

PRONUNCIAMIENTO N° 152-2025/OECE-DSAT

Entidad : Superintendencia Nacional de Fiscalización Laboral

Referencia : Concurso Público N° 1-2025-SUNAFIL-1, convocado para la contratación del “*Servicio de acceso dedicado de internet de banda ancha para la SUNAFIL*”

1. ANTECEDENTES

Mediante el formulario de solicitud de emisión de pronunciamiento recibido el 28¹ de mayo de 2025 y subsanado 5² de junio de 2025, el presidente del Comité de Selección a cargo del procedimiento de selección de la referencia remitió a este Organismo Especializado la solicitud de elevación de cuestionamientos al pliego absolutorio de consultas y observaciones presentada por **GTD PERÚ S.A.**, en cumplimiento de lo dispuesto por el artículo 21 de la Ley N° 30225, Ley de Contrataciones del Estado, en adelante la “Ley”, y el artículo 72 de su Reglamento, aprobado por el Decreto Supremo N° 344-2018-EF, en adelante el “Reglamento” y conforme lo dispuesto en la Cuarta Disposición Complementaria Transitoria de la Ley N° 32069 - Ley General de Contrataciones Públicas.

Adicionalmente, cabe precisar que en la emisión del presente pronunciamiento se utilizó el orden establecido por el Comité de Selección en el pliego absolutorio³ y los temas materia de cuestionamientos del mencionado participante, conforme al siguiente detalle:

- **Cuestionamiento N° 1** : Respecto a la absolución de la consulta y/u observación N° 85, referida al “***Sistema de protección Anti DDoS***”.
- **Cuestionamiento N° 2** : Respecto a la absolución de la consulta y/u observación N° 86, referida al “***Sistema de prevención de intrusos (IPS)***”.

2. CUESTIONAMIENTOS

De manera previa, cabe señalar que:

- Este Organismo Especializado no ostenta la calidad de perito técnico dirimente respecto a las posiciones de determinados aspectos del requerimiento (especificaciones técnicas, términos de referencia y expediente técnico de obra, según corresponda); sin embargo, puede requerir a la Entidad informes que

¹ Mediante el Expediente N° 2025-0017466.

² Mediante el Expediente N° 2025-0021410.

³ Para la emisión del presente Pronunciamiento se utilizará la numeración establecida en el pliego absolutorio en versión PDF.

contengan la posición técnica al respecto, considerando que el área usuaria es la dependencia que cuenta con los conocimientos técnicos necesarios para definir las características técnicas de los bienes, servicios y obras que se habrán de contratar.

- De conformidad con el artículo 9 de la Ley, los funcionarios y servidores que intervienen en el proceso de contratación encargados de elaborar el requerimiento, indagación de mercado, el pliego absolutorio y el Informe Técnico, así como la atención de los pedidos de información requeridos, en virtud a la emisión del presente pronunciamiento, con independencia del régimen jurídico que los vincule a la Entidad, son responsables de la información que se remitió para las adecuaciones realizadas en el presente documento.

Cuestionamiento N° 1:

Respecto al “Sistema de protección Anti DDoS”

El participante **GTD PERÚ S.A** cuestionó la absolución de la consulta y/u observación N° 85 del pliego, alegando que la respuesta brindada por el Comité de Selección vulnera los Principios de Libertad de Concurrencia, Igualdad de Trato, Competencia, así como de Eficacia y Eficiencia; toda vez que, no se considera que los fabricantes AntiDDoS aplican diferentes enfoques y tecnologías; por lo que, exigir exclusivamente la generación automática de firmas en tiempo real, como única metodología tecnológica puede tener efectos negativos como el aumento en la tasa de falsos positivos, especialmente en ataques complejos, al limitar la capacidad de adaptación de la solución ante amenazas emergentes y restringir el acceso a alternativas más “costo-eficientes” con mejor rendimiento técnico.

Por lo tanto, la pretensión del recurrente consiste en que la Entidad **admita que el sistema de protección Anti-DDoS no se limite exclusivamente al uso de mecanismos basados en la creación de firmas en tiempo real, sino que se admita la posibilidad de implementar otras estrategias complementarias de defensa.**

Pronunciamiento

Sobre el particular, de la revisión del acápite 5.2 del numeral 3.1 del Capítulo III de la Sección Específica de las Bases de la convocatoria, se aprecia lo siguiente:

“5.2. Equipamiento de Gestión y Seguridad de Internet:

(...)

B. Solución de Protección AntiDDoS:

(...)

○ El sistema de protección Anti DDoS debe poder mitigar ataques de denegación de servicio de día cero, distribuidos y no distribuidos en base a la generación automática de firmas en tiempo real.

(...)”

(El subrayado y resaltado es agregado)

Es así que, mediante la consulta y/u observación N° 85 del pliego, se solicitó a la Entidad que, con el objetivo de fomentar la pluralidad de proveedores y considerando

que cada fabricante implementa estrategias tecnológicas distintas, se revise el presente requerimiento, a fin de que no dependa exclusivamente de la creación de firmas en tiempo real, sino que permita también la utilización de otras estrategias de defensa, como la implementación de algoritmos adaptativos en múltiples capas (de L3 a L7), que operen de forma conjunta e integren la inteligencia propia del fabricante; toda vez que, esta metodología permite una mitigación dinámica y altamente eficaz frente a ataques emergentes y multivectoriales, al proporcionar una respuesta oportuna y adaptativa ante amenazas complejas, sin requerir la generación de firmas y reduce la probabilidad de falsos positivos, que suelen incrementarse en escenarios con vectores de ataque múltiples.

Ante lo cual, la Entidad aclaró que, de acuerdo con los Términos de Referencia, la solución de protección Anti-DDoS deberá, como mínimo, garantizar una defensa frente a ataques de inundación del tipo TCP SYN, TCP RST, UDP, ICMP, así como otros tipos de ataques de denegación de servicio. Adicionalmente, la solución incorpora un módulo de Sistema de Prevención de Intrusos (IPS), con capacidad de operación en múltiples capas del modelo de red.

En relación con ello, y en atención al cuestionamiento formulado por el participante, mediante el INFORME N° 019-2025-SUNAFIL/GG-OTIC-ECRT⁴, la Entidad señaló lo siguiente:

“(…)

- *La generación automática de firmas en tiempo real es un requisito importante y fundamental para una protección AntiDDoS efectiva, ya que es capaz de mitigar proactivamente ataques desconocidos o de día cero (Zero day) y multivectoriales complejos al detectar patrones maliciosos nunca antes vistos.*
- *Las firmas permiten identificar y bloquear ataques de manera automatizada.*
- *Cuando se identifica patrón de ataque, el sistema puede generar firmas rápidamente y bloquear ataques similares y si el ataque es predecible las firmas pueden bloquear rápidamente el tráfico.*
- *Asimismo, cabe mencionar que la entidad desde hace 03 años cuenta con un sistema de protección AntiDDoS mediante generación automática de firmas, el cual ha operado de manera eficiente y ha brindado una alta seguridad a la entidad.*
- *Las desventajas de trabajar con un sistema de protección AntiDDoS con algoritmos adaptativos, es que pueden generar falsos positivos si no están suficientemente entrenados. Asimismo, los algoritmos adaptativos deben ser alimentados con datos históricos para aprender los patrones de tráfico, los cuales pueden variar en el tiempo y de no ser bien configurados pueden generar falsos positivos.*

Por lo expuesto, es importante y crucial que el sistema de protección AntiDDoS deba poder mitigar ataques de denegación de servicio de día cero, distribuidos y no distribuidos en base a la generación automática de firmas en tiempo real, porque optimiza la respuesta ante ataques DDoS y protege a la red contra una variedad de ataques complejos. Asimismo, es importante mencionar que la entidad desde hace 03 años cuenta con un sistema de protección AntiDDoS mediante generación automática de firmas, el cual ha operado de manera eficiente y ha brindado una alta seguridad a la entidad.

“(…)”

(El subrayado y resaltado es agregado)

⁴ Remitido mediante el Expediente N° 2025-0017466, de fecha 28 de mayo de 2025.

Al respecto, cabe señalar que, en el artículo 16 de la Ley y el artículo 29 del Reglamento, se establece que el área usuaria es la responsable de la elaboración del requerimiento, debiendo éste contener la descripción objetiva y precisa de las características y/o requisitos funcionales relevantes para cumplir la finalidad pública de la contratación y las condiciones en las que debe ejecutarse la contratación, debiendo asegurar la calidad técnica y reducir la necesidad de su reformulación por errores o deficiencias técnicas que repercutan en el proceso de contratación.

Ahora bien, en atención del tenor de lo cuestionado, se aprecia que la Entidad, como responsable y mejor conocedora de sus necesidades, mediante el citado informe, ratificó su requerimiento, manteniendo que el sistema de protección Anti DDoS debe poder mitigar ataques de denegación de servicio de día cero, distribuidos y no distribuidos, en base a la generación automática de firmas en tiempo real, debido a que la capacidad de generación automática de firmas en tiempo real constituye un componente esencial para una protección Anti-DDoS eficaz, pues permite la detección y mitigación proactiva de ataques desconocidos, de día cero y multivectoriales complejos, mediante el reconocimiento de patrones maliciosos inéditos. Así, este mecanismo facilita la identificación y el bloqueo automatizado de amenazas, permitiendo que, una vez detectado un patrón de ataque, el sistema genere de forma ágil las firmas correspondientes, bloqueando tanto el ataque en curso como posibles variantes similares. De forma que, en escenarios donde el comportamiento del ataque es predecible, estas firmas actúan de manera inmediata para frenar el tráfico malicioso.

Asimismo, agregó que una de las limitaciones de utilizar sistemas de protección Anti-DDoS basados en algoritmos adaptativos, es la posibilidad de generar falsos positivos cuando éstos no han sido adecuadamente entrenados. Este tipo de algoritmos requiere ser alimentado con datos históricos representativos, para identificar patrones de tráfico legítimos; sin embargo, dichos patrones pueden cambiar con el tiempo, por lo que, una configuración inadecuada o un entrenamiento insuficiente puede comprometer la precisión del sistema y dar lugar a bloqueos incorrectos de tráfico válido. Afirmación que se encuentra sujeta a rendición de cuentas.

Del mismo modo, agrega que, la Entidad cuenta desde hace tres años con un sistema de protección Anti-DDoS basado en la generación automática de firmas, el cual ha demostrado un desempeño eficiente y ha contribuido significativamente al fortalecimiento de la seguridad institucional.

De otro lado, es preciso indicar que, de la revisión del numeral 3.2 del Formato “Resumen Ejecutivo de las Actuaciones Preparatorias (Servicios)”, se advierte que la Entidad declaró la existencia de pluralidad de proveedores con capacidad de cumplir con el requerimiento, el cual incluye que el sistema de protección Anti DDoS debe poder mitigar ataques de denegación de servicio de día cero, distribuidos y no distribuidos en base a la generación automática de firmas en tiempo real.

En ese sentido, considerando lo señalado en los párrafos que preceden, y dado que la pretensión del recurrente se encuentra orientada a que la Entidad admita que el

sistema de protección Anti-DDoS no se limite exclusivamente al uso de mecanismos basados en la creación de firmas en tiempo real, sino que se admita la posibilidad de implementar otras estrategias complementarias de defensa, y en la medida que, mediante su informe, la Entidad ratificó su requerimiento, así como los argumentos por los cuales no acepta lo solicitado por el recurrente; este Organismo Técnico Especializado ha decidido **NO ACOGER** el presente cuestionamiento.

Cuestionamiento N° 2:

Respecto al “Sistema de prevención de intrusos (IPS)”.

El participante **GTD PERÚ S.A** cuestionó la absolución de la consulta y/u observación N° 86 del pliego, alegando que la Entidad no sustentó adecuadamente su respuesta, lo que podría implicar una vulneración a los Principios de Libertad de Concurrencia, Igualdad de Trato y Competencia, debido a que los sistemas de prevención de intrusiones (IPS) no están diseñados para evaluar de manera integral el comportamiento de millones de sesiones simultáneas, sino que, más bien se enfocan en el análisis individual de cada sesión, lo que limita su capacidad para detectar ataques compuestos por grandes volúmenes de solicitudes -aparentemente legítimas- que operan de forma coordinada.

Por lo tanto, la pretensión del recurrente consiste en que la Entidad **admita que se suprima o sea opcional, el requisito relativo a que la solución tenga integrado un módulo de Sistema de Prevención de Intrusos (IPS).**

Pronunciamiento

Sobre el particular, de la revisión del acápite 5.2 del numeral 3.1 del Capítulo III de la Sección Específica de las Bases de la convocatoria, se aprecia lo siguiente:

“5.2. Equipamiento de Gestión y Seguridad de Internet:

(...)

B. Solución de Protección AntiDDoS:

(...)

o La solución deberá tener integrado un módulo de IPS (Sistema de Prevención de Intrusos).

(...)”

(El subrayado y resaltado es agregado)

Es así que, mediante la consulta y/u observación N° 86 del pliego, se solicitó que la exigencia de contar con un módulo de Sistema de Prevención de Intrusos (IPS) sea considerada como opcional, o -en su defecto- sea retirada, dado que dicha funcionalidad no constituye un componente esencial en una solución orientada específicamente a la mitigación de ataques de denegación de servicio distribuido (DDoS), y por el contrario, su inclusión podría afectar las características stateless del dispositivo.

Ante lo cual, la Entidad aclaró el módulo IPS contribuye a la detección y prevención de intrusiones en la red de SUNAFIL; además, la solución debe ser capaz de bloquear ataques de denegación de servicio, incluyendo aquellos de tipo inundación como TCP SYN, TCP RST, UDP, ICMP, entre otros.

En relación con ello, y en atención al cuestionamiento formulado por el participante, mediante el INFORME N° 019-2025-SUNAFIL/GG-OTIC-ECRT⁵, la Entidad señaló lo siguiente:

“(...)

- Los IPS son importantes para detectar de manera temprana un ataque DDoS entrante.
- Las soluciones AntiDDoS con IPS integrado pueden detectar y bloquear exploits dirigidos a vulnerabilidades conocidas en la infraestructura de la red y aplicaciones web. También pueden interceptar tráfico malicioso que intenta infiltrarse en la red que pudiera generar luego un ataque DDoS.
- Un IPS dentro de la solución AntiDDoS proporciona informes y análisis detallados sobre los patrones de tráfico, lo que permite detectar ataques no solo en tiempo real, sino también identificar tendencias y comportamientos sospechosos que podrían pasar desapercibidos con un sistema AntiDDoS por sí solo. Esto proporciona una visibilidad más clara de los incidentes de seguridad y facilita la toma de decisiones informadas.
- En escenarios más avanzados, los atacantes pueden usar **técnicas de "combinación"** donde lanzan un ataque DDoS como distracción mientras intentan ejecutar intrusiones más sigilosas o ataques a nivel de aplicación. Un sistema que combine AntiDDoS con IPS puede gestionar ambos tipos de amenazas al mismo tiempo, **protegiendo más eficazmente** ante ataques híbridos.
- Con la integración de IPS, las soluciones AntiDDoS pueden proporcionar seguridad adicional para aplicaciones web y servicios críticos. Esto es especialmente importante para empresas que operan plataformas web de entidades del estado, e-commerce, servicios bancarios en línea, o cualquier otro sistema que reciba tráfico externo.

Por lo expuesto tener un módulo de IPS integrado a la solución AntiDDoS proporciona una **protección más completa** contra una amplia gama de amenazas, además **optimiza la respuesta ante incidentes, mejora la visibilidad y la gestión del tráfico, y protege a la red contra una variedad de ataques complejos.**

Además, existen varias soluciones de AntiDDoS en la nube que incluyen dentro de sus funcionalidades la Prevención de Intrusiones (IPS) para una protección más completa.

(...)”

(El subrayado y resaltado es agregado)

Al respecto, cabe señalar que, en el artículo 16 de la Ley y el artículo 29 del Reglamento, se establece que el área usuaria es la responsable de la elaboración del requerimiento, debiendo éste contener la descripción objetiva y precisa de las características y/o requisitos funcionales relevantes para cumplir la finalidad pública de la contratación y las condiciones en las que debe ejecutarse la contratación, debiendo asegurar la calidad técnica y reducir la necesidad de su reformulación por errores o deficiencias técnicas que repercutan en el proceso de contratación.

Ahora bien, en atención del tenor de lo cuestionado, se aprecia que la Entidad, como responsable y mejor conocedora de sus necesidades, ratificó su requerimiento mediante el informe correspondiente, manteniendo como exigencia que la solución cuente con un módulo integrado de Sistema de Prevención de Intrusos (IPS), sustentándolo en que la inclusión del IPS en una solución Anti-DDoS resulta pertinente, debido a que permite la detección temprana de posibles ataques entrantes,

⁵ Remitido mediante el Expediente N° 2025-0017466, de fecha 28 de mayo de 2025.

así como la detección y bloqueo de intentos de explotación de las vulnerabilidades conocidas en la infraestructura de red y en aplicaciones web. Asimismo, agrega que, con los IPS, se posibilita la interceptación de tráfico malicioso que, de no ser neutralizado, podría desencadenar un ataque de denegación de servicio. Adicionalmente, precisa que, este componente ofrece funciones analíticas avanzadas, proporcionando informes detallados sobre el comportamiento del tráfico, lo cual permite una respuesta oportuna ante incidentes y facilita la detección de patrones sospechosos o tendencias que podrían pasar inadvertidas en soluciones Anti-DDoS que no cuenten con dicha funcionalidad. Por lo que, esta capacidad de análisis contribuye a una mayor visibilidad del entorno de seguridad, fortaleciendo el monitoreo y favoreciendo una toma de decisiones más informada.

Aunado a lo anteriormente expuesto, la Entidad agregó que, en escenarios más sofisticados, los atacantes pueden emplear tácticas combinadas, utilizando ataques DDoS como distracción para encubrir intentos simultáneos de intrusión más discretos o ataques dirigidos a nivel de aplicación. Frente a este tipo de amenazas híbridas, una solución que integre funcionalidades Anti-DDoS con un Sistema de Prevención de Intrusos (IPS) permite una gestión conjunta y eficaz, ofreciendo una protección más robusta, y fortaleciendo la seguridad de aplicaciones web y servicios críticos; siendo que, tal aspecto resulta especialmente relevante para entidades públicas, plataformas de comercio electrónico, servicios financieros en línea, y en general, cualquier infraestructura que esté expuesta a tráfico externo, al asegurar un nivel adicional de defensa frente a posibles vectores de ataque múltiples. Afirmación que se encuentra sujeta a rendición de cuentas.

De otro lado, es preciso indicar que, de la revisión del numeral 3.2 del Formato “Resumen Ejecutivo de las Actuaciones Preparatorias (Servicios)”, se advierte que la Entidad declaró la existencia de pluralidad de proveedores con capacidad de cumplir con el requerimiento, el cual incluye que la solución deberá tener integrado un módulo de IPS (Sistema de Prevención de Intrusos).

En ese sentido, considerando lo señalado en los párrafos que preceden, y dado que la pretensión del recurrente se encuentra orientada a que la Entidad admita que se suprima o sea opcional, el requisito relativo a que la solución tenga integrado un módulo de Sistema de Prevención de Intrusos (IPS), y en la medida que, mediante su informe, la Entidad ratificó su requerimiento, así como los argumentos por los cuales no acepta lo solicitado por el recurrente; este Organismo Técnico Especializado ha decidido **NO ACOGER** el presente cuestionamiento.

3. ASPECTOS REVISADOS DE OFICIO

Si bien el procesamiento de la solicitud de pronunciamiento, por norma, versa sobre los supuestos cuestionamientos derivados de la absolución de consultas y/u observaciones, y no representa la convalidación de ningún extremo de las bases, este Organismo Técnico Especializado ha visto por conveniente hacer indicaciones puntuales a partir de la revisión de oficio, según el siguiente detalle:

3.1. Respecto a los documentos para la admisión de la oferta

De la revisión del numeral 2.2.1.1 del Capítulo II perteneciente a la Sección Específica de las Bases Integradas, se aprecia lo siguiente:

“2.2.1.1. DOCUMENTOS PARA LA ADMISIÓN DE LA OFERTA

(...)

e) Carta del fabricante que acredite que la solución de administración y control de ancho de banda debe ser de propósito específico y no una funcionalidad dentro de alguna solución de seguridad o infraestructura IT (ej: firewall, UTM, NGFW, balanceadores, entre otros), como también debe ser una solución totalmente integrada y soportada directamente por el mismo fabricante a fin de garantizar un soporte integro, de acuerdo al literal A del numeral 5.2 de los TDR

f) Carta del fabricante adjuntando la documentación pública de internet que la respalde, respecto a que los equipos no estén en etapa de obsolescencia o que hayan publicado y/o anunciado el “End-of-life” y/o “End-of-Support”, o dejen de ser fabricadas, comercializadas y/o soportadas durante los 05 años siguientes a la instalación de los equipos a ser propuestos, de acuerdo al literal C (Solución de Seguridad Next Generation Firewall (NGFW), del numeral 5.2 (Funcionalidades requeridas) de los TDR.

g) Documento (se aceptará declaración jurada donde se indique página web o link del fabricante) que acredite que los sistemas operativos y/o firmware que operan en los equipos de seguridad firewall ofertados, no deberán tener más de diez (10) vulnerabilidades (CVE) anunciadas y/o publicadas, acumuladas en sus diferentes versiones durante los últimos 12 meses anteriores a la fecha de presentación de la oferta, de acuerdo al literal C (Solución de Seguridad Next Generation Firewall (NGFW), del numeral 5.2 (Funcionalidades requeridas) de los TDR.

h) Documentación técnica (datasheet) y/o manuales y/o bochures emitidos públicamente por el propio fabricante de la solución de firewall, adjuntando el documento y enlace (URL) público de Internet del propio fabricante que lo sustente que acredite el cumplimiento referido a las capacidades de hardware y/o de rendimiento solicitadas, No se aceptarán cartas de fabricante y/o representantes locales, como un fundamento para el cumplimiento de estos requerimientos solicitados, de acuerdo al literal C (Solución de Seguridad Next Generation Firewall (NGFW), del numeral 5.2 (Funcionalidades requeridas) de los TDR.

i) Documentación que acredite al postor tener la autorización del Ministerio de Transportes y Comunicaciones para la prestación del servicio en la modalidad de Internet Servís o Proveedor (ISP), con cobertura a nivel nacional, acreditado con Copia de Autorización del MTC para la prestación del servicio. También se aceptará una copia del link que el MTC tiene publicado de REGISTRO PARA SERVICIO DE VALOR AÑADIDO en la Plataforma Digital Única del Estado Peruano y/o un Oficio emitido por el MTC, el cual precisan las Concesiones y/o Títulos Habilitantes para la prestación de Servicios Públicos de Telecomunicaciones, con las que cuenta el Postor y/o copia simple del Certificado de Registro de Empresas Prestadoras de Servicios de Valor Añadido emitido por el Ministerio de Transporte y Comunicaciones.

(...)

m) Declaración jurada del nivel de certificación y dirección del centro de datos, así como copia del certificado RATED II del centro de datos donde se encuentran los componentes del servicio de Ciberdefensa.

n) Declaración jurada indicando el nivel de certificación y los procesos, así como la copia del certificado del CyberSOC en ISO 27001.

*o) Se acreditará con un certificado emitido por una empresa consultora externa (certificadora en infraestructura) y/o un certificado emitido por una empresa especialista en servicios TI y/o infraestructura y/u otro documento que acredite la operación e infraestructura del NOC & SOC.
(...)”*

Al respecto, cabe indicar que, el “Principio de Transparencia”, consignado en el literal c) del artículo 2 de la Ley, establece que la Entidad debe proporcionar información clara y coherente con el fin de que ésta sea comprendida por todos los potenciales proveedores.

Ahora bien, de la revisión del extremo citado de las Bases, se aprecia que la Entidad exige la presentación de diversos documentos como parte de la acreditación del cumplimiento de los términos de referencia en la etapa de admisión de ofertas. Sin embargo, no se especifica de manera clara qué aspectos deben ser acreditados con dichos documentos.

Sin perjuicio de ello, de lo expuesto en las Bases Estándar aplicables, se aprecia que, dentro de los documentos para la admisión de las ofertas, se puede requerir la presentación de documentación adicional a la acreditada mediante el Anexo N° 3 - Declaración Jurada de Cumplimiento de los Términos de Referencia, para acreditar algún aspecto de los términos de referencia; sin embargo, para ello, la Entidad deberá precisar claramente cuáles aspectos se deben acreditar con el mismo.

En ese sentido, se aprecia que la Entidad exige la presentación de diversos documentos requeridos para la admisión de las ofertas, a pesar de que ello no resulta acorde a lo establecido en las Bases Estándar aplicables. Sin embargo, considerando que dichos documentos resultan de relevancia para la Entidad, se trasladará la exigencia de presentación de estos, para el perfeccionamiento del contrato.

Por lo tanto, con ocasión de la integración definitiva de las Bases, se implementará la siguiente disposición:

- **Se suprimirá** el literal e), f), g), h), i), m), n) y o) del numeral 2.2.1.1 del Capítulo II de la Sección Específica de las Bases Integradas Definitivas.
- **Se adecuará** el numeral 2.3 del Capítulo II de la Sección Específica de las Bases Integradas Definitivas, conforme a lo siguiente:

“2.3 REQUISITOS PARA PERFECCIONAR EL CONTRATO

El postor ganador de la buena pro debe presentar los siguientes documentos para perfeccionar el contrato:

(...)

- *Carta del fabricante que acredite que la solución de administración y control de ancho de banda debe ser de propósito específico y no una funcionalidad dentro de alguna solución de seguridad o infraestructura IT (ej: firewall, UTM, NGFW, balanceadores, entre otros), como también debe ser una solución totalmente integrada y soportada directamente por el mismo fabricante a fin de garantizar un*

soporte integro, de acuerdo al literal A del numeral 5.2 de los TDR

- *Carta del fabricante adjuntando la documentación publica de internet que la respalde, respecto a que los equipos no estén en etapa de obsolescencia o que hayan publicado y/o anunciado el “End-of-life” y/o “End-of-Support”, o dejen de ser fabricadas, comercializadas y/o soportadas durante los 05 años siguientes a la instalación de los equipos a ser propuestos, de acuerdo al literal C (Solución de Seguridad Next Generation Firewall (NGFW), del numeral 5.2 (Funcionalidades requeridas) de los TDR.*
- *Documento (se aceptara declaración jurada donde se indique página web o link del fabricante) que acredite que los sistemas operativos y/o firmware que operan en los equipos de seguridad firewall ofertados, no deberán tener más de diez (10) vulnerabilidades (CVE) anunciadas y/o publicadas, acumuladas en sus diferentes versiones durante los últimos 12 meses anteriores a la fecha de presentación de la oferta, de acuerdo al literal C (Solución de Seguridad Next Generation Firewall (NGFW), del numeral 5.2 (Funcionalidades requeridas) de los TDR.*
- *Documentación técnica (datasheet) y/o manuales y/o bochures emitidos públicamente por el propio fabricante de la solución de firewall, adjuntando el documento y enlace (URL) público de Internet del propio fabricante que lo sustente que acredite el cumplimiento referido a las capacidades de hardware y/o de rendimiento solicitadas, No se aceptarán cartas de fabricante y/o representantes locales, como un fundamento para el cumplimiento de estos requerimientos solicitados, de acuerdo al literal C (Solución de Seguridad Next Generation Firewall (NGFW), del numeral 5.2 (Funcionalidades requeridas) de los TDR.*
- *Documentación que acredite al postor tener la autorización del Ministerio de Transportes y Comunicaciones para la prestación del servicio en la modalidad de Internet Servís o Proveedor (ISP), con cobertura a nivel nacional, acreditado con Copia de Autorización del MTC para la prestación del servicio. También se aceptará una copia del link que el MTC tiene publicado de REGISTRO PARA SERVICIO DE VALOR AÑADIDO en la Plataforma Digital Única del Estado Peruano y/o un Oficio emitido por el MTC, el cual precisan las Concesiones y/o Titulos Habilitantes para la prestación de Servicios Públicos de Telecomunicaciones, con las que cuenta el Postor y/o copia simple del Certificado de Registro de Empresas Prestadoras de Servicios de Valor Añadido emitido por el Ministerio de Transporte y Comunicaciones.*
(...)
- *Declaración jurada del nivel de certificación y dirección del centro de datos, así como copia del certificado RATED II del centro de datos donde se encuentran los componentes del servicio de Ciberdefensa.*
- *Declaración jurada indicando el nivel de certificación y los procesos, así como la copia del certificado del CyberSOC en ISO 27001.*
- *Se acreditará con un certificado emitido por una empresa consultora externa (certificadora en infraestructura) y/o un certificado emitido por una empresa especialista en servicios TI y/o infraestructura y/u otro documento que acredite la operación e infraestructura del NOC & SOC.*

- **Se dejará sin efecto** todo extremo del pliego absolutorio y de las Bases que se opongan a las disposiciones previstas en el párrafo anterior.

3.2. Respecto a los requisitos para perfeccionar el contrato

De la revisión del numeral 2.3 del Capítulo II perteneciente a la Sección Específica de las Bases Integradas, se aprecia lo siguiente:

2.3 REQUISITOS PARA PERFECCIONAR EL CONTRATO

El postor ganador de la buena pro debe presentar los siguientes documentos para perfeccionar el contrato:

(...)

h) Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación (Anexo N° 12).

(...)”

De lo anterior, se aprecia que, la Entidad habría omitido incluir en las Bases integradas el formato correspondiente a la autorización de notificación de la decisión de la entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación.

En relación con ello, mediante CARTA N°05-2025-CP N°01-2025-SUNAFIL-1-CS⁶, la Entidad señaló lo siguiente:

“(...)”

Respecto a los requisitos para perfeccionar el contrato.

- Se adjunta Anexo N° 12 respecto a la Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación.

(...)”

En ese sentido, con ocasión de la integración definitiva de las Bases, y en atención a lo indicado en la Carta de la Entidad, se implementarán las disposiciones siguientes:

- **Se publicará** el Anexo N° 12 - Autorización de notificación de la decisión de la Entidad sobre la solicitud de ampliación de plazo mediante medios electrónicos de comunicación, adjunto a las Bases Integradas Definitivas.

4. CONCLUSIONES

En virtud de lo expuesto, este Organismo Técnico Especializado ha dispuesto lo siguiente:

- 4.1** Se procederá a la integración definitiva de las Bases a través del SEACE, en atención a lo establecido en el artículo 72 del Reglamento.
- 4.2** Es preciso indicar que contra el pronunciamiento emitido por este Organismo Especializado no cabe interposición de recurso administrativo alguno, siendo de

⁶ Remitido mediante el Expediente N° 2025-0021410, de fecha 05 de junio de 2025.

obligatorio cumplimiento para la Entidad y los proveedores que participan en el procedimiento de selección.

Adicionalmente, cabe señalar que, las disposiciones vertidas en el pliego absolutorio que generen aclaraciones, modificaciones o precisiones, priman sobre los aspectos relacionados con las Bases integradas, salvo aquellas que fueron materia del presente pronunciamiento.

- 4.3** Una vez emitido el pronunciamiento y registrada la integración de Bases definitivas, corresponderá al Comité de Selección **modificar** en el cronograma del procedimiento, las fechas del registro de participantes, presentación de ofertas y otorgamiento de la buena pro, teniendo en cuenta que, entre la integración de Bases y la presentación de propuestas, no podrá mediar menos de siete (7) días hábiles, computados a partir del día siguiente de la publicación de las Bases integradas en el SEACE, conforme a lo dispuesto en el artículo 70 del Reglamento.
- 4.4** Finalmente, se recuerda al Titular de la Entidad que el presente pronunciamiento no convalida extremo alguno del procedimiento de selección.

Jesús María, 19 de junio de 2025

Código: 6.1