No obstante, aun así, estas podrían ser visitadas por personal de SII, durante la

ejecución del contrato. En el caso de servicio SOC residente fuera del territorio nacional, este deberá proveer de manera permanente una interfaz en idioma español.

r) El servicio ofertado deberá contar con una contraparte especializada, que sí debe residir en territorio nacional y cuya función será la de servir de apoyo y complemento en el relacionamiento entre el SII y SOC en los siguientes aspectos:

- Seguimiento de casos críticos
- Verificación de cumplimiento de los SLA establecidos para el servicio SOC.
- Ayuda en la resolución de incidentes que requieran una relación directa y/o in situ (presencial) entre en oferente y el SII.

Control

El oferente pondrá a disposición del SII un Dashboard en formato web, con disponibilidad 7 días, las 24 horas, los 365 días del año, para monitorear la disponibilidad del SOC, la cual deberá informar el estado de los dispositivos requeridos para la entrega de servicio SOC, cantidad de registros de eventos por dispositivo monitoreado, cantidad de eventos correlacionados y el estado de los incidentes reportados.

Se debe contemplar el monitoreo permanente del servicio, incluyendo el hardware y software que requiera ser habilitado en los Centro de datos donde opera la plataforma perimetral del SII.

SLA componente 1, ítem 1

Del servicio de monitoreo:

- El servicio debe contemplar un nivel de disponibilidad de 99,9% al año, lo que corresponde a un total de indisponibilidad de 8 horas 45 minutos como máximo. Este porcentaje considera el tiempo asociado a actividades de mantenciones preventivas.

  Se considera indisponibilidad cuando uno o más recursos de hardware y software, provistos para cumplir con el servicio SOC, afecta el envío o la recepción de registros de eventos desde los dispositivos de seguridad que los generan, o afecta el proceso de correlación avanzada de dichos eventos. El oferente debe contemplar todos los elementos de hardware y software para cumplir con el nivel de disponibilidad solicitado, como parte de una solución integral. Las indisponibilidades de uno o más de los dispositivos de seguridad que generan información al SOC, debe ser informada al SII a partir del monitoreo que el oferente realice de los mimos. Mediante esta información se medirán las indisponibilidades para la eventual aplicación de multas.

- El servicio debe contemplar un tiempo máximo de 3 horas completas para reposición del servicio en caso de falla de algún recurso de hardware y software provisto para cumplir con el servicio de SOC, contadas desde el aviso por parte del SII vía telefónica respaldado mediante correo electrónico, u otro medio en el que quede constancia por escrito de la fecha y hora del aviso.

- Se podrá solicitar evidencias de LOGS por un período específico y por una ventana de tiempo, origen y destino.

  En caso de solicitar información de un período igual o menor a 30 días corridos anteriores al día de la solicitud, (almacenamiento online) se considera un tiempo máximo de entrega de 1 día corrido. Para el caso de solicitar información producida en una fecha mayor a 30 días corridos anteriores al día de la solicitud, se considera un tiempo máximo de entrega de 5 días corridos. Esta solicitud será realizada por el SII mediante la mesa de atención proporcionada por el adjudicatario, el cual entregará un ticket de atención, con el detalle de la solicitud.

  El incumplimiento de los plazos indicados en el párrafo anterior dará lugar a la aplicación de la multa señalada en el punto 4.2.5 de las bases administrativas, parte I.

De incidentes:

- El proveedor deberá informar al SII, de los incidentes de seguridad identificados en un máximo de 20 minutos desde detectado el incidente. El contacto debe ser realizado mediante llamado telefónico, según la matriz de escalamiento entregada por el SII al adjudicatario.

  El incumplimiento de los plazos indicados en el párrafo anterior dará lugar a la aplicación de la multa señalada en el punto 4.2.3 de las bases administrativas, parte I.

- El adjudicatario debe hacer entrega de un reporte del incidente mediante correo electrónico, en un máximo de 40 minutos desde el llamado telefónico al SII indicado en el punto anterior, el cual debe incluir detalles de las gestiones realizadas para la atención del incidente en cuestión (al menos, registro del contacto que recibió la llamada, registro LOG del incidente, aplicación o IP/Puerto atacado, tiempo de inicio, formato del ataque y las recomendaciones de mitigación realizadas. Se debe indicar si se requieren acciones por parte del SII).

  El incumplimiento de los plazos indicados en el párrafo anterior dará lugar a la aplicación de la multa señalada en el punto 4.2.6 de las bases administrativas, parte I.

De Administración:

El SII podrá solicitar, en horario de 09:00 a 18:00 hrs, cambios de configuración del hardware o software, parte del servicio SOC, los cuales deben ser atendidos dentro de los siguientes 30 minutos, posterior a la apertura de la solicitud. Esta solicitud se debe realizar por el SII en la mesa de atención proporcionada por el adjudicatario, el cual entregará un ticket de atención, con el detalle de la solicitud. Se entiende por atención de la solicitud, la asignación de un especialista y el contacto telefónico con el SII, para la coordinación de las actividades requeridas para el cierre de la solicitud.

2.1.2. ÍTEMS 2, 3 Y 5 EN AMBIENTES DE NUBE PÚBLICA DEL SII

Para los servicios correspondientes a los ítems 2, 3 y 5, con el fin de contar con las capas de seguridad necesarias para la protección de los sistemas de negocio implementados en ambientes de nube pública, el SII ya cuenta con las siguientes herramientas, y/o productos de nube, los cuales se encuentran actualmente operativos y en uso:

Caso Amazon AWS:

a) Shield
b) Network Firewall
c) CloudTrail
d) F5 Rules for WAAP - Web exploits OWASP Rules
e) WAAP
f) Imperva - Managed Rules for IP Reputation on WAAP
g) Security Hub
h) Secrets Manager

Caso Microsoft Azure:

a) Azure Firewall
b) WAAP Application Gateway with DDoS

El costo de uso de estos productos será asumido por el SII durante todo el período del contrato.

El oferente deberá tener conocimientos respecto de la función, alcance y configuración de las herramientas de seguridad de nube antes mencionadas, integrando a la operación del SOC toda la información necesariacon el fin de activar el monitoreo y detección de eventos, alertas, amenazas y/o incidentes de seguridad en los ambientes de nube

El oferente deberá realizar un análisis de los ambientes de nube del SII dentro de los primeros 30 días corridos del inicio de los servicios contratados, a partir de lo cual deberá proponer mejoras a la plataforma actual y/o implementación y configuración de nuevas herramientas o productos de nube que aporten como mejoras a las condiciones de seguridad de los sistemas, acordando con el SII su implementación o no. El costo de estas eventuales nuevas herramientas será asumido por el SII por todo el periodo del contrato.

El servicio ofertado deberá asumir las acciones de configuración sobre los componentes de nube, principalmente en los siguientes casos:

- Implementación de mejoras a las herramientas y productos existentes.
- Intervención para mitigación de un incidente de seguridad detectado por el SOC.
- Implementación de nuevas herramientas o productos, en acuerdo con el SII.

Para lo anterior, el SII proveerá al oferente de las credenciales necesarias para realizar dichas acciones, para las cuales se deben definir en conjunto, los protocolos de operación que aseguren la trazabilidad y reportabilidad necesarias.

El oferente también deberá incorporar la información de los elementos de nube a los cruces de datos realizados por la herramienta SIEM o similar, con el fin de detectar eventuales amenazas o incidentes de seguridad de naturaleza avanzada.

El oferente, a partir de las acciones del SOC, deberá notificar al SII y también realizar las acciones de respuesta necesarias en las herramientas y/o productos de seguridad en los ambientes de nube, frente a la detección de amenazas o incidentes identificados en los ambientes de nube pública del SII, minimizando las probabilidades de afectación a los sistemas de negocio.

2.1.3. ÍTEMS 2, 3, 4, 5 Y 6 EN AMBIENTES ON PREMISE DEL SII

2.1.3.1. ÍTEM 2: SERVICIO DE PREVENCIÓN Y DETECCIÓN DE INTRUSOS (IPS)

Las características mínimas de este servicio deben ser las siguientes:

- El hardware y software de este servicio debe operar en un equipamiento dedicado, las cuales se habilitarán en las dependencias del SII, quien proveerá de las condiciones de energía y de espacio requerido. En la propuesta se debe indicar los requerimientos de energía y de espacio para habilitar el equipamiento requerido para la entrega del servicio.
- Los dispositivos tecnológicos utilizados por el servicio ofertado, deben aparecer en el “Gartner’s Magic Quadrant for Intrusion Detection and Prevention Systems (IDPS)”
- El servicio ofertado debe proveer una herramienta que permite acceder a información para realizar auditorías acerca de su funcionamiento y verificación de cumplimiento de SLA.
- El nivel de Throughput a considerar es a lo menos de 1Gbps por cada Centro de datos. El SII requiere proteger 2 segmentos públicos clase C, los cuales operan 1 por Centro de datos, con los cuales expone sus servicios. Se debe considerar un peak de 2.000.000 conexiones concurrentes por Centro de datos.
- El servicio debe considerar un uptime del servicio de 99,6% anual.
- Debe poder configurar excepciones, al menos por IP o segmentos de IP (IPv4).
- Debe permitir operar en modo monitor, sin tomar acción, o incluso detener la inspección del IPS si fuera requerido, sin afectar el tráfico de los servicios del SII.
- Debe poder bloquear protocolos P2P.
- Debe poseer protecciones para servicios básicos: Email, DNS, FTP, SNMP
- Debe proveer protección para DNS Cache Poisoning.
- Debe poder habilitarse protección GEOreferencial.
- Debe poseer soporte para inspección de tráfico HTTP/SSL. Se debe indicar los requerimientos para la entrega de este tipo de inspección. Debe considera a lo menos 1 Gbps por cada Centro de datos.

- El servicio ofertado debe contar con al menos 1 especialista con certificaciones técnicas en la solución IPS (Se deben adjuntar los certificados del personal)
- Debe efectuar bypass físico ante falla catastrófica. El oferente debe indicar si el bypass es interno o externo.
- Debe soportar módulos de fibra de 1Gb o 10 GE.
- Se deben realizar mantenciones periódicas sobre los elementos de hardware y software, cada 6 meses, las cuales debe ser programadas con personal del SII, quien validará y gestionará las acciones internas requeridas.
- El proveedor debe mantener un inventario de todos los elementos de software y hardware requeridos para la entrega del servicio, considerando los detalles de ubicación física, conexiones, circuitos eléctricos y vigencia de las licencias requeridas. Este inventario debe ser entregado al SII, con los escalamientos de atención necesarios.

2.1.3.2. ÍTEM 3: SERVICIO DE PROTECCIÓN CONTRA ATAQUES DE DENEGACIÓN DE SERVICIOS (Anti DDos)

Los servicios requeridos de mitigación de ataques de denegación de servicios deben considerar al menos un equipo por Centro de datos del SII, los cuales deben tener capacidad de proteger al menos un througput de 10 Gb de tráfico normal por cada Centro de datos del SII.

El servicio se debe basar en una solución ubicada en cuadro “DDoS Mitigation Solutions report" de Forrester, en la versión vigente a la fecha de publicación de la licitación.

El adjudicatario debe proveer una herramienta que permite acceder a información que permita realizar auditorías acerca de su funcionamiento y verificación de cumplimiento de SLA.

Las características de la solución deben ser las siguientes:

Arquitectura

- El oferente debe considerar al menos un appliance por cada uno de los Centro de datos del SII.
- El servicio ofertado debe contar con al menos 1 especialista con certificaciones técnicas en la solución de protección DDoS (Se deben adjuntar los certificados del personal)
- El servicio debe considerar un uptime del servicio de 99,6% anual, lo cual el oferente debe considerar en el diseño de su propuesta, teniendo en cuenta aspectos tales como: consideraciones de redundancia activo-activo, activo-pasivo, activo-spare, etc., en cada centro de datos, debiendo, además, ajustarse la opción diseñada al presupuesto disponible
- No se aceptarán dispositivos que mantengan estado de las conexiones como firewalls, ni variantes o combinaciones como UTM, NGFW, NGIPS ya que al conservar el estado de la conexión se vuelven ellos mismos susceptibles a ataques DDoS.
- El sistema debe contar con un mecanismo de bypass físico en cada interface para garantizar la alta disponibilidad, el cual deberá activarse automáticamente en los siguientes casos:
  - Pérdida de energía eléctrica.
  - Falla lógica en la interface de control.
  - Pérdida de conectividad con la tarjeta madre del dispositivo.
  - Colapso del sistema operativo.
- El equipo al posicionarse en línea deberá ser completamente transparente, sin introducir ningún cambio de encapsulamiento.
- El equipo debe ser capaz de soportar un modo de prueba "inactivo" cuando se configura en línea, que permita el ajuste de la configuración de protección sin bloquear el tráfico y proporcione reportes de todo el tráfico que bloquearía si se definiera como "activo".
- El equipo debe soportar la implementación en modo "monitor" en el que no introduce ningún punto adicional de falla a la red.

2.1.3.3. ÍTEM 4: SERVICIO DE ANÁLISIS DE VULNERABILIDADES.

EL servicio ofertado deberá abarcar el escaneo/análisis de vulnerabilidades en 2 modalidades:

- **Quincenal**: Análisis de vulnerabilidades en el perímetro externo y DMZ del SII
- **Semestral**: Análisis de vulnerabilidades en dispositivos de la red interna del SII y aplicación del negocio.

2.1.3.3.1. Servicio de análisis quincenal de vulnerabilidades perimetral

Se requiere un servicio periódico de escaneo y análisis de vulnerabilidades en el perímetro tecnológico y DMZ del SII. Perímetro y DMZ corresponde el borde tecnológico por medio del cual el SII interactúa vía internet con contribuyentes, organizaciones públicas/privadas y usuarios en general mediante la disponibilización de aplicaciones web, APIS y servicios de uso masivo.

- El servicio ofertado debe realizar los escaneos en los 2 ambientes que componen el perímetro y DMZ del SII:
    1. Ámbito Nube pública (Amazon AWS y MS Azure)
    2. Ámbito On premise.

- Para ambos casos el SII entregará los segmentos de red sobre los cuales se realizarán los escaneos.

- Los escaneos se realizarán de manera quincenal, previa coordinación/calendarización con el SII.

- El oferente deberá proponer una metodología de trabajo para la realización de los escaneos, la cual deberá contener, al menos las siguientes etapas:
    - Planificación
    - Descubrimiento
    - Escaneo de vulnerabilidades
    - Obtención de resultados
    - Generación de pre-informe
    - Informe final
    - Seguimiento periódico de los hallazgos.
- El servicio ofertado deberá contar con una bitácora en la cual se vayan registrando los hallazgos considerando la información básica de los mismos, además de ir actualizando su estatus. El detalle la metodología propuesta, deberá ser revisada y acordada con el SII.

- El escaneo de perímetro y DMZ se deberá realizar mediante, al menos el enfoque de caja negra.

- Se deberá entregar un pre-informe con las vulnerabilidades detectadas en perímetro y DMZ, identificadas en la plataforma del SII, con el análisis experto de los especialistas, en donde se presente la severidad y el plan de remediación propuesto. El plazo de entrega para el pre-informe del análisis de vulnerabilidad es de 1 día corrido desde realizado el análisis, en horario hábil, entendiéndose horario hábil entre las 09:00 y las 18:30 hrs.

- En caso de identificarse una vulnerabilidad con severidad crítica, esta deberá alertarse en un plazo no mayor a 1 hora a partir de la detección por parte de

la herramienta. El contacto debe ser realizado por medio de una llamada telefónica, según la matriz de escalamiento entregada por el SII y posteriormente mediante un correo, con el detalle de la severidad y las recomendaciones de mitigación propuesto.

- El incumplimiento de los plazos indicados en el párrafo anterior dará lugar a la aplicación de la multa señalada en el punto 4.2.11 y 4.2.12 de las bases administrativas, parte I.

- Se deberá entregar un informe final de las vulnerabilidades del perímetro y DMZ, con el análisis experto de los especialistas, en donde se presente la severidad y el plan de remediación propuesto. El plazo máximo de entrega para el reporte del análisis de vulnerabilidad es de 5 días corridos desde realizado el análisis, en horario hábil, entendiéndose horario hábil hasta las 18:30 hrs.

- El incumplimiento de los plazos indicados en el párrafo anterior dará lugar a la aplicación de la multa señalada en el punto 4.2.13 de las bases administrativas, parte I.

2.1.3.3.2. Servicio semestral de análisis interno de vulnerabilidades

Adicionalmente, el SII requiere la ejecución semestral de un escaneo de vulnerabilidades sobre dispositivos de su red interna, tanto a nivel On premise como a nivel de los sistemas en nube pública..

Dichos dispositivos, abarcan los siguientes tipos:

- Equipos de Comunicaciones,
- Servidores
- Bases de datos
- Herramientas y plataforma de nube pública, tales como Kubernetes entre otros.
- Aplicaciones de negocio.

- Este escaneo debe explorar la presencia de vulnerabilidades en dichos dispositivos y plataformas, para posteriormente entregar un listado donde se indique la gravedad de estas en relación con estándares internacionales de clasificación.
- El servicio ofertado debe contemplar a lo menos, la realización de escaneos sobre 40 servidores, 20 bases de datos y 20 equipos de comunicaciones o dispositivos de seguridad.
- El servicio ofertado deberá, para cada tipo de dispositivo, proponer una metodología de escaneo y análisis, la cual deberá considerar al menos modalidad caja negra, otorgándose un puntaje adicional en la evaluación en caso de que también considere modalidad caja gris en su oferta. lo cual será acordado en conjunto con el SII para cada caso.
- Los equipos específicos para escanear podrán ser cambiados por el SII atendiendo sus necesidades,
- El oferente deberá basar su servicio en una tecnología que cuente con una herramienta que le permita al SII acceder a la información obtenida de los escaneos, de manera que se posibilite realizar auditorías acerca del funcionamiento del servicio.

- El servicio ofertado compromete la inclusión de, al menos, una aplicación de negocio para el análisis avanzado de vulnerabilidades, la cual será determinada por el SII.
- Los reportes de dispositivos deberán permanecer disponibles al menos por unos 3 meses después de dejar de referenciar al escaneo al dispositivo.
- Se deberá entregar un pre-informe con las vulnerabilidades detectadas en las plataformas del SII, con el análisis experto de los especialistas, en donde se presente la severidad y el plan de remediación propuesto. El plazo de entrega para el reporte del análisis de vulnerabilidad es de 1 día desde realizado el análisis, en horario hábil, entendiéndose horario hábil entre las 09:00 y las 18:30 hrs.

- En caso de identificarse una vulnerabilidad con severidad crítica, esta deberá alertarse en un plazo no mayor a 1 hora a partir de la detección por parte de la herramienta. El contacto debe ser realizado por medio de una llamada telefónica, según la matriz de escalamiento entregada por el SII y posteriormente mediante un correo, con el detalle de la severidad y las recomendaciones de mitigación propuesto.
- El incumplimiento de los plazos indicados en el párrafo anterior dará lugar a la aplicación de la multa señalada en el punto 4.2.11 y 4.2.12 de las bases administrativas, parte I.
- Se debe entregar un informe final de las vulnerabilidades de activos internos, con el análisis experto de los especialistas, en donde se presente la severidad y el plan de remediación propuesto. El plazo máximo de entrega para el reporte del análisis de vulnerabilidad es de 5 días corridos desde realizado el análisis, en horario hábil, entendiéndose horario hábil hasta las 18:30 hrs.
- El incumplimiento de los plazos indicados en el párrafo anterior dará lugar a la aplicación de la multa señalada en el punto 4.2.13 de las bases administrativas, parte I.
- El oferente debe indicar el tipo de cumplimiento que ofrece el servicio asociado a estándares de la industria. Se debe considerar el cumplimiento de estándares de controles técnicos, tales como CIS, ISO27001/27002 y NIST.
- Sobre los dispositivos a escanear: Los análisis de vulnerabilidades se realizarán en los siguientes tipos de activos:

    ✓ Aplicaciones de Negocio desarrolladas por el SII.

    ✓ Bases de datos. Los tipos de bases de datos que actualmente posee el SII y que eventualmente pueden ser objeto de análisis son las siguientes:

        - Oracle: Versión 10 o Superior.
        - SQLServer: Versión 2000 o Superior.
        - SYBASE IQ: Versión 15 o Superior
        - PostgreSQL (caso nube publica): Versión 13 o superior.

    ✓ Equipos de comunicaciones y seguridad:
        - Cisco
        - Checkpoint
        - Forcepoint
        - Huawei

✓ Servidores. Los sistemas operativos que contienen los servidores que eventualmente pueden ser objeto de análisis son los siguientes; a lo menos:

- Solaris 10 o superior.

- Aix 5.3 o superior.
- Windows 2008 Server o superior.
- Linux Red Hat 6.5 o superior.
- Caso nube publica:
  - Kubernetes 1.21 o superior
  - Frontend en Apache 2.4.x. o superior

2.1.3.4. ÍTEM 5: SERVICIO DE FIREWALL PARA APLICACIONES WEB Y APIS (WAAP)

El servicio de firewall para aplicaciones Web y APIS (WAAP) ofertado debe entregar los elementos de hardware y software necesarios para la protección a las aplicaciones Web y APIs del Servicio de Impuestos Internos, más el servicio de administración, con el fin de mantener una configuración efectiva que mantenga la protección de las aplicaciones adaptándose a mejoras y cambios de los sistemas de negocio del SII, generados por las áreas de desarrollo internas.

El oferente debe proveer una herramienta que permite acceder a información para realizar auditorías acerca de su funcionamiento y verificación de cumplimiento de SLA.

Se requiere que el servicio WAAP requerido por el SII considere lo señalado a continuación:

1. La solución ofertada debe tener presencia en algún cuadrante de “Gartner Magic Quadrant for API y Web Application Firewalls (WAAP)” en la versión vigente a la fecha de publicación de la licitación.
2. Debe contar con, a lo menos, un especialista certificado en la solución WAAP.
3. La solución debe considerar a lo menor un Througput de 10 Gbs por cada centro de datos.
4. Los servidores de aplicaciones están conectados a una red DMZ de 10GE.
5. La solución debe proteger las credenciales de sesión (cookies), mitigar posibles ataques de fuerza bruta, actualización de firmas o reglas de detección de ataques.
6. Debe proporcionar un registro exhaustivo de los ataques web, el tráfico de acceso y pistas de auditoría de administrador.
7. Debe realizar inspección de tráfico SSL.
8. Debe proveer controles de seguridad mediante reglas configurables contra ataques o incidentes del tipo Bot Management.
9. Debe proveer controles de seguridad para el correcto uso de las API publicadas por el SII hacia internet, por parte de sus usuarios externos.
10. Debe permitir al menos, el bloqueo de consultas HTTP, por dirección IP, por conexión y por sesión de aplicación.
11. La solución debe permitir operar en modo pasivo, de manera de poder inspeccionar tráfico sin realizar bloqueo.
12. Los registros deben ser exportables, en línea a través de syslog, al menos en formato de evento común (CEF) o JSON, que permita la integración con el sistema de gestión de eventos (SIEM o similar).
13. La solución debe ofrecer la posibilidad de definir diferentes políticas para distintas aplicaciones (dinámicas y estáticas) y proporcionar políticas para aplicaciones empresariales, como Outlook Web Access, SharePoint y Oracle.
14. La solución debe incluir la protección de los ataques comunes mencionados en el OWASP top 10 (2017 y futuras versiones) y WASC.
15. El SII posee 3 dominios y 40 subdominios públicos. Como mínimo la solución ofertada debe considerar la protección de 10 subdominios públicos (FQDN) y 100 mbps de tráfico limpio procesado. Si el esquema de licenciamiento lo requiere, es decir, no cubre los 40 subdominios, deberá cotizar como adicional el bloque de crecimiento hasta que se cubran los 27 subdominios.
16. Debe considerar una consola de administración.
17. Debe considerar la administración del servicio en modalidad on-demand en cualquier horario que el servicio defina para pasar aplicaciones a producción.

18. Se debe considerar un uptime del servicio de 99,6% anual.
19. El servicio ofertado debe tener la capacidad de inspeccionar tráfico de aplicativos del SII u otros que no necesariamente cumplen estándares globales relativos a protocolos de internet, tales como los estándares RFC. En este punto, se espera que el servicio ofertado tenga la capacidad de plantear excepciones sobre reglas de cumplimiento de RFC, de tal forma que esta situación no sea excluyente para que el servicio WAAP pueda realizar las inspecciones de seguridad en dichas aplicaciones del SII.

2.1.3.5. ÍTEM 6: SERVICIO GESTIONADO PARA DETECCIÓN Y RESPUESTA FRENTE A AMENAZAS EN RED DE DATOS INTERNA (NDR)

El servicio debe estar basado en tecnología del tipo NDR (network detect and response), la cual debe generar una visibilidad integral y profunda respecto los eventos y amenazas de seguridad de la red de datos interna del SII, así como identificar sucesos o situaciones relevantes que puedan afectar la performance de las comunicaciones internas de sistemas y usuarios de la organización.

El servicio por contratar debe cumplir con las siguientes características:

a) El hardware y software de este servicio debe operar en un equipamiento dedicado, las cuales se habilitarán en las dependencias del SII, quien proveerá de las condiciones de energía y de espacio requerido. En la propuesta se debe indicar los requerimientos de energía y de espacio para habilitar el equipamiento requerido para la entrega del servicio.
b) El servicio ofertado debe ser capaz de monitorear el tráfico de datos interno de servidores y funcionarios. Para ello se deberá trabajar en conjunto con el SII en la etapa de implementación del servicio, para lograr la mejor opción técnica de integración de la solución NDR con la red interna del SII.
c) Datos para el correcto dimensionamiento del servicio:
    - Se cuenta internamente con la interacción de 7500 dispositivos (servidores físicos, virtuales, equipos de comunicaciones, equipos SAN, estaciones de trabajo de funcionarios, equipos LAN, principalmente).
    - Ancho de banda total a inspeccionar de 10GB por cada centro de datos (2).
    - Retención de la información de traza del servicio: 2 meses
d) La tecnología por utilizar debe estar en “Gartner’s Magic Quadrant” para dispositivos tecnológicos del tipo NDR.
e) El servicio ofertado debe proveer una herramienta para uso por parte de SII, que permite acceder a información para realizar auditorías acerca de su funcionamiento y verificación de cumplimiento de SLA.
f) El nivel de Throughput a considerar es a lo menos de 10 Gbps por cada Centro de datos.
g) El servicio debe considerar un uptime del servicio de 99,6% anual.
h) Debe permitir operar en modo monitor, sin tomar acción, o incluso detener la inspección, sin afectar el tráfico de los servicios del SII.
i) El servicio ofertado debe contar con al menos 1 especialista con certificaciones técnicas en la solución NDR (Se deben adjuntar los certificados del personal)
j) Debe soportar módulos de fibra de 1Gb o 10 GE.
k) Se deben realizar mantenciones periódicas sobre los elementos de hardware y software, cada 6 meses, las cuales debe ser programadas con personal del SII, quien validará y gestionará las acciones internas requeridas.
l) El adjudicatario debe mantener un inventario de todos los elementos de software y hardware requeridos para la entrega del servicio, considerando los detalles de ubicación física, conexiones, circuitos eléctricos y vigencia de las licencias requeridas. Este inventario debe ser entregado al SII, con los escalamientos de atención necesarios.
m) La tecnología debe ser capaz de realizar la detección de dispositivos infectados, comprometidos con tráfico sospechoso, detección de exfiltración de información.

n) Detección de ataques de denegación de servicio entrante o saliente.
o) Debe ser compatible con todos los elementos tradicionales de la red (firewall, switch, router)
p) Se debe integrar con el servicio SOC especificado en la componente 1 ítem 1 de la presente licitación.
q) Se debe integrar con la herramienta SIEM o similar especificada para la componente 1 ítem 1 de la presente licitación.
r) Capacidad de rendimiento en redes de hasta 40 Gbps.
s) Análisis de tráfico y detección de amenazas avanzadas: La herramienta debe ser capaz de analizar el tráfico de red en tiempo real y utilizar técnicas avanzadas de detección de amenazas para identificar patrones sospechosos y comportamientos anómalos.
t) Escalabilidad y adaptabilidad: La herramienta debe ser adecuada para redes de diferentes tamaños y complejidades, lo que permite su implementación en un entorno diverso tecnológicamente y en constante crecimiento.
u) Monitoreo en tiempo real: La herramienta debe ofrecer una visibilidad completa y en tiempo real del tráfico de red para detectar y responder rápidamente a las eventuales amenazas y ataques en curso.
v) Interfaz intuitiva y visualización de datos: debe proveer una interfaz fácil de usar y una representación gráfica clara de la actividad de la red, de tal forma que permita a los analistas identificar rápidamente posibles problemas y tomar decisiones informadas.
w) Análisis forense y replay de eventos: La herramienta debe permitir el análisis forense de eventos pasados y la reproducción del tráfico de red asociado para investigar incidentes y tomar medidas correctivas.
x) Integración: capacidad de integración con otras soluciones de seguridad y herramientas de administración de red, como firewalls, IPS y SIEM, garantiza una gestión más efectiva y coordinada de la seguridad. Especialmente lo especificado en la componente 1 ítem 1 de la presente licitación.
y) Identificación y análisis de amenazas internas: La herramienta debe ser capaz de detectar comportamientos sospechosos dentro de la red corporativa para prevenir y detectar amenazas internas.
z) Automatización de respuestas: La herramienta debe permitir la automatización de respuestas ante ciertos tipos de amenazas o eventos para una reacción rápida y precisa a ataques conocidos.
aa) Actualizaciones de amenazas en tiempo real: La herramienta debe estar conectada a una base de datos universal actualizada de amenazas y malware en tiempo real para mejorar la precisión de las detecciones.
bb) Análisis de tráfico encriptado opcional: Si bien no se debe realizar el análisis de cifrado de forma predeterminada debido a la privacidad y confidencialidad de los datos, la herramienta podría ofrecer una opción para que los administradores activen el análisis de tráfico encriptado en ciertos escenarios permitidos legalmente, mejorando aún más la seguridad de la red.

2.1.3.6. SLA componente 1 ítems 2, 3, 4, 5 y 6

Se considerarán los siguientes tiempos de respuestas para el escalamiento ante cualquier problema con el servicio gestionado de seguridad, de acuerdo con lo siguiente:

- **Soporte telefónico especializado:** Consiste en que, frente a un requerimiento del Servicio o escalamiento por incidente de seguridad, un especialista se contactará en el plazo de 20 minutos, contados desde el requerimiento del SII para asistirlo por vía telefónica, en la solución de problemas que se detecten en el servicio, en el funcionamiento del hardware cuando este no opere conforme a las especificaciones del fabricante y/o para ayudarlo a restablecer las condiciones de operación acordadas entre el adjudicatario y SII.

  El incumplimiento del plazo indicado en el párrafo anterior dará lugar a la aplicación de la multa señalada en el punto 4.2.7 de las bases administrativas, parte I.

- **Escalamiento de problemas críticos:** Consiste en que el adjudicatario procederá a involucrar al centro de soporte telefónico del fabricante en la solución de problemas que no puedan ser resueltos en el ámbito local. Este escalamiento no puede exceder las 2 horas corridas, contadas desde la realización del requerimiento del SII, el cual debe contar con un número o identificador para su seguimiento. El adjudicatario deberá proveer al SII el acceso a la plataforma del centro de soporte del fabricante, para poder realizar el seguimiento del caso.

  El incumplimiento del plazo indicado en el párrafo anterior dará lugar a la aplicación de la multa señalada en el punto 4.2.8 de las bases administrativas, parte I.

- **Tiempo de asistencia on-site:** Es el tiempo que toma la presentación en las dependencias del Servicio, de un especialista certificado en la plataforma ofertada para atender el evento, éste no puede exceder las 2 horas corridas contadas desde la realización del requerimiento del SII, lo que debe quedar informado por cualquier medio escrito donde conste hora y fecha de este.

  El incumplimiento del plazo indicado en el párrafo anterior dará lugar a la aplicación de la multa señalada en el punto 4.2.9 de las bases administrativas, parte I.

- **Reposición del servicio:** El adjudicatario debe contemplar un tiempo máximo de 5 horas para la reposición del servicio en caso de falla de algún recurso de hardware y/o software provisto para cumplir los servicios de seguridad, contadas desde el aviso por parte del SII vía telefónica respaldado mediante correo electrónico, u otro medio en el que quede constancia por escrito de la fecha y hora del aviso.

  El incumplimiento del plazo indicado en el párrafo anterior dará lugar a la aplicación de la multa señalada en el punto 4.2.10 de las bases administrativas, parte I.

2.2. Componente 2: Servicios Profesionales.

Dicho componente consiste en la provisión de Servicios Profesionales avanzados en el ámbito de la seguridad de la información mediante el consumo de unidades de trabajo. Las unidades de trabajo serán acumulables mes a mes durante un año contrato, al siguiente año se perderán las unidades de trabajo no utilizadas. Para referencia se estima una tasa de utilización de Unidades de Trabajo que va entre las 25 y 35 unidades mensuales.

2.2.1. **Marco General del servicio**

Se entiende por servicios profesionales avanzados a los prestados por especialistas que cuenten con conocimientos y experiencia en la definición e implementación de políticas de seguridad corporativas, entre otras, normas Nch-ISO 27001, 27002, 22301, Ciberseguridad de NIST, ITIL, Decreto Supremo 83, Instructivo Presidencial de Seguridad y Ciberseguridad 2018, Ley Chilena de Protección de Datos Personales, Política Nacional de Ciberseguridad, Ley Nº 19.223 sobre delitos informáticos, Ley Nº 19.628 sobre protección de la vida privada, ISO 27032 Gestión de la Ciberseguridad, COBIT.

2.2.2. **Modalidad de Uso**

Se solicitará asesoría proactiva, es decir, que esté al tanto de las necesidades de la institución en el ámbito de seguridad informática, a partir de lo cual se propongan lineamientos y/o soluciones a necesidad del SII.

Por cada actividad de asesoría que se realice se deberá efectuar una planificación inicial (cuando corresponda), la que contendrá los requerimientos del SII, una estimación de las horas que se utilizarán para satisfacer dichos requerimientos y un plazo de entrega del trabajo realizado, el que se convendrá en conjunto entre los administradores de contrato de ambas partes.

La modalidad de uso de los servicios profesionales será mediante unidades de trabajo. La equivalencia de valor de éstas será medida de la siguiente manera:

- 1 Hora cronológica de Consultor Senior Gestión de Seguridad equivale a 1,0 Unidad de Trabajo
- 1 Hora cronológica de Consultor Senior Ciber Seguridad equivale a 1,0 Unidades de trabajo
- 1 Hora cronológica de Consultor Junior Seguridad TI equivale a 0,5 Unidades de trabajo

2.2.3. **Perfiles Requeridos**

- Consultor Senior Gestión de Seguridad: experiencia y conocimientos en los siguientes temas:
  - Implementación / Certificación ISO/IEC 27001 - Sistema de Gestión de Seguridad de la Información
  - Implementación BCP/DRP - Sistema de Gestión de Continuidad del Negocio ISO/IEC 22301
  - Creación CSIRT - Red/Blue Teams
  - Ingeniería de Roles y Perfiles
  - Capacitación especializada en seguridad y Awareness
  - Compliance DS83 - PCI - PMG/MEI - SSI – CMF

- Consultor Senior CiberSeguridad: experiencia y conocimientos en los siguientes temas:
  - Implementación Framework de Ciberseguridad NIST
  - Análisis de Vulnerabilidades / Pentesting / Ethical Hacking
  - Capacitación especializada técnica en Ciberseguridad
  - Implementación dispositivos de Seguridad (SIEM, NAC, FW, WAAP, FWDB)
  - Seguridad de la información en sistemas de nube pública AWS, AZURE y GOOGLE
  -
- Consultor Junior Seguridad TI: experiencia y conocimientos en los siguientes temas:
  - Implementación sistemas de Antivirus
  - Consultoría en redes de comunicaciones
  - Análisis de tráficos y redes WiFi
  - Soporte redes, Servers y Sistemas Operativos
  - Herramientas y productos de Seguridad de la información en sistemas de nube publica AWS, AZURE y GOOGLE

2.2.4. **Envío Mensual de Reporte**

El adjudicatario comprometerá el envío mensual de un reporte con el resumen de utilización de unidades de trabajo del mes y la acumulación a la fecha.

Las actividades realizadas en el marco de cumplimiento de este componente deberán constar en este informe mensual el cual deberá ser entregado a administrador de contrato del SII, la cual tendrá un plazo de 10 días hábiles para pronunciarse sobre el informe.

En caso de detectar algún error o alcance se solicitará al adjudicatario realizar la corrección del o los errores o la inclusión del o los alcances faltantes, lo que se deberá efectuar en un plazo a convenir, lo que en ningún caso podrá superar los 4 días hábiles. Dicho periodo de tiempo no se

considera parte de las unidades de trabajo puestas a disposición por el adjudicatario a favor del SII.

En caso de que el nuevo informe persista con errores o no se hubieren contemplado el o los alcances anteriormente informados, la empresa deberá efectuar los cambios en un plazo no superior a 2 días hábiles. Después de la tercera iteración se aplicarán multas indicadas en el punto 4.2.16, situación que no libera al adjudicatario de la obligación de entregar el informe.

Dicho periodo de tiempo no se considera parte de las unidades de trabajo puestas a disposición por el adjudicatario a favor del SII.

El SII se reserva el derecho de realizar una evaluación permanente de la calidad del servicio de asesoría recibido por parte de los **especialistas de seguridad**, pudiendo eventualmente solicitar el cambio de los especialistas asignados.

Las unidades de trabajo podrán comenzar a ser requeridas por parte del SII, a partir de la recepción conforme de la instalación y puesta en marcha de los servicios.

3. COORDINACIÓN PARA LA MITIGACIÓN DE PROBLEMAS

Para garantizar una atención rápida y oportuna, el adjudicatario deberá entregar un protocolo de contacto para la atención de fallas de los equipamientos de su propiedad (y administrados por éste), que se encuentran en dependencias del SII. Los Centro de datos del SII pueden recibir la visita de técnicos en horario 7 días, las 24 horas, previa coordinación entre las partes. Cualquier demora en la atención generada por condiciones del SII (por ejemplo, freezing, ausencia de personal, entre otros) no se considerará en los SLA contratados.

Excepciones de servicio:

En caso de que uno de los Centro de datos presente un fallo catastrófico, **NO** se considerará una falta a los SLA contratados, mientras este se encuentre fuera de servicio. Sin perjuicio de lo anterior, el adjudicatario debe tomar los recaudos necesarios para reponer cualquier equipo dañado para el momento en que el Centro de datos vuelva a entrar en funcionamiento.

4. SOBRE LA INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN MARCHA DE LOS SERVICIOS

Se entenderá por puesta en marcha, la ejecución exitosa por parte del adjudicatario de las siguientes tareas:

1. Instalación de todo el hardware y software ofertado por parte del adjudicatario en las ubicaciones físicas indicadas por el SII o definidos en su oferta.

2. Instalación de todos los licenciamientos correspondientes, así como también, de las últimas actualizaciones recomendadas por el fabricante.

3. Configuración de todos los sistemas de acuerdo con las políticas y criterios que le serán entregados por el SII. En el caso de los servicios de componente 1 (items 1, 2, 3, 4, 5 y 6) que requieran la definición de políticas y/o configuración de reglas, en esta etapa considerará, a lo menos, la activación de reglas que sean comunes a nivel industria, quedando para una etapa posterior la configuración de reglas más específicas y dependientes de la realidad del SII.

4. Definición de los procedimientos de backups que aplicará el adjudicatario.

5. Integraciones necesarias, de los servicios ofertados, con la infraestructura de red del SII.

6. Integración de los servicios ofertados con los procesos del SII, según se requiera.

7. Entrega de los procedimientos de escalamiento y vuelta atrás en el caso de ser necesario.

Se dará por finalizada la etapa de instalación, configuración y puesta en marcha de los servicios, cuando el SII concluya a plena satisfacción las pruebas y chequeos necesarios para constatar que los servicios activados, se ajustan en su totalidad a las especificaciones antes mencionadas, así como a las prestaciones ofertadas por el adjudicatario.

Las pruebas serán realizadas con el asesoramiento técnico del adjudicatario. El adjudicatario emitirá informes de avance (el plazo y el contenido de estos se acordará entre las partes) y uno final, que será aprobado por el Jefe de Departamento Informática Aseguramiento de Estándares Tecnológicos de la Subdirección de Informática.

Entre otras, se considera la realización de las siguientes pruebas:

- ✓ Verificación de la instalación de todos los servicios contratados.
- ✓ Comprobación del funcionamiento de los servicios ofertados.
- ✓ Comprobación de todos los "features" descritos como disponibles en la oferta para cada componente.
- ✓ Comprobación de los uptime comprometidos, a partir de la simulación de fallas o indisponibilidad de componentes, verificando la activación de redundancias o contingencias los servicios, según sea el diseño implementado por el oferente.

En los casos que se requiera direcciones IP para los dispositivos a instalar, las mismas le serán entregadas por el SII oportunamente.

El adjudicatario contará con colaboración del personal del SII, sin embargo, la instalación, configuración y puesta en marcha de los servicios son de su exclusiva responsabilidad.

El adjudicatario deberá hacer entrega de toda la documentación y procedimientos necesarios para el correcto uso de los servicios ofertados. Dicha documentación deberá estar actualizada, obligándose el adjudicatario a remitir toda modificación de esta durante la vigencia del contrato.

5. **PROPUESTA TÉCNICA**

El oferente deberá adjuntar en un documento el desarrollo de la propuesta técnica, considerando todo lo señalado en los puntos anteriores y lo solicitado en el Anexo N°6.

IV)ANEXOS BASES

ANEXO N° 1: ANTECEDENTES DEL OFERENTE Y SUBCONTRATISTA

1.- Nombre o Razón Social :

2.- RUT o Cédula Identidad :

3.- Giro :

4.- Dirección :

5.- Comuna :

6.- Teléfono :

7.- E-mail :

8.- Representante Legal (Si corresponde) :

9.- RUT Representante Legal (Si corresponde) :

10.- Personería del Representante Legal (Si corresponde)
- Fecha de la Escritura Pública:
- Notaría:

11.- Encargado de la solicitud de cotización
Nombre:
Teléfono:
E- Mail:

12.- Estructura Societaria a **la fecha de cierre de la oferta**:

(COMPLETAR INDICANDO TODOS LOS SOCIOS o ACCIONISTA CON UN 10% O MÁS DE PARTICIPACIÓN EN EL CAPITAL, si no está completo el SII solicitará esta información en el proceso de aclaración de ofertas, a través del Portal)

RUT SOCIO/ACCIONISTA	NOMBRE COMPLETO SOCIO/ACCIONISTA	% PARTICIPACIÓN	Indicar si es funcionario del SII (SI/NO)

13.- Subcontratistas.

RUT	NOMBRE/RAZÓN SOCIAL	TRABAJOS A REALIZAR	% aproximado (según monto) que representa el subcontrato en el valor total de la oferta económica

Nota: Este Anexo debe presentarse en este formato.

14.- Unión Temporal de Proveedores

RUT	NOMBRE/RAZÓN SOCIAL

Nota: Este Anexo debe presentarse en este formato.

ANEXO N° 2: PROPUESTA ECONÓMICA (Nombre del oferente)

El oferente debe ofertar por todos las componentes e ítems indicados en este anexo, de lo contrario su oferta será declarada inadmisible.

Componente 1	Valor Mensual Neto por Ítem (UF)
Ítem 1: Servicio de centro de operación de seguridad (SOC)	
Ítem 2: Sistema de Prevención y Detección de Intrusos (IPS).	
Ítem 3: Sistema de Protección contra ataques de denegación de servicios.	
Ítem 4: Servicio de Análisis de vulnerabilidades.	
Ítem 5: Servicio de firewall aplicativo (WAAP)*	
Ítem 6: Servicio Gestionado de detección y respuesta de amenazas en red de datos interna (NDR).	

***** Considerar la protección de al menos 10 subdominios públicos (FQDN) y 100 mbps de tráfico limpio procesado**.**

Componente 2	Valor mensual Neto (UF)
Alternativa 1: Bolsa de 1404 unidades de trabajo para toda la vigencia del contrato	
Alternativa 2: Bolsa de 1224 unidades de trabajo para toda la vigencia del contrato	
Alternativa 3: Bolsa de 1008 unidades de trabajo para toda la vigencia del contrato	

Nota: El Servicio seleccionará la alternativa que se ajuste al presupuesto global disponible de acuerdo a lo señalado en el punto 4 de las Bases Administrativas de Licitación, Parte I.

Valor Unidad de Trabajo Adicional Componente 2	Valor Neto (UF)
Valor unidad de trabajo adicional	

NOTAS:

- Para efectos de valorizar la unidad de trabajo considerar lo indicado en el punto 2.2 de las Bases Técnicas.

ANEXO N° 3: FICHA EXPERIENCIA DE LA EMPRESA

Completar tantas fichas como experiencia demostrable relevante quiera presentar. Asignar correlativo a cada una de ellas y presente en un documento único. Se deberá utilizar este formato para los siguientes criterios de evaluación:

Componente 1:

- "Cantidad de clientes en la prestación de servicios SOC"
- "Experiencia general del oferente en el mercado de servicios de seguridad de la información"
- "Experiencia especifica del oferente en el mercado de servicios gestionados de seguridad"

Componente 2:

- "Cantidad de clientes para las cuales presta los servicios de asesoría de seguridad de la información y ciberseguridad".
- "Experiencia del oferente en el mercado en el rubro de servicios de consultoría avanzados en seguridad de la información y ciberseguridad."

N° Ficha	(asignar correlativo por cada experiencia demostrable)		
N° de Componente y/o ítem que acredita la ficha			
Nombre del Cliente o mandante			
Tipo de cliente (Público o Privado)			
Contacto del cliente:			
Nombre			
Cargo			
Teléfono		e-mail institucional	
Nombre del proyecto			
Fecha de inicio		Fecha de término	
Plataforma Tecnológica			
Descripción del proyecto (breve)			
Firma del mandante	En los casos que no se acredite la experiencia con otro documento. La firma podrá ser electrónica simple o avanzada o bien física, escaneando el documento.		

NOTAS: Por cada ficha se debe incluir contrato, orden de compra u otro documento que acredite la experiencia señalada. Sin perjuicio de lo anterior, y en casos que el oferente no pueda presentar dichos documentos debido a acuerdos de confidencialidad suscritos con sus clientes, se podrá presentar esta ficha suscrita por el mandante a fin de acreditar la experiencia.

Si el proveedor posee experiencia en órganos de la Administración del Estado, para efectos de acreditar tal experiencia, bastará con que indique el número de orden de compra y/o ID de

Licitación Pública correspondientes, siempre y cuando la información publicada en el portal www.mercadopublico.cl permita verificar lo declarado en la ficha de experiencia.

Sólo serán consideradas las fichas de experiencia asociadas a servicios de seguridad informática.

Para efectos del criterio de experiencia del oferente, se considerarán años cumplidos a la fecha de publicación de la presente licitación, contados desde la fecha de inicio del proyecto más antiguo presentado.

ANEXO N° 4: FICHA CURRÍCULUM VÍTAE

En el **listado de personal del proyecto**, se debe señalar todos los especialistas que prestarán servicios en el contexto del servicio licitado, **acompañando el Curriculum Vitae y la imagen de la certificación en las herramientas asociadas** a componentes e ítems licitados, que la oferta indique. La presente información será utilizada para evaluar los siguientes criterios de evaluación:

Componente 1:

Item1: "Analistas de seguridad con certificaciones nivel 1, en las herramientas con las que entregará el servicio SOC"
Item1: "Analistas de seguridad con certificaciones para nivel 2, que forman parte del servicio SOC"
Ítem 2: "Especialistas con certificaciones técnicas en la solución IPS con la que entregará el servicio"
Ítem 3: "Especialistas con certificaciones técnicas en la solución de servicios de protección contra ataques DDoS con la que entregará el servicio"
Ítem5: "Especialistas con certificaciones técnicas en la solución WAAP con la que entrega el servicio"
Ítem6: "Especialistas con certificaciones técnicas en la solución NDR con la que se entrega el servicio"

Componente 2:

- "Certificaciones de reconocimiento internacional del o los consultores senior en seguridad de la información tales como, CISSP, CISM, CISA o similar".
- "Certificaciones de reconocimiento internacional del o los consultores senior en ciberseguridad tales como, CISSP, CISM, CISA o similar"
- "Certificaciones del o los consultores junior en seguridad TI (Diplomados, cursos de especialización, certificaciones internacionales u otros asociados a seguridad TI)."

Listado de Personal del Proyecto				
Componente	**Ítem**	**Herramientas ofertadas asociada al ítem (INDICAR)**	**Certificación del especialista (ACOMPAÑAR DOCUMENTO)**	**Nombre del Especialista(s)**
1	ITEM 1: Servicio de centro de operación de seguridad (SOC) (Analistas de seguridad con certificaciones nivel 1 y nivel 2)			
	ITEM 2: Servicio Gestionado de Detección y Prevención de Intrusos (IPS).			

	ITEM 3: Servicio Gestionado de Protección contra ataques de denegación de servicios (Anti DDOS).			
	ITEM 4: Servicio Gestionado de Análisis de vulnerabilidades.			
	ITEM 5: Servicio Gestionado de Firewall para aplicaciones Web y APIS (WAAP).			
	ITEM 6: Servicio Gestionado de detección y respuesta de amenazas en red de datos interna (NDR).			
2	Certificaciones de reconocimiento internacional del o los **consultores senior en seguridad** de la información tales como, CISSP, CISM, CISA o similar.			
	Certificaciones de reconocimiento internacional del o los **consultores senior en ciberseguridad** tales como, CISSP, CISM, CISA o similar.			
	Certificaciones del o los **consultores junior en seguridad TI** (Diplomados, cursos de especialización, certificaciones internacionales u otros asociados a seguridad TI).			

FICHA CURRÍCULUM VÍTAE

ANTECEDENTES PERSONALES Nombre Completo RUT Teléfono	
CARGO EN EL PROYECTO	
ESTUDIOS UNIVERSITARIOS Profesión	
Año egreso	
OTROS ESTUDIOS	

ANEXO N° 5: REQUISITOS MÍNIMOS DE LOS PRODUCTOS Y/O SERVICIOS OFERTADOS

La presentación de este anexo y el cumplimiento de todos los requisitos mínimos indicados en él, son indispensables para evaluar la oferta. La **NO** presentación de este anexo o el no cumplimiento de alguno de los aspectos mínimos indicados, significará la **inadmisibilidad** de la misma.

Indicar SI/NO según el servicio ofertado posee o NO, las condiciones que se señalan. **Cualquier otro texto u omitir una respuesta, se entenderá que la oferta NO cumple con la condición requerida.**

REQUISITOS MÍNIMOS		Indicar SI/NO
Técnico Residente	El servicio de gestión de la plataforma considera un especialista técnico onsite, en modalidad 5x9, residente en las instalaciones del SII durante toda la vigencia del contrato, quien será responsable de la administración de los servicios y la canalización de requerimientos.	
Componente 1, Ítem 1: **Servicio SOC**	El servicio ofertado cumple con cada uno de los puntos especificados en el apartado 2.1.1. de las actuales Bases de Licitación (ÍTEM 1: SERVICIO DE CENTRO DE OPERACIÓN DE SEGURIDAD (SOC)).	
Componente 1, Ítem 2: **Prevención y Detección de Intrusos (IPS)**	El servicio ofertado cumple con cada uno de los puntos especificados en el apartado 2.1.2. (ÍTEMS 2, 3 Y 5 EN AMBIENTES DE NUBE PÚBLICA DEL SII) y el apartado 2.1.3.1. para el ámbito on-premise, (ÍTEM 2: SERVICIO DE PREVENCIÓN Y DETECCIÓN DE INTRUSOS (IPS)),de las actuales Bases de Licitación.	
Componente 1, Ítem 3: **Protección contra ataques de denegación de servicios**	El servicio ofertado cumple con cada uno de los puntos especificados en el apartado 2.1.2. (ÍTEMS 2, 3 Y 5 EN AMBIENTES DE NUBE PÚBLICA DEL SII) y el apartado 2.1.3.2. para el ámbito on-premise, (ÍTEM 3: SERVICIO DE PROTECCIÓN CONTRA ATAQUES DE DENEGACIÓN DE SERVICIOS),de las actuales Bases de Licitación.	
Componente 1, Ítem 4: **Análisis de vulnerabilidades**	El servicio ofertado cumple con cada uno de los puntos especificados en el apartado 2.1.3.3. (ÍTEM 4: SERVICIO DE ANÁLISIS DE VULNERABILIDADES), de las actuales Bases de Licitación.	
Componente 1, Ítem 5: **(Firewall para aplicaciones Web y APIS)**	El servicio ofertado cumple con cada uno de los puntos especificados en el apartado 2.1.2. (ÍTEMS 2, 3 Y 5 EN AMBIENTES DE NUBE PÚBLICA DEL SII) y el apartado 2.1.3.4. para el ámbito on-premise, (ÍTEM 5: SERVICIO DE FIREWALL PARA APLICACIONES WEB Y APIS (WAAP), de las actuales Bases de Licitación.	
Componente 1, Ítem 6: **(Servicio Gestionado de detección y respuesta de amenazas en red de datos interna (NDR, Network Detección and Response)**	El servicio ofertado cumple con cada uno de los puntos especificados en el apartado 2.1.3.5. (ÍTEM 6: SERVICIO GESTIONADO PARA DETECCIÓN Y RESPUESTA FRENTE A AMENAZAS EN RED DE DATOS INTERNA), de las actuales Bases de Licitación.	
Componente 2: (servicios profesionales)	El servicio ofertado cumple con cada uno de los puntos especificados en el apartado 2.2. (Componente 2: Servicios Profesionales), de las actuales Bases de Licitación	

ANEXO N°6 CARACTERÍSTICAS TÉCNICAS DE LOS SERVICIOS OFERTADOS

COMPONENTES	Característica	INDICAR OFERTA
General	Plazo de implementación de todos los servicios ofertados, tanto de componente 1 como de componente 2 (ref. 4.4 bases administrativas: **"**Plazo de puesta en marcha de los servicios contratados")	Indicar días corridos
	Detallar el plan de implementación general de todos los servicios , indicando, a lo menos, los siguientes elementos: - Definición de contrapartes. - Levantamientos de información requeridos por el oferente. - Definición de los protocolos necesarios para la operación de los servicios. - Tiempo de implementación de cada servicio - Definición de criterios de aceptación conforme con el SII. - Hitos para el de inicio de explotación de los servicios.	Detallar
Componente 1, ítem 1: **Servicio de SOC**	Indicar las certificaciones del SOC vigentes, de nivel internacional en el ámbito de seguridad de la información.	Detallar
	Indicar como el servicio SOC se alimentará de los registros LOGs o eventos generados a partir de los servicios IPS, WAAP, AntiDDos y NDR, asociados a la componente 1, tanto en ambientes on-premise como de nube pública del SII, así como también de los equipos de seguridad que son parte de la infraestructura perimetral del SII (firewalls perimetrales, principalmente).	Detallar
	Indicar como servicio SOC entregará permanentemente una mirada global de la situación y estado de la plataforma de seguridad, tanto a nivel on premise como a nivel de nube pública del SII, tomando y ejerciendo el rol de detección, análisis y gestión de los incidentes y/o alarmas detectadas, y de informar al SII sobre cualquier hallazgo o incidente que vaya dirigido a afectar o dañar algún recurso del SII.	Detallar
	Indicar las que herramientas contempla el servicio que permitan al SII tener una visualización de resultados, patrones y gráficos interactivos respecto una visión global de los eventos.	Detallar
	Indicar como el servicio contempla la integración y uso de los registros de tráfico de las plataformas de seguridad perimetral del SII (firewalls perimetrales) presentes en los Centro de datos que utiliza el SII para la entrega de sus servicios.	Detallar
	Indicar como el servicio contempla la integración y uso de los registros de tráfico de las herramientas de seguridad perimetral presentes en los ambientes de nube pública del SII, para la entrega de sus servicios.	Detallar
	Indicar si el servicio cuenta con operadores-analistas de seguridad que posean certificaciones en la herramienta SIEM o similar para correlación avanzada de eventos. Indicar la cantidad de analistas con las certificaciones indicadas y adjuntarlas.	Detallar
	Indicar si el servicio cuenta con analistas de seguridad que posean certificaciones para nivel 2, ya sea CCNA Security, Ethical Hacking o similares. Indicar la cantidad de analistas con las certificaciones indicadas y adjuntarlas.	Detallar
	Indicar si el servicio ofertado contempla la implementación, en coordinación con el SII. de procedimientos para respuesta y resolución de alarmas de seguridad generadas a partir de los servicios correspondientes de los ítems 2, 3, 5 y 6 de la componente 1 de la presente licitación.	Detallar

	Indicar si el servicio ofertado contempla la entrega semanal y mensual de reportes en formato pdf., resumen ejecutivo y detallado a nivel técnico, respecto de los eventos relevantes ocurridos durante el período.	Detallar
	El servicio contempla la elaboración y entrega, cuando el SII lo solicite, de un informe de la gestión realizada respecto de un determinado incidente de seguridad que sea de interés.	Detallar
	Detallar sobre la herramienta para correlación de eventos que se encuentren Cuadrante Gartner, ya sea SIEM o similar, en la versión vigente a la fecha de publicación de la licitación. Indicar la herramienta y sus características técnicas.	Detallar
	Detallar sobre la herramienta, vista o Dashboard, mediante el cual el SII tendrá acceso a la verificación de las acciones de correlación realizadas por el SIEM o similar, con el fin de efectuar sus propias consultas y descargar informes resultantes.	Detallar
	Indicar la capacidad del SOC para almacenamiento histórico de información, online (días) y el tiempo de retención (meses).	Detallar
	Indicar si el servicio considera el o los dispositivos físicos y/o lógicos requeridos para la recolección de LOGS, de manera de garantizar la recepción de los eventos de los dispositivos de seguridad de la componente 1 (IPS, AntiDDos, WAAP, NDR, herramientas de seguridad en nube pública) y los equipos de seguridad que el SII requiera integrar.	Detallar
	Indicar la ubicación física de las instalaciones del SOC. En caso de corresponder a instalaciones fuera del país, indicar si cuenta con una contraparte especializada, residente en el territorio nacional, cuya función será la de servir de apoyo y complemento para el relacionamiento entre el SII y SOC.	Detallar
	Indicar si el servicio ofertado cuenta con un Dashboard, con disponibilidad 7 días, las 24 horas, los 365 días del año, para monitorear la disponibilidad del SOC, informando el estado de los dispositivos requeridos para la entrega de servicio, cantidad de registros de eventos por dispositivo monitoreado, cantidad de eventos correlacionados y el estado de los incidentes reportados.	Detallar
	Indicar el porcentaje anual de disponibilidad del servicio SOC.	Detallar
	Indicar el tiempo máximo para reposición del servicio en caso de falla de algún recurso de hardware y software necesario para cumplir con el servicio de SOC, contadas desde el aviso por parte del SII vía telefónica respaldado mediante correo electrónico, u otro medio en el que quede constancia por escrito de la fecha y hora del aviso.	Detallar
	Indicar el tiempo máximo contemplado por el servicio SOC para informar al SII de los incidentes de seguridad identificados. El contacto debe ser realizado mediante llamado telefónico, según la matriz de escalamiento entregada por el SII al adjudicatario.	Detallar
Componente 1, ítems 2, 3 y 5 en ambientes de nube pública del SII.	Detallar como el servicio ofertado considera implementación y configuración de nuevas herramientas o productos de nube que aporten como mejoras a las condiciones de seguridad de los sistemas de nube del SII, acordando con el SII su eventual implementación o no (El costo de estas eventuales nuevas herramientas será asumido por el SII por todo el periodo del contrato).	Detallar
	Indicar como el servicio ofertado cuenta con conocimientos respecto la función, alcance y configuración de las herramientas de seguridad de nube mencionadas como parte de la plataforma se seguridad de los sistemas de nube pública del SII (indicadas en el apartado 2.1.2), incorporando toda la información necesaria a la operación del servicio SOC especificado en el ítem 1 de la	Detallar

	Componente 1, con el fin de activar el monitoreo y detección de eventos, alertas, amenazas y/o incidentes de seguridad.	
	Indicar como el servicio ofertado incorpora la información generada en las componentes de seguridad de nube, a los cruces de datos realizados en el SOC por la herramienta SIEM o similar, en el fin de detectar eventuales amenazas o incidentes de seguridad de naturaleza avanzada.	Detallar
Componente 1, Ítem 2 **Prevención y Detección de Intrusos (IPS)**	Indicar como el servicio ofertado se basa en hardware y software dedicado, los cuales se habilitarán en las dependencias del SII.	Detallar
	Indicar si el servicio ofertado utiliza tecnología ubicada en cuadrante "Gartner's Magic Quadrant for Intrusion Detection and Prevention Systems (IDPS)", indicando su posicionamiento en dicho cuadrante, con datos actualizados (adjuntar evidencia de lo declarado pantallazo, certificado, etcétera)	Detallar y adjuntar evidencia
	Indicar como el servicio ofertado provee una herramienta que le permita al SII acceder a información para realizar auditorías acerca de su funcionamiento y verificación de cumplimiento de SLA. Especificar el tipo de herramienta.	Detallar
	Indicar la capacidad de throughput del servicio ofertado por cada Centro de datos.	Detallar
	Indicar el nivel de uptime de servicio ofertado, expresado en porcentaje de disponibilidad por año. Al menos 99,6%. Se debe informar mensualmente la disponibilidad	Detallar
	Indicar si el servicio ofertado es capaz de configurar excepciones, al menos por IP o segmentos de IP (IPv4).	Detallar
	Indicar los modos de operación del servicio ofertado (ej: si permite operar en modo monitor, es decir, sin tomar acciones o inclusive detener la inspección del IPS si fuera requerido, sin afectar el tráfico de los servicios del SII, entre otros modos)	Detallar
	Indicar si el servicio ofertado permite el bloqueo de protocolos P2P.	Detallar
	Indicar si el servicio ofertado permite configurar protecciones para servicios básicos: Email, DNS, FTP, SNMP	Detallar
	Indicar si el servicio ofertado permite protección para DNS Cache Poisoning.	Detallar
	Indicar si el servicio ofertado permite la protección GEOreferencial.	Detallar
	Indicar si el servicio ofertado permite inspección de tráfico HTTP/SSL. Indicar los requerimientos para la entrega de este tipo de inspección.	Detallar
	Indicar el número de especialista con certificaciones técnicas en la solución IPS (Se deben adjuntar los certificados del personal)	Detallar
	Indicar como el servicio ofertado posibilita bypass físico ante falla catastrófica. Indicar si el bypass es interno o externo a la plataforma.	Detallar
	Indicar si el servicio ofertado incluye dispositivos tecnológico IPS que soportar módulos de fibra de 1Gb o 10 GE.	Detallar
	Indicar como el servicio ofertado considera mantenciones periódicas sobre los elementos de hardware y software (indicar periodicidad) las cuales debe ser programadas en coordinación con personal del SII.	Detallar

		Indicar como el servicio ofertado mantendrá un inventario de todos los elementos de software y hardware requeridos para la entrega del servicio, considerando los detalles de ubicación física, conexiones, circuitos eléctricos y vigencia de las licencias requeridas.	Detallar
Componente 1, Ítem 3 **Protección contra ataques de denegación de servicios**		Detallar la arquitectura del servicio ofertado, que garantice el compromiso de uptime comprometido y la capacidad de tráfico requerido (GBs).	Detallar
		Indicar, para la tecnología sobre la cual se basa el servicio, la ubicación en el cuadro “DDoS Mitigation Solutions report" de Forrester, en la versión vigente a la fecha de publicación de la licitación. (adjuntar evidencia de lo declarado pantallazo, certificado, etcétera)	Detallar y adjuntar evidencia
		Indicar como el servicio ofertado provee una herramienta que permite acceder a información para la realizar auditorías sobre su funcionamiento y verificación de cumplimiento de SLA.	Detallar
		Indicar el uptime comprometido para servicio ofertado, expresado en porcentaje de disponibilidad anual. Al menos 99,6%. Se debe informar mensualmente la disponibilidad	Detallar
		Indicar la cantidad de especialista con certificaciones técnicas respecto la tecnología de protección DDoS utilizada (Se deben adjuntar los certificados del personal)	Detallar
		Indicar el compromiso de uptime expresado en porcentaje de disponibilidad anual. En este punto, el oferente debe explicitar cual es el diseño tecnológico que sustenta su propuesta, teniendo en cuenta, además, el ajuste al presupuesto disponible.	Detallar
		Para el servicio ofertado detallar el o los mecanismos de bypass de las interfaces para garantizar la continuidad de los servicios del SII en caso de falla o acción controlada de mantenimiento.	Detallar
		Indicar el rango de capacidad de inspección y mitigación de la solución tecnológica, sin necesidad de cambiar el equipo completo o adicionar hardware nuevo, si se desea aumentar la capacidad contratada.	Detallar
		Indicar los modos de funcionamiento del servicio ofertado (ej: El equipo debe ser capaz, al menos, de soportar un modo de prueba "inactivo" cual suspenda la protección y proporcione reportes del tráfico que bloquearía si se definiera como modo "activo")	Detallar
Componente 1, Ítem 4 **Servicio de análisis de vulnerabilidades**	**Servicio quincenal de análisis perimetral de vulnerabilidades**	Indicar la metodología de trabajo para la realización de los escaneos tanto en el perímetro y DMZ On Premise como en la nube pública.	Detallar
		Indicar el tipo de cumplimiento que ofrece el servicio, asociado a estándares de industria.	Detallar
		Indicar el tipo estándar que ofrece el servicio para la clasificación de gravedad de los hallazgos	Detallar
		Indicar descripción de la solución tecnológica para análisis de vulnerabilidad del perímetro, indicando además su posicionamiento en benchmarking internacional**.**	Detallar
		Indicar y describir herramienta que permite acceder a información que permita realizar auditorías acerca de su funcionamiento y verificación de cumplimiento de SLA.	Detallar
		Para el servicio ofertado, indicar la metodología de trabajo para la realización de los escaneos, tanto en el ámbito interno On Premise como el ámbito interno de nube pública.	Detallar

	Servicio semestral de análisis de vulnerabilidades en dispositivos de red interna	Indicar el tipo de cumplimiento que ofrece el servicio, asociado a estándares de industria.	Detallar
		Indicar el tipo estándar que ofrece el servicio para la clasificación de gravedad de los hallazgos	Detallar
		Indicar la cantidad ofertada de dispositivos a escanear durante la ejecución del análisis de vulnerabilidades.	Detallar
		Indicar descripción de solución tecnológica para análisis de vulnerabilidad de bases de datos, servidores (sistemas operativos, equipos de comunicaciones, herramientas y/o plataformas de nube pública), indicando además su posicionamiento en benchmarking internacional.	Detallar
		Indicar y describir herramienta que permite acceder a información que permita realizar auditorías acerca de su funcionamiento y verificación de cumplimiento de SLA.	Detallar
Componente 1, Ítem 5 **(Firewall para aplicaciones Web y APIS)**		Indicar y describir la herramienta que incluye el servicio y que permite acceder a información que permita realizar auditorías acerca de su funcionamiento y verificación de cumplimiento de SLA.	Detallar
		Indicar la ubicación en “Gartner Magic Quadrant for Web Application Firewalls (WAAP)” en la versión vigente a la fecha de publicación de la licitación. (adjuntar evidencia de lo declarado pantallazo, certificado, etcétera)	Detallar adjuntar evidencia
		Indicar la cantidad de especialistas certificados en la solución del tipo WAAP incluida en el servicio.	Detallar
		Indicar la capacidad de Througput de tráfico en Gbs por cada centro de datos del SII.	Detallar
		Indicar las funcionalidades de la solución tecnológica, indicando tipos de dashboard, funciones de administración, configuración , trazabilidad, auditoria, entre otras.	Detallar
		Indicar el tipo de tráfico para el cual que es capaz de realizar inspección.	Detallar
		Indicar tipos de bloqueos que realiza el servicio (ej: por tipo de tráfico HTTP, por dirección IP, por conexión y por sesión de aplicación, etc.)	Detallar
		Indicar los modos de operación del servicio (ej: modo pasivo, de manera de poder inspeccionar tráfico sin realizar bloqueo, etc.).	Detallar
		Indicar los tipos de políticas o reglas de bloqueo que es posible definir para el análisis de tráfico, ya sea a partir de aplicaciones propietarias del SII y/o sistemas empresariales tales como Outlook, SharePoint, Apache, JBoss, Oracle, entre otros.	Detallar
		Indicar los tipos de ataque que el servicio es capaz de detectar y bloquear, indicando los referentes globales que utiliza.	Detallar
		Indicar con detalle la arquitectura de la solución tecnológica del servicio ofertado.	Detallar
		Indicar el uptime comprometido para servicio ofertado, expresado en porcentaje de disponibilidad anual. Al menos 99,6%. Se debe informar mensualmente la disponibilidad	Detallar

	Indicar la capacidad del servicio para inspeccionar tráfico de aplicativos del SII u otros que no necesariamente cumplen estándares globales relativos a protocolos de internet, tales como los estándares RFC. En este punto, se espera que el servicio ofertado tenga la capacidad de plantear excepciones sobre reglas de cumplimiento de RFC, de tal forma que esta situación no sea excluyente para que el servicio WAAP pueda realizar las inspecciones de seguridad en dichas aplicaciones del SII.	Detallar
Componente 1, Ítem 6 **(Servicio Gestionado de detección y respuesta de amenazas en red de datos interna (NDR, Network Detección and Response)**	Indicar cuadrante de "Gartner's Magic Quadrant" para dispositivos tecnológicos del tipo NDR, en la versión vigente a la fecha de publicación de la licitación (adjuntar evidencia de lo declarado pantallazo, certificado, etcétera)	Indicar y adjuntar evidencia
	Indicar cantidad de especialista con certificaciones técnicas en la solución. Se deben adjuntar los certificados	Indicar
	detallar herramienta para uso por parte de SII, que permite acceder a información para realizar auditorías acerca de su funcionamiento y verificación de cumplimiento de SLA.	Indicar
	Indicar capacidad de inspección de tráfico en Gbps en cada Centro de datos.	Indicar
	Indicar uptime comprometido por servicio ofertado. Al menos 99,6%. Se debe informar mensualmente la disponibilidad	Indicar
	Indicar si el servicio es capaz de operar en modo monitor, sin tomar acción.	Indicar
	Indicar cantidad de especialistas con certificaciones técnicas en la solución NDR (Se deben adjuntar los certificados del personal)	Indicar
	Indicar si tecnología soporta módulos de fibra de 1Gb o 10 GE para conectividad con red del SII.	Indicar
	Indicar el esquema de mantenciones periódicas sobre los elementos de hardware y software.	Indicar
	Indicar el esquema planteado por el servicio ofertado para la mantención del inventario de todos los elementos de software, hardware, ubicación física, conectividad de red, alimentación eléctrica, vigencia de licencias, entre otros.	Indicar
	Indicar como el servicio realiza la detección de dispositivos infectados, comprometidos con tráfico sospechoso, detección de exfiltración de información.	Indicar
	Indicar como el servicio realiza la detección de ataques de denegación de servicio entrante o saliente.	Indicar
	Indicar si la tecnología es compatible con todos los elementos tradicionales de la red (firewall, switch, router)	Indicar
	Indicar como el servicio se integrará con el servicio SOC especificado en la componente 1 ítem 1 de la presente licitación.	Indicar
	Indicar como servicio se integrará con la herramienta SIEM o similar especificada para la componente 1 ítem 1 de la presente licitación.	Indicar
	Indicar como el servicio es capaz de analizar el tráfico de red en tiempo real y que técnicas avanzadas de detección de amenazas	Indicar

	utiliza para identificar patrones sospechosos y comportamientos anómalos.	
	Indicar como el servicio es capaz de ofrecer una visibilidad completa y en tiempo real del tráfico de red para detectar y responder rápidamente a las eventuales amenazas y ataques en curso.	Indicar
	Indicar como el servicio es capaz de proveer una interfaz fácil de usar y una representación gráfica clara de la actividad de la red, de tal forma que permita a los analistas identificar rápidamente posibles problemas y generar una toma decisiones informadas.	Indicar
	Indicar como el servicio es capaz de permitir el análisis forense de eventos pasados y la reproducción del tráfico de red asociado para investigar incidentes y tomar medidas correctivas.	Indicar
	Indicar como servicio es capaz de lograr la integración con otras soluciones de seguridad y herramientas de administración de red, como firewalls, IPS y SIEM, para garantizar una gestión efectiva y coordinada de la seguridad. Especialmente lo especificado en la componente 1 ítem 1 de la presente licitación.	Indicar
	Indicar como el servicio es capaz de detectar comportamientos sospechosos dentro de la red corporativa para prevenir y detectar amenazas internas.	Indicar
	Indicar como el servicio es capaz de permitir la automatización de respuestas ante amenazas o eventos que requieren una reacción rápida y precisa para minimizar los efectos sobre la plataforma del SII.	Indicar
	Indicar como el servicio es capaz de mantenerse actualizado respecto a bases de datos externas, actualizadas respecto de amenazas, en tiempo real para mejorar la precisión de las detecciones.	Indicar
Componente 2 **Servicio Profesionales**	Indicar Cantidad de clientes para los cuales presta servicios de asesoría de seguridad de la información y ciberseguridad. Sólo se tomará en cuenta para la evaluación lo efectivamente respaldado de acuerdo con el anexo N° 4	Indicar
	Indicar los años de experiencia del oferente en el mercado en el rubro de servicios de consultoría avanzados en seguridad de la información y ciberseguridad. Sólo se tomará en cuenta para la evaluación lo efectivamente respaldado de acuerdo con el anexo N° 4.	Indicar
	Horario en que se puede efectuar una solicitud de servicios y ser atendido inmediatamente.	7x24x365 7x24 5x9 5x8 — Indicar
	Cantidad de certificaciones con reconocimiento internacional del o los consultores senior en seguridad del a información tales como, CISSP, CISM, CISA o similar. Sólo se tomara en cuenta para la evaluación lo efectivamente respaldado de acuerdo con el anexo N° 4	Indicar
	Cantidad de certificaciones con reconocimiento internacional del o los consultores senior en ciberseguridad tales como, CISSP, CISM, CISA o similar. Sólo se tomara en cuenta para la	Indicar

	evaluación lo efectivamente respaldado de acuerdo con el anexo N° 4.	
	Cantidad Certificaciones con reconocimiento internacional del o los consultores junior en seguridad TI. Sólo se tomara en cuenta para la evaluación lo efectivamente respaldado de acuerdo con el anexo N° 5.	Indicar
NOTAS: * Se entiende por analistas nivel 1, a aquellos que monitorean y evalúan continuamente las alertas del SIEM o similar, para alertarlas y escalarlas al nivel 2, si corresponde. ** Los analistas nivel 2 determinan si los sistemas se han visto afectados y entregan las recomendaciones de mitigación		

ANEXO N° 7: DECLARACION JURADA PLANES DE INTEGRIDAD; MODELOS DE PREVENCION DE DELITOS; PROGRAMAS DE COMPLIANCE; CAPACITACIONES

Completar la opción que corresponda:

A) Cuenta con planes de integridad; programas de compliance, entre otros.

Yo,……, cédula de identidad N°…….. con domicilio en ,……, en representación de ……., RUT N°……..., del mismo domicilio, declaro que mi representada:

"SÍ cuenta con planes de integridad, modelos de prevención de delitos, programas de compliance; código de ética y son conocidos por el personal de la empresa".

Tipo de Programa Nombre del programa

ADJUNTAR PROGRAMAS Y DOCUMENTACION QUE ACREDITE EL CONOCIMIENTO DE LOS TRABAJADORES.

B) Cuenta solo con capacitaciones en materias relacionadas.

Yo,……, cédula de identidad N°…….. con domicilio en ,……, en representación de ……., RUT N°……..., del mismo domicilio, declaro que mi representada:

"Solo cuenta con capacitaciones a su personal en materias relacionadas a cumplimientos normativos; trasparencia, probidad; ética, entre otras.

Tipo de Capacitación Nombre de la capacitación

ADJUNTAR CAPACITACIONES Y DOCUMENTACION QUE ACREDITE EL CONOCIMIENTO DE LOS TRABAJADORES.

C) No cuenta con planes de integridad; programas de compliance y capacitaciones en materias relacionadas.

Yo,……, cédula de identidad N°…….. con domicilio en ,……, en representación de ……., RUT N°……., del mismo domicilio, declaro que mi representada:

“NO cuenta con planes de integridad; modelo de prevención de delito; programas de compliance o de ética. Además, no tiene capacitaciones en esta materia a sus trabajadores.

Nota: Para efectos de la evaluación y en el evento de marcar la opción A) y B), éstas deben ser acreditadas, debiendo adjuntar la documentación que respalde lo declarado. Es decir, no basta con contar con programas, planes normativos o capacitaciones, sino que debe acreditarse, además, el conocimiento de éstos por parte de los trabajadores.

ANEXO N° 8: GUÍA DE AYUDA PARA FACTURACIÓN ELECTRÓNICA

En la sección “E.- INFORMACIÓN DE REFERENCIA” del XML se debe detallar la información del N° de Contrato y/o N° de Orden de Compra.

Nombre campo	Código	Descripción
Tipo Documento de referencia	<TpoDocRef>	Corresponde al código del documento de referencia que se le solicita al proveedor, en nuestro caso sería: ▪ 801: Orden de Compra ▪ 803: Contrato o Acuerdo Complementario
Folio de referencia	<FolioRef>	Corresponde al número de la Orden de Compra o el número del Contrato o Acuerdo Complementario.
Fecha de la referencia	<FchRef>	Corresponde a la fecha del documento de referencia (fecha envío orden de compra, fecha de firma acuerdo complementario o contrato)
Razón de la referencia	<RazonRef>	Es un campo opcional que se añade

En la sección “A.- ENCABEZADO.” Del XML se debe indicar en la Glosa el N° de cuotas o el hito a especificar.

Nombre campo	Código	Descripción
Glosa descripción Pago	<GlosaPagos>	En esta glosa se debe detallar el número de la cuota o el hito que representa la factura. En el caso de que el pago se realice en dólares, UF o UTM, se debe indicar el valor o fecha utilizado para la conversión.

En la sección “B.- DETALLE DE PRODUCTOS O SERVICIOS.” Del XML se debe indicar la información de los ítems.

Nombre campo	Código	Descripción
Nombre del Ítem	<NmbItem>	Nombre del producto o servicio
Descripción Adicional	<DscItem>	Descripción Adicional del producto o servicio. Se utiliza para pack, servicios con detalle

En la sección “A.- ENCABEZADO.” Del XML se debe indicar el periodo de facturación del servicio prestado.

Nombre campo	Código	Descripción
Período desde	<PeriodoDesde>	Período de facturación para Servicios Periódicos. Fecha desde (Fecha inicial del servicio facturado)
Período hasta	<PeriodoHasta>	Período de facturación para Servicios Periódicos. Fecha hasta (Fecha final del servicio facturado)

En la sección “A.- ENCABEZADO.” Del XML se debe indicar el detalle de la cuenta corriente o cuenta vista del proveedor

Nombre campo	Código	Descripción
Medio de Pago	<MedioPago>	Indica en que modalidad se pagará. ▪ CH: Cheque ▪ CF: Cheque a fecha ▪ LT:letra ▪ EF:Efectivo ▪ PE: Pago A Cta. Cte ▪ TC:Tarjeta Crédito ▪ OT:Otr
Tipo Cuenta de Pago	<TipoCtaPago>	Cuenta ▪ CT: Cta.Cte ▪ AH:Ahorro ▪ OT:Otra
Cuenta de Pago	<NumCtaPago>	Número de la Cuenta
Banco de Pago	<BcoPago>	Banco de la Cuenta

TÓMESE RAZÓN, ANÓTESE, COMUNÍQUESE Y PUBLÍQUESE EN EL SISTEMA DE INFORMACIÓN Y CONTRATACIÓN PÚBLICA

“POR ORDEN DEL DIRECTOR”

SERGIO CRISTIAN PALMA ARANCIBIA
Firmado digitalmente por SERGIO CRISTIAN PALMA ARANCIBIA
Fecha: 2023.11.07 12:28:17 -03'00'

CRISTIAN PALMA ARANCIBIA
SUBDIRECTOR DE ADMINISTRACIÓN

Jocelyn Toro Zambra

Paola Gonzalez Castro
Firmado digitalmente por Paola Gonzalez Castro
Fecha: 2023.11.07 10:05:00 -03'00'

PATRICIO ANDRES BARRIA LEHYT
Firmado digitalmente por PATRICIO ANDRES BARRIA LEHYT
Fecha: 2023.11.07 10:15:33 -03'00'

CONTRALORIA GENERAL DE LA REPUBLICA CHILE 26-III-1927

TOMADO DE RAZÓN
Fecha: 24/11/2023
JORGE ANDRES BERMUDEZ SOTO
Contralor General de la República