SUBDIRECCIÓN DE TECNOLOGIAS DE LA INFORMACION
DEPARTAMENTO DE CIBERSEGURIDAD

Santiago, 27 de mayo de 2026

INFORME COMISIÓN EVALUADORA

EVALUACIÓN TÉCNICO ECONÓMICO

En el marco del proceso licitatorio ID N°**1605-23-LP26** denominado **LP-4609** "**Servicio de Ciberinteligencia**", se reúne la Comisión Evaluadora nombrada mediante Memorándum N° 30, de fecha 14 de abril de 2026, de acuerdo lo dispuesto en el punto 3.3.1 de las Bases Administrativas – Parte I, de las Bases de Licitación aprobadas mediante Resolución Exenta SII N° 1669 de 13 de abril de 2026, y modificadas posteriormente por la Resolución SII N° 1934, de fecha 24 de abril de 2026.

El presente informe se emite en conformidad a lo señalado en el artículo 54, del Decreto N°661, de 2024, del Ministerio de Hacienda, que aprueba el Reglamento de la Ley Nº19.886, de Bases sobre Contratos Administrativos de Suministro y Prestación de Servicios.

Se tienen a la vista y se analizan los antecedentes y documentos que, en la apertura electrónica de las ofertas, fueron presentados por los siguientes oferentes:

1. DETALLE OFERTA PROVEEDORES

RUT	RAZÓN SOCIAL
76.644.983-2	ADAPTIVE SECURITY SPA
77.680.090-2	ANIDA CONSULTORES S.A.
76.804.300-0	BUSINESS CONTINUITY SPA
92.580.000-7	EMPRESA NACIONAL DE TELECOMUNICACIONES S.A.
76.092.207-2	INTEGRACIÓN DE TECNOLOGÍAS ITQ LIMITADA
78.197.454-4	KEPLER LATAM SPA
76.337.109-3	NASTEC SPA
76.363.873-1	NETICS SPA
77.660.154-3	SECAPPS TECHNOLOGIES SPA
76.334.381-2	TICHILE REVENTA DE SOFTWARE Y HARDWARE SPA
76.130.712-6	TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA

2. OFERTAS DECLARADAS INADMISIBLES EN ANÁLISIS PREVIO A LA EVALUACIÓN

Se hace revisión de los requisitos mínimos establecidos en las Bases Administrativas – Parte I, punto 2.2 de la Licitación Pública **ID N°1605-23-LP26 denominado LP-4609** "**Servicio de Ciberinteligencia**"**,** en donde se establece que las ofertas deberán cumplir con lo siguiente:

a) El oferente debe ser Partner del o los fabricantes de las herramientas, plataformas o aplicaciones que conforman la solución de Cyber Threat Intelligence (CTI) utilizada para la prestación del servicio de ciberinteligencia ofertado. Para estos efectos el oferente deberá presentar el Anexo N°4 y deberá declarar explícitamente en el mismo la totalidad de las herramientas, plataformas o aplicaciones que conforman la solución ofertada. Asimismo, el oferente deberá presentar el o los certificados que acrediten su respectiva calidad de Partner. Si el oferente no es Partner, si su certificación de Partner no se encuentra vigente o si no acredita la certificación de Partner debidamente, su oferta será declarada inadmisible. En caso de que el oferente sea una Unión Temporal de Proveedores, basta con que uno cualquiera de sus integrantes cuente con la referida calidad de Partner. 5

b) En caso de que el oferente presente una oferta asociada a soluciones de construcción propia deberá declararlo como parte de la propuesta técnica, en el Anexo N° 4 letra B. Adicionalmente, para este caso no requiere presentar certificado de Partner descrito en el párrafo anterior. En caso de que no cumpla con lo indicado, su oferta será declarada inadmisible.

c) Las ofertas técnicas deben cumplir con los requisitos mínimos indicados en el Anexo N° 5A. Asimismo, las ofertas deben considerar el cumplimiento de al menos 6 requisitos funcionales (dentro de los cuales debe contemplarse necesariamente el requisito número 5. Operación Takedown Services) y al menos 3 requisitos no funcionales indicados en dicho anexo. Si el oferente no presenta el Anexo 5A, si en el mismo señala que no cumple con los requisitos mínimos y/o con los requisitos funcionales y no funcionales requeridos, o si se constata que la oferta respectiva no cumple con lo anterior, su oferta será declarada inadmisible.

d) La propuesta técnica del oferente debe incluir como fuente de información, al menos: Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web. Lo anterior se acreditará según la información indicada en el Anexo 5B. Si el oferente no presenta el Anexo 5B, si en el mismo señala que no cumple al menos con las fuentes de información anteriormente señaladas o si se constata que la oferta respectiva no cumple con las fuentes de información señaladas como mínimo, su oferta será declarada inadmisible.

En esa línea, el SII verificó la acreditación de la situación financiera e idoneidad técnica de los proveedores a través de su inscripción en el Registro de Proveedores y, además, verificó que estos se encontraran hábiles para participar en él.

De lo anterior, la Comisión Evaluadora concluye que las ofertas presentadas por las siguientes empresas cumplen con los requisitos mínimos establecidos, por lo que todas son declaradas admisibles y califican para ser evaluadas técnicamente.

1. **ANIDA CONSULTORES S.A.**
2. **BUSINESS CONTINUITY SPA**
3. **EMPRESA NACIONAL DE TELECOMUNICACIONES S.A.**
4. **INTEGRACIÓN DE TECNOLOGÍAS ITQ LIMITADA**
5. **KEPLER LATAM SPA**
6. **NASTEC SPA**
7. **NETICS SPA**
8. **SECAPPS TECHNOLOGIES SPA**
9. **TICHILE REVENTA DE SOFTWARE Y HARDWARE SPA**
10. **TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA.**

Por otra parte, la empresa **ADAPTIVE SECURITY SPA** no presentó la documentación requerida para acreditar su condición de *"Partner del o los fabricantes de las herramientas, plataformas o aplicaciones que conforman la solución de Cyber Threat Intelligence (CTI)"*. Al no cumplir con este requisito esencial, la Comisión Evaluadora propone declarar su **propuesta inadmisible**, situación que impide su respectiva evaluación técnica.

3. CONSULTAS Y RESPUESTAS REALIZADAS A LOS OFERENTES

En la presente licitación no se realizaron consultas a los oferentes.

4. CRITERIOS DE EVALUACIÓN

Según se establece en el **punto 3.3.2** de las Bases Administrativas – Parte I de las Bases de Licitación, relativo al proceso de evaluación de las ofertas, estas fueron evaluadas de acuerdo con los siguientes criterios:

Evaluación Técnica:

ITEM	%	Característica	Puntaje Asignado

Servicio de gestión de casos de investigación. Fuentes de información (Este criterio será evaluado de acuerdo con el Anexo N° 5B: Aspectos Evaluables de la Oferta).	25	Incluye como fuente de información: 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web Y adicionalmente incorpora el total de las siguientes fuentes: 3. Plataformas de contenido audiovisual (Youtube). 4. Foros y sitios de publicación abierta (Reddit y/o Pastebin). 5. Repositorios de código y desarrollo (GitHub y GitLab). 6. Medios de comunicación digitales (Portales de noticias y Newspapers -prensa digital-). 7. Otras fuentes adicionales (Cualquier otra fuente abierta, cerrada o especializada que resulte pertinente para los fines del servicio).	100
		Incluye como fuente de información: 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web Y, adicionalmente, considera al menos cuatro de las siguientes fuentes: 3. Plataformas de contenido audiovisual (Youtube). 4. Foros y sitios de publicación abierta (Reddit y/o Pastebin). 5. Repositorios de código y desarrollo (GitHub y GitLab). 6. Medios de comunicación digitales (Portales de noticias y Newspapers -prensa digital-). 7. Otras fuentes adicionales (Cualquier otra fuente abierta, cerrada o especializada que resulte pertinente para los fines del servicio).	75
		Incluye como fuente de información: 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web Y, adicionalmente, considera al menos tres de las siguientes fuentes: 3. Plataformas de contenido audiovisual (Youtube). 4. Foros y sitios de publicación abierta (Reddit y/o Pastebin). 5. Repositorios de código y desarrollo (GitHub y GitLab). 6. Medios de comunicación digitales (Portales de noticias y Newspapers -prensa digital-).	50

		7. Otras fuentes adicionales (Cualquier otra fuente abierta, cerrada o especializada que resulte pertinente para los fines del servicio).	
		Incluye como fuente de información: 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web Y, adicionalmente, considera una o dos de las siguientes: 3. Plataformas de contenido audiovisual (Youtube). 4. Foros y sitios de publicación abierta (Reddit y/o Pastebin). 5. Repositorios de código y desarrollo (GitHub y GitLab). 6. Medios de comunicación digitales (Portales de noticias y Newspapers -prensa digital-). 7. Otras fuentes adicionales (Cualquier otra fuente abierta, cerrada o especializada que resulte pertinente para los fines del servicio).	35
		Incluye sólo como fuente de información: 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web	25
		No informa o no incluye a lo menos las siguientes fuentes de información: 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web	Inadmisible
Cantidad de activos digitales (*) **según bases técnicas punto 2.2** **(Este criterio será evaluado de acuerdo con el Anexo N° 5B: Aspectos Evaluables de la Oferta).**	10	Más de 300	100
		Desde 271 hasta 300	75
		Desde 250 hasta 270	30
		Menos de 250	Inadmisible
Requerimientos Funcionales y No Funcionales **según bases técnicas punto 2.8**	25	El servicio ofertado considera la totalidad de los Requerimientos Funcionales y no Funcionales	100
		El servicio ofertado no considera la totalidad de los requerimientos funcionales y no funcionales, pero considera al menos 6 de los Requerimientos Funcionales (dentro de los cuales se contempla el requisito número 5. Operación	50

		Takedown Services) y al menos 3 de los no Funcionales	
		-Servicio NO considera al menos 6 de los Requerimientos Funcionales y al menos de 3 de los No Funcionales; o -No presenta Anexo 5A; o -No declara el cumplimiento de lo requerido en el Anexo 5A; o -Considera al menos 6 de los Requerimientos Funcionales y al menos 3 de los no Funcionales, pero sin contemplar el requisito funcional número 5. Operación Takedown Services	Inadmisible
Consola de Investigación (**) **(Este criterio será evaluado de acuerdo con el Anexo N° 5B: Aspectos Evaluables de la Oferta).**	20	La oferta considera la provisión de una consola de investigación	100
		La oferta NO considera la provisión de una consola de investigación	0
Cantidad de horas corridas para realizar Takedown Service (Capacidad para dar de baja sitios de phishing, perfiles falsos en redes sociales y aplicaciones móviles fraudulentas) **(Este criterio será evaluado de acuerdo con el Anexo N° 5B: Aspectos Evaluables de la Oferta).**	10	En menos de 24 horas	100
		Entre 24 horas y 47 horas	50
		Entre 48 horas y 72 horas	25
		Más de 72 horas	Inadmisible
Cantidad de veces que ha impartido servicios de Ciberinteligencia (***) Entregar antecedentes en Anexo N° 3 y adjuntar documento(s) que acredite(n) la experiencia respectiva, según corresponda.	10	5 o más veces en el mercado	100
		3 o 4 veces en el mercado	75
		1 o 2 veces en el mercado	50
		Ninguna vez en el mercado o no acredita experiencia en el servicio ofertado	0

Evaluación Administrativa

ITEM	%	Característica	Puntaje Asignado
Cuenta con Programas de Integridad y Ética Empresarial. Para evaluar este criterio, los oferentes deben completar y presentar la declaración jurada contenida en el Anexo N°7 y, en caso de contar con	50%	El oferente acredita que cuenta con programas de integridad y ética empresarial, y los mismos son efectivamente conocidos y aplicados por su personal.	**100**

Programas de Integridad y Ética Empresarial, deben adjuntar además los respectivos Programas de Integridad y Ética Empresarial. Los Programas de Integridad y Ética Empresarial son entendidos como una guía que ayuda a las empresas a actuar correctamente y a prevenir conductas indebidas que sean contrarias a la probidad e integridad. En este sentido, se consideran como Programas de Integridad y Ética Empresarial, por ejemplo, los modelos de prevención de delito, los programas de compliance, los códigos de ética, entre otros.		El oferente no cuenta o no acredita programas de integridad y ética empresarial.	**0**
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 cumple con todos los requisitos de presentación de la oferta o no lo realiza dentro del plazo adicional otorgado por el SII de acuerdo con lo establecido en el N°3.8 del punto II Bases Administrativas –Parte II.	**0**

A. Servicio de gestión de casos de investigación. Fuentes de información.

La Comisión Evaluadora concluye que las ofertas presentadas por las empresas **ANIDA CONSULTORES S.A., BUSINESS CONTINUITY SPA, EMPRESA NACIONAL DE TELECOMUNICACIONES S.A., INTEGRACIÓN DE TECNOLOGÍAS ITQ LIMITADA, KEPLER LATAM SPA, NASTEC SPA, NETICS SPA, SECAPPS TECHNOLOGIES SPA, TICHILE REVENTA DE SOFTWARE Y HARDWARE SPA y TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA.** cumplen con el requisito mínimo de "**Servicio de gestión de casos de investigación. Fuentes de información"** establecido en las bases de licitación.

A continuación, se muestra una tabla con las ofertas entregadas por cada oferente y el puntaje asignado:

OFERENTE	OFERTA	SERVICIO DE GESTIÓN DE CASOS DE INVESTIGACIÓN. FUENTES DE INFORMACIÓN - DECLARADAS EN ANEXO N° 5B	PUNTAJE ASIGNADO

ANIDA CONSULTORES S.A.	X	Incluye como fuente de información: 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web Y adicionalmente incorpora el total de las siguientes fuentes: 3. Plataformas de contenido audiovisual (Youtube). 4. Foros y sitios de publicación abierta (Reddit y/o Pastebin). 5. Repositorios de código y desarrollo (GitHub y GitLab). 6. Medios de comunicación digitales (Portales de noticias y Newspapers - prensa digital-). 7. Otras fuentes adicionales (Cualquier otra fuente abierta, cerrada o especializada que resulte pertinente para los fines del servicio).	100
BUSINESS CONTINUITY SPA	X	Incluye como fuente de información: 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web Y adicionalmente incorpora el total de las siguientes fuentes: 3. Plataformas de contenido audiovisual (Youtube). 4. Foros y sitios de publicación abierta (Reddit y/o Pastebin). 5. Repositorios de código y desarrollo (GitHub y GitLab). 6. Medios de comunicación digitales (Portales de noticias y Newspapers - prensa digital-). 7. Otras fuentes adicionales	100

		(Cualquier otra fuente abierta, cerrada o especializada que resulte pertinente para los fines del servicio).	
EMPRESA NACIONAL DE TELECOMUNICACIONES S.A.	X	Incluye como fuente de información: 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web Y adicionalmente incorpora el total de las siguientes fuentes: 3. Plataformas de contenido audiovisual (Youtube). 4. Foros y sitios de publicación abierta (Reddit y/o Pastebin). 5. Repositorios de código y desarrollo (GitHub y GitLab). 6. Medios de comunicación digitales (Portales de noticias y Newspapers - prensa digital-). 7. Otras fuentes adicionales (Cualquier otra fuente abierta, cerrada o especializada que resulte pertinente para los fines del servicio).	100
INTEGRACIÓN DE TECNOLOGÍAS ITQ LIMITADA	X	Incluye como fuente de información: 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web Y adicionalmente incorpora el total de las siguientes fuentes: 3. Plataformas de contenido audiovisual (Youtube). 4. Foros y sitios de publicación abierta (Reddit y/o Pastebin). 5. Repositorios de código y desarrollo (GitHub y GitLab).	100

		6. Medios de comunicación digitales (Portales de noticias y Newspapers - prensa digital-). 7. Otras fuentes adicionales (Cualquier otra fuente abierta, cerrada o especializada que resulte pertinente para los fines del servicio).	
KEPLER LATAM SPA	X	Incluye como fuente de información: 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web Y adicionalmente incorpora el total de las siguientes fuentes: 3. Plataformas de contenido audiovisual (Youtube). 4. Foros y sitios de publicación abierta (Reddit y/o Pastebin). 5. Repositorios de código y desarrollo (GitHub y GitLab). 6. Medios de comunicación digitales (Portales de noticias y Newspapers - prensa digital-). 7. Otras fuentes adicionales (Cualquier otra fuente abierta, cerrada o especializada que resulte pertinente para los fines del servicio).	100
NASTEC SPA	X	Incluye como fuente de información: 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web Y adicionalmente incorpora el total de las siguientes fuentes: 3. Plataformas de contenido audiovisual (Youtube).	100

		4. Foros y sitios de publicación abierta (Reddit y/o Pastebin). 5. Repositorios de código y desarrollo (GitHub y GitLab). 6. Medios de comunicación digitales (Portales de noticias y Newspapers - prensa digital-). 7. Otras fuentes adicionales (Cualquier otra fuente abierta, cerrada o especializada que resulte pertinente para los fines del servicio).	
NETICS SPA	X	Incluye como fuente de información: 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web Y adicionalmente incorpora el total de las siguientes fuentes: 3. Plataformas de contenido audiovisual (Youtube). 4. Foros y sitios de publicación abierta (Reddit y/o Pastebin). 5. Repositorios de código y desarrollo (GitHub y GitLab). 6. Medios de comunicación digitales (Portales de noticias y Newspapers - prensa digital-). 7. Otras fuentes adicionales (Cualquier otra fuente abierta, cerrada o especializada que resulte pertinente para los fines del servicio).	100
SECAPPS TECHNOLOGIES SPA	Incluye redes sociales y plataformas de mensajería (WhatsApp, Facebook, X/Twitter, LinkedIn, TikTok, Instagram y Telegram), Deep Web y Dark Web; y adicionalmente incorpora la totalidad de fuentes adicionales: YouTube,	Incluye como fuente de información: 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web	100

	Reddit/Pastebin, GitHub/GitLab, medios digitales/prensa, y otras fuentes abiertas, cerradas o especializadas de IronFence.	Y adicionalmente incorpora el total de las siguientes fuentes: 3. Plataformas de contenido audiovisual (Youtube). 4. Foros y sitios de publicación abierta (Reddit y/o Pastebin). 5. Repositorios de código y desarrollo (GitHub y GitLab). 6. Medios de comunicación digitales (Portales de noticias y Newspapers - prensa digital-). 7. Otras fuentes adicionales (Cualquier otra fuente abierta, cerrada o especializada que resulte pertinente para los fines del servicio).	
TICHILE REVENTA DE SOFTWARE Y HARDWARE SPA	Cumple en la gestión de casos y en la mayoría de las fuentes: redes sociales, mensajería, Deep Web, Dark Web, foros, Pastebin, medios digitales y fuentes abiertas/cerradas especializadas. Sin embargo, la cobertura específica de repositorios GitHub/GitLab no está confirmada y en la matriz aparece como punto no cumplido. Cumple con redes sociales/mensajería, Deep Web, Dark Web y puede cubrir al menos 4 fuentes adicionales: YouTube, foros/Pastebin, medios digitales y otras fuentes abiertas/cerradas/especializadas.	Incluye como fuente de información: 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web Y, adicionalmente, considera al menos cuatro de las siguientes fuentes: 3. Plataformas de contenido audiovisual (Youtube). 4. Foros y sitios de publicación abierta (Reddit y/o Pastebin). 5. Repositorios de código y desarrollo (GitHub y GitLab). 6. Medios de comunicación digitales (Portales de noticias y Newspapers - prensa digital-). 7. Otras fuentes adicionales (Cualquier otra fuente abierta, cerrada o especializada que resulte pertinente para los fines del servicio).	75

TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA	X	Incluye como fuente de información: 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web Y adicionalmente incorpora el total de las siguientes fuentes: 3. Plataformas de contenido audiovisual (Youtube). 4. Foros y sitios de publicación abierta (Reddit y/o Pastebin). 5. Repositorios de código y desarrollo (GitHub y GitLab). 6. Medios de comunicación digitales (Portales de noticias y Newspapers - prensa digital-). 7. Otras fuentes adicionales (Cualquier otra fuente abierta, cerrada o especializada que resulte pertinente para los fines del servicio).	100

B. Cantidad de activos digitales, según bases técnicas punto 2.2.

La Comisión Evaluadora concluye que las ofertas presentadas por las empresas **ANIDA CONSULTORES S.A., BUSINESS CONTINUITY SPA, EMPRESA NACIONAL DE TELECOMUNICACIONES S.A., INTEGRACIÓN DE TECNOLOGÍAS ITQ LIMITADA, NASTEC SPA, NETICS SPA, SECAPPS TECHNOLOGIES SPA, TICHILE REVENTA DE SOFTWARE Y HARDWARE SPA y TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA.** cumplen con el requisito mínimo de "**activos digitales"** establecido en las bases de licitación.

Por otra parte, la empresa **KEPLER LATAM SPA** no presentó la cantidad de activos a monitorear que permita a la Comisión Evaluadora evaluar este punto. Debido a lo anterior, se propone declarar su oferta **inadmisible**.

OFERENTE	CANTIDAD DE ACTIVOS A MONITOREAR
ANIDA CONSULTORES S.A.	301
BUSINESS CONTINUITY SPA	301

EMPRESA NACIONAL DE TELECOMUNICACIONES S.A.	301
INTEGRACIÓN DE TECNOLOGÍAS ITQ LIMITADA	Superar el requerimiento de **300 assets** (Brand Protection Module – External Risk Management (ERM), ASM: Attack Surface Management y TI: Threat Inteligence (Deep & Dark web). **Alrededor de 1.000 (mil) assets** (Dominio sii.cl y sus subdominios, Direcciones IP asociadas a sii.cl, Marca 'servicio de impuestos internos', Cuentas de RRSS asociadas a SII, Principales proveedores de la Cadena de Suministros y 12 perfiles VIP)
KEPLER LATAM SPA	NO Indica
NASTEC SPA	350
NETICS SPA	310
SECAPPS TECHNOLOGIES SPA	305
TICHILE REVENTA DE SOFTWARE Y HARDWARE SPA	250
TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA	301

C. Requerimientos Funcionales y No Funcionales según bases técnicas punto 2.8

La Comisión Evaluadora concluye que las ofertas presentadas por las empresas **ANIDA CONSULTORES S.A., BUSINESS CONTINUITY SPA, EMPRESA NACIONAL DE TELECOMUNICACIONES S.A., INTEGRACIÓN DE TECNOLOGÍAS ITQ LIMITADA, KEPLER LATAM SPA, NASTEC SPA, NETICS SPA, SECAPPS TECHNOLOGIES SPA y TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA.** cumplen con el requisito mínimo de "**Requerimientos Funcionales y No Funcionales"** establecido en las bases de licitación.

Por otra parte, la empresa TICHILE REVENTA DE SOFTWARE Y HARDWARE SPA no cumple la cantidad de requerimientos funcionales y no funcionales mínimos exigidos en las bases de licitación. Debido a lo anterior, se propone declarar su oferta inadmisible

A continuación, se muestran las tablas con las ofertas entregadas por cada oferente y el puntaje asignado:

a) ANIDA CONSULTORES S.A.

La empresa **ANIDA CONSULTORES S.A.** confirma el cumplimiento de **8** requerimientos funcionales (RF) y **5** requerimientos no funcionales (RNF), por lo cual, obtiene una puntuación de **100** puntos.

El detalle de la evaluación se indica a continuación:

TIPO	REQUERIMIENTO	OFERTA	OBSERVACIÓN	CONSIDERADA
1. Requisitos Funcionales (RF)	**1.- Recolección - Multifuente (OSINT, Dark Web, Deep Web)**: Acceso a foros cerrados, mercados de leaks, canales de Telegram criminales y repositorios de código (GitHub).	X		SI
	2.- Monitoreo - Brand Protection: Detección de dominios typosquatting, aplicaciones móviles fraudulentas y suplantación de identidad en redes sociales.	X		SI
	3.- Integración - API & STIX/TAXII: Capacidad de ingesta automatizada hacia SIEM/SOAR mediante protocolos estándar $STIX/TAXII$ v2.1.	X		SI
	4.- Análisis - Atribución de Actores de Amenaza: Perfilamiento de adversarios (ej. Lazarus, Wizard Spider) con TTPs mapeados a MITRE ATT&CK.	X		SI
	5.- Operación - Takedown Services: Gestión activa para la baja de sitios de Phishing o perfiles falsos.	X		SI
	6.- Geopolítica - Análisis de Contexto: Informes específicos sobre amenazas al sector Tributario, sin limitación	X		SI

	geográfica.			
	7.- Detección de "Infostealers": El proveedor debe alertar en tiempo real si existen credenciales de empleados o contribuyentes han sido capturadas por malware y puestas a la venta en logs de la Dark Web.	X		SI
	8.- Fugas en Repositorios de Código: Monitoreo activo en GitHub/GitLab para detectar llaves de API, secretos de AWS o fragmentos de código fuente institucional subidos por error o a propósito.	X		SI
2. Requisitos No Funcionales (RNF)	**1.- Disponibilidad (SLA):** El portal de inteligencia debe garantizar un **99.9%** de disponibilidad.	X		SI
	2.- Confidencialidad y Privacidad: Cumplimiento con **ISO 27001** y regulaciones locales de protección de datos.	X		SI
	3.- Falsos Positivos: El proveedor debe garantizar una tasa de falsos positivos inferior al **5%** en alertas de marca.	X		SI
	4.- Escalabilidad: Capacidad de añadir activos (dominios, IPs, marcas) de forma ilimitada o mediante paquetes elásticos.	X		SI
	5.- Soporte: Soporte técnico 24/7 con analistas humanos (no solo bots) para consultas sobre incidentes críticos.	X		SI

b) BUSINESS CONTINUITY SPA

La empresa **BUSINESS CONTINUITY SPA** confirma el cumplimiento de **8** requerimientos funcionales (RF) y **5** requerimientos no funcionales (RNF), por lo cual, obtiene una puntuación de **100** puntos.

El detalle de la evaluación se indica a continuación:

TIPO	REQUERIMIENTO	OFERTA	OBSERVACIÓN	CONSIDERADA
1. Requisitos Funcionales (RF)	**1.- Recolección - Multifuente (OSINT, Dark Web, Deep Web)**: Acceso a foros cerrados, mercados de leaks, canales de Telegram criminales y repositorios de código (GitHub).	X		SI
	2.- Monitoreo - Brand Protection: Detección de dominios typosquatting, aplicaciones móviles fraudulentas y suplantación de identidad en redes sociales.	X		SI
	3.- Integración - API & STIX/TAXII: Capacidad de ingesta automatizada hacia SIEM/SOAR mediante protocolos estándar $STIX/TAXII$ v2.1.	X		SI
	4.- Análisis - Atribución de Actores de Amenaza: Perfilamiento de adversarios (ej. Lazarus, Wizard Spider) con TTPs mapeados a MITRE ATT&CK.	X		SI
	5.- Operación - Takedown Services: Gestión activa para la baja de sitios de Phishing o perfiles falsos.	X		SI
	6.- Geopolítica - Análisis de Contexto: Informes específicos sobre amenazas al sector	X		SI

	Tributario, sin limitación geográfica.			
	7.- Detección de "Infostealers": El proveedor debe alertar en tiempo real si existen credenciales de empleados o contribuyentes han sido capturadas por malware y puestas a la venta en logs de la Dark Web.	X		SI
	8.- Fugas en Repositorios de Código: Monitoreo activo en GitHub/GitLab para detectar llaves de API, secretos de AWS o fragmentos de código fuente institucional subidos por error o a propósito.	X		SI
2. Requisitos No Funcionales (RNF)	**1.- Disponibilidad (SLA):** El portal de inteligencia debe garantizar un **99.9%** de disponibilidad.	X		SI
	2.- Confidencialidad y Privacidad: Cumplimiento con **ISO 27001** y regulaciones locales de protección de datos.	X		SI
	3.- Falsos Positivos: El proveedor debe garantizar una tasa de falsos positivos inferior al **5%** en alertas de marca.	X		SI
	4.- Escalabilidad: Capacidad de añadir activos (dominios, IPs, marcas) de forma ilimitada o mediante paquetes elásticos.	X		SI
	5.- Soporte: Soporte técnico 24/7 con analistas humanos (no solo bots) para consultas sobre incidentes críticos.	X		SI

c) EMPRESA NACIONAL DE TELECOMUNICACIONES S.A.

La **EMPRESA NACIONAL DE TELECOMUNICACIONES S.A.** confirma el cumplimiento de **8** requerimientos funcionales (RF) y **5** requerimientos no funcionales (RNF), por lo cual, obtiene una puntuación de **100** puntos.

El detalle de la evaluación se indica a continuación:

TIPO	REQUERIMIENTO	OFERTA	OBSERVACIÓN	CONSIDERADA
1. Requisitos Funcionales (RF)	**1.- Recolección - Multifuente (OSINT, Dark Web, Deep Web)**: Acceso a foros cerrados, mercados de leaks, canales de Telegram criminales y repositorios de código (GitHub).	X		SI
	2.- Monitoreo - Brand Protection: Detección de dominios typosquatting, aplicaciones móviles fraudulentas y suplantación de identidad en redes sociales.	X		SI
	3.- Integración - API & STIX/TAXII: Capacidad de ingesta automatizada hacia SIEM/SOAR mediante protocolos estándar $STIX/TAXII$ v2.1.	X		SI
	4.- Análisis - Atribución de Actores de Amenaza: Perfilamiento de adversarios (ej. Lazarus, Wizard Spider) con TTPs mapeados a MITRE ATT&CK.	X		SI
	5.- Operación - Takedown Services: Gestión activa para la baja de sitios de Phishing o perfiles falsos.	X		SI

	6.- Geopolítica - Análisis de Contexto: Informes específicos sobre amenazas al sector Tributario, sin limitación geográfica.	X		SI
	7.- Detección de "Infostealers": El proveedor debe alertar en tiempo real si existen credenciales de empleados o contribuyentes han sido capturadas por malware y puestas a la venta en logs de la Dark Web.	X		SI
	8.- Fugas en Repositorios de Código: Monitoreo activo en GitHub/GitLab para detectar llaves de API, secretos de AWS o fragmentos de código fuente institucional subidos por error o a propósito.	X		SI
2. Requisitos No Funcionales (RNF)	**1.- Disponibilidad (SLA):** El portal de inteligencia debe garantizar un **99.9%** de disponibilidad.	X		SI
	2.- Confidencialidad y Privacidad: Cumplimiento con **ISO 27001** y regulaciones locales de protección de datos.	X		SI
	3.- Falsos Positivos: El proveedor debe garantizar una tasa de falsos positivos inferior al **5%** en alertas de marca.	X		SI
	4.- Escalabilidad: Capacidad de añadir activos (dominios, IPs, marcas) de forma ilimitada o mediante paquetes elásticos.	X		SI

	5.- Soporte: Soporte técnico 24/7 con analistas humanos (no solo bots) para consultas sobre incidentes críticos.	X		SI

d) INTEGRACIÓN DE TECNOLOGÍAS ITQ LIMITADA

La empresa **INTEGRACIÓN DE TECNOLOGÍAS ITQ LIMITADA** confirma el cumplimiento de **8** requerimientos funcionales (RF) y **5** requerimientos no funcionales (RNF), por lo cual, obtiene una puntuación de **100** puntos.

El detalle de la evaluación se indica a continuación:

TIPO	REQUERIMIENTO	OFERTA	OBSERVACIÓN	CONSIDERADA
1. Requisitos Funcionales (RF)	**1.- Recolección - Multifuente (OSINT, Dark Web, Deep Web)**: Acceso a foros cerrados, mercados de leaks, canales de Telegram criminales y repositorios de código (GitHub).	X		SI
	2.- Monitoreo - Brand Protection: Detección de dominios typosquatting, aplicaciones móviles fraudulentas y suplantación de identidad en redes sociales.	X		SI
	3.- Integración - API & STIX/TAXII: Capacidad de ingesta automatizada hacia SIEM/SOAR mediante protocolos estándar $STIX/TAXII$ v2.1.	X		SI
	4.- Análisis - Atribución de Actores de Amenaza: Perfilamiento de adversarios (ej. Lazarus, Wizard Spider) con TTPs mapeados a MITRE ATT&CK.	X		SI
	5.- Operación - Takedown Services: Gestión activa para la	X		SI

	baja de sitios de Phishing o perfiles falsos.			
	6.- Geopolítica - Análisis de Contexto: Informes específicos sobre amenazas al sector Tributario, sin limitación geográfica.	X		SI
	7.- Detección de "Infostealers": El proveedor debe alertar en tiempo real si existen credenciales de empleados o contribuyentes han sido capturadas por malware y puestas a la venta en logs de la Dark Web.	X		SI
	8.- Fugas en Repositorios de Código: Monitoreo activo en GitHub/GitLab para detectar llaves de API, secretos de AWS o fragmentos de código fuente institucional subidos por error o a propósito.	X		SI
2. Requisitos No Funcionales (RNF)	**1.- Disponibilidad (SLA):** El portal de inteligencia debe garantizar un **99.9%** de disponibilidad.	X		SI
	2.- Confidencialidad y Privacidad: Cumplimiento con **ISO 27001** y regulaciones locales de protección de datos.	X		SI
	3.- Falsos Positivos: El proveedor debe garantizar una tasa de falsos positivos inferior al **5%** en alertas de marca.	X		SI
	4.- Escalabilidad: Capacidad de añadir activos (dominios, IPs, marcas) de forma ilimitada o mediante	X		SI

	paquetes elásticos.			
	5.- Soporte: Soporte técnico 24/7 con analistas humanos (no solo bots) para consultas sobre incidentes críticos.	X		SI

e) KEPLER LATAM SPA

La empresa **KEPLER LATAM SPA** confirma el cumplimiento de **8** requerimientos funcionales (RF) y **5** requerimientos no funcionales (RNF), por lo cual, obtiene una puntuación de **100** puntos.

El detalle de la evaluación se indica a continuación:

TIPO	REQUERIMIENTO	OFERTA	OBSERVACIÓN	CONSIDERADA
1. Requisitos Funcionales (RF)	**1.- Recolección - Multifuente (OSINT, Dark Web, Deep Web)**: Acceso a foros cerrados, mercados de leaks, canales de Telegram criminales y repositorios de código (GitHub).	X		SI
	2.- Monitoreo - Brand Protection: Detección de dominios typosquatting, aplicaciones móviles fraudulentas y suplantación de identidad en redes sociales.	X		SI
	3.- Integración - API & STIX/TAXII: Capacidad de ingesta automatizada hacia SIEM/SOAR mediante protocolos estándar $STIX/TAXII$ v2.1.	X		SI
	4.- Análisis - Atribución de Actores de Amenaza: Perfilamiento de adversarios (ej. Lazarus, Wizard Spider) con TTPs mapeados a MITRE ATT&CK.	X		SI

	5.- Operación - Takedown Services: Gestión activa para la baja de sitios de Phishing o perfiles falsos.	X		SI
	6.- Geopolítica - Análisis de Contexto: Informes específicos sobre amenazas al sector Tributario, sin limitación geográfica.	X		SI
	7.- Detección de "Infostealers": El proveedor debe alertar en tiempo real si existen credenciales de empleados o contribuyentes han sido capturadas por malware y puestas a la venta en logs de la Dark Web.	X		SI
	8.- Fugas en Repositorios de Código: Monitoreo activo en GitHub/GitLab para detectar llaves de API, secretos de AWS o fragmentos de código fuente institucional subidos por error o a propósito.	X		SI
2. Requisitos No Funcionales (RNF)	**1.- Disponibilidad (SLA):** El portal de inteligencia debe garantizar un **99.9%** de disponibilidad.	X		SI
	2.- Confidencialidad y Privacidad: Cumplimiento con **ISO 27001** y regulaciones locales de protección de datos.	X		SI
	3.- Falsos Positivos: El proveedor debe garantizar una tasa de falsos positivos inferior al **5%** en alertas de marca.	X		SI
	4.- Escalabilidad: Capacidad de añadir activos (dominios, IPs, marcas) de forma	X		SI

	ilimitada o mediante paquetes elásticos.			
	5.- Soporte: Soporte técnico 24/7 con analistas humanos (no solo bots) para consultas sobre incidentes críticos.	X		SI

f) NASTEC SPA

La empresa **NASTEC SPA** confirma el cumplimiento de **8** requerimientos funcionales (RF) y **5** requerimientos no funcionales (RNF), por lo cual, obtiene una puntuación de **100** puntos.

El detalle de la evaluación se indica a continuación:

TIPO	REQUERIMIENTO	OFERTA	OBSERVACIÓN	CONSIDERADA
1. Requisitos Funcionales (RF)	**1.- Recolección - Multifuente (OSINT, Dark Web, Deep Web)**: Acceso a foros cerrados, mercados de leaks, canales de Telegram criminales y repositorios de código (GitHub).	X		SI
	2.- Monitoreo - Brand Protection: Detección de dominios typosquatting, aplicaciones móviles fraudulentas y suplantación de identidad en redes sociales.	X		SI
	3.- Integración - API & STIX/TAXII: Capacidad de ingesta automatizada hacia SIEM/SOAR mediante protocolos estándar $STIX/TAXII$ v2.1.	X		SI
	4.- Análisis - Atribución de Actores de Amenaza: Perfilamiento de adversarios (ej. Lazarus, Wizard Spider) con TTPs mapeados a MITRE ATT&CK.	X		SI

	5.- Operación - Takedown Services: Gestión activa para la baja de sitios de Phishing o perfiles falsos.	X		SI
	6.- Geopolítica - Análisis de Contexto: Informes específicos sobre amenazas al sector Tributario, sin limitación geográfica.	X		SI
	7.- Detección de "Infostealers": El proveedor debe alertar en tiempo real si existen credenciales de empleados o contribuyentes han sido capturadas por malware y puestas a la venta en logs de la Dark Web.	X		SI
	8.- Fugas en Repositorios de Código: Monitoreo activo en GitHub/GitLab para detectar llaves de API, secretos de AWS o fragmentos de código fuente institucional subidos por error o a propósito.	X		SI
2. Requisitos No Funcionales (RNF)	**1.- Disponibilidad (SLA):** El portal de inteligencia debe garantizar un **99.9%** de disponibilidad.	X		SI
	2.- Confidencialidad y Privacidad: Cumplimiento con **ISO 27001** y regulaciones locales de protección de datos.	X		SI
	3.- Falsos Positivos: El proveedor debe garantizar una tasa de falsos positivos inferior al **5%** en alertas de marca.	X		SI
	4.- Escalabilidad: Capacidad de añadir activos (dominios, IPs, marcas) de forma	X		SI

	ilimitada o mediante paquetes elásticos.			
	5.- Soporte: Soporte técnico 24/7 con analistas humanos (no solo bots) para consultas sobre incidentes críticos.	X		SI

g) NETICS SPA

La empresa **NETICS SPA** confirma el cumplimiento de **8** requerimientos funcionales (RF) y **5** requerimientos no funcionales (RNF), por lo cual, obtiene una puntuación de **100** puntos.

El detalle de la evaluación se indica a continuación:

TIPO	REQUERIMIENTO	OFERTA	OBSERVACIÓN	CONSIDERADA
1. Requisitos Funcionales (RF)	**1.- Recolección - Multifuente (OSINT, Dark Web, Deep Web)**: Acceso a foros cerrados, mercados de leaks, canales de Telegram criminales y repositorios de código (GitHub).	X		SI
	2.- Monitoreo - Brand Protection: Detección de dominios typosquatting, aplicaciones móviles fraudulentas y suplantación de identidad en redes sociales.	X		SI
	3.- Integración - API & STIX/TAXII: Capacidad de ingesta automatizada hacia SIEM/SOAR mediante protocolos estándar $STIX/TAXII$ v2.1.	X		SI
	4.- Análisis - Atribución de Actores de Amenaza: Perfilamiento de adversarios (ej. Lazarus, Wizard Spider) con TTPs mapeados a MITRE ATT&CK.	X		SI

	5.- Operación - Takedown Services: Gestión activa para la baja de sitios de Phishing o perfiles falsos.	X		SI
	6.- Geopolítica - Análisis de Contexto: Informes específicos sobre amenazas al sector Tributario, sin limitación geográfica.	X		SI
	7.- Detección de "Infostealers": El proveedor debe alertar en tiempo real si existen credenciales de empleados o contribuyentes han sido capturadas por malware y puestas a la venta en logs de la Dark Web.	X		SI
	8.- Fugas en Repositorios de Código: Monitoreo activo en GitHub/GitLab para detectar llaves de API, secretos de AWS o fragmentos de código fuente institucional subidos por error o a propósito.	X		SI
2. Requisitos No Funcionales (RNF)	**1.- Disponibilidad (SLA):** El portal de inteligencia debe garantizar un **99.9%** de disponibilidad.	X		SI
	2.- Confidencialidad y Privacidad: Cumplimiento con **ISO 27001** y regulaciones locales de protección de datos.	X		SI
	3.- Falsos Positivos: El proveedor debe garantizar una tasa de falsos positivos inferior al **5%** en alertas de marca.	X		SI
	4.- Escalabilidad: Capacidad de añadir activos (dominios, IPs, marcas) de forma	X		SI

	ilimitada o mediante paquetes elásticos.			
	5.- Soporte: Soporte técnico 24/7 con analistas humanos (no solo bots) para consultas sobre incidentes críticos.	X		SI

h) SECAPPS TECHNOLOGIES SPA

La empresa **SECAPPS TECHNOLOGIES SPA** confirma el cumplimiento de **7** requerimientos funcionales (RF) y **4** requerimientos no funcionales (RNF), por lo cual, obtiene una puntuación de **50** puntos.

El detalle de la evaluación se indica a continuación:

TIPO	REQUERIMIENTO	OFERTA	OBSERVACIÓN	CONSIDERADA
1. Requisitos Funcionales (RF)	**1.- Recolección - Multifuente (OSINT, Dark Web, Deep Web)**: Acceso a foros cerrados, mercados de leaks, canales de Telegram criminales y repositorios de código (GitHub).	Recolección - Multifuente (OSINT, Dark Web, Deep Web): IronFence considera acceso y monitoreo de fuentes abiertas, foros, mercados de leaks, canales públicos de mensajería, repositorios de código y fuentes especializadas.		SI
	2.- Monitoreo - Brand Protection: Detección de dominios typosquatting, aplicaciones móviles fraudulentas y suplantación de identidad en redes sociales.	Monitoreo - Brand Protection: detección de dominios typosquatting, aplicaciones móviles fraudulentas, perfiles falsos, phishing y suplantación de identidad en redes sociales.		SI
	3.- Integración - API & STIX/TAXII: Capacidad de ingesta automatizada hacia SIEM/SOAR mediante protocolos estándar	Integración - API & STIX/TAXII: capacidad de integración mediante API documentada y estándares STIX/TAXII v2.1 para interoperar con SIEM/SOAR.		SI

	$STIX/TAXII$ v2.1.			
	4.- Análisis - Atribución de Actores de Amenaza: Perfilamiento de adversarios (ej. Lazarus, Wizard Spider) con TTPs mapeados a MITRE ATT&CK.	Análisis - Atribución de Actores de Amenaza: perfilamiento de adversarios, TTPs y mapeo a MITRE ATT&CK cuando corresponda.		SI
	5.- Operación - Takedown Services: Gestión activa para la baja de sitios de Phishing o perfiles falsos.	Operación - Takedown Services: gestión activa para baja de sitios de phishing, perfiles falsos, dominios fraudulentos y aplicaciones móviles fraudulentas.		SI
	6.- Geopolítica - Análisis de Contexto: Informes específicos sobre amenazas al sector Tributario, sin limitación geográfica.	Geopolítica - Análisis de Contexto: informes específicos sobre amenazas al sector tributario, sin limitación geográfica, conforme modificación de bases.		SI
	7.- Detección de "Infostealers": El proveedor debe alertar en tiempo real si existen credenciales de empleados o contribuyentes han sido capturadas por malware y puestas a la venta en logs de la Dark Web.	Detección de Infostealers: alertas ante credenciales de empleados o contribuyentes capturadas por malware y publicadas o comercializadas en logs de Dark Web.		SI
	8.- Fugas en Repositorios de Código: Monitoreo activo en GitHub/GitLab para detectar llaves de API, secretos de AWS o fragmentos de código fuente	Fugas en Repositorios de Código: monitoreo activo en GitHub/GitLab para detectar llaves de API, secretos, credenciales o código fuente institucional expuesto.	No hace referencia a al cumplimiento de: secretos de AWS.	NO

	institucional subidos por error o a propósito.			
2. Requisitos No Funcionales (RNF)	**1.- Disponibilidad (SLA):** El portal de inteligencia debe garantizar un **99.9%** de disponibilidad.	Disponibilidad (SLA): portal/consola de inteligencia con disponibilidad objetivo de 99,9%.		SI
	2.- Confidencialidad y Privacidad: Cumplimiento con **ISO 27001** y regulaciones locales de protección de datos.	Confidencialidad y Privacidad: tratamiento reservado de información, control de accesos, reportes protegidos y prácticas alineadas a ISO/IEC 27001 y normativa local de protección de datos.		SI
	3.- Falsos Positivos: El proveedor debe garantizar una tasa de falsos positivos inferior al **5%** en alertas de marca.	Falsos Positivos: proceso de validación y enriquecimiento por analistas para reducir falsos positivos en alertas de marca.	No hace referencia a al cumplimiento de: garantizar una tasa de falsos positivos inferior al 5% en alertas de marca.	NO
	4.- Escalabilidad: Capacidad de añadir activos (dominios, IPs, marcas) de forma ilimitada o mediante paquetes elásticos.	Escalabilidad: capacidad de incorporar activos, dominios, IPs, marcas, palabras clave y fuentes adicionales según coordinación con el SII.		SI
	5.- Soporte: Soporte técnico 24/7 con analistas humanos (no solo bots) para consultas sobre incidentes críticos.	Soporte: soporte técnico y funcional 24/7 con analistas humanos para eventos críticos y consultas asociadas al servicio.		SI

i) TICHILE REVENTA DE SOFTWARE Y HARDWARE SPA

La empresa **TICHILE REVENTA DE SOFTWARE Y HARDWARE SPA** confirma el cumplimiento de **3** requerimientos funcionales (RF) y **4** requerimientos no funcionales (RNF), por lo cual, la oferta se declara inadmisible.

El detalle de la evaluación se indica a continuación:

TIPO	REQUERIMIENTO	OFERTA	OBSERVACIÓN	CONSIDERADA
1. Requisitos Funcionales (RF)	**1.- Recolección - Multifuente (OSINT, Dark Web, Deep Web)**: Acceso a foros cerrados, mercados de leaks, canales de Telegram criminales y repositorios de código (GitHub).	Cumple en OSINT, Dark Web, Deep Web, foros cerrados, leaks, canales de Telegram y fuentes multifuente. Observación: la cobertura específica de repositorios GitHub/GitLab debe validarse, ya que en el análisis aparece como punto no cubierto o no confirmado.	No confirma el cumplimiento de la cobertura específica de repositorios GitHub/GitLab.	NO
	2.- Monitoreo - Brand Protection: Detección de dominios typosquatting, aplicaciones móviles fraudulentas y suplantación de identidad en redes sociales.	Cumple. La solución contempla monitoreo de marca, detección de dominios fraudulentos, typosquatting, perfiles falsos en redes sociales y aplicaciones móviles fraudulentas.		SI
	3.- Integración - API & STIX/TAXII: Capacidad de ingesta automatizada hacia SIEM/SOAR mediante protocolos estándar $STIX/TAXII$ v2.1.	Cumple parcialmente. Se dispone de API para integración, pero no se confirma expresamente compatibilidad con formato STIX/TAXII v2.1. Recomiendo marcarlo solo si se puede adjuntar respaldo del fabricante o aclarar que la integración es vía API.	Señala que "Cumple parcialmente", por lo que no cumple con el Requerimiento Funcional.	NO
	4.- Análisis - Atribución de Actores de Amenaza: Perfilamiento de adversarios (ej. Lazarus, Wizard Spider) con TTPs mapeados a MITRE ATT&CK.		No indica si cumple con el Requerimiento Funcional.	NO

	5.- Operación - Takedown Services: Gestión activa para la baja de sitios de Phishing o perfiles falsos.	CUMPLE		SI
	6.- Geopolítica - Análisis de Contexto: Informes específicos sobre amenazas al sector Tributario, sin limitación geográfica.	Cumple parcialmente. Hay análisis regional y sectorial, pero no se confirma foco específico en sector tributario; podría declararse como análisis regional/gobierno, sujeto a alcance del servicio	Señala que "Cumple parcialmente", por lo que no cumple con el Requerimiento Funcional.	NO
	7.- Detección de "Infostealers": El proveedor debe alertar en tiempo real si existen credenciales de empleados o contribuyentes han sido capturadas por malware y puestas a la venta en logs de la Dark Web.	Cumple. La solución contempla monitoreo de credenciales comprometidas y logs de infostealers en Dark Web.		SI
	8.- Fugas en Repositorios de Código: Monitoreo activo en GitHub/GitLab para detectar llaves de API, secretos de AWS o fragmentos de código fuente institucional subidos por error o a propósito.	La solución contempla capacidades de detección de fugas de información, credenciales comprometidas, documentos expuestos, filtraciones en fuentes abiertas, paste sites, Deep Web y Dark Web. Sin embargo, el monitoreo activo específico sobre repositorios de código como GitHub/GitLab para detectar llaves API, secretos cloud, credenciales AWS o fragmentos de código fuente institucional deberá ser confirmado por el fabricante o considerado mediante	No confirma el cumplimiento del monitoreo activo específico sobre repositorios de código como GitHub/GitLab para detectar llaves API, secretos cloud, credenciales AWS o fragmentos de código fuente institucional.	NO

		una herramienta/servicio complementario especializado.		
2. Requisitos No Funcionales (RNF)	**1.- Disponibilidad (SLA):** El portal de inteligencia debe garantizar un **99.9%** de disponibilidad.	Cumple según la matriz, asociándolo a plataforma enterprise con infraestructura de alta disponibilidad		SI
	2.- Confidencialidad y Privacidad: Cumplimiento con **ISO 27001** y regulaciones locales de protección de datos.	Cumple. Kaspersky cuenta con certificación ISO 27001:2022 y controles asociados a seguridad de la información.		SI
	3.- Falsos Positivos: El proveedor debe garantizar una tasa de falsos positivos inferior al **5%** en alertas de marca.	Cumple parcialmente. El análisis humano ayuda a reducir falsos positivos, pero no aparece respaldo de una garantía contractual inferior al 5%.	Señala que "Cumple parcialmente", por lo que no cumple con el Requerimiento Funcional.	NO
	4.- Escalabilidad: Capacidad de añadir activos (dominios, IPs, marcas) de forma ilimitada o mediante paquetes elásticos.	Cumple. La solución permite escalar activos como dominios, IPs, marcas y otros elementos digitales monitoreados		SI
	5.- Soporte: Soporte técnico 24/7 con analistas humanos (no solo bots) para consultas sobre incidentes críticos.	Cumple. Considera soporte 24/7 y acceso a analistas humanos mediante el servicio asociado.		SI

j) TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA

La empresa **TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA** confirma el cumplimiento de **8** requerimientos funcionales (RF) y **5** requerimientos no funcionales (RNF), por lo cual, obtiene una puntuación de **100** puntos.

El detalle de la evaluación se indica a continuación:

TIPO	REQUERIMIENTO	OFERTA	OBSERVACIÓN	CONSIDERADA
1. Requisitos Funcionales (RF)	**1.- Recolección - Multifuente (OSINT, Dark Web, Deep Web)**: Acceso a foros cerrados, mercados de leaks, canales de Telegram criminales y repositorios de código (GitHub).	X		SI
	2.- Monitoreo - Brand Protection: Detección de dominios typosquatting, aplicaciones móviles fraudulentas y suplantación de identidad en redes sociales.	X		SI
	3.- Integración - API & STIX/TAXII: Capacidad de ingesta automatizada hacia SIEM/SOAR mediante protocolos estándar $STIX/TAXII$ v2.1.	X		SI
	4.- Análisis - Atribución de Actores de Amenaza: Perfilamiento de adversarios (ej. Lazarus, Wizard Spider) con TTPs mapeados a MITRE ATT&CK.	X		SI
	5.- Operación - Takedown Services: Gestión activa para la baja de sitios de Phishing o perfiles falsos.	X		SI
	6.- Geopolítica - Análisis de Contexto: Informes específicos sobre amenazas al sector Tributario, sin limitación geográfica.	X		SI
	7.- Detección de "Infostealers": El proveedor debe alertar en tiempo real si existen credenciales de empleados o contribuyentes han sido	X		SI

	capturadas por malware y puestas a la venta en logs de la Dark Web.			
	8.- Fugas en Repositorios de Código: Monitoreo activo en GitHub/GitLab para detectar llaves de API, secretos de AWS o fragmentos de código fuente institucional subidos por error o a propósito.	X		SI
2. Requisitos No Funcionales (RNF)	**1.- Disponibilidad (SLA):** El portal de inteligencia debe garantizar un **99.9%** de disponibilidad.	X		SI
	2.- Confidencialidad y Privacidad: Cumplimiento con **ISO 27001** y regulaciones locales de protección de datos.	X		SI
	3.- Falsos Positivos: El proveedor debe garantizar una tasa de falsos positivos inferior al **5%** en alertas de marca.	X		SI
	4.- Escalabilidad: Capacidad de añadir activos (dominios, IPs, marcas) de forma ilimitada o mediante paquetes elásticos.	X		SI
	5.- Soporte: Soporte técnico 24/7 con analistas humanos (no solo bots) para consultas sobre incidentes críticos.	X		SI

D. Consola de Investigación

La Comisión Evaluadora concluye que las ofertas presentadas por las empresas **ANIDA CONSULTORES S.A., BUSINESS CONTINUITY SPA, EMPRESA NACIONAL DE TELECOMUNICACIONES S.A., INTEGRACIÓN DE TECNOLOGÍAS ITQ LIMITADA, KEPLER LATAM SPA, NASTEC SPA, NETICS SPA, SECAPPS TECHNOLOGIES SPA, TICHILE**

REVENTA DE SOFTWARE Y HARDWARE SPA y TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA. cumplen con el requisito "**Consola de Investigación"** establecido en las bases de licitación.

A continuación, se muestra una tabla con las ofertas entregadas por cada oferente y el puntaje asignado.

OFERENTE	CARACTERÍSTICA	OFERTA	Puntaje
ANIDA CONSULTORES S.A.	La oferta considera la provisión de una consola de investigación	X	100,00
	La oferta NO considera la provisión de una consola de investigación		
Business Continuity SpA	La oferta considera la provisión de una consola de investigación	X	100,00
	La oferta NO considera la provisión de una consola de investigación		
Empresa Nacional de Telecomunicaciones S.A.	La oferta considera la provisión de una consola de investigación	X	100,00
	La oferta NO considera la provisión de una consola de investigación		
Integración de Tecnologías ITQ Limitada	La oferta considera la provisión de una consola de investigación	X	100,00
	La oferta NO considera la provisión de una consola de investigación		
Kepler Latam SpA	La oferta considera la provisión de una consola de investigación	X	100,00
	La oferta NO considera la provisión de una consola de investigación		
Nastec SpA	La oferta considera la provisión de una consola de investigación	X	100,00

	La oferta NO considera la provisión de una consola de investigación		
NETICS SPA	La oferta considera la provisión de una consola de investigación	X	100,00
	La oferta NO considera la provisión de una consola de investigación		
SECAPPS TECHNOLOGIES SpA	La oferta considera la provisión de una consola de investigación	X	100,00
	La oferta NO considera la provisión de una consola de investigación		
TIChile Reventa de Software y Hardware SpA	La oferta considera la provisión de una consola de investigación	X	100,00
	La oferta NO considera la provisión de una consola de investigación		
TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA	La oferta considera la provisión de una consola de investigación	X	100,00
	La oferta NO considera la provisión de una consola de investigación		

E. Cantidad de horas corridas para realizar Takedown Service

La Comisión Evaluadora concluye que las ofertas presentadas por las empresas **ANIDA CONSULTORES S.A., BUSINESS CONTINUITY SPA, EMPRESA NACIONAL DE TELECOMUNICACIONES S.A., INTEGRACIÓN DE TECNOLOGÍAS ITQ LIMITADA, KEPLER LATAM SPA, NASTEC SPA, NETICS SPA, SECAPPS TECHNOLOGIES SPA, TICHILE REVENTA DE SOFTWARE Y HARDWARE SPA y TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA.** cumplen con el requisito mínimo asociado a la "**Cantidad de horas corridas para realizar Takedown Service"** establecido en las bases de licitación.

A continuación, se muestra una tabla con las ofertas entregadas por cada oferente y el puntaje asignado.

OFERENTE	OFERTA (horas corridas)	PUNTAJE

ANIDA CONSULTORES S.A.	47	50,00
Business Continuity SpA	23	100,00
Empresa Nacional de Telecomunicaciones S.A.	23	100,00
Integración de Tecnologías ITQ Limitada	23	100,00
Kepler Latam SpA	2 a 71 (*)	25,00
Nastec SpA	23	100,00
NETICS SPA	En menos de 24 horas	100,00
SECAPPS TECHNOLOGIES SpA	23	100,00
TIChile Reventa de Software y Hardware SpA	23	100,00
TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA	47	50,00

(*) Considerando que el oferente señala un rango de 2 a 71 horas, para efecto de la evaluación de este criterio se considera 71 horas.

F. Cantidad de veces que ha impartido servicios de Ciberinteligencia.

Los oferentes presentan los antecedentes relativos a la experiencia en el Anexo N° 3 Ficha Experiencia del Oferente y la documentación de respaldo que acrediten la experiencia del oferente.

a) ANIDA CONSULTORES S.A.

La empresa **ANIDA CONSULTORES S.A.** presenta **5** fichas de experiencia de las cuales ninguna fue acreditada de forma válida, por lo cual, obtiene una puntuación de **0** puntos.

El detalle de la evaluación se indica a continuación:

EMPRESA PRESENTADA	DESCRIPCIÓN DEL PROYECTO	OBSERVACIÓN	CONSIDERADA
SAAM TERMINALS (PUERTO DE IQUIQUE - ITI S.A).	Servicio de administración de FW, Antivirus, Monitoreo NOC, parchado de Seguridad y Jobs de respaldo, Consultoría de Ciberseguridad para todas las filiales de SAAM.	La descripción del proyecto y la documentación que se adjuntó para acreditar la experiencia NO corresponde al servicio de Ciberinteligencia solicitado en la licitación. La Factura N° 17921 que respalda la experiencia hace referencia a "Servicios de Monitoreo y Seguridad Informática ANIDA. Servicios consultoría en Informática". Lo que no permite tener total claridad si esta experiencia corresponde al Servicio de Ciberinteligencia requerido.	NO
SERVICIOS AEROPORTUARIOS AEROSAN S.A.	Servicio de administración de FW, Antivirus, Monitoreo NOC, parchado de Seguridad y Jobs de respaldo, Consultoría de Ciberseguridad.	La descripción del proyecto y la documentación que se adjuntó para acreditar la experiencia NO corresponde al servicio de Ciberinteligencia solicitado en la licitación. La Factura N° 17698 que respalda la experiencia hace referencia a "Servicios Informáticos - Servicios Gestionados ANIDA/ TI Servicios SOC y NOC". Lo que no permite tener total claridad si esta experiencia corresponde al Servicio de Ciberinteligencia requerido.	NO

CAJA DE PREVISIÓN DE LA DEFENSA NACIONAL (CAPREDENA)	Servicio de monitoreo SOC (Security Operation Center) y provisión de plataforma de seguridad perimetral y switches core.	La descripción del proyecto y la documentación que se adjuntó para acreditar la experiencia NO corresponde al servicio de Ciberinteligencia solicitado en la licitación. Las Facturas N° 17861 y N° 18247 que respaldan la experiencia hacen referencia a "Operaciones N&S, Prórroga del Servicio de SOC (Security Operation Center) y Seguridad Perimetral" y "Administración Firewall. Servicios SOC (Security Operation Center), Seguridad Perimetral y Switches Core, por 36 meses, más plazo de implementación". Lo que no permite tener total claridad si esta experiencia corresponde al Servicio de Ciberinteligencia requerido.	NO
SALFACORP	Servicio de Administración y Monitoreo de Ciberseguridad - Palo Alto - Gestión de incidencias	La descripción del proyecto y la documentación que se adjuntó para acreditar la experiencia NO corresponde al servicio de Ciberinteligencia solicitado en la licitación. La Factura N° 17770 que respalda la experiencia hace referencia a "Operaciones N&S. Administración FireWall". Lo que no permite tener total claridad si esta experiencia corresponde al Servicio de Ciberinteligencia requerido.	NO
EMPRESA NACIONAL DE CERTIFICACION ELECTRONICA S A	Servicio gestionado de ciberseguridad.	La descripción del proyecto y la documentación que se adjuntó para acreditar la experiencia NO corresponde al servicio de Ciberinteligencia solicitado en la licitación. La Factura N° 17891 que respalda la experiencia hace referencia a "Servicio Gestionado SOC (NW/FW). New Infraestructura (Gestionados	NO

		Ciberseguridad)". Lo que no permite tener total claridad si esta experiencia corresponde al Servicio de Ciberinteligencia requerido.	

b) BUSINESS CONTINUITY SPA

La empresa **BUSINESS CONTINUITY SPA**. presenta **3** fichas de experiencia de las cuales acredita **3** correctamente, por lo cual, obtiene una puntuación de **75** puntos.

El detalle de la evaluación se indica a continuación:

EMPRESA PRESENTADA	DESCRIPCIÓN DEL PROYECTO	OBSERVACIÓN	CONSIDERADA
Unidad Administradora de los Tribunales Tributarios y Aduaneros	Administración, monitoreo y soporte de la plataforma tecnológica de la Unidad, incluyendo servicios de monitoreo y gestión en materia de Ciberseguridad y Servicios de Ciberinteligencia.	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado.	SI
Grupo Planet SpA	Servicio SOC. Incluye administración, monitoreo y soporte de múltiples tecnologías de Ciberseguridad y Servicios de Ciberinteligencia con Kartos	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado.	SI
Bupa Chile S.A.	Servicio de administración, monitoreo y soporte de múltiples tecnologías de Ciberseguridad y Servicios de Ciberinteligencia	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado.	SI

c) EMPRESA NACIONAL DE TELECOMUNICACIONES S.A.

La **EMPRESA NACIONAL DE TELECOMUNICACIONES S.A.** presenta **6** fichas de experiencia de las cuales acredita **5** correctamente, por lo cual, obtiene una puntuación de **100** puntos.

El detalle de la evaluación se indica a continuación:

EMPRESA PRESENTADA	DESCRIPCIÓN DEL PROYECTO	OBSERVACIÓN	CONSIDERADA
Administradora de Fondos de Cesantía (AFC)	Implementación de plataforma de gestión de eventos de ciberseguridad 2024 y Threat Assessment 36 meses	La descripción del proyecto y/o la documentación que se adjuntó para acreditar la experiencia NO corresponde al servicio de Ciberinteligencia solicitado en la licitación. La Factura N° 20345556 que respalda la experiencia, hace referencia a "Servicio Datacenter línea Base". Lo que no permite tener total claridad si esta experiencia corresponde al Servicio de Ciberinteligencia requerido.	NO
Comisión para el Mercado Financiero (CMF)	El objetivo de la licitación es la contratación de un servicio de monitoreo de ciberseguridad, Threat Hunting, Cibervigilancia y Ciberinteligencia, Servicios Red Team, Servicios de IR (Incident Response) 24 meses	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado (descripción ficha).	SI
Ministerio de Obras Públicas (MOP)	Implementación de Proyecto Integral de comunicaciones, redes, Ciberseguridad Ciberinteligencia pág 62 a 67 de las bases / 60 meses	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado (descripción ficha).	SI

MATERIALES Y SOLUCIONES S A. (MTS)	Implementación de plataforma de servicios de Threat Assessment / Ciber inteligencia	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado (descripción ficha).	SI
Servicio de Impuestos Internos (SII)	El objetivo de la licitación es la contratación de un servicio que permita fortalecer el proceso de respuesta ante ataques cibernéticos, realizando acciones de protección preventivas a partir de la detección temprana de indicadores de amenazas o situaciones de riesgo que intenten afectar a la institución.	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado.	SI
Transelec	Implementación de plataforma de servicios de Threat Assessment / Ciberinteligencia (IRR)	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado (descripción ficha).	SI

d) INTEGRACIÓN DE TECNOLOGÍAS ITQ LIMITADA

La empresa **INTEGRACIÓN DE TECNOLOGÍAS ITQ LIMITADA** presenta **9** fichas de experiencia de las cuales acredita **8** correctamente, por lo cual, obtiene una puntuación de **100** puntos.

El detalle de la evaluación se indica a continuación:

EMPRESA PRESENTADA	DESCRIPCIÓN DEL PROYECTO	OBSERVACIÓN	CONSIDERADA

SUBSECRETARIA DE REDES ASISTENCIALES	Extensión de servicios de Cyber SOC por 6 meses para incluir un servicio de Ciberinteligencia para monitoreo de Deep y Dark Web, Monitoreo de Marca y Attack Surface Management	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado (contrato).	SI
Red Salud - TI RED SPA.	Licencia Cyberint (Checkpoint)	La descripción del proyecto y/o la documentación que se adjuntó para acreditar la experiencia NO corresponde al servicio de Ciberinteligencia solicitado en la licitación. La ORDEN DE COMPRA que se adjunta para respalda la experiencia hace referencia a " 421-Ciber-TI-Seg-Sec-ScoreCard-CIBERINT". Lo que no permite tener total claridad si esta experiencia corresponde al Servicio de Ciberinteligencia requerido.	NO
KGHM CHILE SPA	Servicios Gestionados de Ciberseguridad y Ciber inteligencia	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado. (Servicios Gestionados de Ciberseguridad y Ciber inteligencia con Tecnología CrowdStrike)	SI
ESVAL	Servicio Centro de Operaciones de Seguridad (SOC) – Contiene servicio de Inteligencia de Amenazas, Análisis de publicación o venta de información en la web oscura. (Dark Web y Deep Web) y Análisis de Vulnerabilidades	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado (descripción ficha).	SI

TOYOTA CHILE S.A.	Renovación Servicio de CyberSOC incluyendo servicio de Ciberinteligencia.	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado (descripción ficha).	SI
CORPORACIÓN XIX JUEGOS PANAMERICANOS SANTIAGO 2023	Servicios Integrales de Ciberseguridad, Servicios de análisis preventivo y monitoreo de amenazas informáticas (Ciberinteligencia) y Análisis de vulnerabilidades.	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado (descripción ficha).	SI
ADMINISTRADORA DE FONDOS DE PENSIONES UNO	SOC MDR Con Servicio de Inteligencia de Amenazas (CTI)	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado (descripción ficha).	SI
Cemento Polpaico SA	NextGen SOC con Ciberinteligencia basada en CyberINT – Infinity ERM	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado (descripción ficha).	SI
INVERSIONES MARINA DEL SOL S.A.	NextGen SOC, Virtual CISO con Servicio Ciberinteligencia basado en CyberInt – Infinity ERM	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado (descripción ficha).	SI

e) NASTEC SPA

La empresa **NASTEC SPA** presenta **6** fichas de experiencia de las cuales acredita **6** correctamente, por lo cual, obtiene una puntuación de **100** puntos.

El detalle de la evaluación se indica a continuación:

EMPRESA PRESENTADA	DESCRIPCIÓN DEL PROYECTO	OBSERVACIÓN	CONSIDERADA

CORFO	Servicio de Monitoreo, Ciberinteligencia y SOC	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado (descripción ficha).	SI
IPS	Sevicio SOC y Ciberinteligencia + Implementación y soporte de la herramienta Crowdstrike en el cliente para 1500 equipos	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado (descripción ficha).	SI
Orizon	Servicio de Monitoreo, Ciberinteligencia y SOC	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado (descripción ficha).	SI
Servel	Servicio de Monitoreo, Ciberinteligencia y SOC	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado (descripción ficha).	SI
SSFFAA	Servicio de Monitoreo, Ciberinteligencia y SOC	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado (descripción ficha).	SI
TRANSTECNIA	Contrato Servicio Nastec y Transtecnia CF.pdf / Contrato de Ciberintelegencia y CyberSOC	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado (descripción ficha).	SI

f) NETICS SPA

La empresa **NETICS SPA** presenta **6** fichas de experiencia de las cuales ninguna fue acreditada de forma válida, por lo cual, obtiene una puntuación de **0** puntos.

El detalle de la evaluación se indica a continuación:

EMPRESA PRESENTADA	DESCRIPCIÓN DEL PROYECTO	OBSERVACIÓN	CONSIDERADA

Superintendencia de Casinos de Juegos.	PROYECTO DE CONSULTORÍA Y/O AUDITORÍA EN CIBERSEGURIDAD	La descripción del proyecto y/o la documentación que se adjuntó para acreditar la experiencia NO corresponde al servicio de Ciberinteligencia solicitado en la licitación. La ORDEN DE COMPRA NRO 4246-123-CM25 que se adjunta para respalda la experiencia hace referencia a "PROYECTO DE CONSULTORÍA Y/O AUDITORÍA EN CIBERSEGURIDAD". Lo que no permite tener total claridad si esta experiencia corresponde al Servicio de Ciberinteligencia requerido.	NO
Defensoría Penal Pública	PROYECTO DE CONSULTORÍA Y/O AUDITORÍA EN CIBERSEGURIDAD DEVSECOPS	La descripción del proyecto y/o la documentación que se adjuntó para acreditar la experiencia NO corresponde al servicio de Ciberinteligencia solicitado en la licitación. La ORDEN DE COMPRA NRO OC 1876-92-CM25 que se adjunta para respalda la experiencia hace referencia a "PROYECTO DE CONSULTORÍA Y/O AUDITORÍA EN CIBERSEGURIDAD". Lo que no permite tener total claridad si esta experiencia corresponde al Servicio de Ciberinteligencia requerido.	NO
Pacífico Cable Spa.	Para JUNJI: Servicio CDC 24/7 (Cyber Defense Center) para JUNJI, con SIEM IBM QRadar dimensionado a 1.900 EPS, e incluye servicios complementarios: Ethical Hacking y Pentesting, capacitación y test de phishing para 3.500 usuarios, gestión de	La descripción del proyecto y/o la documentación que se adjuntó para acreditar la experiencia NO corresponde al servicio de Ciberinteligencia solicitado en la licitación. No se adjunta el Contrato de Servicio que se señala en la Ficha del Anexo N° 3. Lo que no permite tener total claridad si esta experiencia corresponde al Servicio de Ciberinteligencia requerido.	NO

	Vicarius y operación del servicio CDC.		
Pacífico Cable Spa.	Para Defensoría Penal Pública: Servicio gestionado de Ciberseguridad tipo Cyber Defense Center (SOC/CDC) para DPP, con correlación y gestión de eventos, monitoreo 24x7x365 para 1.000 EPS, y gestión y seguimiento de incidentes por analistas N1/N2/N3, con reportería técnico-ejecutiva y capacidad de respuesta a incidentes (IR).)	La descripción del proyecto y/o la documentación que se adjuntó para acreditar la experiencia NO corresponde al servicio de Ciberinteligencia solicitado en la licitación. No se adjunta el Contrato de Servicio que se señala en la Ficha del Anexo N° 3. Lo que no permite tener total claridad si esta experiencia corresponde al Servicio de Ciberinteligencia requerido.	NO
Corporación Administrativa del Poder Judicial	Licenciamiento anual suscripción plataforma de seguridad extendida del poder judicial.	La descripción del proyecto y/o la documentación que se adjuntó para acreditar la experiencia NO corresponde al servicio de Ciberinteligencia solicitado en la licitación. La ORDEN DE COMPRA NRO OC 425-888-SE25 que se adjunta para respalda la experiencia hace referencia a "Software de gestión de licencias". Lo que no permite tener total claridad si esta experiencia corresponde al Servicio de Ciberinteligencia requerido.	NO
Servicio Agrícola Ganadero.	Servicio Mensual Soporte Monitoreo Firewall	La descripción del proyecto y/o la documentación que se adjuntó para acreditar la experiencia NO corresponde al servicio de Ciberinteligencia solicitado en la licitación. La ORDEN DE COMPRA NRO OC 612-792-SE24 que se adjunta para respalda la experiencia hace referencia a "Equipo de seguridad de red de firewall". Lo que no permite tener total claridad si esta experiencia	NO

		corresponde al Servicio de Ciberinteligencia requerido.	

g) SECAPPS TECHNOLOGIES SPA

La empresa **SECAPPS TECHNOLOGIES SPA** presenta **5** fichas de experiencia de las cuales acredita **5** correctamente, por lo cual, obtiene una puntuación de **100** puntos.

El detalle de la evaluación se indica a continuación:

EMPRESA PRESENTADA	DESCRIPCIÓN DEL PROYECTO	OBSERVACIÓN	CONSIDERADA
INFINITY IT CONSULTING SpA	Cliente final del proyecto: Compañía Minera Collahuasi. Servicio de ciberinteligencia con Harpia Tech/IronFence para cliente final del sector minería, orientado a monitoreo de amenazas, análisis de exposición digital, seguimiento de riesgos, detección de señales en fuentes abiertas, Deep/Dark Web, reportabilidad y alertamiento (07/2024 al 11/2024)	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado.	SI
INFINITY IT CONSULTING SpA	Cliente final del proyecto: Compañía Minera Collahuasi. Continuidad del servicio de ciberinteligencia e inteligencia de amenazas para entorno minero, con monitoreo persistente, análisis de indicadores, identificación de amenazas, reportabilidad y alertamiento sobre riesgos digitales y exposición de activos (12/2024 al 06/2025)	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado.	SI

INFINITY IT CONSULTING SpA	Cliente final del proyecto: Compañía Minera Collahuasi. Servicio de ciberinteligencia con IronFence, incluyendo setup, puesta en marcha, operación mensual, monitoreo de amenazas, exposición digital, Deep/Dark Web, fuentes abiertas, alertamiento y reportabilidad para cliente final de alta criticidad (10/2025 al 01/2026)	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado.	SI
INFINITY IT CONSULTING SpA	Cliente final del proyecto: Banco Internacional. Proyecto de ciberinteligencia con Harpia Tech/IronFence para Banco Internacional, orientado a monitoreo de amenazas, análisis de exposición digital, detección de riesgos en fuentes abiertas, Deep/Dark Web, fraude digital, suplantación y alertamiento de inteligencia (09/2024 al 10/2024)	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado.	SI
IRONFENCE CHILE INTELIGENCIA ARTIFICIAL SpA.	Cliente final del proyecto: ABIF. Servicio de consultoría y apoyo en deshabilitación de infraestructura maliciosa on demand, asociado a gestión de takedown, baja de activos fraudulentos, phishing, suplantación y protección frente a amenazas digitales (04/2025)	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado.	SI

h) TICHILE REVENTA DE SOFTWARE Y HARDWARE SPA

La empresa **TICHILE REVENTA DE SOFTWARE Y HARDWARE SPA** presenta **0** fichas de experiencia, por lo cual, obtiene una puntuación de **0** puntos.

i) TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA.

La empresa **TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA** presenta **2** fichas de experiencia de las cuales acredita 1 correctamente, por lo cual, obtiene una puntuación de **50** puntos.

El detalle de la evaluación se indica a continuación:

EMPRESA PRESENTADA	DESCRIPCIÓN DEL PROYECTO	OBSERVACIÓN	CONSIDERADA
Dirección de compras y Contratación Publica	CONTRATACIÓN DEL SERVICIO DE CENTRO DE OPERACIONES DE SEGURIDAD Implementación del servicio de monitoreo de seguridad y Ciberseguridad, Servicio de detección temprana de eventos potenciales de incidentes de seguridad, Servicio de análisis técnico y contextual de eventos, Servicio de respuesta ante incidentes de seguridad, Servicio de recuperación ante incidentes de seguridad, Aplicación de medidas de protección ante amenazas o incidentes de Ciberseguridad, Monitoreo de marca y auditoría en la Dark Web, Informe diario de accesos por VPN, servicios On-Premise y en la nube, Informe semanal de actividad del WAF (Google y AWS), Informe mensual de vulnerabilidades en servidores y estaciones de trabajo.)	La documentación que se adjuntó permite acreditar que está experiencia corresponde al servicio solicitado.	SI

EMBOTELLADORA ANDINA S.A.	Servicio de administración y soporte de infraestructura firewall, WAF, IDS, IPS y todo el hardware en operación, Antivirus/EDR/XDR, PAM, Administración, Operación y Soporte Evolutivo, Servicio SIEM-SOAR, suite defender, plataforma integrada de seguridad, herramientas de búsqueda y gestión de vulnerabilidades, Azure identity protection, Security web gateway/Security internet Gateway, Servicios de protección de DNS, Servicios SASE, Soluciones DLP, Soluciones MDM, Soluciones de protección de correo, Herramienta de gestión de dispositivos de red y otras herramientas de gestión de dispositivos de seguridad, Análisis y Gestión de Vulnerabilidades, Servicio SOAR, orquestación de alertas y flujos de incidentes, Servicio de Pentesting a Aplicativos WEB, Servicio Pentesting a Infraestructura Interna, Servicio de Threat Intelligence-Monitoreo de marca y fuga de datos, Análisis e Informe Forense, Chequeo y Cumplimiento de Postura de Seguridad, Servicio de Threat Hunting, Servicio de Gestión y Respuesta de incidentes o eventos de seguridad (CSIRT).	La descripción del proyecto y/o la documentación que se adjuntó para acreditar la experiencia NO corresponde al servicio de Ciberinteligencia solicitado en la licitación. El Contrato de Servicio que se adjunta para respalda la experiencia hace referencia a "Servicios de administración, soporte, mantención y seguridad informática en relación con las redes, hardware, software, plataformas tecnológicas y dispositivos digitales utilizados por Andina para ejecutar sus operaciones. *En cuanto a la gestión de Redes*, el Proveedor se obliga a proveer servicios de administración, configuración, monitoreo, soporte y mantención de las redes de comunicaciones LAN, WAN, VPN, Wi-Fi, telefonía y software de base requerido, asegurando su funcionamiento, capacidad y continuidad operacional. *En cuanto a la gestión de Seguridad Informática,* el Proveedor se obliga a identificar y proteger los activos de información y prevenir activamente brechas de seguridad; detectar actividades maliciosas y/o vulnerabilidades; dar respuesta y/o solución a inconvenientes de cualquier naturaleza; y	NO

		recuperar adecuada y oportunamente los sistemas en caso de compromiso, suspensiones o interrupciones de acceso a los datos". Lo que no permite tener total claridad si esta experiencia corresponde al Servicio de Ciberinteligencia requerido.	

G. Cuenta con Programas de Integridad y Ética Empresarial.

Las empresas **ANIDA CONSULTORES S.A., BUSINESS CONTINUITY SPA, EMPRESA NACIONAL DE TELECOMUNICACIONES S.A., INTEGRACIÓN DE TECNOLOGÍAS ITQ LIMITADA, NASTEC SPA, NETICS SPA, SECAPPS TECHNOLOGIES SPA y TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA.,** logran acreditar que cuentan con programas de integridad y ética empresarial, logrando la puntuación máxima de 100 puntos.

H. Cumplimiento de los requisitos de presentación de las ofertas.

Las empresas **ANIDA CONSULTORES S.A., BUSINESS CONTINUITY SPA, EMPRESA NACIONAL DE TELECOMUNICACIONES S.A., INTEGRACIÓN DE TECNOLOGÍAS ITQ LIMITADA, NASTEC SPA, NETICS SPA, SECAPPS TECHNOLOGIES SPA y TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA.,** logran acreditar que cuentan con programas de integridad y ética empresarial, logrando la puntuación máxima de 100 puntos.

5. RESULTADO EVALUACIÓN TÉCNICA

La siguiente tabla muestra el resumen de los puntajes ponderados obtenidos en cada uno de los criterios técnicos de evaluación, considerando las ponderaciones establecidas para cada uno de los criterios.

Dado lo anterior, el puntaje en la evaluación técnica de cada oferente es el siguiente:

ITEM	%	Característica	Puntaje Asignado	ANIDA CONSULTORES S.A.	Business Continuity SpA	Empresa Nacional de Telecomunicaciones S.A.	Integración de Tecnologías ITQ Limitada	Nastec SpA	NETICS SPA	SECAPPS TECHNOLOGIES SpA	TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA
Servicio de gestión de casos de investigación. Fuentes de información (Este criterio será evaluado de acuerdo con el Anexo N° 5B: Aspectos Evaluables de la Oferta).	25	Incluye como fuente de información: 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web Y adicionalmente incorpora el total de las siguientes fuentes: 3. Plataformas de contenido audiovisual (Youtube). 4. Foros y sitios de publicación abierta (Reddit y/o Pastebin). 5. Repositorios de código y desarrollo (GitHub y GitLab). 6. Medios de comunicación digitales (Portales de noticias y Newspapers -prensa digital-). 7. Otras fuentes adicionales (Cualquier otra fuente abierta, cerrada o especializada que resulte pertinente para los fines del servicio).	100	100	100	100	100	100	100	100	100
		Incluye como fuente de información: 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web Y, adicionalmente, considera al menos cuatro de las siguientes fuentes: 3. Plataformas de contenido audiovisual (Youtube). 4. Foros y sitios de publicación abierta (Reddit y/o Pastebin). 5. Repositorios de código y desarrollo (GitHub y GitLab). 6. Medios de comunicación digitales (Portales de noticias y Newspapers -prensa digital-). 7. Otras fuentes adicionales (Cualquier otra fuente abierta, cerrada o especializada que resulte pertinente para los fines del servicio).	75								
		Incluye como fuente de información: 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web Y, adicionalmente, considera al menos tres de las siguientes fuentes: 3. Plataformas de contenido audiovisual (Youtube). 4. Foros y sitios de publicación abierta (Reddit y/o Pastebin). 5. Repositorios de código y desarrollo (GitHub y GitLab). 6. Medios de comunicación digitales (Portales de noticias y Newspapers -prensa digital-). 7. Otras fuentes adicionales (Cualquier otra fuente abierta, cerrada o especializada que resulte pertinente para los fines del servicio).	50								
		Incluye como fuente de información: 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web Y, adicionalmente, considera una o dos de las siguientes: 3. Plataformas de contenido audiovisual (Youtube). 4. Foros y sitios de publicación abierta (Reddit y/o Pastebin). 5. Repositorios de código y desarrollo (GitHub y GitLab). 6. Medios de comunicación digitales (Portales de noticias y Newspapers -prensa digital-). 7. Otras fuentes adicionales (Cualquier otra fuente abierta, cerrada o especializada que resulte pertinente para los fines del servicio).	35								
		Incluye sólo como fuente de información: 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok, Instagram y Telegram). 2. Deep Web y Dark Web	25								
		No informa o no incluye a lo menos las siguientes fuentes de información : 1. Redes sociales y plataformas de mensajería (WhatsApp, Facebook, X (Twitter), LinkedIn, TikTok,	Inadmisible								
Requerimientos Funcionales y No Funcionales según bases técnicas punto 2.8	25	El servicio ofertado considera la totalidad de los Requerimientos Funcionales y no Funcionales	100	100	100	100	100	100	100	50	100
		El servicio ofertado no considera la totalidad de los requerimientos funcionales y no funcionales, pero considera al menos 6 de los Requerimientos Funcionales (dentro de los cuales se contempla el requisito número 5. Operación Takedown Services) y al menos 3 de los no Funcionales	50								
		* Servicio NO considera al menos 6 de los Requerimientos Funcionales y al menos de 3 de los No Funcionales; o - No presenta Anexo 5A; o - No declara el cumplimiento de lo requerido en el Anexo 5A; o - Considera al menos 6 de los Requerimientos Funcionales y al menos 3 de los no Funcionales, pero sin contemplar el requisito funcional número 5. Operación Takedown Services	Inadmisible								
Consola de Investigación (**) (Este criterio será evaluado de acuerdo con el Anexo N° 5B: Aspectos Evaluables de la Oferta).	20	La oferta considera la provisión de una consola de investigación	100	100	100	100	100	100	100	100	100
		La oferta NO considera la provisión de una consola de investigación	0								
Cantidad de horas corridas para realizar Takedown Service (Capacidad para dar de baja sitios de phishing, perfiles falsos en redes sociales y aplicaciones móviles fraudulentas) (Este criterio será evaluado de acuerdo con el Anexo N° 5B: Aspectos Evaluables de la Oferta).	10	En menos de 24 horas	100	50	100	100	100	100	100	100	50
		Entre 24 horas y 47 horas	50								
		Entre 48 horas y 72 horas	25								
		Más de 72 horas	Inadmisible								
Cantidad de veces que ha impartido servicios de Ciberinteligencia (***) Entregar antecedentes en Anexo N° 3 y adjuntar documento(s) que acredite(n) la experiencia respectiva, según corresponda.	10	5 o más veces en el mercado	100	0	75	100	100	100	0	100	50
		3 o 4 veces en el mercado	75								
		1 o 2 veces en el mercado	50								
		Ninguna vez en el mercado o no acredita experiencia en el servicio ofertado	0								
			Puntaje Total	85,00	97,50	100,00	100,00	100,00	90,00	87,50	90,00

Dado lo anterior, el puntaje en la evaluación técnica de cada oferente es el siguiente:

OFERENTE	Puntaje Final Evaluación
EMPRESA NACIONAL DE TELECOMUNICACIONES S.A.	100,00
INTEGRACIÓN DE TECNOLOGÍAS ITQ LIMITADA	100,00
NASTEC SPA	100,00
BUSINESS CONTINUITY SPA	97,50
NETICS SPA	90,00
TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA	90,00
SECAPPS TECHNOLOGIES SPA	87,50
ANIDA CONSULTORES S.A.	85,00

Como resultado de la evaluación técnica, la comisión evaluadora establece que:

a. La oferta de la empresa **KEPLER LATAM SPA** no cumple con lo requerido en el punto "**2.2. Servicio de monitoreo de activos digitales expuestos a internet**" de las Bases Técnicas – Parte III, por lo tanto, su oferta es declarada **Inadmisible** y, por ende, no pasa a la etapa de evaluación económica.

b. La oferta de la empresa **TICHILE REVENTA DE SOFTWARE Y HARDWARE SPA** no cumple con lo requerido en el **punto "2.8. Requerimientos del servicio, Requisitos Funcionales (RF)",** de las Bases Técnicas – Parte III**,** ya que el Servicio NO considera al menos 6 de los Requerimientos Funcionales y al menos de 3 de los No Funcionales, por lo tanto, su oferta es declarada Inadmisible y, por ende, no pasa a la etapa de evaluación económica.

c. Las ofertas de las otras empresas cumplen con lo establecido en el punto 3.3.2 de las bases, por tanto, pasan a la etapa de evaluación económica.

6. EVALUACIÓN ECONÓMICA

En consideración a los antecedentes presentados, se procede a evaluar económicamente las ofertas presentadas por las empresas: **ANIDA CONSULTORES S.A., BUSINESS CONTINUITY SPA, EMPRESA NACIONAL DE TELECOMUNICACIONES S.A., INTEGRACIÓN DE TECNOLOGÍAS ITQ LIMITADA, NASTEC SPA, NETICS SPA, SECAPPS TECHNOLOGIES SPA y TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA.**

Según lo establecido en las Bases de Licitación, Evaluación Económica, punto 3.3.4., las ofertas económicas serán evaluadas en base a la siguiente fórmula:

$$Puntaje\ oferta\ económica\ i = \left(\frac{Oferta\ mínima}{Oferta\ económica\ "i"}\right)\ x\ 100$$

Dónde:

- **Puntaje oferta económica i**: Puntaje asociado a la oferta económica "i"
- **Oferta mínima**: Precio de la oferta más económica entre todos los oferentes
- **Oferta económica i**: Precio de la oferta económica del oferente "i". Para estos efectos, se considerará el PRECIO MENSUAL NETO EN US$ indicado por el oferente en el punto 1 Anexo N°2.

El detalle de los puntajes de cada oferente se describe a continuación:

Oferente	**Servicio de Ciberinteligencia** Precio mensual Neto (US$)	**Servicio de Ciberinteligencia** Precio mensual Bruto (US$)	Puntaje
Integración de Tecnologías ITQ Limitada	**5.489,9800**	**6.533,0762**	**100,00**
TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA	**5.934,0000**	**7.061,4600**	**92,52**
Business Continuity SpA	**6.000,0000**	**7.140,0000**	**91,50**
SECAPPS TECHNOLOGIES SpA	**6.701,0200**	**7.974,2138**	**81,93**
Nastec SpA	**6.715,0000**	**7.990,8500**	**81,76**
Empresa Nacional de Telecomunicaciones S.A.	**7.145,0000**	**8.502,5500**	**76,84**
NETICS SPA	**7.216,0000**	**8.587,0400**	**76,08**

ANIDA CONSULTORES S.A.	**7.387,4900**	**8.791,1131**	**74,31**

7. RESULTADO FINAL EVALUACIÓN TÉCNICA-ECONÓMICA

La siguiente tabla muestra el resumen de los puntajes ponderados finales obtenidos en la evaluación técnica y económica:

OFERENTE	Puntaje Técnico	Puntaje Técnico Ponderado (58%)	Puntaje económico	Puntaje económico Ponderado (40%)	Puntaje Administrativo	Puntaje Administrativo Ponderado (2%)	Puntaje Final
Integración de Tecnologías ITQ Limitada	**100,00**	**58,00**	**100,00**	**40,00**	**100,00**	**2,00**	**100,00**
Business Continuity SpA	**97,50**	**56,55**	**91,50**	**36,60**	**100,00**	**2,00**	**95,15**
Nastec SpA	**100,00**	**58,00**	**81,76**	**32,70**	**100,00**	**2,00**	**92,70**
TIVIT CHILE TERCERIZACION DE PROCESOS, SERVICIOS Y TECNOLOGIA SPA	**90,00**	**52,20**	**92,52**	**37,01**	**100,00**	**2,00**	**91,21**
Empresa Nacional de Telecomunicaciones S.A.	**100,00**	**58,00**	**76,84**	**30,73**	**100,00**	**2,00**	**90,73**
SECAPPS TECHNOLOGIES SpA	**87,50**	**50,75**	**81,93**	**32,77**	**100,00**	**2,00**	**85,52**
NETICS SPA	**90,00**	**52,20**	**76,08**	**30,43**	**50,00**	**1,00**	**83,63**
ANIDA CONSULTORES S.A.	**85,00**	**49,30**	**74,31**	**29,73**	**100,00**	**2,00**	**81,03**

8. PROPUESTA DE LA COMISIÓN EVALUADORA:

Como resultado de la evaluación, la Comisión Evaluadora propone adjudicar a la empresa **INTEGRACIÓN DE TECNOLOGÍAS ITQ LIMITADA RUT: 76.092.207-2**, el proceso licitatorio N°**1605-23-LP26**, denominado **LP-4609** "**Servicio de Ciberinteligencia**", obteniendo un puntaje

total de 98,55 puntos. La empresa alcanza la puntuación más alta y cumple con el presupuesto establecido para este proceso de licitación.

El monto ofertado por la empresa asciende a **US$ 6.533,08** por mes, lo que equivale aproximadamente a **$ 5.820.252.-,** ambos valores incluyen IVA. El valor total del servicio a 36 meses es **$ 209.529.081.-**

Para la conversión a pesos chilenos, se consideró el valor del dólar observado publicado por el Banco Central de Chile al **11 de mayo de 2026**, correspondiente a $890,89.

Además, los integrantes de la comisión declaran no presentar conflictos de interés en este proceso.

JUAN LIPAN MELLA

Firmado digitalmente por JUAN LIPAN MELLA
Fecha: 2026.05.27 10:39:44 -04'00'

Juan Lipán Mella
Presidente

LESTER MANUEL VILLEGAS PALMA

Firmado digitalmente por LESTER MANUEL VILLEGAS PALMA
Nombre de reconocimiento (DN): cn=LESTER MANUEL VILLEGAS PALMA, o, ou, email=lester.villegas@sii.cl, c=CL
Fecha: 2026.05.27 15:01:01 -04'00'

Lester Villegas Palma
Secretario

LUZ OLGA LIZANA ROJAS

Firmado digitalmente por LUZ OLGA LIZANA ROJAS
Fecha: 2026.05.27 10:55:56 -04'00'

Luz Olga Lizana Rojas
Integrante

Mario Raúl Rojas Villarroel

Firmado digitalmente por Mario Raúl Rojas Villarroel
Fecha: 2026.05.27 15:28:10 -04'00'

DARIO EDUARDO VILLALON DE LA VEGA

Firmado digitalmente por DARIO EDUARDO VILLALON DE LA VEGA
Fecha: 2026.05.29 08:59:57 -04'00'