PRONUNCIAMIENTO N° 545-2024/OSCE-DGR

Entidad : Autoridad Nacional del Agua

Referencia : Licitación Pública N° 1-2024-ANA-1, convocada para la "Adquisición de una Solución de Seguridad Perimetral para la Autoridad Nacional del Agua"

---

1. ANTECEDENTES

Mediante el formulario de solicitud de emisión de pronunciamiento, recibido el 12[1] de septiembre de 2024 y subsanado con fecha 23[2] de septiembre de 2024, el presidente del comité de selección a cargo del procedimiento de selección de la referencia remitió al Organismo Supervisor de las Contrataciones del Estado (OSCE) la solicitud de elevación de cuestionamientos al pliego absolutorio de consultas y observaciones e integración de bases presentada por el participante **IT ONE S.A.C.,** en cumplimiento de lo dispuesto por el artículo 21 de la Ley de Contrataciones del Estado, aprobada mediante la Ley N° 30225, en adelante la "Ley", y el artículo 72 de su Reglamento, aprobado por el Decreto Supremo Nº 344-2018-EF, en adelante el "Reglamento".

Firmado digitalmente por LAURA SILVA Anthony David FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 11.10.2024 17:37:26 -05:00

Ahora bien, cabe indicar que en la emisión del presente pronunciamiento se empleó la información remitida por la Entidad, con fecha el 23[3] de septiembre de 2024, mediante la Mesa de Partes de este Organismo Técnico Especializado, la cual tiene carácter de declaración jurada.

Firmado digitalmente por CHAMOCHUMBI CHERRE Carlos Ernesto FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 11.10.2024 17:16:47 -05:00

Asimismo, cabe precisar que en la emisión del presente pronunciamiento se utilizó el orden establecido por el comité de selección en el pliego absolutorio y los temas materia de cuestionamientos de los mencionados participantes, conforme al siguiente detalle:

Firmado digitalmente por VARGAS PEREZ Wilberth FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 11.10.2024 17:06:57 -05:00

- **Cuestionamiento N° 1** : Respecto a la absolución de la consulta y/u observación N° 1, referida a la **"Capacidad de Rendimiento de Threat"**
- **Cuestionamiento N° 2** : Respecto a la absolución de las consultas y/u observaciones N° 7, N° 8 y N° 14, referidas a los **"Gestores centralizados de los firewalls"**
- **Cuestionamiento N° 3** : Respecto a la absolución de las consultas y/u observaciones N° 9 y N° 15, referidas a los **"Gestores de Eventos y Reportes"**

---

[1] Mediante Trámite Documentario N° 2024-0123119.
[2] Mediante Trámite Documentario N° 2024-0128167.
[3] Mediante Trámite Documentario N° 2024-0128167.

- **Cuestionamiento N° 4** : Respecto a la absolución de la consulta y/u observación N° 55, referida a las **"Capacidades de los gestores de perímetro"**

- **Cuestionamiento N° 5** : Respecto a la absolución de la consulta y/u observación N° 64, referida al **"Módulo de URL Filtering"**

- **Cuestionamiento N° 6** : Respecto a la absolución de la consulta y/u observación N° 127, referida al **"Cumplimiento de metas y objetivos institucionales"**

2. CUESTIONAMIENTOS

De manera previa, cabe señalar que el OSCE 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 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.

Cuestionamiento N° 1 : **Respecto a la "Capacidad de Rendimiento de Threat"**

El participante **IT ONE S.A.C.,** respecto a la "Capacidad de Rendimiento de Threat Prevention de los gestores de perímetro", cuestionó la absolución de la consulta y/u observación N° 1, alegando que la Entidad no habría acogido lo señalado por el participante, suponiendo una proyección de progreso en los próximos cinco (5) años, la cual, el recurrente indica que sólo resulta válido, siempre que el total del throughput del equipamiento actual checkpoint sea de 15400, con capacidad de 6.4 Gbps; de forma que llegue al 100% del uso en la capacidad de throughput y agrega que, de no ser así, se estaría sobredimensionando el equipamiento generando un costo sobreestimado que representa un perjuicio para la Entidad.

Por lo que, el recurrente **solicitó que la Entidad confirme si se considerará un rendimiento mínimo de 10 Gbps en rendimiento de threat prevention.**

Pronunciamiento

De manera previa, corresponde señalar que a través de la Opinión N° 002-2020/DTN se indicó 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.

Al respecto, de la revisión del acápite A.2, del numeral 3.1 del Capítulo III de la sección específica de las Bases de la convocatoria, se aprecia lo siguiente:

> *"(...)*
>
> ***CAPÍTULO III***
>
> *(...)*
>
> ***A.2. Capacidad:***
>
> ▪ *Tener un rendimiento Threat Prevention (cuando opera en simultáneo: Application Control, firewall, IPS, Antivirus/Anti-Bot/Antispyware) de 15 Gbps mínimo, medido en condiciones de prueba o mixtura empresariales o en transacciones HTTP de 64KB.*
>
> *(...)"*

Mediante la consulta y/u observación N° 1 del pliego, respecto a la capacidad de rendimiento de threat prevention de los gestores de perímetro, el participante **ENEBRO INGENIERIA S.A.C.** solicitó confirmar si se considerará un rendimiento mínimo de 10 Gbps en rendimiento de Threat Prevention, ya que la solicitud de 15 Gbps es casi el triple de lo que se encuentra en producción y no será utilizada en su totalidad.

Ante lo cual, la Entidad decidió no acoger lo solicitado, debido a que se ha proyectado un crecimiento en los próximos cinco (5) años como la necesidad de contar con la capacidad de enfrentar escenarios de alta demanda sin comprometer la seguridad o el rendimiento de la infraestructura tecnológica.

En ese contexto, mediante el INFORME TÉCNICO N° 0012-2024-ANA-DSNIRH/AALR[4], el área usuaria de la Entidad precisó lo siguiente:

> *"**Se ratifica la decisión del pliego**, además, se brinda mayores argumentos técnicos: La necesidad de actualizar a 15 Gbps de Threat Prevention es inminente y se ve reforzada por la expansión a más de 84 sedes bajo un servicio MPLS. Es crucial destacar que el valor de 15 Gbps fue proyectado a 5 años, lo que significa que incluso si actualmente el tráfico no alcanza ese nivel, el crecimiento esperado en los próximos años hará que esta capacidad sea necesaria para mantener la seguridad y el rendimiento de la red.*
>
> *(...)*
>
> *El servicio MPLS para más sedes (alrededor de 166 sedes) y la posible transición a SDWAN, **justifica aún más la necesidad de una mayor capacidad de Threat Prevention**. **Estos cambios implicarán un aumento significativo en el***

[4] Mediante el Expediente N° 2024-0128167, de fecha 23 de septiembre de 2024.

tráfico, la complejidad y la necesidad de seguridad descentralizada, lo que superará rápidamente las capacidades del equipo actual de 6.4 Gbps*.*

En 2023, la empresa NETSCOUT reportó aproximadamente 6 millones de ataques DDoS

a nivel global solo en el primer semestre, con un promedio de 45 ataques por minuto. Este tipo de ataques puede incrementar el tráfico hasta un 200%, lo que provoca una ralentización significativa e incluso la interrupción total del servicio en las entidades afectadas. Por ello, es fundamental contar con un throughput mínimo de 15 Gbps para mitigar el impacto de estos ataques y asegurar una mayor resiliencia ante estas amenazas.

En conclusión, ***la actualización a 15 Gbps de Threat Prevention es una inversión estratégica vital para garantizar la seguridad, el rendimiento y la escalabilidad de la red a largo plazo. Al abordar el crecimiento proyectado, la expansión de sedes y la posible adopción de nuevas tecnologías de red, esta actualización permitirá a la organización proteger sus activos, mantener la continuidad de las operaciones y aprovechar al máximo sus inversiones en infraestructura de red.*** *Ignorar esta necesidad no solo pondría en riesgo la seguridad y el rendimiento, sino que también limitaría la capacidad de la organización para crecer y adaptarse a las demandas cambiantes del entorno tecnológico.* (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 éstos 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, lo que incluye, además, los requisitos de calificación que se consideren necesarios, debiendo asegurar la calidad técnica y reducir la necesidad de su reformulación por errores o deficiencias técnicas que repercutan en el proceso de contratación.

Por su parte, cabe señalar que, el Principio de Vigencia Tecnológica, consignado en el literal g) del artículo 2 de la Ley, establece que los bienes deben reunir las condiciones de calidad y modernidad tecnológicas necesarias para cumplir con efectividad la finalidad pública para los que son requeridos, por un determinado y previsible tiempo de duración, con posibilidad de adecuarse, integrarse y repotenciarse si fuera el caso, con los avances científicos y tecnológicos.

Ahora bien, en atención al aspecto cuestionado por el recurrente, se aprecia que la Entidad, mediante su informe técnico y en atención al mejor conocimiento de las necesidades que desea satisfacer, ha ratificado su absolución, detallando mayor argumento técnico respecto al pliego conforme a lo siguiente:

- La necesidad de actualizar a 15 Gbps de Threat Prevention es inminente y se ve reforzada por la expansión a más de 84 sedes bajo un servicio MPLS.
- Destaca que la finalidad de tener el valor de 15 Gbps es debido a que el servicio se proyecta a 5 años futuros, y que el crecimiento esperado en los próximos años hará que esta capacidad sea necesaria para mantener la seguridad y el rendimiento de la red.
- El servicio MPLS está destinado para más sedes (alrededor de 166 sedes) y la posible transición a SD-WAN, justifica aún más la necesidad de una mayor capacidad de Threat Prevention.
- Los cambios implicarán un aumento significativo en el tráfico, así como la complejidad y la necesidad de seguridad descentralizada, lo que superará rápidamente las capacidades del equipo actual de 6.4 Gbps.
- Establece que conforme al antecedente del 2023 la empresa NETSCOUT reportó aproximadamente 6 millones de ataques DDoS a nivel global solo en el primer semestre, con un promedio de 45 ataques por minuto, puede incrementar el tráfico hasta un 200%, lo que provoca una ralentización significativa e incluso la interrupción total del servicio en las entidades afectadas.
- Finalmente ha establecido que es fundamental contar con un throughput mínimo de 15 Gbps para mitigar el impacto de los ataques DDoS.

De esta forma, la Entidad ha brindado mayor sustento técnico y concluye en la necesidad de que el rendimiento de "Threat Prevention, debe ser 15 Gbps" conforme a lo establecido en los términos de referencia, debido a que esta especificación técnica está orientada a un futuro bajo una proyección de 5 años; resultando, de otro lado, una inversión estratégica de vital importancia que garantizara la seguridad, el rendimiento, la escalabilidad de la red a largo plazo. Por otro lado la Entidad ha establecido que el crecimiento proyectado, la expansión de sedes y la posible adopción de nuevas tecnologías de red, permitirá que la Entidad proteja sus activos, así como mantener la continuidad de las operaciones y aprovechar al máximo sus inversiones en infraestructura de red, y bajo esa concepción advierte que ignorar esta necesidad no solo pondría en riesgo la seguridad y el rendimiento, sino que también limitaría la capacidad de la organización para crecer y adaptarse a las demandas cambiantes del entorno tecnológico; siendo que, considerando el sustento técnico descrito por el área usuaria, dicha información posee carácter de declaración jurada y está sujeta a rendición de cuentas.

Adicionalmente, cabe indicar que, en el numeral 3.2 y 3.3 del "Formato de Resumen ejecutivo de las actuaciones preparatorias (Bienes)", la Entidad declaró la existencia de pluralidad de proveedores y marcas con capacidad de cumplir con el requerimiento, lo que incluye las especificaciones técnicas "Capacidad de Rendimiento de Threat Prevention de los gestores de perímetro".

En ese sentido, considerando lo señalado en los párrafos precedentes y en la medida que la pretensión del recurrente se encuentra orientada a que la Entidad indique si se considerara un rendimiento mínimo de 10 Gbps en rendimiento de Threat Prevention, y en tanto que la Entidad, mediante su informe técnico, ha ratificado lo absuelto, manteniendo el contenido del requerimiento, este Organismo Técnico

Especializado ha decidido **NO ACOGER** el presente cuestionamiento. Por lo que se implementará las siguientes disposiciones:

- **Se deberá tener en cuenta**[5] lo indicado en el INFORME TÉCNICO N° 0012-2024-ANA-DSNIRH/AALR[6], como respuesta complementaria a la absolución a la consulta y/u observación N° 1 del pliego.

Finalmente, cabe precisar que 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 obra en los actuados para la adecuada realización de la contratación.

Cuestionamiento N° 2 : **Respecto a los "Gestores centralizados de los firewalls"**

El participante **IT ONE S.A.C.,** respecto a la función de la gestión de los firewalls, cuestionó la absolución de las consultas y/u observaciones N° 7, N° 8 y N° 14, alegando lo siguiente:

- **Respecto a la consulta y/u observación N° 7**, precisa que la respuesta brindada por la Entidad resulta ambigua debido a que la funcionalidad de un equipo "gestor centralizado" es desempeñar el rol de administración unificada para una seguridad consistente en entornos híbridos complejos; lo que resulta en protección contra amenazas de seguridad. No obstante, la absolución a la consulta precisa que se está adquiriendo un gestor centralizado para cada uno de los gestores de perímetro (4 equipos gestores de perímetro) y contrariando su principal función de administrar centralizadamente múltiples equipos.

- **Respecto a la consulta y/u observación N° 8 y N° 14,** precisa que la respuesta de la Entidad no presenta una apertura a múltiples propuestas versátiles que se adecuen a sus necesidades, actualmente en el mercado existen equipos de gestión centralizada (Fortimanager de Fortinet, Panorama de Palo Alto, etc.) que pueden desempeñar el rol de administración unificada con un solo equipo de gestión centralizada.

Por lo que, el recurrente **solicitó que la Entidad confirme que se admitirá el empleo de un único equipo de gestión centralizada para los múltiples equipos.**

Pronunciamiento

De manera previa, corresponde señalar que a través de la Opinión N° 002-2020/DTN se indicó que el área usuaria es la dependencia que cuenta con los conocimientos

[5] La presente disposición deberá ser tomada en cuenta en la etapa respectiva del procedimiento, por lo que no requerirá de ser implementada en las Bases Integradas Definitivas.
[6] Mediante el Expediente N° 2024-0128167, de fecha 23 de septiembre de 2024.

técnicos necesarios para definir las características técnicas de los bienes, servicios y obras que se habrán de contratar.

Al respecto, de la revisión del acápite B.1, del numeral 3.1 del Capítulo III de la sección específica de las Bases de la convocatoria, se aprecia lo siguiente:

> *" (...)*
>
> ***B. Cuatro (04) gestores centralizados (Código SIGA:952278320027):***
>
> ***B.1. Características generales:***
>
> ▪ *Se requiere la gestión de los firewalls sea dedicada, es decir que cumpla únicamente la gestión centralizada de los Firewalls.*
>
> ▪ *Los gestores centralizados deben ser instalados y configurados, dos (02) para el Centro de procesamiento de datos principal (CPDP) y dos (02) para el Centro de procesamiento de datos secundario (CPDS).*
>
> *(...)"*

Mediante la consulta y/u observación N° 7 del pliego, respecto a la localización y modalidad de trabajo del servicio, el participante **ENEBRO INGENIERIA S.A.C.** solicitó reafirmar si estos gestores centralizados cumplirán su función de gestionar los firewalls de forma centralizada o desempeñarán el rol de gestionar cada uno los gestores de perímetros de forma individual. Ante lo cual, la Entidad precisó que se requiere que la gestión de firewall sea dedicada y centralizada, enfocada exclusivamente a la administración del firewall.

Mediante la consulta y/u observación N° 8 del pliego, respecto a los gestores centralizados del servicio, el participante **ENEBRO INGENIERIA S.A.C.** solicitó considerar un mínimo de dos (2) gestores centralizados, uno por cada centro de procesamiento de datos, en concordancia con la arquitectura propuesta, debido a que su finalidad es la de administrar múltiples firewalls desde una única interfaz; facilitando la configuración, monitoreo y control de políticas de seguridad de forma consistente en toda la infraestructura reduciendo la cantidad de hardware. Ante lo cual, la Entidad precisó que debe conservar la topología actual, requiriendo disponer de cuatro (4) gestores centralizados, debiendo ser dos en cada sede, los cuales deben estar configurados en alta disposición.

Mediante la consulta y/u observación N° 14 del pliego, respecto a los gestores centralizados, el participante **IMPERIA SOLUCIONES TECNOLÓGICAS S.A.C.** solicitó admitir un único gestor centralizado que garantice una verdadera administración de todos los componentes de infraestructura, debido a que solicitar cuatro (4) de ellos, no se condice con la obtención de ninguna mejora. Ante lo cual, la Entidad precisó que se debe conservar la topología actual, requiriendo disponer de cuatro (4) gestores centralizados, debiendo ser dos en cada sede, los cuales deben estar configurados en alta disposición.

En ese contexto, mediante el INFORME TÉCNICO N° 0012-2024-ANA-DSNIRH/AALR[7], el área usuaria de la Entidad precisó lo siguiente:

*"**Respecto a la consulta y/u observación N° 7:***

Se ratifica la decisión del pliego**, además, se brinda mayores argumentos técnicos: **El diseño de arquitectura propuesto, que incluye la implementación de firewalls en alta disponibilidad (HA) tanto en la sede principal como en la de contingencia, junto con gestores centralizados redundantes y equipos dedicados a reportería y eventos en cada ubicación, se alinea de manera sólida con las necesidades de seguridad y continuidad operativa de la Entidad.

La estrategia de alta disponibilidad, aplicada tanto a los firewalls como a los gestores centralizados, minimiza el riesgo de interrupciones en los servicios críticos de la Entidad.

En caso de fallo de un componente, su contraparte en HA asumirá de inmediato sus funciones, garantizando que la protección de la red y la gestión de la seguridad no se vean comprometidas. Adicionalmente, la distribución de equipos de reportería y eventos en ambas sedes asegura la capacidad de monitoreo constante y generación de informes, incluso si una de las sedes se vuelve inaccesible.

***Este diseño no solo fortalece la postura de seguridad de la Entidad al crear una defensa en profundidad y facilitar la aplicación de políticas de seguridad consistentes, sino que también ofrece escalabilidad y flexibilidad para adaptarse a futuras necesidades.** La separación de funciones entre gestores de perímetro, gestores centralizados y equipos de reportería brinda una gestión más eficiente y un mantenimiento simplificado de la infraestructura. Además, al cumplir con los requisitos de alta disponibilidad y generación de informes detallados, el diseño contribuye al cumplimiento normativo en sectores regulados. En resumen, **esta arquitectura representa una inversión estratégica que protege los activos de la Entidad, respalda sus operaciones críticas y sienta las bases para un crecimiento seguro y sostenible**."*

Respecto a la consulta y/u observación N° 8:

Se ratifica la decisión del pliego**, además, se brinda mayores argumentos técnicos: **La solicitud de cuatro gestores centralizados, con dos en cada Centro de Procesamiento de Datos (CPDP y CPDS) configurados en alta disponibilidad, está alineada con la topología actual y las necesidades específicas de la infraestructura de la Entidad.

Esta configuración no solo asegura una administración continua y redundante de los firewalls, garantizando que la gestión no se interrumpa en caso de fallos o mantenimiento, sino que también ofrece una protección óptima

[7] Mediante el Expediente N° 2024-0128167, de fecha 23 de septiembre de 2024.

en términos de disponibilidad y continuidad operativa en las sedes de la ANA. La Entidad ha evaluado que, a pesar de la existencia de soluciones centralizadas en el mercado, la configuración de cuatro gestores proporciona beneficios clave en alta disponibilidad y distribución equitativa de la carga de trabajo en cada sede.

Esta estrategia no solo evita la sobrecarga de un único dispositivo, sino que también asegura una administración eficiente y confiable, además de facilitar la integración con la infraestructura existente y minimizar las interrupciones durante la implementación. *La decisión de mantener la topología actual, con gestores centralizados en cada sede, permite un control más granular y específico sobre la seguridad de cada ubicación, lo que puede ser crucial si las sedes tienen requisitos de seguridad diferentes. En última instancia, esta configuración representa una inversión estratégica en la robustez y eficacia de la infraestructura de seguridad, priorizando la continuidad operativa, la adaptabilidad y una gestión eficiente."*

Respecto a la consulta y/u observación N° 14:

Se ratifica la decisión del pliego, además, se brinda mayores argumentos técnicos. La decisión de la Entidad de mantener esta configuración se basa en un análisis exhaustivo de sus requisitos específicos de alta disponibilidad y continuidad operativa.

La implementación de cuatro gestores centralizados, dos en cada Centro de Procesamiento de Datos (CPDP y CPDS) y configurados en alta disponibilidad, garantiza una gestión ininterrumpida de los firewalls, incluso en escenarios de fallo o mantenimiento. Esta redundancia es crucial para asegurar que la infraestructura de seguridad de la entidad se mantenga operativa y responda de manera efectiva ante cualquier eventualidad.

Si bien soluciones como FortiManager o Panorama ofrecen capacidades de gestión unificada, ***la entidad ha determinado, tras una evaluación detallada, que la disposición de cuatro gestores es fundamental para cumplir con sus requisitos operacionales específicos.*** *Esta configuración no solo brinda una mayor robustez y tolerancia a fallos, sino que también permite una distribución equilibrada de la carga de trabajo entre los gestores, optimizando el rendimiento y la eficiencia de la gestión de la seguridad. En última instancia, la decisión de la entidad prioriza la continuidad operativa y la capacidad de respuesta ante incidentes, garantizando una infraestructura de seguridad resiliente y adaptable a sus necesidades.* (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 éstos 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, lo que

incluye, además, los requisitos de calificación que se consideren necesarios, debiendo asegurar la calidad técnica y reducir la necesidad de su reformulación por errores o deficiencias técnicas que repercutan en el proceso de contratación.

Por su parte, cabe señalar que, el Principio de Vigencia Tecnológica, consignado en el literal g) del artículo 2 de la Ley, establece que los bienes deben reunir las condiciones de calidad y modernidad tecnológicas necesarias para cumplir con efectividad la finalidad pública para los que son requeridos, por un determinado y previsible tiempo de duración, con posibilidad de adecuarse, integrarse y repotenciarse si fuera el caso, con los avances científicos y tecnológicos.

Así mismo, cabe señalar 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 que ésta sea comprendida por todos los potenciales proveedores; es así que, el artículo 72 del Reglamento y la Directiva N° 23-2016-OSCE/CD, dispone que al absolver las consultas y/u observaciones, el comité de selección deberá detallar de manera clara y motivada la totalidad de las respuestas a las solicitudes formuladas por los participantes y el análisis respectivo.

Ahora bien, en atención al aspecto cuestionado por el recurrente, se aprecia que la Entidad, mediante su informe técnico y en atención al mejor conocimiento de las necesidades que desea satisfacer, ha ratificado su absolución, brindando mayor sustento técnico conforme a lo siguiente:

- Respecto a la consulta y/u observación N° 7: En cuanto a la posible ambigüedad de la absolución, la Entidad ha aclarado que el diseño de arquitectura propuesta incluye la implementación de firewalls en alta disponibilidad en ambas sedes (principal y contingencia), lo cual se alinea de manera sólida con las necesidades de seguridad y continuidad operativa, por lo que éste diseño no solo fortalece la postura de seguridad al crear una defensa en profundidad y facilitar la aplicación de políticas de seguridad consistentes, sino que también ofrece escalabilidad y flexibilidad para adaptarse a futuras necesidades, que brindará una gestión más eficiente, considerando además finalmente que esta arquitectura representa una inversión estratégica que protege los activos de la Entidad, respalda sus operaciones críticas y sienta las bases para un crecimiento seguro y sostenible.

- Respecto a la consulta y/u observación N° 8 y N° 14: Ha precisado que la solicitud de cuatro (4) gestores centralizados, con dos en cada centro de procesamiento de datos (CPDP y CPDS), está alineada a la topología actual y conforme a la necesidad, la cual asegura una administración continua y redundante de los firewalls, en tanto garantiza que la gestión no se interrumpa en caso de fallas debido a su protección óptima de las sedes de la ANA, por lo que la configuración de cuatro gestores proporciona beneficios clave en alta disponibilidad y distribución equitativa.

Además, agrega que la topología actual no sólo evita la sobrecarga de un único dispositivo, sino que también asegura una administración eficiente y confiable, y por

tanto, decide mantener la topología actual mediante gestores centralizados en cada sede, que permitan un control granular y más específico sobre la seguridad de su ubicación; lo cual además representa una inversión estratégica en la robustez y eficacia de la infraestructura de seguridad, priorizando la continuidad operatividad, adaptabilidad a una gestión eficiente.

En consecuencia, considerando el sustento técnico descrito por el área usuaria, a través del cual se ratifica en la necesidad de mantener el alcance de los términos de referencia cuestionados; siendo que, esta información posee carácter de declaración jurada y está sujeta a rendición de cuentas.

Adicionalmente, cabe indicar que, en el numeral 3.2 y 3.3 del "Formato de Resumen ejecutivo de las actuaciones preparatorias (Bienes)", la Entidad declaró la existencia de pluralidad de proveedores y marcas con capacidad de cumplir con el requerimiento, lo que incluye la cantidad de gestores centralizados.

En ese sentido, considerando lo señalado en los párrafos precedentes, y en la medida que la pretensión del recurrente se encuentra orientada a que la Entidad admita el empleo de un único gestor centralizado, y en tanto que la Entidad, mediante su informe técnico, ha ratificado su absolución en ambos extremos, brindando mayor argumento técnico donde ha determinado que el diseño actual de arquitectura se alinea con las necesidades de seguridad y continuidad operativa y representa una inversión estratégica que protege los activos de la Entidad, por lo que este Organismo Técnico Especializado ha decidido **NO ACOGER** el presente cuestionamiento. Por lo que se implementará las siguientes disposiciones:

- **Se deberá tener en cuenta**[8] lo indicado en el INFORME TÉCNICO N° 0012-2024-ANA-DSNIRH/AALR[9], como respuesta complementaria a la absolución a la consulta y/u observación N° 7, N° 8 y N° 14 del pliego.

Finalmente, cabe precisar que 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 obra en los actuados para la adecuada realización de la contratación.

Cuestionamiento N° 3 : **Respecto a los "Gestores de Eventos y Reportes"**

El participante **IT ONE S.A.C.,** respecto a los Gestores de Eventos y Reportes cuestionó la absolución de las consultas y/u observaciones N° 9 y N° 15, alegando que la respuesta brindada por la Entidad no presenta una apertura a múltiples propuestas versátiles que se ajusten a sus necesidades, debido a que actualmente en

[8] La presente disposición deberá ser tomada en cuenta en la etapa respectiva del procedimiento, por lo que no requerirá de ser implementada en las Bases Integradas Definitivas.
[9] Mediante el Expediente N° 2024-0128167, de fecha 23 de septiembre de 2024.

el mercado existen equipos de gestión centralizada que incluyen capacidades de gestor de eventos y reportes (Fortimanager de Fortinet, Panorama de Palo Alto, etc.)

Por lo que, el recurrente **solicitó que la Entidad admita el empleo de equipos de gestión centralizada que incluyan capacidades de gestor de eventos y reportes.**

Pronunciamiento

De manera previa, corresponde señalar que a través de la Opinión N° 002-2020/DTN se indicó 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.

Al respecto, de la revisión del acápite C.1, del numeral 3.1 del Capítulo III de la sección específica de las Bases de la convocatoria, se aprecia lo siguiente:

> *" (...)*
>
> *A. Dos (02) gestores de eventos y reportes (Código SIGA: 740892000226):*
>
> *C.1. Características generales:*
>
> *(...)*
>
> ▪ *Los gestores de eventos y reportes deben ser instalados y configurados, uno (01) para el Centro de procesamiento de datos principal (CPDP) y uno (01) para el Centro de procesamiento de datos secundario (CPDS).*
>
> *(...)"*

Mediante la consulta y/u observación N° 9 del pliego, respecto a los gestores de eventos y reportes, el participante **ENEBRO INGENIERIA S.A.C.** solicitó confirmar si se podrá habilitar la funcionalidad de gestores de eventos y reportes dentro del mismo equipo de gestores centralizados, en tanto cumpla con todos los requerimientos técnicos funcionales. Ante lo cual, la Entidad decidió no acoger, precisando que la Entidad requiere un gestor de reportes dedicado exclusivamente para esa funcionalidad.

Mediante la consulta y/u observación N° 15 del pliego, respecto a los gestores de eventos y reportes, el participante **IMPERIA SOLUCIONES TECNOLÓGICAS S.A.C.** solicitó reconsiderar la posibilidad de aceptar soluciones que integren las capacidades de gestores de eventos y reportes, debido a que existen otras arquitecturas disponibles en el mercado que pueden ofrecer la misma o mayor capacidad con diseño más escalables y flexibles, que optimizan el desempeño y la integración en el entorno actual.

Ante lo cual, la Entidad no acogió precisando que la entidad requiere mantener la topología actual, por lo que se solicita que los gestores de reportes, como el gestor centralizado sean equipos dedicados, ósea de función específica.

En ese contexto, mediante el INFORME TÉCNICO N° 0012-2024-ANA-DSNIRH/AALR[10], el área usuaria de la Entidad precisó lo siguiente:

> *"**Se ratifica la decisión del pliego**, además, se brinda mayores argumentos técnicos. La decisión de la Entidad de optar por equipos dedicados se basa en un análisis cuidadoso de sus requerimientos específicos y busca garantizar una gestión de seguridad robusta y eficiente.*
>
> *Si bien soluciones como FortiManager o Panorama ofrecen la ventaja de consolidar funciones, la separación de la gestión centralizada y la generación de reportes en equipos dedicados brinda beneficios significativos. En primer lugar, asegura un manejo más especializado y preciso de los datos críticos, evitando posibles cuellos de botella o conflictos de recursos que podrían afectar el rendimiento en un sistema integrado.*
>
> *Además, esta estrategia promueve una gestión más eficiente y continua de las necesidades de análisis y monitoreo en cada sede, permitiendo una respuesta más rápida y efectiva ante incidentes de seguridad.*
>
> *La Entidad ha evaluado cuidadosamente las alternativas y ha determinado que la inversión en gestores de reportes dedicados no representa un sobredimensionamiento, sino una estrategia para optimizar el rendimiento, la disponibilidad y la escalabilidad de la infraestructura de seguridad. Al evitar la sobrecarga de un único sistema centralizado y garantizar una gestión especializada, se asegura que la solución integral cumpla con los requisitos técnicos de manera óptima, brindando a la entidad la capacidad de analizar y responder de manera proactiva a las amenazas de seguridad, protegiendo así sus activos críticos y garantizando la continuidad de sus operaciones".* (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 éstos 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, lo que incluye, además, los requisitos de calificación que se consideren necesarios, 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 al aspecto cuestionado por el recurrente, se aprecia que la Entidad, mediante su informe técnico y en atención al mejor conocimiento de las necesidades que desea satisfacer, ha ratificado lo absuelto en el pliego absolutorio,

[10] Mediante el Expediente N° 2024-0128167, de fecha 23 de septiembre de 2024.

brindando mayor sustento técnico, por el cual ha aclarado que mediante una evaluación se ha determinado que la inversión en gestores de reportes dedicados no representa un sobredimensionamiento, sino una estrategia para optimizar el rendimiento. Por otro lado, establece que la disponibilidad y la escalabilidad de la infraestructura de seguridad, al evitar la sobrecarga de un único sistema centralizado y garantizar una gestión especializada, asegura que la solución integral cumpla con los requisitos técnicos de manera óptima, brindando a la Entidad la capacidad de analizar y responder de manera proactiva a las amenazas de seguridad, protegiendo así sus activos críticos y garantizando la continuidad de sus operaciones.

Adicionalmente, cabe indicar que, en el numeral 3.2 y 3.3 del "Formato de Resumen ejecutivo de las actuaciones preparatorias (Bienes)", la Entidad declaró la existencia de pluralidad de proveedores y marcas con capacidad de cumplir con el requerimiento, lo que incluye las especificaciones técnicas relativas a los equipos Gestores de Eventos y Reportes.

En ese sentido, considerando lo señalado en los párrafos precedentes, y en la medida que la pretensión del recurrente se encuentra orientada a que la Entidad admita el empleo de equipos de gestión centralizada que incluyan capacidades de gestor de eventos y reportes, y en tanto que la Entidad, mediante su informe técnico, ha ratificado su absolución, brindando mayor argumento técnico donde ha determinado que el extremo cuestionado no representa un sobredimensionamiento, sino más bien, una estrategia para optimizar el rendimiento disponibilidad, por lo que este Organismo Técnico Especializado ha decidido **NO ACOGER** el presente cuestionamiento. Por lo que se implementará las siguientes disposiciones:

- **Se deberá tener en cuenta**[11] lo indicado en el INFORME TÉCNICO N° 0012-2024-ANA-DSNIRH/AALR[12], como respuesta complementaria a la absolución a la consulta y/u observación N° 9 y N° 15 del pliego.

Finalmente, cabe precisar que 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 obra en los actuados para la adecuada realización de la contratación.

Cuestionamiento N° 4 : **Respecto a las "Capacidades de los gestores de perímetro"**

El participante **IT ONE S.A.C.,** respecto a las capacidades de los gestores de perímetro, cuestionó la absolución de la consulta y/u observación N° 55, alegando que las características de la solución actual (Checkpoint 15400), cuenta con características técnicas implementadas y aprovechadas dentro de la política de

[11] La presente disposición deberá ser tomada en cuenta en la etapa respectiva del procedimiento, por lo que no requerirá de ser implementada en las Bases Integradas Definitivas.
[12] Mediante el Expediente N° 2024-0128167, de fecha 23 de septiembre de 2024.

seguridad que protege actualmente a la Autoridad Nacional del Agua (ANA), a través del Módulo de Seguridad de Control de Aplicaciones (Application Control), que cuenta con más de 10000 aplicaciones descubiertas a la fecha; las cuales permiten un control granular en la navegación de los usuarios internos. No obstante, en el presente requerimiento, la cantidad de aplicaciones descubiertas y disponibles solicitadas en este módulo solo asciende a 4500.

Por lo que, el recurrente **solicitó que la Entidad precise que se requerirá el reconocimiento de diez mil (10000) aplicaciones descubiertas, tal como se requiere en el módulo que la Entidad emplea actualmente.**

Pronunciamiento

De manera previa, corresponde señalar que a través de la Opinión N° 002-2020/DTN se indicó 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.

Al respecto, de la revisión del acápite A.1, del numeral 3.1 del Capítulo III de la sección específica de las Bases de la convocatoria, se aprecia lo siguiente:

> *" (...)*
>
> ***A. Cuatro (04) gestores del perímetro (Código SIGA: 952278320001):***
>
> ***A.1. Características generales:***
>
> *(...)*
>
> ▪ *Reconocer por lo menos 4500 aplicaciones diferentes incluyendo, más no limitando: el tráfico relacionado a peer-to-peer, redes sociales, acceso remoto, update de software, protocolos de red, VoIP, audio, vídeo, proxy, mensajería instantánea, email.*
>
> *(...)"*

Mediante la consulta y/u observación N° 55 del pliego, respecto a la capacidad de gestores de perímetro, el participante **INTEGRIT SOCIEDAD ANONIMA CERRADA – INTEGRIT S.A.C.,** solicitó que se admita contar como mínimo con un módulo que reconozca 10000 aplicaciones para el módulo de Application control o Control de Aplicaciones y no las 4500 aplicaciones diferentes, propuestas en el requerimiento. Ante lo cual, la Entidad decidió no acoger lo solicitado, precisando que ello contraviene la pluralidad de postores, además de permitir a la Entidad contar con una solución acorde al tamaño y complejidad del presente servicio.

En ese contexto, mediante el INFORME TÉCNICO N° 0012-2024-ANA-DSNIRH/AALR[13], el área usuaria de la Entidad precisó lo siguiente:

> *"La decisión de la Entidad de establecer este requerimiento se basa en un análisis cuidadoso que* ***busca equilibrar las necesidades operativas con la promoción de un mercado competitivo y diverso****.*
>
> *Si bien es cierto que la solución actual (Checkpoint 15400) cuenta con un reconocimiento de más de 10,000 aplicaciones, establecer un límite de 4500 aplicaciones en las especificaciones técnicas cumple un propósito fundamental. Al evitar un requerimiento excesivamente alto, que podría favorecer a un único proveedor con una solución de alta gama, se garantiza que una variedad de fabricantes, incluyendo aquellos que ofrecen soluciones más accesibles, puedan participar en la licitación. Esto promueve la competencia, impulsa la innovación y evita la creación de un monopolio en el mercado, lo que a su vez beneficia a la entidad al brindarle un mayor abanico de opciones y precios más competitivos.*
>
> *Es importante destacar que el límite de 4500 aplicaciones no implica una restricción significativa en la capacidad de la solución para satisfacer las necesidades operativas de*
>
> *la entidad. El análisis realizado ha determinado que este número es suficiente para cubrir los requerimientos actuales y futuros, asegurando un control efectivo sobre las aplicaciones utilizadas en la red. Además, la entidad se reserva el derecho de ampliar este límite en el futuro si sus necesidades evolucionan, garantizando así la flexibilidad y adaptabilidad de la solución. En conclusión, la decisión de la entidad refleja una planificación responsable, buscando no solo una solución técnica robusta y eficiente, sino también un mercado de proveedores diverso y competitivo que beneficie a la entidad*
>
> *a largo plazo".* (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 éstos 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, lo que incluye, además, los requisitos de calificación que se consideren necesarios, 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 al aspecto cuestionado por el recurrente, se aprecia que la Entidad, mediante su informe técnico y en atención al mejor conocimiento de las necesidades que desea satisfacer, ha aclarado lo absuelto, brindando mayor sustento técnico mediante el cual indica que con objeto de equilibrar las necesidades

[13] Mediante el Expediente N° 2024-0128167, de fecha 23 de septiembre de 2024.

operativas con la promoción de un mercado competitivo y diverso, se establece un límite mínimo de 4500 aplicaciones reconocidas, debido a que ello cumple un propósito fundamental y refleja una planificación responsable, buscando no solo una solución técnica robusta y eficiente, sino también un mercado de proveedores diverso y competitivo que beneficie a la Entidad a largo plazo. Esta característica está determinada considerando la libre concurrencia y pluralidad de postores con la cual se promueve la competencia, debido a que es un parámetro mínimo, entendido que si el postor quiere ofertar algo superior también sería admitido, no obstante, de aceptar lo solicitado por el recurrente podría favorecerse a un único proveedor con una solución de alta gama.

Por consiguiente, la Entidad ha determinado la importancia de destacar que el límite de 4500 aplicaciones reconocidas como mínimo, no implica una restricción significativa en la capacidad de la solución para satisfacer las necesidades operativas, debido a que el análisis realizado ha determinado que este número resulta suficiente para cubrir los requerimientos actuales y futuros, asegurando un control efectivo sobre las aplicaciones utilizadas en la red.

Adicionalmente, cabe indicar que, en el numeral 3.2 y 3.3 del "Formato de Resumen ejecutivo de las actuaciones preparatorias (Bienes)", la Entidad declaró la existencia de pluralidad de proveedores y marcas con capacidad de cumplir con el requerimiento, lo que incluye las "Capacidades de los gestores de perímetro".

En ese sentido, considerando lo señalado en los párrafos precedentes, y en la medida que la pretensión del recurrente se encuentra orientada a que la Entidad amplíe el requerimiento a un reconocimiento de 10000 aplicaciones descubiertas, y en tanto que la Entidad, mediante su informe técnico, ha brindado mayores alcances mediante los cuales se ratifica en el contenido del requerimiento, este Organismo Técnico Especializado ha decidido **NO ACOGER** el presente cuestionamiento. Por lo que se implementará las siguientes disposiciones:

- **Se deberá tener en cuenta**[14] lo indicado en el INFORME TÉCNICO N° 0012-2024-ANA-DSNIRH/AALR[15], como respuesta complementaria a la absolución a la consulta y/u observación N° 55 del pliego.

Finalmente, cabe precisar que 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 obra en los actuados para la adecuada realización de la contratación.

[14] La presente disposición deberá ser tomada en cuenta en la etapa respectiva del procedimiento, por lo que no requerirá de ser implementada en las Bases Integradas Definitivas.
[15] Mediante el Expediente N° 2024-0128167, de fecha 23 de septiembre de 2024.

<u>Cuestionamiento N° 5</u> : **Respecto al "Módulo de URL Filtering"**

El participante **IT ONE S.A.C.,** respecto al filtro web, cuestionó la absolución de la consulta y/u observación N° 64, alegando que la solución actualmente operativa (Checkpoint 15400) cuenta con características técnicas implementadas y aprovechadas dentro de la política de seguridad que protege actualmente a la Autoridad Nacional del Agua (ANA), a través del Módulo de Seguridad de Filtrado de URL (URL Filtering), que cuenta con más de ciento diez (110) categorías de URL; las cuales permiten un control granular en filtrado de la navegación de los usuarios internos del ANA. No obstante, conforme a las especificaciones técnicas del Filtro Web, la cantidad de categorías de URL solo asciende a setenta (70). Lo que equivale a una disminución o merma de más del 35% de categorías disponibles, listas para usar en beneficio del control granular de navegación respecto de la solución que actualmente emplea la Autoridad Nacional del Agua (ANA).

Por lo que, el recurrente **<u>solicitó que la Entidad precise que se requerirá contar como mínimo con ciento diez (110) categorías para el módulo de URL Filtering o Filtrado de URL, tal como se requiere en el módulo que la Entidad emplea actualmente.</u>**

Pronunciamiento

De manera previa, corresponde señalar que a través de la Opinión N° 002-2020/DTN se indicó 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.

Al respecto, de la revisión del acápite A.8, del numeral 3.1 del Capítulo III de la sección específica de las Bases de la convocatoria, se aprecia lo siguiente:

> *" (...)*
>
> ***A. Cuatro (04) gestores del perímetro (Código SIGA: 952278320001):***
>
> ***A.8. Filtro Web***
>
> *(...)*
>
> - *Tener por lo menos 70 categorías de URL.*
>
> *(...)"*

Mediante la consulta y/u observación N° 64 del pliego, respecto al módulo de URL Filtering, el participante **INTEGRIT SOCIEDAD ANONIMA CERRADA – INTEGRIT S.A.C.** solicitó confirmar como mandatorio contar como mínimo con 110 categorías para el módulo de URL Filtering o Filtrado de URL. Ante lo cual, la Entidad decidió no acoger, precisando que lo solicitado en las Bases son

características técnicas mínimas, por lo que los postores pueden ofrecer características diferentes de considerarlo necesario.

En ese contexto, mediante el INFORME TÉCNICO N° 0012-2024-ANA-DSNIRH/AALR[16], el área usuaria de la Entidad precisó lo siguiente:

> *"Se ratifica la decisión del pliego, además, se brinda mayores argumentos técnicos. Si bien la solución actual (Checkpoint 15400) ofrece un número superior de categorías de URL, establecer un mínimo de 70 categorías en las bases cumple un propósito estratégico clave: fomentar la pluralidad de marcas y soluciones en el mercado. Algunos fabricantes ofrecen soluciones con un número de categorías de URL cercano al mínimo requerido, como es el caso de Palo Alto con 70 categorías. Al evitar un requerimiento excesivamente alto, que podría favorecer únicamente a soluciones de gama alta, se garantiza que una variedad de proveedores puedan participar en la licitación, promoviendo así la competencia y evitando la exclusividad.*
>
> *Es importante resaltar que este mínimo de 70 categorías no implica una limitación en la capacidad de la solución para satisfacer las necesidades de control y filtrado de contenido de la entidad. El análisis realizado ha determinado que este número es suficiente para cubrir los requerimientos actuales, permitiendo un control granular sobre*
>
> *el acceso a diferentes tipos de contenido web. Además, la especificación técnica no limita*
>
> *la posibilidad de que los proveedores ofrezcan soluciones con un número superior de categorías, brindando a la entidad la flexibilidad de elegir la opción que mejor se adapte*
>
> *a sus necesidades y presupuesto.*
>
> *En conclusión, la decisión de establecer un mínimo de 70 categorías de URL busca equilibrar las capacidades técnicas con la promoción de la competencia, garantizando una solución efectiva que cumpla con los requisitos básicos y fomente un mercado más abierto y dinámico. Esta estrategia beneficia a la entidad al brindarle un mayor abanico de opciones y la posibilidad de acceder a soluciones avanzadas sin comprometer la funcionalidad esencial ni limitar innecesariamente las opciones de los fabricantes".* (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 éstos 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, lo que incluye, además, los requisitos de calificación que se consideren necesarios,

[16] Mediante el Expediente N° 2024-0128167, de fecha 23 de septiembre de 2024.

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 al aspecto cuestionado por el recurrente, se aprecia que la Entidad, mediante su informe técnico y en atención al mejor conocimiento de las necesidades que desea satisfacer, se ha ratificado en lo absuelto, brindando mayor sustento técnico por el cual aclara que si bien la solución actual (Checkpoint 15400) ofrece un número superior de categorías de URL, el establecer un mínimo de setenta (70) categorías en las Bases, cumple un propósito estratégico clave, que es el de fomentar la pluralidad de marcas y soluciones en el mercado que garanticen una variedad de proveedores; resaltando además que, lo requerido no implica una limitación en la capacidad de la solución para satisfacer las necesidades de control y filtrado de contenido de la Entidad, pues ha precisado que resulta suficiente para cubrir los requerimientos actuales, permitiendo un control granular sobre el acceso a diferentes tipos de contenido web. Siendo de notar que lo declarado por la Entidad, posee calidad de declaración jurada y está sujeto a rendición de cuentas.

Adicionalmente, cabe indicar que, en el numeral 3.2 y 3.3 del "Formato de Resumen ejecutivo de las actuaciones preparatorias (Bienes)", la Entidad declaró la existencia de pluralidad de proveedores y marcas con capacidad de cumplir con el requerimiento, lo que incluye las especificaciones técnicas "Capacidades de los gestores de perímetro".

En ese sentido, considerando lo señalado en los párrafos precedentes, y en la medida que la pretensión del recurrente se encuentra orientada a que la Entidad admita que se requerirá contar como mínimo con ciento diez (110) categorías para el módulo de URL Filtering o Filtrado de URL, tal como se requiere en el módulo que la Entidad emplea actualmente, y en tanto que la Entidad, mediante su informe técnico, se ha ratificado en el contenido del requerimiento, este Organismo Técnico Especializado ha decidido **NO ACOGER** el presente cuestionamiento. Por lo que se implementará las siguientes disposiciones:

- **Se deberá tener en cuenta**[17] lo indicado en el INFORME TÉCNICO N° 0012-2024-ANA-DSNIRH/AALR[18], como respuesta complementaria a la absolución a la consulta y/u observación N° 64 del pliego.

Finalmente, cabe precisar que 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 obra en los actuados para la adecuada realización de la contratación.

[17] La presente disposición deberá ser tomada en cuenta en la etapa respectiva del procedimiento, por lo que no requerirá de ser implementada en las Bases Integradas Definitivas.
[18] Mediante el Expediente N° 2024-0128167, de fecha 23 de septiembre de 2024.

<u>Cuestionamiento N° 6</u> : **Respecto al "Cumplimiento de metas y objetivos institucionales"**

El participante **IT ONE S.A.C.,** respecto al cumplimiento de metas y objetivos institucionales, cuestionó la absolución de la consulta y/u observación N° 127, alegando que la solución actualmente operativa (Checkpoint 15400), cuenta con características técnicas implementadas y aprovechadas dentro de la Política de Seguridad que protege actualmente a la Autoridad Nacional del Agua (ANA), con lo cual protege de ataques de Phishing conocido (comúnmente detectado/prevenido por soluciones basadas en reputación), así como desconocido, es decir los llamados "Zero Days" (con tecnología basada en motores avanzados de análisis estático y de Inteligencia Artificial). Sin embargo, esta característica técnica fue modificada como opcional dentro del requerimiento del proceso actual; por lo que, se solicitó tomar en consideración que los fabricantes de las soluciones oferentes no cuenten con más de diez (10) vulnerabilidades (CVE) anunciadas y/o publicadas durante el 2023, sin embargo, el sustento de la consulta no fue admitida, lo cual no deja en riesgo la Seguridad actual de la ANA.

Por lo que, el recurrente **<u>solicitó que la Entidad admita que los fabricantes de las soluciones oferentes no cuenten con más de 10 vulnerabilidades (CVE) anunciadas y/o publicadas durante el 2023 a la fecha de presentación de ofertas.</u>**

Pronunciamiento

De manera previa, corresponde señalar que a través de la Opinión N° 002-2020/DTN se indicó 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.

Al respecto, de la revisión del acápite 2, del numeral 3.1 del Capítulo III de la sección específica de las Bases de la convocatoria, se aprecia lo siguiente:

> *" (...)*
>
> ***2. ANTECEDENTES***
>
> *(...)*
>
> *Para el cumplimiento de metas y objetivos institucionales, la Dirección del Sistema Nacional de Información de Recursos Hídricos (en adelante DSNIRH) requiere contar con una solución de seguridad perimetral para la ANA, con la finalidad de mantener la seguridad para el correcto funcionamiento de toda la plataforma tecnológica que soporta la totalidad de los servicios de red y sistemas institucionales.*
>
> *(...)"*

Mediante la consulta y/u observación N° 127 del pliego, respecto al cumplimiento de metas y objetivos institucionales, el participante **TELEFÓNICA TECH PERÚ S.A.C.,** solicitó confirmar como mandatorio que los fabricantes de las soluciones oferentes no cuenten con más de diez (10) vulnerabilidades (CVE) anunciadas y/o publicadas durante el 2023 a la fecha de presentación de propuestas. Ante lo cual, la Entidad decidió no acoger, precisando que lo solicitado en las Bases son características técnicas mínimas, y no limitan a que los postores propongan características superiores.

En ese contexto, mediante el INFORME TÉCNICO N° 0012-2024-ANA-DSNIRH/AALR [19], el área usuaria de la Entidad precisó lo siguiente:

> *"**Se ratifica la decisión del pliego**, además, se brinda mayores argumentos técnicos. **La observación de limitar a diez (10) vulnerabilidades (CVE) publicadas en 2023 resulta altamente restrictivo y no garantiza una mayor seguridad**. Las vulnerabilidades publicadas no son un indicador directo de debilidad, sino un reflejo de la transparencia y*
>
> *proactividad de fabricantes líderes como Cisco, Palo Alto, Fortinet y Checkpoint, quienes cuentan con políticas robustas para gestionar vulnerabilidades de manera rápida y efectiva. Limitar el número de CVE podría excluir soluciones altamente efectivas y transparentes, favoreciendo inadvertidamente a fabricantes con menor capacidad de respuesta y compromiso con la seguridad.*
>
> *Es crucial entender que el número de CVE no refleja directamente la capacidad de una solución para enfrentar amenazas emergentes. Lo esencial es cómo el fabricante gestiona estas vulnerabilidades, asegurando actualizaciones rápidas y efectivas que mantengan la solución protegida en todo momento. Una gestión proactiva y efectiva de vulnerabilidades, que incluya actualizaciones periódicas, parches de seguridad y comunicación transparente con los usuarios, es mucho más relevante que un número limitado de CVE. Existen soluciones de seguridad reconocidas que, a pesar de tener un historial de CVE, son consideradas altamente seguras debido a su capacidad de respuesta y gestión de vulnerabilidades.*
>
> *La observación actual no solo es inapropiada, sino que también restringe la pluralidad de marcas al excluir potencialmente soluciones robustas que podrían tener más de diez vulnerabilidades publicadas, sin que eso comprometa su seguridad real. Además, este enfoque limita la innovación y la competencia en el mercado de soluciones de seguridad, desalentando la entrada de nuevos fabricantes y tecnologías. Es importante fomentar un entorno competitivo que promueva la mejora continua y la oferta de soluciones cada vez más efectivas, considerando otros factores de evaluación como certificaciones de seguridad, resultados de pruebas de penetración, reputación del fabricante y capacidad del equipo de soporte técnico. El panorama de amenazas cibernéticas está en constante evolución, por lo que es*

[19] Mediante el Expediente N° 2024-0128167, de fecha 23 de setiembre de 2024.

crucial contar con soluciones flexibles y adaptables que puedan responder de manera efectiva a nuevas amenazas y vulnerabilidades. En lugar de centrarse únicamente en un número limitado de CVE, se recomienda adoptar un enfoque más integral que valore la capacidad de respuesta, la gestión efectiva de vulnerabilidades y otros indicadores relevantes de seguridad y eficacia."
(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 éstos 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, lo que incluye, además, los requisitos de calificación que se consideren necesarios, 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 al aspecto cuestionado por el recurrente, se aprecia que la Entidad, mediante su informe técnico y en atención al mejor conocimiento de las necesidades que desea satisfacer, ha ratificado lo absuelto, brindando mayor sustento técnico, del cual se desprende lo siguiente:

- La exigencia de limitar a diez (10) vulnerabilidades (CVE) publicadas en 2023, resulta altamente restrictiva y no garantiza una mayor seguridad.
- Las vulnerabilidades publicadas no son un indicador directo de debilidad, sino solo un reflejo de la transparencia y proactividad de fabricantes que cuentan con políticas robustas para gestionar vulnerabilidades de manera rápida y efectiva.
- Limitar el número de CVE podría excluir soluciones altamente efectivas y transparentes, favoreciendo inadvertidamente a fabricantes con menor capacidad de respuesta y compromiso con la seguridad. Es decisivo entender que el número de CVE no refleja directamente la capacidad de una solución para enfrentar amenazas emergentes. Lo fundamental es cómo el fabricante gestiona estas vulnerabilidades, asegurando actualizaciones rápidas y efectivas que mantengan la solución protegida en todo momento.
- La exigencia requerida resulta ser inapropiada, y restringe la pluralidad de marcas al excluir potencialmente a soluciones robustas que podrían tener más de diez vulnerabilidades publicadas, sin que eso comprometa su seguridad real.
- El panorama de amenazas cibernéticas está en constante evolución, por lo que es crucial contar con soluciones flexibles y adaptables que puedan responder de manera efectiva a nuevas amenazas y vulnerabilidades.

En consecuencia, considerando el sustento técnico descrito por el área usuaria, a través del cual se ratifica en la necesidad de mantener el alcance de los términos de referencia cuestionados; siendo que, esta información posee carácter de declaración jurada y está sujeta a rendición de cuentas.

Adicionalmente, cabe indicar que, en el numeral 3.2 y 3.3 del "Formato de Resumen ejecutivo de las actuaciones preparatorias (Bienes)", la Entidad declaró la existencia de pluralidad de proveedores y marcas con capacidad de cumplir con el requerimiento.

En ese sentido, considerando lo señalado en los párrafos precedentes, y en la medida que la pretensión del recurrente se encuentra orientada a que la Entidad exija que los fabricantes de las soluciones oferentes no cuenten con más de diez (10) vulnerabilidades (CVE) anunciadas y/o publicadas durante el 2023, y en tanto que la Entidad, mediante su informe técnico, ha brindado mayores alcances de carácter técnico, mediante los cuales se ratifica en denegar el extremo solicitado por el recurrente, este Organismo Técnico Especializado ha decidido **NO ACOGER** el presente cuestionamiento. Por lo que se implementará las siguientes disposiciones:

- **Se deberá tener en cuenta**[20] lo indicado en el INFORME TÉCNICO N° 0012-2024-ANA-DSNIRH/AALR[21], como respuesta complementaria a la absolución a la consulta y/u observación N° 127 del pliego.

Finalmente, cabe precisar que 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 obra en los actuados para la adecuada realización de la contratación.

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 la forma de pago

De la revisión conjunta del numeral 2.5 del capítulo II y el acápite 14 del numeral 3.1 del capítulo III, ambos pertenecientes a la sección específica de las Bases Integradas no definitivas, se aprecia que la Entidad consignó lo siguiente:

CAPÍTULO II
"(...)

[20] La presente disposición deberá ser tomada en cuenta en la etapa respectiva del procedimiento, por lo que no requerirá de ser implementada en las Bases Integradas Definitivas.
[21] Mediante el Expediente N° 2024-0128167, de fecha 23 de septiembre de 2024.

2.5. FORMA DE PAGO

2.5.1. PRESTACIÓN PRINCIPAL

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en ÚNICO PAGO del 70% del monto total del contrato.

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- *Recepción del responsable de Almacén Central de la Autoridad Nacional del Agua.*
- *Informe del funcionario responsable de la Dirección del Sistema Nacional de Información de Recursos Hídricos de la ANA, previa Opinión Técnica Favorable del profesional a cargo de la supervisión, emitiendo la conformidad de la prestación efectuada.*
- *Comprobante de pago.*

2.5.2. PRESTACIÓN ACCESORIA

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en TRES (3) PAGOS PARCIALES, según el siguiente detalle:

Primer pago, 10% que corresponde al primer mantenimiento preventivo y correctivo.

Segundo pago, 10% que corresponde al segundo mantenimiento preventivo y correctivo.

Tercer pago, 10% que corresponde al tercer mantenimiento preventivo y correctivo.

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- *Informe del funcionario responsable de la Dirección del Sistema Nacional de Información de Recursos Hídricos de la ANA, previa Opinión Técnica Favorable del profesional a cargo de la supervisión, emitiendo la conformidad de la prestación efectuada.*
- *Comprobante de pago.*

Dicha documentación se debe presentar en la Mesa de partes física de la Entidad en horario de oficina, sito en Calle Los Petirrojos N.° 355 - San Isidro – Lima o en la Mesa de Partes virtual ingresando al siguiente enlace: http://sisged.ana.gob.pe/tramitevirtual/.

(...)

CAPÍTULO III

14. Forma de Pago

(...)

Prestación	***Pago***	***Monto de pago***	
Principal	*Pago 1*	*El 70% del monto total del contrato.*	*Pago 1: Posterior a la presentación del Entregable N° 02 que incluye el Informe Técnico, Acta de recepción de la solución de seguridad perimetral y el Acta de inicio del servicio de la solución de seguridad perimetral.*
Accesoria	*Pago 2*	*El 10% del monto total del contrato*	*Pago 2: Posterior a la presentación del Entregable N° 03 que incluye el informe técnico del servicio mantenimiento. A partir de los 365 días calendarios, previa conformidad de la DSNIRH.*
	Pago 3	*El 10% del monto total del contrato*	*Pago 3: A la presentación del Entregable N° 04 que aborda el servicio de mantenimiento. A partir de los 730 días calendarios, previa conformidad de la DSNIRH*
	Pago 4	*El 10% del monto total del contrato*	*Pago 4: A la presentación del Entregable N° 05 que aborda el servicio de mantenimiento. A partir de los 1095 días calendarios, previa conformidad de la DSNIRH*

Asimismo, y a efectos de que la Entidad pueda realizará el pago de la contraprestación pactada a favor del contratista, previa conformidad de los entregables otorgado por parte de la Dirección del Sistema Nacional de Información de Recursos Hídricos, el contratista deberá presentar las facturas respectivas.

(...)"

Al respecto, de la revisión de los extremos citados de las Bases, se aprecia que la Entidad dispuso en las especificaciones técnicas establecidas en el Capítulo III respecto a la "forma de pago", documentos, acciones y condiciones diferentes a los establecidos en el numeral 2.5 del Capítulo II. Siendo de notar que, ambos extremos resultan disímiles, por lo que vulneran lo establecido en el Principio de Transparencia.

En ese contexto, mediante el INFORME TÉCNICO DEL COMITÉ DE SELECCIÓN N° 001-2024-CS/LP001-2024-ANA[22], la Entidad precisó lo siguiente:

"(...)

Se implementará la forma de pago de la siguiente manera:

2.5. FORMA DE PAGO

2.5.1. PRESTACIÓN PRINCIPAL

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en ÚNICO PAGO del 70% del monto total del contrato.

Prestación	***Pago***	***Monto de pago***	
Principal	*Pago 1*	*El 70% del monto total del contrato.*	*Pago 1: Posterior a la presentación del Entregable N° 02 que incluye el Informe Técnico, Acta de recepción de la solución de seguridad perimetral y el Acta de inicio del servicio de la solución de seguridad perimetral.*

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- *Recepción del responsable de Almacén Central de la Autoridad Nacional del Agua.*
- *Informe del funcionario responsable de la Dirección del Sistema Nacional de Información de Recursos Hídricos de la ANA, previa Opinión Técnica Favorable del profesional a cargo de la supervisión, emitiendo la conformidad de la prestación efectuada.*
- *Comprobante de pago.*

2.5.2. PRESTACIÓN ACCESORIA

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en TRES (3) PAGOS PARCIALES, según el siguiente detalle:

[22] Mediante el Expediente N° 2024-0128012, de fecha 23 de setiembre de 2024.

Accesoria	*Pago 2*	*El 10% del monto total del contrato*	*Pago 2: Posterior a la presentación del Entregable N° 03 que incluye el informe técnico del servicio mantenimiento. A partir de los 365 días calendarios, previa conformidad de la DSNIRH.*
	Pago 3	*El 10% del monto total del contrato*	*Pago 3: A la presentación del Entregable N° 04 que aborda el servicio de mantenimiento. A partir de los 730 días calendarios, previa conformidad de la DSNIRH*
	Pago 4	*El 10% del monto total del contrato*	*Pago 4: A la presentación del Entregable N° 05 que aborda el servicio de mantenimiento. A partir de los 1095 días calendarios, previa conformidad de la DSNIRH*

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- *Informe del funcionario responsable de la Dirección del Sistema Nacional de Información de Recursos Hídricos de la ANA, previa Opinión Técnica Favorable del profesional a cargo de la supervisión, emitiendo la conformidad de la prestación efectuada.*
- *Comprobante de pago.*

Dicha documentación se debe presentar en la Mesa de partes física de la Entidad en horario de oficina, sito en Calle Los Petirrojos N.° 355 - San Isidro – Lima o en la Mesa de Partes virtual ingresando al siguiente enlace: http://sisged.ana.gob.pe/tramitevirtual/."

En ese sentido, considerando lo declarado en el informe técnico de la Entidad y con ocasión de la integración definitiva de las Bases, se implementará la siguiente disposición:

- **Se adecuará** el contenido del numeral 2.5 del capítulo II de la sección específica de las Bases Integradas Definitivas, según el siguiente detalle:

> *"(...)*

Se implementará la forma de pago de la siguiente manera:

2.5. FORMA DE PAGO

2.5.1. PRESTACIÓN PRINCIPAL

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en ÚNICO PAGO del 70% del monto total del contrato.

Prestación	***Pago***	***Monto de pago***	
Principal	*Pago 1*	*El 70% del monto total del contrato.*	*Pago 1: Posterior a la presentación del Entregable N° 02 que incluye el Informe Técnico, Acta de recepción de la solución de seguridad perimetral y el Acta de inicio del servicio de la solución de seguridad perimetral.*

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- *Recepción del responsable de Almacén Central de la Autoridad Nacional del Agua.*
- *Informe del funcionario responsable de la Dirección del Sistema Nacional de Información de Recursos Hídricos de la ANA, previa Opinión Técnica Favorable del profesional a cargo de la supervisión, emitiendo la conformidad de la prestación efectuada.*
- *Comprobante de pago.*

2.5.2. PRESTACIÓN ACCESORIA

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en TRES (3) PAGOS PARCIALES, según el siguiente detalle:

~~*Primer pago, 10% que corresponde al primer mantenimiento preventivo y correctivo.*~~

~~*Segundo pago, 10% que corresponde al segundo mantenimiento preventivo y correctivo.*~~

~~*Tercer pago, 10% que corresponde al tercer mantenimiento preventivo y correctivo.*~~

Accesoria	*Pago 2*	*El 10% del monto total del contrato*	*Pago 2: Posterior a la presentación del Entregable N° 03 que incluye el informe técnico del servicio mantenimiento. A partir de los 365 días calendarios, previa conformidad de la DSNIRH.*
	Pago 3	*El 10% del monto total del contrato*	*Pago 3: A la presentación del Entregable N° 04 que aborda el servicio de mantenimiento. A partir de los 730 días calendarios, previa conformidad de la DSNIRH*
	Pago 4	*El 10% del monto total del contrato*	*Pago 4: A la presentación del Entregable N° 05 que aborda el servicio de mantenimiento. A partir de los 1095 días calendarios, previa conformidad de la DSNIRH*

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Entidad debe contar con la siguiente documentación:

- *Informe del funcionario responsable de la Dirección del Sistema Nacional de Información de Recursos Hídricos de la ANA, previa Opinión Técnica Favorable del profesional a cargo de la supervisión, emitiendo la conformidad de la prestación efectuada.*
- *Comprobante de pago.*

Dicha documentación se debe presentar en la Mesa de partes física de la Entidad en horario de oficina, sito en Calle Los Petirrojos N.° 355 - San Isidro – Lima o en la Mesa de Partes virtual ingresando al siguiente enlace: http://sisged.ana.gob.pe/tramitevirtual/."

Firmado digitalmente por LAURA SILVA Anthony David FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 11.10.2024 17:37:36 -05:00

Firmado digitalmente por CHAMOCHUMBI CHERRE Carlos Ernesto FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 11.10.2024 17:17:16 -05:00

Firmado digitalmente por VARGAS PEREZ Wilberth FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 11.10.2024 17:07:45 -05:00

- **Se dejará sin efecto y/o ajustará** todo extremo del pliego absolutorio, las Bases o Informe Técnico que se oponga a las disposiciones previstas en los párrafos anteriores.

4. CONCLUSIONES

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

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 el OSCE no cabe interposición de recurso administrativo alguno, siendo de 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 aquellos que fueron materia del presente pronunciamiento.

4.3 Una vez emitido el pronunciamiento y registrada la integración de Bases definitivas por el OSCE, 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, 11 de octubre de 2024

Código: 6.1, 6.3. 12.6.

Firmado digitalmente por FLORES BAZAN Miguel Angel FAU 20419026809 soft
Motivo: Soy el autor del documento
Fecha: 11.10.2024 18:21:04 -05:00