**PRONUNCIAMIENTO N° 162-2025/OECE-DSAT**

Entidad : Ministerio de Cultura

Referencia : Concurso Público N° 5-2025-/MC-1, convocado para la contratación del *"Servicio de acceso a internet, seguridad perimetral gestionada, telefonía e interconexión de datos"*

---

## 1. ANTECEDENTES

Mediante el formulario de solicitud de emisión de pronunciamiento recibido el 23[1] de mayo de 2025, y subsanado el 10[2] de junio de 2025, el presidente del Comité de Selección a cargo del procedimiento de selección de la referencia remitió a este Organismo Especializado las solicitudes de elevación de cuestionamientos al pliego absolutorio de consultas y observaciones presentadas por **GTD PERÚ S.A** y **AMERICA MOVIL PERU S.A.C.**, 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 Nº 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 absolutorio[3] 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° 7, referida al ***"Servicio de análisis de vulnerabilidades".***
- **Cuestionamiento N° 2** : Respecto a la absolución de las consultas y/u observaciones N° 22, N° 23, N° 24, N° 25, N° 205 y N° 206, referidas al ***"Anexo A: Punto N° 05".***
- **Cuestionamiento N° 3** : Respecto a la absolución de la consulta y/u observación N° 38, referida al ***"Servicio de líneas de telefonía".***

Firmado digitalmente por LAURA SILVA Anthony David FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 25.06.2025 19:44:53 -05:00

Firmado digitalmente por CHAMOCHUMBI CHERRE Carlos Ernesto FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 25.06.2025 19:37:23 -05:00

[1] Mediante el Expediente N° 2025-0015783.
[2] Mediante el Expediente N° 2025-0023633.
[3] Para la emisión del presente Pronunciamiento se utilizará la numeración establecida en el pliego absolutorio en versión PDF.

- **<u>Cuestionamiento N° 4</u>** : Respecto a la absolución de las consultas y/u observaciones N° 147, N° 270 y N° 271, referidas al ***"Servicio de acceso a internet sede central".***

- **<u>Cuestionamiento N° 5</u>** : Respecto a la absolución de la consulta y/u observación N° 175, referida a los ***"Aspectos generales del Anexo A: Punto N° 2".***

- **<u>Cuestionamiento N° 6</u>** : Respecto a la absolución de la consulta y/u observación N° 182, referida a la ***"Gestión y reporte del Anexo A: Punto N° 2".***

- **<u>Cuestionamiento N° 7</u>** : Respecto a la absolución de la consulta y/u observación N° 193, referida a las ***"Características físicas y rendimiento del Anexo A: Punto N° 4".***

- **<u>Cuestionamiento N° 8</u>** : Respecto a la absolución de la consulta y/u observación N° 316, referida *a los* ***"Documentos para la admisión de ofertas".***

- **<u>Cuestionamiento N° 9</u>** : Respecto a la absolución de la consulta y/u observación N° 327, referida al ***"Servicio de interconexión de datos con las 12 sedes de Lima y 22 sedes en provincias a nivel nacional".***

- **<u>Cuestionamiento N° 10</u>** : Respecto a la absolución de la consulta y/u observación N° 362, referida *a las* ***"Características técnicas del Anexo A: Punto 01".***

Por otro lado, cabe señalar que el participante **GTD PERÚ S.A** cuestionó la absolución de la consulta y/u observación N° 7, conforme al detalle siguiente, "*se solicita que la Entidad precise claramente: "(...) Cualquier restricción o expectativa de profundidad del análisis.*"

Al respecto, de la revisión del pliego absolutorio, se advierte que la consulta y/u observación N°7, no versa sobre la aclaración relativa a la restricción o expectativa de profundidad del análisis, sino a que se i) detalle la cantidad total de servidores que serán considerados en el análisis, ii) el sistema operativo y el rol correspondiente de cada uno, y iii) la forma en que se distribuyen las aplicaciones entre los servidores.

En ese sentido, lo indicado por el recurrente en su solicitud de elevación no fue abordado en la etapa de formulación de consultas y/u observaciones; por lo que, al tratarse de una pretensión adicional que debió ser presentada en la etapa pertinente, ésta deviene en extemporánea; razón por la cual, **este Organismo Técnico Especializado no se pronunciará respecto a dicho extremo del cuestionamiento a la consulta y/u observación N° 7 del pliego**.

## 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 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 *"Servicio de análisis de vulnerabilidades".***

El participante **GTD PERÚ S.A** cuestionó la consulta y/u observación N° 7 del pliego, alegando que, la respuesta emitida por el Comité de Selección transgrede los Principios de Transparencia, Igualdad de Trato y Competencia, debido a que la Entidad no ha brindado información técnica suficiente que permita delimitar con precisión el alcance del servicio requerido. En efecto, al limitarse a indicar que se deberá efectuar el escaneo de hasta 70 aplicaciones, no se especifica si éstas se encuentran alojadas en un único servidor o distribuidas en varios, lo que genera incertidumbre en los postores, respecto a la planificación de recursos, costos de licenciamiento y dimensionamiento del servicio a contratar.

Por lo tanto, la pretensión del recurrente consiste en que la Entidad **detalle i) la cantidad total de servidores que serán considerados en el análisis, ii) el sistema operativo y el rol correspondiente de cada uno, y iii) la forma en que se distribuyen las aplicaciones entre los servidores.**

**Pronunciamiento**

Sobre el particular, de la revisión al acápite 4.2 del numeral 3.1 del Capítulo III de la Sección Específica de las Bases de la convocatoria, se aprecia lo siguiente:

> ***"4.2 <u>SERVICIO DE SEGURIDAD PERIMETRAL GESTIONADA</u>***
>
> *(...)*
> ***SERVICIO DE ANÁLISIS DE VULNERABILIDADES***
> *(...)*
>
> ***✔ <u>El informe deberá contener el tipo de vulnerabilidad, los servicios y/o servidores afectados, evidencias y recomendaciones para la mitigación de la(s) posible(s) vulnerabilidad(es) encontrada(s) como parte del análisis.</u>***
> *(...)"*

(El subrayado y resaltado es agregado)

Es así como, mediante la consulta y/u observación N° 7 del pliego de absolución, se solicitó a la Entidad que precise si el servicio requerido comprende tanto servidores como aplicaciones. Asimismo, se requirió que confirme la cantidad de servidores que serán objeto de análisis, indicando el sistema operativo y el rol de cada uno, y que, de ser posible, proporcione un listado detallado. Del mismo modo, se solicitó que señale la cantidad de aplicaciones comprendidas en el alcance del servicio. Ante lo cual, la Entidad precisó que deberá realizarse un escaneo de hasta 70 aplicaciones, conforme a lo establecido en las Bases Integradas. Asimismo, señaló que se proporcionará mayor detalle antes del inicio de la ejecución del análisis correspondiente.

En relación con ello, y en atención al cuestionamiento formulado por el participante, mediante INFORME N° 000422-2025-OIT-OGETIC-SG/MC[4], la Entidad señaló lo siguiente:

> ***"(...)** el sustento técnico adoptado por el área usuaria en relación a dicha pregunta fue que, el análisis de vulnerabilidades debe realizarse **<u>en base a las aplicaciones que tiene la Entidad</u>** dado que varias aplicaciones pueden estar alojadas en **<u>un solo servidor</u>** y posteriormente puedan ir migrándose a servidores independientes por lo que **<u>no debería variar la cantidad de aplicaciones analizadas</u>**, además, el brindar información de manera pública como sistemas operativos, versiones, roles del servidor u otra información puede ser utilizado para ataques específicos según las vulnerabilidades del sistema operativo siendo perjudicial para la Entidad, por lo que dicha información detallada **<u>será brindada previo a la ejecución del análisis respectivo como se ha venido trabajando los últimos años.</u>***
> *(...)"*

(El subrayado y resaltado es agregado)

Adicionalmente, mediante el INFORME N° 000022-2025-OIT-OGETIC-SG-HPS/MC[5], la Entidad indicó lo siguiente:

> ***"(...)** Al respecto en calidad de área usuaria se informa lo siguiente:*

[4] Remitido mediante el Expediente N° 2025-0015783, de fecha 23 de mayo de 2025.
[5] Remitido mediante el Expediente N° 2025-0023633, de fecha 10 de junio de 2025.

*• La arquitectura tecnológica de la Entidad se encuentra **en constante proceso de migración, virtualización y consolidación**, por lo que el número de servidores físicos o virtuales que alojan aplicaciones **no es fijo ni relevante para el alcance definido**, dado que el análisis se centra en **las aplicaciones y no en su ubicación específica**, así mismo una misma aplicación puede estar distribuida en **más de un servidor, o múltiples aplicaciones pueden compartir un mismo servidor**, lo cual varía frecuentemente en función de la gestión de recursos, actualizaciones o despliegues planificados.*

*• Brindar públicamente detalles como el sistema operativo, versiones, roles, estructura de servidores y distribución interna constituye una exposición innecesaria de vectores de ataque, lo que contradice los principios de seguridad establecidos en normas internacionales tales como ISO 27001, NIST SP 800, OWASP, entre otros, por lo que la publicación de este tipo de información en una etapa previa a la contratación **vulnera los principios de confidencialidad y puede ser aprovechada por actores maliciosos para lanzar ataques dirigidos.***

*• En los procesos de análisis de vulnerabilidades y pruebas de seguridad (pentesting), es una práctica común que el detalle técnico y el alcance específico se determine **una vez contratado el servicio, previa firma de acuerdos de confidencialidad (NDA) y/o aprobación del plan de trabajo técnico**, esta modalidad se alinea con los **procedimientos realizados en años anteriores en esta Entidad, sin que ello haya afectado la ejecución del servicio**, lo cual demuestra su viabilidad operativa.*

*• Dicho esto, el área usuaria mantiene su posición **de no brindar públicamente los datos solicitados por el Postor**, dado que no impacta directamente en la planificación de recursos, costos de licenciamiento, ni dimensionamiento del servicio a contratar, siendo además el único postor en requerir dicha información para la presentación de su oferta.*
*(...)"*

(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, ha ratificado su requerimiento mediante el informe citado, aclarando que el informe correspondiente al servicio de análisis de vulnerabilidades deberá contener el tipo de vulnerabilidad, los servicios y/o servidores afectados, evidencias y recomendaciones para la mitigación de la(s) posible(s) vulnerabilidad(es) encontrada(s) como parte del análisis. Asimismo, agrega que, dicha decisión se sustenta en que la arquitectura tecnológica de la Entidad se encuentra en constante proceso de migración, virtualización y consolidación; por tanto, el número de servidores físicos o virtuales que alojan las aplicaciones no constituye un dato fijo, ni relevante para el alcance definido, ya que el análisis se centra en las aplicaciones y no en su localización específica. Finalmente, precisa que una misma aplicación puede estar distribuida en varios servidores, y que múltiples

aplicaciones pueden coexistir en un solo servidor, lo cual varía continuamente en función de la gestión de recursos, actualizaciones o despliegues planificados.

Por tanto, la Entidad aclara que brindar públicamente información detallada, como el sistema operativo, sus versiones, los roles asignados, la estructura de los servidores y su distribución interna, constituye una exposición innecesaria a potenciales vectores de ataque, contraviniendo los principios de seguridad de la información, establecidos en estándares internacionales como la ISO 27001, NIST SP 800 y OWASP. En ese sentido, la divulgación de dicha información, en una etapa previa a la contratación, podría comprometer la confidencialidad de la infraestructura tecnológica institucional y ser aprovechada por actores maliciosos para ejecutar ataques dirigidos. Agrega además que, esta metodología ha sido implementada en procesos anteriores desarrollados por la Entidad, sin perjuicio de la adecuada ejecución del servicio, lo cual respalda su factibilidad técnica y operativa. Afirmación que se encuentra sujeta a rendición de cuentas.

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 detalle i) la cantidad total de servidores que serán considerados en el análisis, ii) el sistema operativo y el rol correspondiente de cada uno, y iii) la forma en que se distribuyen las aplicaciones entre los servidores; y en la medida que, mediante su informe, la Entidad ratificó su requerimiento, así como los argumentos por los cuales no resulta posible precisar los extremos consultados por el recurrente; este Organismo Técnico Especializado ha decidido **NO ACOGER** el presente cuestionamiento.

**Cuestionamiento N° 2:** **Respecto al *"Anexo A: Punto N° 05"***

El participante **GTD PERÚ S.A.** cuestionó la respuesta otorgada por el Comité de Selección en la **consulta y/u observación Nº 22** del pliego, alegando que dicha respuesta vulnera los Principios de Vigencia Tecnológica y de Eficiencia y Eficacia, debido a que, la Entidad decidió mantener como parte del requerimiento el soporte a sistemas operativos obsoletos (en estado de *End of Support*), como Windows 7 y MacOS X, los cuales, según informes técnicos de sus propios fabricantes —Microsoft y Apple—, no cuentan con actualizaciones oficiales desde hace varios años, lo que los convierte en plataformas altamente vulnerables. Asimismo, el participante sostiene que exigir su inclusión en un entorno destinado al análisis de archivos maliciosos contradice los fines del servicio requerido, dado que no se garantiza compatibilidad ni precisión técnica, se introduce un riesgo innecesario en el ambiente de análisis controlado, y se incrementan los costos de la solución sin aportar valor técnico real al objetivo de la contratación.

Por lo tanto, la pretensión del recurrente consiste en que la Entidad, **respecto de la Tecnología de Sandboxing, admita los siguientes sistemas operativos: Windows 10 en adelante, MacOS 12 en adelante, Linux 10 en adelante, y Android 10 en adelante.**

Asimismo, cuestionó la respuesta otorgada por el Comité de Selección en la **consulta y/u observación Nº 23** del pliego, alegando que dicha respuesta resultaría contradictoria con el propio requerimiento de seguridad establecido por la Entidad, en

la medida que admite como válidas plataformas que, según informes técnicos del fabricante Microsoft, presentan altos niveles de vulnerabilidad.

Por lo tanto, la pretensión del recurrente consiste en que la Entidad, **respecto de la Características del agente, no considere como válidas a las versiones de sistemas operativos Windows 7, Windows 8 y Windows 8.1.**

Además, cuestionó la respuesta otorgada por el Comité de Selección en la **consulta y/u observación Nº 24** del pliego, alegando que la decisión de mantener como requerimiento la compatibilidad con versiones del sistema operativo macOS 10.x —actualmente en estado de End of Support, según el fabricante Apple— resulta técnicamente improcedente, toda vez que: (i) dichas versiones ya no reciben actualizaciones ni parches de seguridad, lo que implica un riesgo elevado de exposición a vulnerabilidades críticas; (ii) exigir compatibilidad con sistemas descontinuados impacta negativamente en la calidad y eficiencia del servicio, al forzar a los proveedores a adecuarse a plataformas tecnológicamente obsoletas; y (iii) dicho requerimiento se contrapone a las buenas prácticas en ciberseguridad, comprometiendo la integridad y protección de los activos tecnológicos de la Entidad.

Por lo tanto, la pretensión del recurrente consiste en que la Entidad, **respecto de las Características del agente, admita como mínimo macOS 12.x en adelante.**

Además, cuestionó la respuesta otorgada por el Comité de Selección en la **consulta y/u observación Nº 25** del pliego, alegando que la aceptación de versiones como Oracle Linux 6 resulta contraria a los principios establecidos en el artículo 2 de la Ley de Contrataciones del Estado, toda vez que dichas plataformas: (i) se encuentran fuera de soporte oficial por parte del fabricante; (ii) no reciben actualizaciones de seguridad ni parches críticos; y (iii) representan un riesgo para la integridad y confidencialidad de la información de la Entidad.

Por lo tanto, la pretensión del recurrente consiste en que la Entidad, **respecto de las Características del agente, suprima la admisión del Oracle 6 y confirme que solo admitirá Oracle Linux 6.7 en adelante.**

Por otro lado, el participante **AMERICA MOVIL PERU S.A.C.** cuestionó la absolución de las **consultas y/u observaciones N° 24, N° 205 y N° 206** del pliego, alegando que, mediante las respuestas emitidas, el Comité de Selección ha dispuesto mantener como parte del requerimiento, la compatibilidad con sistemas operativos que actualmente se encuentran en estado de 'End of Support'. Señaló que dicha situación podría comprometer la adecuada ejecución del servicio, en la medida que se trata de plataformas que ya no cuentan con soporte técnico oficial por parte de sus fabricantes, lo que impide la aplicación de actualizaciones de seguridad o mantenimiento esenciales para el correcto y seguro funcionamiento del producto.

Por lo tanto, la pretensión del recurrente consiste en que la Entidad, **respecto de la Características del agente, suprima la obligación de brindar soporte a los sistemas operativos "OSX 10.11 (El Capitan), macOS 10.12 (Sierra), macOS 10.14, macOS 10.15"; "CentOS 6 y CentOS 7"; y "Linux 6, 7 y 8"; y, en**

**consecuencia, confirme que se brindará soporte a los sistemas operativos "macOS 12.x"; CentOS 6.8+, 7.2+; y Oracle Linux 6.10, 7.7+, y 8.2+.**

**Pronunciamiento**

Sobre el particular, de la revisión del Anexo A: Punto N° 5 del numeral 3.1 del Capítulo III de la Sección Específica de las Bases de la convocatoria, se aprecia lo siguiente:

> *"**ANEXO A: PUNTO N° 05***
>
> ***SERVICIO DE SEGURIDAD DE PROTECCIÓN AVANZADA PARA ENDPOINTS***
>
> *(...)*
> ***Tecnología de Sandboxing***
> *(...)*
> ● *Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows XP, Windows 7, Windows 10, Mac OS X, Linux y Android.*
>
> ***(…)***
> ***Características del agente***
> ***(…)***
> ● *Soporte para las siguientes versiones de sistemas operativos:*
> *o Windows 7 (32-bit, 64-bit, RTM & SP1; excepto Home), Windows 8* (32-bit, 64-bit), Windows 8.1 (32-bit, 64-bit; FIPS mode), Windows Embedded 8.1 Pro, Windows 10 Pro, Windows 10 Enterprise LTSB, Windows Server 2003* (32-bit, SP2 o posterior), Windows Server 2003 R2 (32-bit, SP2 o posterior), Windows Server 2008 (32-bit, 64-bit; FIPS mode), Windows Server 2008 R2 (32-bit, 64-bit; FIPS mode), Windows Server 2012 (todas las ediciones; FIPS mode), Windows Server 2012 R2 (todas las ediciones; FIPS mode), Windows Server 2016, Windows Server Core option 2012, 2012 R2 y 2016, Windows Server 2016 Datacenter.*
> ● *OSX 10.11 (El Capitan), macOS 10.12 (Sierra), macOS 10.14, macOS 10.15*
> ● *CentOS 6, CentOS 7, Centos 8, Red Hat Enterprise Linux 6, Red Hat Enterprise Linux 7, Suse for Enterprise 12.1, Suse for Enterprise 12.2, Oracle Linux 6, 7 y 8, Ubuntu Server 12, Ubuntu Server 14, Ubuntu Server 16, Ubunto 18.*
> ***(…)"***

(El subrayado y resaltado es agregado)

Ahora bien, en atención a los aspectos cuestionados por el recurrente, y a la afinidad entre los mismos, se procederá a efectuar su análisis bajo los siguientes **tres (3) extremos**:

**a) Respecto de la absolución de la consulta y/u observación N° 22:**

Es así que, mediante consulta y/u observación N° 22 del pliego, se solicitó modificar el requerimiento referido a uno de los criterios técnicos de la tecnología de sandboxing, proponiendo que dicho requerimiento contemple "*Soportar el análisis de archivos maliciosos en ambiente controlado como mínimo, sistema operacional Windows 10 en adelante, Mac OS 12 en adelante, distribuciones de Linux y Android 10 en adelante",* argumentando que algunos de los sistemas operativos inicialmente contemplados por la Entidad se encuentran en estado de "End of Support", de

acuerdo con la información publicada por sus respectivos fabricantes. Ante lo cual, el Comité de Selección precisó que, con el fin de ampliar la participación de postores y en atención a las necesidades de la Entidad, se aceptará como mínimo el soporte para los sistemas operativos Windows 7, Windows 10, MacOS X, distribuciones de Linux y Android 10 en adelante.

En relación con ello, y en atención al cuestionamiento formulado por el participante, mediante INFORME N° 000422-2025-OIT-OGETIC-SG/MC[6], la Entidad señaló lo siguiente:

> *"(...) El sustento técnico adoptado por el área usuaria en relación a dicha pregunta fue que, actualmente **la Entidad aún cuenta con equipamiento Windows 7 y MAC OS X** por lo que, a fin de mitigar o reducir los riesgos de dichos sistemas operativos, se solicita que la solución pueda soportar dichas versiones, dado que debido a la cantidad de usuarios y de equipamiento tanto en Lima como a nivel nacional **no se ha podido concretar la migración o actualización de dichos sistemas** por lo que se requiere aún que la solución de seguridad cuente con dicha compatibilidad.*
> *(...)"*

(El subrayado y resaltado es agregado)

Adicionalmente, mediante el INFORME N° 000022-2025-OIT-OGETIC-SG-HPS/MC[7], la Entidad indicó lo siguiente:

> *"(...) Al respecto en calidad de área usuaria se informa lo siguiente:*
>
> *• La Entidad actualmente **mantiene un parque informático heterogéneo, donde coexisten dispositivos con sistemas operativos anteriores a las últimas versiones soportadas por los fabricantes**, principalmente debido a limitaciones presupuestales para renovación de equipos, dependencia de aplicaciones institucionales y sistemas legados que **no son compatibles con versiones recientes** por lo que limitar el soporte únicamente a versiones actuales obligaría a la Entidad a realizar una renovación masiva e inmediata del parque tecnológico, lo cual no es factible por razones presupuestales ni logísticas. Asimismo, la seguridad debe adaptarse al entorno existente, no a uno ideal aún no alcanzado y la función del proveedor debe ser la de proteger el ecosistema real, incluyendo versiones antiguas mientras se lleva a cabo el proceso de modernización tecnológica, por lo que mientras ello ocurre, **se requiere que la solución de seguridad brinde cobertura a todo el parque instalado, sin exclusiones que puedan dejar equipos desprotegidos o sin visibilidad en la solución de seguridad solicitado.***
>
> *• Además, se precisa que **actualmente existen soluciones de seguridad en el mercado que permiten brindar soporte a entornos mixtos**, incluyendo endpoints con versiones EOL (end-of-life) mediante agentes, políticas de control u otros destinados para tal fin.*
>
> *(...)*
>
> *• Dado que la Entidad aún cuenta con infraestructura y endpoints que utilizan versiones antiguas de sistemas operativos, es necesario que el proveedor tenga capacidad de cobertura para esos entornos y si en caso se exige como condición que solo se soporte sistemas operativos actuales, **se estaría dificultando la presentación de ofertas por parte de empresas y/o marcas que tienen capacidades amplias de soporte**, pero requieren que el pliego lo permita*

[6] Remitido mediante el Expediente N° 2025-0015783, de fecha 23 de mayo de 2025.
[7] Remitido mediante el Expediente N° 2025-0023633, de fecha 10 de junio de 2025.

*expresamente, así como también la inclusión de sistemas legados o antiguos como parte del soporte requerido es una práctica común, dada la realidad presupuestal y tecnológica del sector público y de no considerarlo restringiría el alcance sólo a sistemas modernos el cual no refleja adecuadamente el entorno operativo institucional, y puede generar ineficiencias y vacíos de cobertura. Finalmente, el área usuaria menciona que SI se restringiría la participación de postores potenciales, dado que* ***no todas las soluciones del mercado están diseñadas exclusivamente para entornos modernos; algunas ofrecen soporte extendido para entornos mixtos o sistemas legados, y limitar el requerimiento eliminaría esas opciones****.*

*• Por último,* ***el párrafo final se mantendría sin cambios.***
*(...)"*

(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 a lo cuestionado por el recurrente, el Comité de Selección en coordinación con el área usuaria de la Entidad, siendo la responsable de la determinación de su requerimiento y, por ende, la mejor conocedora de sus necesidades, a través del citado informe, ratificó lo absuelto en el pliego, manteniendo que el sistema Tecnología de Sandboxing debe soportar el análisis de archivos maliciosos, incluido en los sistemas operacionales Windows 7, Windows 10, MacOS X, Linux y Android 10 en adelante; argumentando que, la Entidad actualmente cuenta con un parque informático heterogéneo, en el que operan dispositivos con sistemas operativos anteriores a las versiones más recientes soportadas por los fabricantes. Siendo ésta, una situación originada principalmente por las restricciones presupuestales del sector público, que dificultan la renovación de equipos, así como por la dependencia de aplicaciones institucionales y sistemas legados no compatibles con versiones actualizadas. En ese sentido, restringir el soporte únicamente a sistemas operativos vigentes, obligaría a la Entidad a ejecutar una renovación masiva e inmediata de su infraestructura tecnológica, lo cual resulta inviable tanto desde el punto de vista presupuestal como logístico.

Asimismo, la Entidad indicó que las soluciones de seguridad deben responder a las condiciones reales del entorno tecnológico en uso, y no a escenarios ideales que aún no han sido implementados. En ese sentido, se considera que la función del proveedor debe centrarse en proteger la infraestructura tecnológica existente, incluyendo aquellos equipos que operan con versiones antiguas de software, en tanto se avanza progresivamente en el proceso de modernización. Por ello, se considera indispensable que la solución de seguridad requerida brinde cobertura integral al parque informático actualmente instalado, evitando exclusiones que puedan generar brechas en la protección o afectar la visibilidad y eficacia del servicio contratado.

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, respecto de la Tecnología de Sandboxing, admita los siguientes sistemas operativos: Windows 10 en adelante, MacOS 12 en adelante, Linux 10 en adelante, y Android 10 en adelante; y en la medida que mediante su informe, la Entidad ratificó lo absuelto en el pliego, 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.

**b) Respecto de la absolución de la consulta y/u observación N° 23:**

Es así que, mediante consulta y/u observación N° 23 del pliego, se solicitó modificar el requerimiento referido al soporte de versiones de sistemas operativos, proponiendo que dicho requerimiento contemple "*Windows 10 Pro, Windows 10 Enterprise LTSB y Windows 11, Windows Server 2012 (todas las ediciones; FIPS mode), Windows Server 2012 R2 (todas las ediciones; FIPS mode), Windows Server 2016, Windows Server Core option 2012, 2012 R2 y 2016, Windows Server 2016 Datacenter y posteriores",* argumentando que los sistemas operativos Windows 7, 8, 8.1 y Windows Server 2008 han sido declarados en estado de End of Support por el fabricante Microsoft.

Ante lo cual, el Comité de Selección precisó que, con el objetivo de ampliar la participación de postores y en atención a las necesidades de la Entidad, se aceptará como mínimo el soporte para los sistemas operativos Windows 7 SP1, Windows 8.1 (32 y 64 bits), Windows 10, Windows Server 2008 R2, Windows Server 2012 (todas las ediciones), Windows Server 2012 R2 (todas las ediciones), Windows Server 2016, Windows Server Core option 2012, 2012 R2 y 2016, así como Windows Server 2016 Datacenter.

En relación con ello, y en atención al cuestionamiento formulado por el participante, mediante INFORME N° 000422-2025-OIT-OGETIC-SG/MC[8], la Entidad señaló lo siguiente:

> ***"(...)** El sustento técnico adoptado por el área usuaria en relación a dicha pregunta fue que, actualmente **la Entidad aún cuenta con equipamiento Windows 7, Windows 8.1 y Windows Server 2008R2** por lo que, a fin de mitigar o reducir los riesgos de dichos sistemas operativos, se solicita que la solución pueda soportar dichas versiones, así mismo existen aplicaciones que aún están alojadas en versiones Windows Server 2008R2 por lo que se requiere lo solicitado en las Bases Integradas.*
> *(...)"*

(El subrayado y resaltado es agregado)

Adicionalmente, mediante el INFORME N° 000022-2025-OIT-OGETIC-SG-HPS/MC[9], la Entidad indicó lo siguiente:

> ***"(...)** Al respecto en calidad de área usuaria se informa lo siguiente:*

[8] Remitido mediante el Expediente N° 2025-0015783, de fecha 23 de mayo de 2025.
[9] Remitido mediante el Expediente N° 2025-0023633, de fecha 10 de junio de 2025.

*• (...) la Entidad actualmente **mantiene un parque informático heterogéneo, donde coexisten dispositivos con sistemas operativos anteriores a las últimas versiones soportadas por los fabricantes**, principalmente debido a limitaciones presupuestales para renovación de equipos, dependencia de aplicaciones institucionales y sistemas legados que **no son compatibles con versiones recientes** por lo que limitar el soporte únicamente a versiones actuales obligaría a la Entidad a realizar una renovación masiva e inmediata del parque tecnológico, lo cual no es factible por razones presupuestales ni logísticas. Asimismo, la seguridad debe adaptarse al entorno existente, no a uno ideal aún no alcanzado y la función del proveedor debe ser la de proteger el ecosistema real, incluyendo versiones antiguas mientras se lleva a cabo el proceso de modernización tecnológica, por lo que mientras ello ocurre, **se requiere que la solución de seguridad brinde cobertura a todo el parque instalado, sin exclusiones que puedan dejar equipos desprotegidos o sin visibilidad en la solución de seguridad solicitado.***

*• Además, se precisa que **actualmente existen soluciones de seguridad en el mercado que permiten brindar soporte a entornos mixtos**, incluyendo endpoints con versiones EOL (end-of-life) mediante agentes, políticas de control u otros destinados para tal fin.*

*(...)*

*• Exigir que la solución de seguridad solo soporte Windows 10 y Windows Server 2012 en adelante, **dejaría fuera de cobertura a un número importante de activos operativos actualmente en uso dentro de la Entidad**, dado que el servicio contratado debe tener alcance a todo el parque informático, no es técnica ni operativamente viable excluir los dispositivos con sistemas operativos antiguos hasta que se complete su migración, además limitar la cobertura solo a versiones modernas implica dejar completamente desprotegidos a los activos más vulnerables, lo que contradice las mejores prácticas del NIST, los Controles CIS e incluso la ISO/IEC 27001, que enfatizan la protección de todo los activos en uso, sin importar su antigüedad, por lo tanto esta área usuaria concluye que **no es técnica ni operativamente viable adecuar el requerimiento exclusivamente a versiones de sistema operativo Windows 10 (en todas sus versiones) y Windows Server 2012 en adelante, debido a que se comprometería la cobertura integral del servicio de seguridad que se pretende contratar y se reduciría la efectividad de las medidas de mitigación de riesgos en los equipos más vulnerables.***
*(...)"*

(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 a lo cuestionado por el recurrente, el Comité de Selección en coordinación con el área usuaria de la Entidad, siendo la responsable de la determinación de su requerimiento y, por ende, la mejor conocedora de sus necesidades, a través del citado informe, ratificó lo absuelto en el pliego, manteniendo como mínimo el soporte para los sistemas operativos Windows 7 SP1, Windows 8.1 (32-bit, 64-bit), Windows 10, Windows Server 2008 R2, Windows Server 2012 (todas las ediciones), Windows Server 2012 R2 (todas las ediciones), Windows Server 2016, Windows Server Core option 2012, 2012 R2 y 2016,

Windows Server 2016 Datacenter; argumentando que la Entidad actualmente cuenta con un parque informático heterogéneo, en el que operan dispositivos con sistemas operativos anteriores a las versiones más recientes soportadas por los fabricantes. Siendo ésta, una situación originada principalmente por las restricciones presupuestales del sector público, que dificultan la renovación de equipos, así como por la dependencia de aplicaciones institucionales y sistemas legados no compatibles con versiones actualizadas. En ese sentido, restringir el soporte únicamente a sistemas operativos vigentes, obligaría a la Entidad a ejecutar una renovación masiva e inmediata de su infraestructura tecnológica, lo cual resulta inviable tanto desde el punto de vista presupuestal como logístico.

Asimismo, la Entidad indicó que las soluciones de seguridad deben responder a las condiciones reales del entorno tecnológico en uso, y no a escenarios ideales que aún no han sido implementados. En ese sentido, se considera que la función del proveedor debe centrarse en proteger la infraestructura tecnológica existente, incluyendo aquellos equipos que operan con versiones antiguas de software, en tanto se avanza progresivamente en el proceso de modernización. Por ello, se considera indispensable que la solución de seguridad requerida brinde cobertura integral al parque informático actualmente instalado, evitando exclusiones que puedan generar brechas en la protección o afectar la visibilidad y eficacia del servicio contratado.

Del mismo modo, precisó que en la actualidad existen soluciones tecnológicas disponibles en el mercado que permiten brindar soporte a entornos mixtos, incluyendo aquellos conformados por equipos que operan con sistemas en estado de *end-of-life* (EOL), a través de la implementación de agentes, políticas de control u otros mecanismos específicamente diseñados para tales escenarios.

Finalmente, la Entidad considera que no resulta técnica ni operativamente factible limitar el requerimiento únicamente a sistemas operativos a partir de Windows 10 y Windows Server 2012, toda vez que dicha restricción comprometería la cobertura total del servicio de seguridad a contratar y disminuiría la efectividad de las acciones destinadas a mitigar riesgos, particularmente en los equipos que presentan mayor nivel de exposición.

Por lo tanto, considerando lo señalado en los párrafos que preceden, y dado que la pretensión del recurrente se encuentra orientada a que la Entidad, respecto de la Características del agente, no considere como válidas a las versiones de sistemas operativos Windows 7, Windows 8 y Windows 8.1; y en la medida que mediante su informe, la Entidad ratificó lo absuelto en el pliego, 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.

**c) Respecto de la absolución de las consultas y/u observaciones N° 24, N° 25, N° 205 y N° 206:**

Es así que, mediante las consultas y/u observaciones N° 24, N° 25, N° 205 y N° 206 del pliego, se solicitó modificar el requerimiento en relación al soporte de versiones de sistemas operativos, proponiendo que dicho requerimiento contemple "*macOS 12.x en adelante*"; "*CentOS 6.7, CentOS 7, Red Hat Enterprise Linux 6.7, Red Hat*

*Enterprise Linux 7, Suse for Enterprise 12.1, Suse for Enterprise 12.2, Oracle Linux 6.7, 7 y 8, Ubuntu Server 12, Ubuntu Server 14, Ubuntu Server 16, Ubuntu Server 22, alma Linux 8 y 9."; "CentOS 6.8+, 7.2+ en lugar de CentOS 6 y CentOS 7"; "Oracle Linux 6.10, 7.7+, y 8.2+ en lugar de Oracle Linux 6, 7 y 8".*

Ante lo cual, el Comité de Selección precisó que, con el objetivo de ampliar la participación de postores y en atención a las necesidades de la Entidad, se aceptará como mínimo el soporte para los sistemas operativos CentOS 6.7, CentOS 7, Centos 8, Red Hat Enterprise Linux 6.7, Red Hat Enterprise Linux 7, Suse for Enterprise 12.1, Suse for Enterprise 12.2, Oracle Linux 6, 7 y 8, Ubuntu Server 12 (opcional), Ubuntu Server 14 (opcional), Ubuntu Server 16, Ubuntu 18 en adelante.

En relación con ello, y en atención al cuestionamiento formulado por el participante, mediante, mediante el INFORME N° 000022-2025-OIT-OGETIC-SG-HPS/MC[10], la Entidad señaló lo siguiente:

> ***"(...)** Al respecto en calidad de área usuaria se informa lo siguiente:*
>
> *• (...) la Entidad actualmente **mantiene un parque informático heterogéneo, donde coexisten dispositivos con sistemas operativos anteriores a las últimas versiones soportadas por los fabricantes**, principalmente debido a limitaciones presupuestales para renovación de equipos, dependencia de aplicaciones institucionales y sistemas legados que **no son compatibles con versiones recientes** por lo que limitar el soporte únicamente a versiones actuales obligaría a la Entidad a realizar una renovación masiva e inmediata del parque tecnológico, lo cual no es factible por razones presupuestales ni logísticas. Asimismo, la seguridad debe adaptarse al entorno existente, no a uno ideal aún no alcanzado y la función del proveedor debe ser la de proteger el ecosistema real, incluyendo versiones antiguas mientras se lleva a cabo el proceso de modernización tecnológica, por lo que mientras ello ocurre, **se requiere que la solución de seguridad brinde cobertura a todo el parque instalado, sin exclusiones que puedan dejar equipos desprotegidos o sin visibilidad en la solución de seguridad solicitado.***
>
> *• Además, se precisa que **actualmente existen soluciones de seguridad en el mercado que permiten brindar soporte a entornos mixtos**, incluyendo endpoints con versiones EOL (end-of-life) mediante agentes, políticas de control u otros destinados para tal fin.*
>
> *(...)*
>
> *• Respecto a los equipos Apple, algunos de estos no son técnicamente actualizables a macOS 12.x por obsolescencia del hardware, sin embargo, requieren de protección en el marco del servicio a contratar, por lo tanto, la exclusión debilitaría la cobertura de seguridad exigida.*
> *• Sobre los sistemas CentOS y Oracle Linux, estos aún están en uso para servicios institucionales que dependen de versiones específicas de bases de datos y aplicaciones personalizadas por lo que migrar estas plataformas implica no solo actualizar el sistema operativo, sino también reprogramar, revalidar y certificar funcionalmente las aplicaciones sobre nuevos entornos, asimismo, limitar el soporte únicamente a las versiones modernas propuestas restringe la cobertura del servicio sobre sistemas reales actualmente en producción, dejando vacíos de protección crítica en la infraestructura, **es por ello que no es posible aceptar un soporte solo de las versiones macOS 12.x, CentOS 6.8+, 7.2+ y Oracle Linux 6.7+,6.10, 7.7+, y 8.2+***
> *(...)"*

[10] Remitido mediante el Expediente N° 2025-0023633, de fecha 10 de junio de 2025.

(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 a lo cuestionado por el recurrente, el Comité de Selección en coordinación con el área usuaria de la Entidad, siendo la responsable de la determinación de su requerimiento y, por ende, la mejor conocedora de sus necesidades, a través del citado informe, ratificó lo absuelto en el pliego, manteniendo como mínimo el soporte para los sistemas operativos CentOS 6.7, CentOS 7, Centos 8, Red Hat Enterprise Linux 6.7, Red Hat Enterprise Linux 7, Suse for Enterprise 12.1, Suse for Enterprise 12.2, Oracle Linux 6, 7 y 8, Ubuntu Server 12 (opcional), Ubuntu Server 14 (opcional), Ubuntu Server 16, Ubuntu 18 en adelante; argumentando que la Entidad actualmente cuenta con un parque informático heterogéneo, en el que operan dispositivos con sistemas operativos anteriores a las versiones más recientes soportadas por los fabricantes, situación originada principalmente por restricciones presupuestales que dificultan la renovación de equipos, así como por la dependencia de aplicaciones institucionales y sistemas legados no compatibles con versiones actualizadas. En ese sentido, restringir el soporte únicamente a sistemas operativos vigentes obligaría a la Entidad a ejecutar una renovación masiva e inmediata de su infraestructura tecnológica, lo cual resulta inviable tanto desde el punto de vista presupuestal como logístico.

Aunado a ello, la Entidad indicó que las soluciones de seguridad deben responder a las condiciones reales del entorno tecnológico en uso, y no a escenarios ideales que aún no han sido implementados. En ese sentido, se considera que la función del proveedor debe centrarse en proteger la infraestructura tecnológica existente, incluyendo aquellos equipos que operan con versiones antiguas de software, en tanto se avanza progresivamente en el proceso de modernización. Por ello, se considera indispensable que la solución de seguridad requerida brinde cobertura integral al parque informático actualmente instalado, evitando exclusiones que puedan generar brechas en la protección o afectar la visibilidad y eficacia del servicio contratado.

Del mismo modo, precisó que en la actualidad existen soluciones tecnológicas disponibles en el mercado que permiten brindar soporte a entornos mixtos, incluyendo aquellos conformados por equipos que operan con sistemas en estado de *end-of-life* (EOL), a través de la implementación de agentes, políticas de control u otros mecanismos específicamente diseñados para tales escenarios.

En ese mismo sentido, la Entidad indicó que algunos no pueden ser actualizados técnicamente a macOS 12.x, considerando que siguen operativos, y por tanto, requieren protección en el marco del servicio a contratar; por lo que, su exclusión comprometería la cobertura de seguridad requerida. Asimismo, en cuanto a los sistemas CentOS y Oracle Linux, éstos continúan siendo utilizados en servicios

institucionales que dependen de versiones específicas de bases de datos y aplicaciones desarrolladas a medida, por lo que su migración no solo implicaría actualizar el sistema operativo, sino también realizar procesos complejos de reprogramación, validación y certificación funcional en nuevos entornos. Por tanto, restringir el soporte exclusivamente a versiones modernas como macOS 12.x, CentOS 6.8+, 7.2+ y Oracle Linux 6.7+, 6.10, 7.7+ y 8.2+, limitaría la cobertura del servicio sobre plataformas que aún están en producción, generando vacíos críticos en la protección de la infraestructura tecnológica.

Por lo tanto, considerando lo señalado en los párrafos que preceden, y dado que la pretensión del recurrente se encuentra orientada a que la Entidad, respecto de las Características del agente: i) admita como mínimo macOS 12.x en adelante, ii) suprima la admisión del Oracle 6 y confirme que solo admitirá Oracle Linux 6.7 en adelante, y iii) confirme que se brindará soporte a los sistemas operativos CentOS 6.8+, 7.2+; y en la medida que mediante su informe, la Entidad ratificó lo absuelto en el pliego, 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° 3:** **Respecto al *"Servicio de líneas de telefonía".***

El participante **GTD PERÚ S.A.** cuestionó la absolución de la consulta y/u observación N° 38 del pliego, alegando que dicha absolución vulneraría el Principio de Eficacia y Eficiencia, al no estar debidamente sustentada en criterios técnicos ni normativos. En ese sentido, señaló que la normativa vigente emitida por OSIPTEL —en particular la Resolución N.º 123-2014-CD/OSIPTEL— autoriza expresamente la tarificación por segundo para todo tipo de llamadas. Asimismo, sostuvo que tanto la práctica comercial del sector como las capacidades tecnológicas actualmente disponibles, por parte de los operadores, permiten la implementación de esquemas tarifarios más eficientes y económicos, utilizando como unidad de medida el segundo.

Por lo tanto, la pretensión del recurrente consiste en que la Entidad **admita propuestas que consideren la tarificación por segundo, para todas las llamadas tanto fijas como móviles.**

**Pronunciamiento**

Sobre el particular, de la revisión del acápite 4.3 del numeral 3.1 del Capítulo III de la Sección Específica de las Bases de la convocatoria, se aprecia lo siguiente:

> *"4.3 SERVICIO DE LÍNEAS DE TELEFONÍA*
>
> *(...)*
> - ***El Contratista deberá tener en cuenta que la tarificación y/o facturación deberá realizarse utilizando la unidad de medida de tiempo del minuto con excepción de las llamadas móviles que será al segundo.***
>
> *(...)"*

(El subrayado y resaltado es agregado)

Es así que, mediante consulta y/u observación N° 38 del pliego, se solicitó confirmar si también se aceptarán propuestas que contemplen la facturación utilizando como unidad de medida el segundo para todo tipo de llamadas, tanto a líneas móviles como fijas. Ante lo cual, el Comité de Selección precisó que la facturación del servicio deberá realizarse utilizando como unidad de medida el minuto, con excepción de las llamadas a móviles, las cuales podrán ser facturadas por segundos.

En relación con ello, y en atención al cuestionamiento formulado por el participante, mediante INFORME N° 000422-2025-OIT-OGETIC-SG/MC[11], la Entidad señaló lo siguiente:

> ***"(...)** el sustento técnico adoptado por el área usuaria en relación a dicha pregunta fue que, la normativa de OSIPTEL no impide la exigencia de una tarificación por minuto, es cierto que la Resolución Nº 123-2014-CD/OSIPTEL habilita a los operadores a ofrecer esquemas tarifarios por segundo, sin embargo, esta resolución **no obliga a las entidades contratantes a aceptar exclusivamente esta modalidad, ni prohíbe la tarificación por minuto.***
>
> *Por tanto, la disposición de OSIPTEL otorga libertad comercial al operador, pero **no limita la potestad de la Entidad para requerir condiciones tarifarias específicas dentro de un proceso de contratación pública**, conforme al artículo 18 de la Ley de Contrataciones del Estado, que permite establecer especificaciones técnicas cuando estas son objetivamente necesarias para el cumplimiento de la finalidad contractual.*
>
> *De igual forma, la afirmación de que esta exigencia vulnera el principio de eficiencia es inexacta, dado que, la tarificación por minuto, al ser una práctica ampliamente aceptada y ofrecida por todos los operadores del mercado, **no limita la participación ni restringe la competencia**, y permite una simplificación en la facturación y auditoría del servicio.*
> *(...)"*

(El subrayado y resaltado es agregado)

Adicionalmente, mediante el INFORME N° 000022-2025-OIT-OGETIC-SG-HPS/MC[12], la Entidad indicó lo siguiente:

> ***"(...)** Al respecto en calidad de área usuaria se informa lo siguiente:*
>
> *• Según lo mencionado por OSIPTEL los planes corporativos de telefonía fija en el Perú generalmente **aplican tarificación por minuto**, ya que están alineadas con el modelo de facturación empresarial y simplificación del monitoreo del consumo.*
>
> *• **Sin embargo, como área usuaria, se ha visto conveniente aperturar lo solicitado por el proveedor quedando de la siguiente manera** "El Contratista deberá tener en cuenta que la tarificación y/o facturación deberá realizarse utilizado la unidad de medida de tiempo del minuto o segundo con excepción de las llamadas móviles que será al segundo" dado que no causa un impacto en la solución solicitada del presente concurso público.*
> *(...)"*

(El subrayado y resaltado es agregado)

[11] Remitido mediante el Expediente N° 2025-0015783, de fecha 23 de mayo de 2025.
[12] Remitido mediante el Expediente N° 2025-0023633, de fecha 10 de junio 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 a lo cuestionado por el recurrente, el Comité de Selección en coordinación con el área usuaria de la Entidad, siendo la responsable de la determinación de su requerimiento y, por ende, la mejor conocedora de sus necesidades, a través del citado informe, se rectifica de lo absuelto, argumentando que si bien la Resolución N.º 123-2014-CD/OSIPTEL permite a los operadores ofrecer esquemas tarifarios basados en segundos, dicha norma no establece una obligación para las entidades del Estado de aceptar exclusivamente esa modalidad, ni prohíbe expresamente la utilización de la tarificación por minuto. En ese sentido, la normativa del regulador reconoce la libertad comercial de los operadores para definir sus ofertas, pero no restringe la facultad de las entidades contratantes para establecer condiciones tarifarias específicas en función de sus necesidades y objetivos de eficiencia en el marco de un proceso de contratación pública.

Asimismo, la Entidad agrega que, conforme a lo señalado por OSIPTEL, los planes corporativos de telefonía fija ofrecidos en el Perú suelen aplicar una tarificación por minuto, en tanto esta modalidad se encuentra alineada con los modelos de facturación empresarial y facilita la supervisión y control del consumo por parte de las instituciones usuarias. No obstante, lo afirmado, el área usuaria de la Entidad dispone admitir lo solicitado por el participante, por lo que, se admitirá también la tarificación por segundos.

Por lo tanto, considerando el análisis de los párrafos precedentes, y en tanto la pretensión del recurrente se encuentra orientada a que la Entidad admita propuestas que consideren la tarificación por segundos para todas las llamadas tanto fijas como móviles; y en la medida que, mediante informe técnico, la Entidad admite la petición formulada por el recurrente, este Organismo Técnico Especializado ha decidido **ACOGER** el presente cuestionamiento. Por lo que, con ocasión de la integración definitiva de las Bases, se implementará la siguiente disposición:

- **Se dejará sin efecto** lo absuelto en la consulta y/u observación N° 38 del pliego, y se deberá considerar la siguiente absolución: *"El Contratista deberá tener en cuenta que la tarificación y/o facturación deberá realizarse utilizado la unidad de medida de tiempo del minuto o segundo con excepción de las llamadas móviles que será al segundo."*

- **Se adecuará** el contenido del acápite 4.3 del numeral 3.1 del Capítulo III correspondiente a la Sección Específica de las Bases Integradas Definitivas, conforme a lo siguiente:

| |
|---|
| *"**4.3 SERVICIO DE LÍNEAS DE TELEFONÍA*** |

*(...)*
- *El Contratista deberá tener en cuenta que la tarificación y/o facturación deberá realizarse utilizando la unidad de medida de tiempo del minuto o segundo con excepción de las llamadas móviles que será al segundo.*

*(...)"*

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

**Cuestionamiento N° 4:** **Respecto al *"Servicio de acceso a internet sede central"***

El participante **GTD PERÚ S.A** cuestionó la absolución de las consultas y/u observaciones N° 147, N° 270 y N° 271 del pliego, alegando que las respuestas emitidas por el Comité de Selección introducen precisiones que direccionan la contratación hacia una solución de marca específica, contraviniendo lo dispuesto en el artículo 32.3 del Reglamento de la Ley de Contrataciones del Estado, al incorporar una funcionalidad técnica que únicamente sería implementada por un determinado fabricante. Finalmente, sostuvo que ello restringiría injustificadamente la pluralidad de postores al excluir otras soluciones técnicamente equivalentes que emplean mecanismos alternativos para cumplir con la misma finalidad de seguridad.

Por lo tanto, la pretensión del recurrente consiste en que la Entidad **modifique las características técnicas mínimas del servicio de acceso a internet, incorporando el texto *"y/o mecanismos de bloqueo"***.

**Pronunciamiento**

Sobre el particular, de la revisión del acápite 4.1 del numeral 3.1 del Capítulo III de la Sección Específica de las Bases de la convocatoria, se aprecia lo siguiente:

***"4.1 SERVICIO DE ACCESO A INTERNET SEDE CENTRAL***

*(...)*
*Las características técnicas mínimas del servicio de acceso a internet son:*
- ***La red del operador deberá tener implementada en su red (dentro del país) o a través del proveedor internacional de internet una solución de protección DDoS de propósito específico, que deberá proteger y asegurar el tráfico de la Entidad de 1000 Mbps, de manera que el tráfico malicioso sea inspeccionado a través de dicho equipamiento instalado en la red del operador.***

*(...)"*

(El subrayado y resaltado es agregado)

- **Respecto de la absolución de la consulta y/u observación N° 147 y N° 271:**

Sobre el particular, mediante las consultas y/u observaciones N° 147 y N° 271, se solicitó confirmar que la solución propuesta incluya un componente de hardware

dedicado con soporte para TLS 1.3 integrado en el equipo, precisando que dicho componente no debía representar un costo adicional para la Entidad ni ser ofrecido como una solución basada en software o mediante un proxy TLS 1.3.

- **Respecto de la absolución de la consulta y/u observación N° 270:**

Sobre el particular, mediante la consulta y/u observación N° 270, se solicitó confirmar que, ante un eventual ataque DDoS totalmente desconocido, la solución de protección propuesta sea capaz de detectar y mitigar dicho ataque mediante el análisis del comportamiento del tráfico y la creación automática de firmas en tiempo real.

Ante lo cual, frente a las referidas consultas y/u observaciones, el Comité de Selección precisó que, con el objetivo de garantizar la pluralidad de postores, la solución debe analizar el comportamiento del tráfico en tiempo real para mitigar ataques desconocidos y a su vez registrarlos mediante la creación automática de firma.

En consecuencia, de la revisión al acápite 4.1 del numeral 3.1 del Capítulo III, correspondientes a la Sección Específica de las Bases de la convocatoria, se aprecia que la Entidad implementó lo absuelto, conforme a lo siguiente:

> ***"4.1 <u>SERVICIO DE ACCESO A INTERNET SEDE CENTRAL</u>***
>
> *(...)*
> *Las características técnicas mínimas del servicio de acceso a internet son:*
> - *La red del operador deberá tener implementada en su red (dentro del país) o a través del proveedor internacional de internet una solución de protección DDoS de propósito específico, que deberá proteger y asegurar el tráfico de la Entidad de 1000 Mbps, de manera que el tráfico malicioso sea inspeccionado a través de dicho equipamiento instalado en la red del operador o asimismo se podrá considerar que la solución pueda incluir un componente de hardware con soporte TLS 1.3, integrado y sin depender de software adicional ni funciones tipo proxy por lo que se pide una solución especializada que no solo bloquee ataques conocidos, sino que también pueda detectar y frenar ataques nuevos o desconocidos de forma inmediata. **<u>Por eso, la solución debe analizar el comportamiento del tráfico en tiempo real para mitigar ataques desconocidos y a su vez registrarlos mediante la creación automática de firma.</u>***
>
> *(...)"*

(El subrayado y resaltado es agregado)

En relación con ello, y en atención al cuestionamiento formulado por el participante, mediante INFORME N° 000422-2025-OIT-OGETIC-SG/MC[13], la Entidad señaló lo siguiente:

> ***"(...)** la incorporación de este requerimiento técnico responde a una legítima **<u>mejora de los términos técnicos y no constituye una alteración intempestiva del procedimiento</u>** ni una afectación a la seguridad jurídica.*
>
> *Así mismo, la funcionalidad solicitada "...registro mediante la creación automática de firma"*

[13] Remitido mediante el Expediente N° 2025-0015783, de fecha 23 de mayo de 2025.

*constituye una característica funcional avanzada, alineada con los estándares internacionales de soluciones DDoS modernas, como las exigidas por el mercado para detectar ataques zero-day (día cero) o desconocidos, de igual forma esta capacidad* ***no es exclusiva de un único fabricante****, sino que es ofrecida por diversas soluciones del mercado en materia de ciberseguridad y mitigación de ataques DDoS, incluyendo aquellas que utilizan técnicas de análisis comportamental y machine learning.*

*(…) la exigencia de una solución que registre ataques mediante la creación automática de firma* ***no excluye la posibilidad de que los postores propongan tecnologías equivalentes****, siempre que estas cumplan con el objetivo funcional establecido: mitigar en tiempo real ataques desconocidos, registrar eventos de seguridad y generar insumos para protección futura, la expresión "…creación automática de firma" se refiere a una funcionalidad de respuesta ante amenazas basada en el aprendizaje del comportamiento de tráfico, una práctica común en soluciones de nueva generación y no limitada a una arquitectura o fabricante específico.*
*(...)"*

(El subrayado y resaltado es agregado)

Adicionalmente, mediante el INFORME N° 000022-2025-OIT-OGETIC-SG-HPS/MC[14], la Entidad indicó lo siguiente:

***"(...)*** *Al respecto en calidad de área usuaria se informa lo siguiente:*

*• Los ataques de día cero (o ataques desconocidos) son aquellos que explotan vulnerabilidades no documentadas o no mitigadas. Aunque las firmas de ataque se utilizan para detectar patrones conocidos de ataques DDoS, los ataques desconocidos requieren una detección basada en el comportamiento del tráfico de red y técnicas de análisis en tiempo real.*
*• Actualmente existen soluciones de protección DDoS que implementan análisis de tráfico en tiempo real y son capaces de detectar anomalías en patrones de tráfico y bloquear ataques desconocidos, sin necesidad de una firma predefinida. Estas soluciones generalmente utilizan tecnologías como machine learning (aprendizaje automático) para generar firmas automáticamente, lo que permite bloquear nuevos tipos de ataques antes de que sean completamente identificados.*
*• Las soluciones de protección DDoS que utilizan análisis de comportamiento y detección en tiempo real ya están disponibles en el mercado y se consideran eficaces para mitigar los ataques DDoS desconocidos o de día cero.* ***Por lo tanto, se debe permitir que la solución incluya funcionalidades de detección automática de tráfico malicioso, incluyendo la creación de firmas en tiempo real basadas en el comportamiento del tráfico****.*
*• La razón principal por la que se debe evitar considerar la frase "y a su vez registrarlos mediante la creación automática de firma y/o mecanismos de bloqueo" radica en la ambigüedad de los mecanismos de bloqueo, lo que puede generar problemas a la hora de interpretar los requisitos y de implementar una solución efectiva, dado que* ***el término "mecanismos de bloqueo" es demasiado vago y no describe con precisión qué tipo de medidas deben implementarse****. Puede interpretarse de diversas maneras, como bloquear IPs, limitar el ancho de banda, filtrar por patrones de tráfico, entre otros, lo que puede llevar a interpretaciones diversas y a una implementación inconsistente. Asimismo, si el "bloqueo" no se encuentra bien definido, puede llevar a situaciones donde el tráfico legítimo también se verá afectado, lo que puede comprometer la calidad de servicio. Una solución debe ser capaz de mitigar el ataque sin interrumpir el tráfico legítimo, lo cual requiere un enfoque más matizado que un simple "bloqueo".*
*(…) la ambigüedad de* ***"mecanismos de bloqueo" puede dar lugar a una interpretación***

[14] Remitido mediante el Expediente N° 2025-0023633, de fecha 10 de junio de 2025.

***flexible que no cubre adecuadamente las necesidades de una protección DDoS eficaz y especializada.*** *Para garantizar que la solución propuesta sea efectiva, es preferible centrarse en la detección en tiempo real y en la mitigación inteligente de ataques, sin depender de bloqueos genéricos o de fácil interpretación que puedan afectar la operación normal de la red. (...)"*

(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 a lo cuestionado por el recurrente, el Comité de Selección en coordinación con el área usuaria de la Entidad, siendo la responsable de la determinación de su requerimiento y, por ende, la mejor conocedora de sus necesidades, a través del citado informe, se ratifica en lo absuelto, argumentando que la inclusión del término *"y/o mecanismos de bloqueo"* resulta ambigua y susceptible de múltiples interpretaciones, lo que podría derivar en propuestas que no respondan adecuadamente a los requerimientos técnicos de una protección DDoS efectiva. Finalmente, se aclara que no se han incorporado nuevas obligaciones ni condiciones adicionales para los proveedores. Afirmación que se encuentra sujeta a rendición de cuentas.

Por lo tanto, considerando el análisis de los párrafos precedentes, y en tanto la pretensión del recurrente se encuentra orientada a que la Entidad modifique las características técnicas mínimas del servicio de acceso a internet, incorporando el texto *"y/o mecanismos de bloqueo"*; y en la medida que, a través del informe técnico correspondiente, la Entidad ha denegado el extremo solicitado por el recurrente, este Organismo Técnico Especializado ha decidido **NO ACOGER** el presente cuestionamiento.

**Cuestionamiento N° 5:** **Respecto a los *"Aspectos generales del Anexo A: Punto N° 2".***

El participante **AMERICA MOVIL PERU S.A.C.** cuestionó la absolución de las consultas y/u observaciones N° 175 del pliego, alegando que la respuesta brindada por el Comité de Selección vulnera el Principio de Libertad de Concurrencia; toda vez que los reportes de Gartner, aunque no mencionan marcas comerciales de forma explícita, son herramientas de análisis con fines comerciales que identifican productos específicos, lo cual restringe injustificadamente la participación de otros fabricantes no incluidos en dichos estudios. Asimismo, advirtió que el informe "Gartner Peer Insights Voice of the Customer for Data Loss Prevention" se basa en opiniones subjetivas de usuarios y no constituye una evaluación técnica formal, por lo que su utilización como criterio técnico en el proceso de selección resultaría improcedente y contrario a los principios de objetividad y pluralidad de postores.

Por lo tanto, la pretensión del recurrente consiste en que la Entidad **suprima la exigencia relativa a que la solución a utilizarse se encuentre reconocida como "líder" en el mercado por analistas de terceros como Gartner, acreditable mediante el informe de Gartner Peer Insights Voice of the Customer for Data Loss Prevention y/o fuentes equivalentes.**

**Pronunciamiento**

Sobre el particular, de la revisión del Anexo A: Punto N° 02 del numeral 3.1 del Capítulo III de la Sección Específica de las Bases de la convocatoria, se aprecia lo siguiente:

> *"**ANEXO A: PUNTO N° 02***
>
> ***SOLUCIÓN DE SEGURIDAD DE CORREO ELECTRÓNICO. SOLUCIÓN CLOUD***
>
> *(...)*
> ***Aspectos Generales***
> *(...)*
> ● *Debe brindar protección contra phishing, malware y contar con DLP, la tecnología de DLP que utilice la solución, debe ser líder reconocido en el mercado por Analistas de terceros como Gartner, durante el tiempo que estuvo activo.*
>
> ***(…)"***

Es así como, mediante consulta y/u observación N° 175 del pliego, se solicitó suprimir el requerimiento de que la tecnología de DLP que utilice la solución de seguridad de correo electrónico sea reconocida por analistas de terceros como Gartner; ante lo cual, el Comité de Selección precisó que con la finalidad de permitir la pluralidad de postores, se considerará como referencia el informe de Gartner Peer Insights Voice of the Customer for Data Loss Prevention y/o fuentes equivalentes.

En consecuencia, de la revisión del Anexo A: Punto N° 02 del numeral 3.1 del Capítulo III, correspondiente a la Sección Específica de las Bases Integradas, se aprecia que la Entidad implementó lo absuelto, conforme a lo siguiente:

> *"**ANEXO A: PUNTO N° 02***
>
> ***SOLUCIÓN DE SEGURIDAD DE CORREO ELECTRÓNICO. SOLUCIÓN CLOUD***
>
> *(...)*
> ***Aspectos Generales***
> *(...)*
> ● *Debe brindar protección contra phishing, malware y contar con DLP, la tecnología de DLP que utilice la solución, debe ser líder reconocido en el mercado por Analistas de terceros como Gartner, durante el tiempo que estuvo activo o también se considerará como referencia el informe de Gartner Peer Insights Voice of the Customer for Data Loss Prevention y/o fuentes equivalentes, durante el tiempo que estuvo activo.*

*(...)"*

En relación con ello, y en atención al cuestionamiento formulado por el participante, mediante INFORME N°000020-2025-OIT-OGETIC-SG-HPS/MC[15], la Entidad señaló lo siguiente:

*"(...)* ***se ha referido como marco de validación la inclusión histórica de dicha tecnología en análisis de terceros reconocidos, como Gartner Peer Insights Voice of the Customer u otras fuentes equivalentes, durante el tiempo en que dichos informes estuvieron activos****.*

*No obstante, a fin de mantener una participación plural, se ha dispuesto que:*
*• No será obligatorio que el proveedor figure actualmente como "líder", sino que se aceptará que haya sido reconocido como solución validada en reportes de analistas independientes mientras estos estuvieron disponibles.*
*• Asimismo, se aceptarán fuentes equivalentes que permitan sustentar la validación de la tecnología DLP ofertada, sin restringir su participación a listados comerciales únicos.*
*(...)"*

(El subrayado y resaltado es agregado)

Adicionalmente, mediante el INFORME N° 000022-2025-OIT-OGETIC-SG-HPS/MC[16], la Entidad indicó lo siguiente:

***"(...)*** *Al respecto en calidad de área usuaria se informa lo siguiente:*

*• Los fabricantes mejor valorados publican actualizaciones frecuentes y ofrecen redes de asistencia global, esto reduce tiempos de inactividad, urgencias de última hora y gastos extra en consultoría o parches, además,* ***plataformas como Gartner Peer Insights recogen reseñas verificadas de clientes actuales, por lo que saber cómo les va a otras entidades con el producto ayuda a anticipar posibles obstáculos y a confirmar beneficios****.*
*• Asimismo, los informes de analistas se actualizan cada 12 a 18 meses, por lo que* ***exigir reconocimiento "mientras estuvo activo" garantiza que la solución seguirá siendo relevante y segura durante toda la vigencia del contrato*** *por lo que pedir el respaldo de analistas externos (o fuentes equivalentes) asegura que la solución elegida ya esté probada, sea comparable de forma justa, tenga buen soporte, cuente con usuarios satisfechos y se mantenga actualizada, dado que no se está limitando al cuadrante de Gartner únicamente o algún informe en particular y cuenta con pluralidad de opciones.*
*(...)"*

(El subrayado y resaltado es agregado)

Ahora bien, en atención a lo cuestionado por el recurrente, el Comité de Selección en coordinación con el área usuaria de la Entidad, siendo la responsable de la determinación de su requerimiento, a través del citado informe, ratificó la exigencia relativa a que la solución a utilizarse se encuentre reconocida como "líder" en el mercado por analistas de terceros como Gartner, acreditable mediante un informe de Gartner Peer Insights Voice of the Customer for Data Loss Prevention y/o fuentes equivalentes, durante el tiempo que estuvo activo; argumentando que los fabricantes mejor posicionados en el mercado suelen publicar actualizaciones constantes y

[15] Remitido mediante el Expediente N° 2025-0017186, de fecha 27 de mayo de 2025.
[16] Remitido mediante el Expediente N° 2025-0023633, de fecha 10 de junio de 2025.

brindar soporte técnico a nivel global, lo cual permite reducir tiempos de inactividad, contingencias imprevistas y costos adicionales. En ese sentido, el respaldo mediante informes de analistas especializados o fuentes equivalentes resulta valioso, ya que proporciona evidencia sobre la eficacia, soporte, satisfacción de usuarios y vigencia de la solución ofertada. Dado que dichos informes se actualizan periódicamente, permitir su reconocimiento *"mientras estuvo activo"* garantiza la relevancia y seguridad del producto durante la vigencia del contrato.

Sin perjuicio de ello, considerando lo expuesto en el informe de la Entidad, es preciso señalar que, requerir que la tecnología de DLP que utilice la solución, debe haber tenido la categoría de "líder", reconocida en el mercado por analistas de terceros, como Gartner, acreditado con el informe de Gartner Peer Insights Voice of the Customer for Data Loss Prevention y/o fuentes equivalentes, *"durante el tiempo que estuvo activo"*, limita la participación de potenciales postores, toda vez que dicho cuadrante "líder" está basado en informes de investigación publicados por la empresa "Gartner", considerando que los resultados de dicha investigación se basan en lo que se denomina "cuadrante mágico"; por lo que, ello se ha clasificado en cuatro (4) categorías, denominada una de ellas como los "líderes", y en dicha categoría se encuentra un grupo de empresas con los más altos puntajes.

Por lo que, la mencionada exigencia no resultaría razonable, en la medida que se estaría vulnerando el Principio de Libre Competencia y Concurrencia, limitando la participación de potenciales postores que no hayan sido considerados dentro del referido cuadrante, en la categoría de "líder".

Por lo tanto, considerando el análisis de los párrafos precedentes, y en tanto la pretensión del recurrente se encuentra orientada a que la Entidad suprima la exigencia relativa a que la solución a utilizarse se encuentre reconocida como "líder" en el mercado por analisis de terceros como Gartner, acreditable mediante el informe de Gartner Peer Insights Voice of the Customer for Data Loss Prevention y/o fuentes equivalentes; y en la medida que, el extremo cuestionado estaría limitando la participación de potenciales postores, este Organismo Técnico Especializado ha decidido **ACOGER** el presente cuestionamiento. Por lo que, con ocasión de la integración definitiva de las Bases, se implementará la siguiente disposición:

- **Se dejará sin efecto** lo absuelto en la consulta y/u observación N° 175 del pliego.

- **Se adecuará** el contenido del Anexo A: Punto N° 02 del numeral 3.1 del Capítulo III correspondiente a la Sección Específica de las Bases Integradas Definitivas, conforme a lo siguiente:

> *"**ANEXO A: PUNTO N° 02***
>
> ***SOLUCIÓN DE SEGURIDAD DE CORREO ELECTRÓNICO.***
> ***SOLUCIÓN CLOUD***
>
> *(...)*
> ***Aspectos Generales***

*(...)*

- *Debe brindar protección contra phishing, malware y contar con DLP, ~~la tecnología de DLP que utilice la solución, debe ser líder reconocido en el mercado por Analistas de terceros como Gartner, durante el tiempo que estuvo activo o también se considerará como referencia el informe de Gartner Peer Insights Voice of the Customer for Data Loss Prevention y/o fuentes equivalentes, durante el tiempo que estuvo activo.~~*

*(...)"*

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

**<u>Cuestionamiento N° 6</u>:** **Respecto a la *"Gestión y reporte del Anexo A: Punto N° 2".***

El participante **AMÉRICA MÓVIL PERÚ S.A.C.** cuestionó la absolución de la consulta y/u observación Nº 182 del pliego, alegando que la respuesta emitida por el Comité de Selección vulneraría el Principio de Libertad de Concurrencia, dado que la exigencia de entregar reportes cifrados y protegidos con contraseña únicamente para la solución de seguridad de correo electrónico, carece de justificación técnica objetiva, toda vez que, existen otras soluciones dentro del servicio, como firewalls, WAF o EDR, que también manejan información sensible, pero no están sujetas a la misma condición. En ese sentido, advirtió que esta exigencia podría evidenciar un posible direccionamiento hacia una marca específica, restringiendo injustificadamente la libre participación de postores y limitando la posibilidad de que la Entidad acceda a un mayor número de alternativas tecnológicas en el marco del presente procedimiento de contratación.

Por lo tanto, la pretensión del recurrente consiste en que la Entidad **<u>modifique el requerimiento para que la entrega de informes en formato encriptado y protegido con contraseña sea considerada como una característica opcional y no obligatoria.</u>**

**Pronunciamiento**

Sobre el particular, de la revisión del Anexo A: Punto N° 02 del numeral 3.1 del Capítulo III de la Sección Específica de las Bases de la convocatoria, se aprecia lo siguiente:

*"**<u>ANEXO A: PUNTO N° 02</u>***

***SOLUCIÓN DE SEGURIDAD DE CORREO ELECTRÓNICO.***
***SOLUCIÓN CLOUD***

*(...)*
***Gestión y Reporte***
***(...)***

- *Debe permitir programar informes para la entrega en una determinada frecuencia (diaria,*

*semanal, mensual). Los informes pueden exportarse en formato PDF y CSV. Además, debe poder enviar el informe en formato encriptado y protegido por password.*
***(…)"***

Es así como, mediante consulta y/u observación N° 182 del pliego, se solicitó confirmar que la entrega del informe en formato encriptado y protegido por password será opcional. Ante lo cual, el Comité de Selección señaló que, dada la necesidad de contar con los mecanismos de seguridad establecidos, se requiere contar con lo estipulado en los Términos de Referencia.

En relación con ello, y en atención al cuestionamiento formulado por el participante, mediante INFORME N° 000020-2025-OIT-OGETIC-SG-HPS/MC[17], la Entidad señaló lo siguiente:

*"(...)*
*El requerimiento de enviar informes automatizados en formato encriptado y con contraseña* ***responde a criterios funcionales de seguridad de la información, y no a una marca específica.*** *Actualmente, múltiples soluciones comerciales de distintos fabricantes ofrecen esta funcionalidad, por lo que* ***no constituye una limitación tecnológica ni una funcionalidad exclusiva de un único proveedor.***

*Esta medida de seguridad* ***no es una característica adicional*** *sino parte de las buenas prácticas mínimas en entornos de seguridad perimetral. La entrega de informes encriptados y protegidos por contraseña permite:*

*• Prevenir accesos no autorizados al contenido del informe.*
*• Asegurar la confidencialidad e integridad de datos sensibles (como alertas, registros de amenazas, logs de firewall, etc.).*
*• Cumplir con las exigencias del Decreto Supremo N.º 050-2021-PCM, sobre el Esquema Nacional de Seguridad Digital, que exige mecanismos de protección de la información en tránsito y almacenamiento.*

*De igual forma, el argumento de una presunta "barrera de acceso" no cuenta con sustento dado que:*

*• La funcionalidad es estándar en la mayoría de soluciones de seguridad modernas.*
*• No requiere hardware adicional ni representa un sobrecosto significativo.*
*• No impide la participación de postores con soluciones robustas que cumplan con la norma técnica.*

*En ese sentido, y en coherencia con las decisiones adoptadas en los cuestionamientos previos,* ***se ratifica el requerimiento técnico en los términos indicados.***
*(...)"*

(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

[17] Remitido mediante el Expediente N° 2025-0015186, de fecha 27 de mayo de 2025.

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 la exigencia de que los informes sean remitidos en formato encriptado y protegidos con contraseña. Esta condición responde a criterios funcionales orientados a garantizar la seguridad de la información, y no implica la referencia a una marca específica. Cabe señalar que, dicha funcionalidad está disponible en diversas soluciones comerciales ofrecidas por múltiples fabricantes, por lo que no constituye una restricción tecnológica ni una característica exclusiva de un determinado proveedor.

Asimismo, agregó que la exigencia de remitir los informes en formato encriptado y protegidos con contraseña no constituye una característica adicional, sino que responde a prácticas mínimas recomendadas en entornos de seguridad perimetral. Esta medida tiene como finalidad prevenir accesos no autorizados, garantizar la confidencialidad e integridad de información sensible —como registros de amenazas, alertas o logs de firewall— y, además, asegurar el cumplimiento de lo dispuesto en el Decreto Supremo N.º 050-2021-PCM, que aprueba el Esquema Nacional de Seguridad Digital y establece la obligación de implementar mecanismos de protección de la información tanto en tránsito como en almacenamiento.

Por otro lado, en relación con lo manifestado por el participante, respecto a que la exigencia en mención constituye una barrera de acceso, la Entidad precisó que dicho argumento carece de sustento técnico, toda vez que la funcionalidad requerida es estándar en la mayoría de soluciones de seguridad actuales, no implica la necesidad de equipamiento adicional ni representa un sobrecosto relevante, y tampoco limita la participación de postores que cuenten con soluciones sólidas y compatibles con la normativa técnica vigente.

De otro lado, es preciso indicar que, de la revisión del numeral 4.2 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 se debe poder enviar el informe en formato encriptado y protegido por password.

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 modifique el requerimiento para que la entrega de informes en formato encriptado y protegido con contraseña sea considerada como una característica opcional y no obligatoria; 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° 7:** | **Respecto a las *"Características físicas y rendimiento del Anexo A: Punto N° 4".*** |

El participante **AMÉRICA MÓVIL PERÚ S.A.C.** cuestionó la absolución de la consulta y/u observación Nº 193 del pliego, alegando una presunta vulneración al Principio de Transparencia, al considerar que existe una contradicción técnica en el requerimiento. Señala que, por un lado, se establece que el equipo debe soportar 90,000 conexiones concurrentes en HTTPS —lo que representa su capacidad máxima—, mientras que, por otro lado, se exige que el equipo maneje 125,000 conexiones por segundo en capa HTTPS —es decir, nuevas sesiones por segundo—, lo cual, a su criterio, resulta técnicamente incongruente, ya que considera que el número de conexiones por segundo no podría superar la cantidad de conexiones concurrentes que soporta el equipo, por tratarse de una capacidad límite que no puede ser excedida bajo ningún supuesto lógico o técnico.

Por lo tanto, la pretensión del recurrente consiste en que la Entidad **(i) deje sin efecto la contradicción e incongruencia advertida, y (ii) reduzca a un mínimo de 30,000 conexiones por segundo a nivel de capa de transporte HTTPS.**

**Pronunciamiento**

Sobre el particular, de la revisión del Anexo A: Punto N° 04 del numeral 3.1 del Capítulo III de la Sección Específica de las Bases de la convocatoria, se aprecia lo siguiente:

> *"**ANEXO A: PUNTO N° 04***
>
> ***SERVICIO DE SEGURIDAD PERIMETRAL GESTIONADA EQUIPO DE SEGURIDAD PARA APLICACIONES WEB (01)***
>
> ***CARACTERÍSTICAS FÍSICAS Y RENDIMIENTO***
> ***(...)***
> - *En caso de ser Appliance cada equipo debe cumplir con las siguientes características:*
>   *(...)*
>   *o Soportara mínimamente 90,000 de conexiones concurrentes en HTTPS.*
>   *o Deberá soportar mínimamente conexiones de 125 mil conexiones por segundo a nivel de capa de transporte HTTPS Soportar mínimamente 2500 transacciones por segundo SSL (RSA2K) y Soportar 2100 transacciones por segundo SSL (EC P-256 o ECDH).*
>
> ***(…)"***

Es así como, mediante consulta y/u observación N° 193 del pliego, se solicitó confirmar que el equipo debe tener una capacidad al menos de la tercera parte de la concurrencia máxima soportada, es decir, que debe soportar al menos 30,000 conexiones por segundo a nivel de capa de transporte HTTPS, o confirmar que es un error tipográfico. Ante lo cual, el Comité de Selección señaló que, con la finalidad de promover la pluralidad de postores, se considerará como mínimo lo estipulado en los Términos de Referencia.

En relación con ello, y en atención al cuestionamiento formulado por el participante, mediante INFORME N° 000020-2025-OIT-OGETIC-SG-HPS/MC[18], la Entidad señaló lo siguiente:

> *"(...)*
> *En atención al requerimiento técnico referido al soporte de 90,000 conexiones concurrentes en HTTPS y de 125,000 conexiones por segundo (CPS) a nivel de capa de transporte, se aclara que* ***no existe contradicción entre ambas especificaciones.***
>
> *Como ya ha sido precisado mediante la absolución de consultas previas,* ***dichas capacidades corresponden a métricas distintas del comportamiento transaccional del equipo****:*
>
> *• La concurrencia hace referencia a sesiones TCP activas simultáneas sobre tráfico HTTPS, dimensionadas en términos de capacidad sostenida.*
> *• Las conexiones por segundo (CPS) corresponden a la tasa de establecimiento de nuevas sesiones TCP, como parte del rendimiento esperado del dispositivo en la capa de transporte (L4).*
>
> *Dada su naturaleza transitoria,* ***el volumen de conexiones por segundo puede ser superior al número de sesiones concurrentes activas, sin implicar una contradicción técnica.*** *Este comportamiento es común en arquitecturas que procesan tráfico con alta rotación de sesiones.*
>
> *Por tanto,* ***se ratifican ambos parámetros*** *como técnicamente consistentes y complementarios para validar la capacidad del equipo, conforme a los objetivos de seguridad, visibilidad y balanceo requeridos en la solución.*
> *(...)"*

(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, mediante el citado informe, ratificó su requerimiento, manteniendo la exigencia relativa a que, en caso de ser Appliance, cada equipo soportará mínimamente 90,000 de conexiones concurrentes en HTTPS, y deberá soportar mínimamente conexiones de 125,000 conexiones por segundo a nivel de capa de transporte HTTPS, así como soportar mínimamente 2500 transacciones por segundo SSL (RSA2K) y 2100 transacciones por segundo SSL (EC P-256 o ECDH); argumentando que no existe contradicción entre ambas especificaciones.

Asimismo, agregó que los extremos cuestionados como contradictorios por el recurrente, responden a métricas distintas, relacionadas con el desempeño transaccional del equipo. En ese sentido, la concurrencia alude al número de sesiones

[18] Remitido mediante el Expediente N° 2025-0015186, de fecha 27 de mayo de 2025.

TCP activas simultáneas sobre tráfico HTTPS, calculadas como parte de su capacidad sostenida, mientras que las conexiones por segundo (CPS) hacen referencia a la cantidad de nuevas sesiones TCP que el dispositivo puede establecer por unidad de tiempo, como parte de su rendimiento en la capa de transporte (L4). Por tanto, debido a la naturaleza transitoria de las conexiones por segundo, es técnicamente válido que dicho valor supere al número de sesiones concurrentes, sin que ello represente una inconsistencia. Este comportamiento es habitual en soluciones diseñadas para manejar entornos con alta rotación de sesiones. Afirmación que se encuentra sujeta a rendición de cuentas.

De otro lado, es preciso indicar que, de la revisión del numeral 4.2 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 incluyó el extremo cuestionado.

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 (i) deje sin efecto la contradicción e incongruencia advertida, y (ii) reduzca a un mínimo de 30,000 conexiones por segundo a nivel de capa de transporte HTTPS; y en la medida que, mediante su informe, la Entidad ratificó su requerimiento, así como los argumentos por los cuales no acepta los extremos solicitados por el recurrente; este Organismo Técnico Especializado ha decidido **NO ACOGER** el presente cuestionamiento.

**Cuestionamiento N° 8:** **Respecto a los *"Documentos para la admisión de ofertas".***

El participante **GTD PERÚ S.A.** cuestionó la absolución de la consulta y/u observación N° 316 del pliego, alegando que el Comité de Selección, sin respaldo técnico ni normativo, dispuso como requisito para la admisión de la oferta la presentación de un listado de los componentes que integrarán la solución propuesta, así como una matriz que detalle el cumplimiento técnico de cada servicio solicitado, acompañada de datasheets, manuales, fichas técnicas u otros documentos análogos. Asimismo, indicó que, en caso de que algunos aspectos no puedan ser respaldados con información pública, estos podrían ser acreditados mediante carta del fabricante y/o impresión de un enlace. El participante también precisó que dicha documentación deberá presentarse al momento de la suscripción del contrato y observó que, pese a requerirse en la etapa de presentación de ofertas, tales exigencias no fueron incluidas expresamente en el numeral correspondiente de las Bases Integradas.

Por lo tanto, la pretensión del recurrente consiste en que la Entidad **deje sin efecto la respuesta emitida en la consulta y/u observación Nº 316 del pliego, y en consecuencia suprima el extremo incorporado.**

**Pronunciamiento**

Sobre el particular, de la revisión del pliego absolutorio se aprecia lo siguiente:

| Consulta/Observación | Absolución |
|---|---|

| | |
|---|---|
| *"Sírvanse a la entidad a confirmar si el postor deberá presentar, como parte de su propuesta técnica, un listado detallado de todos los componentes que conforman la solución ofertada, indicando modelo, descripción, cantidad y función de cada uno. Esto con la finalidad de permitir una evaluación clara y completa de la propuesta, así como facilitar a la entidad asegurar que el postor está ofertando la solución requerida"* | *"(...) a fin de validar el cumplimiento técnico de la solución ofertada, el Postor deberá presentar un listado de los componentes que formarán parte de la solución ofertada y una matriz para el cumplimiento técnico punto por punto de cada servicio solicitado, adjuntando adicionalmente los datasheets, manuales, ficha técnica u otro documento similar, adicionalmente los puntos que no puedan ser sustentados con información pública podrán ser sustentados con carta del fabricante y/o link impreso"* |

En consecuencia, de la revisión del acápite 4 del numeral 3.1 del Capítulo III, correspondiente a la Sección Específica de las Bases de la convocatoria, se aprecia que la Entidad implementó lo absuelto, conforme a lo siguiente:

> ***"4. <u>DESCRIPCIÓN DE LOS SERVICIOS REQUERIDOS</u>***
>
> *(...)*
> - ***<u>El Postor deberá presentar para la admisión de ofertas un listado de los componentes que formarán parte de la solución ofertada y una matriz para el cumplimiento técnico punto por punto de cada servicio solicitado, adjuntando adicionalmente los datasheets, manuales, ficha técnica u otro documento similar, adicionalmente los puntos que no puedan ser sustentados con información pública podrán ser sustentados con carta del fabricante y/o link impreso.</u>***
>
> *(...)"*

(El subrayado y resaltado es agregado)

En relación con ello, y en atención al cuestionamiento formulado por el participante, mediante INFORME N° 000422-2025-OIT-OGETIC-SG/MC[19], la Entidad señaló lo siguiente:

> ***"(...)** Cabe precisar que el objeto de la contratación incluye componentes tecnológicos de seguridad informática críticos, como por ejemplo equipos de seguridad firewall de siguiente generación, cuyo funcionamiento y cumplimiento técnico **<u>no puede verificarse únicamente mediante una declaración genérica o una promesa de cumplimiento</u>** y el nivel de especificación requerido se enmarca en el principio de idoneidad de la oferta y permite una evaluación objetiva, transparente y verificable.*
> *(...)"*

(El subrayado y resaltado es agregado)

Adicionalmente, mediante el INFORME N° 000022-2025-OIT-OGETIC-SG-HPS/MC[20], la Entidad indicó lo siguiente:

> ***"(...)** Al respecto en calidad de área usuaria se informa lo siguiente:*
>
> *• El objetivo principal de este requerimiento es garantizar que el comité de evaluación pueda*

[19] Remitido mediante el Expediente N° 2025-0015783, de fecha 23 de mayo de 2025.
[20] Remitido mediante el Expediente N° 2025-0023633, de fecha 10 de junio de 2025.

*realizar una evaluación clara, precisa y completa de las propuestas recibidas, **el listado de componentes y la matriz de cumplimiento técnico permiten a la entidad asegurarse de que el postor ofrece una solución que cumple con los requisitos técnicos establecidos** en las bases del proceso de contratación ya que esto también contribuye a una evaluación objetiva y transparente.*

*• La solicitud de un listado detallado de los componentes, junto con la matriz de cumplimiento técnico, **es una práctica común en procesos de contratación pública para la adquisición de soluciones tecnológicas complejas**, dado que permite a la entidad verificar que cada parte del producto o servicio ofertado es adecuado y cumple con las especificaciones requeridas*

*• Cabe precisar que, el requerimiento de datos técnicos (datasheets, manuales, fichas técnicas, etc.) **garantiza que el postor está ofreciendo los componentes adecuado**s y esto se alinea con el principio de transparencia en los procedimientos de contratación, que busca evitar cualquier duda sobre el cumplimiento de los requisitos establecidos.*

*(...)*

*• **No restringiría la participación de postores potenciales**, sin embargo, la entidad debe asegurarse de que las ofertas cumplen con todos los requisitos técnicos previos a la adjudicación del contrato y solicitar esta información en el momento de la admisión permite realizar una evaluación objetiva y completa, que es esencial para garantizar que las soluciones ofertadas son adecuadas para el contrato (...)"*

(El subrayado y resaltado es agregado)

Ahora bien, en atención a lo cuestionado por el recurrente, el Comité de Selección en coordinación con el área usuaria de la Entidad, siendo la responsable de la determinación de su requerimiento, a través del citado informe, ratificó la exigencia de presentar, en la etapa de admisión de ofertas, el listado de componentes, así como la matriz de cumplimiento técnico y la documentación de soporte (como datasheets, manuales o fichas técnicas), toda vez que el objeto contractual involucra componentes tecnológicos críticos en materia de seguridad informática que no pueden ser validados mediante declaraciones generales. Esta información resulta indispensable para que el comité evaluador pueda realizar una verificación técnica precisa, clara y completa del cumplimiento de los requisitos establecidos en las Bases, asegurando así una evaluación objetiva, transparente y alineada con prácticas comunes en procesos de adquisición de soluciones tecnológicas complejas.

Sin perjuicio de ello, considerando lo expuesto en el informe de la Entidad, en concordancia con lo establecido en las Bases Estándar, 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 las Especificaciones Técnicas, 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 un listado de los componentes que conformarán la solución ofertada, junto con una matriz de cumplimiento técnico detallada por cada servicio requerido, adjuntando además datasheets, manuales, fichas técnicas u otros documentos equivalentes. No obstante, dicha exigencia no se encuentra alineada con lo dispuesto en las Bases Estándar aplicables; máxime cuando éstas prevén que no se puede exigir la acreditación documental de equipamiento. Por tal motivo, y considerando la relevancia de dicha

documentación para la Entidad, se ha dispuesto trasladar su presentación a la etapa de perfeccionamiento del contrato.

Por lo tanto, considerando el análisis de los párrafos precedentes, y en tanto la pretensión del recurrente se encuentra orientada a que la Entidad deje sin efecto la respuesta emitida en la consulta y/u observación Nº 316 del pliego, y en consecuencia suprima el extremo incorporado; y en la medida que, el extremo cuestionado no resulta acorde a lo establecido en las Bases Estándar aplicables, este Organismo Técnico Especializado ha decidido **ACOGER** el presente cuestionamiento. Por lo que, con ocasión de la integración definitiva de las Bases, se implementará la siguiente disposición:

- **Se dejará sin efecto** lo absuelto en la consulta y/u observación N° 316 del pliego.

- **Se adecuará** el contenido del acápite 4 del numeral 3.1 del Capítulo III correspondiente a la Sección Específica de las Bases Integradas Definitivas, conforme a lo siguiente:

> ***"4. DESCRIPCIÓN DE LOS SERVICIOS REQUERIDOS***
>
> *(...)*
> - *El Postor deberá presentar para ~~la admisión de ofertas~~ el perfeccionamiento de contrato un listado de los componentes que formarán parte de la solución ofertada y una matriz para el cumplimiento técnico punto por punto de cada servicio solicitado, adjuntando adicionalmente los datasheets, manuales, ficha técnica u otro documento similar, adicionalmente los puntos que no puedan ser sustentados con información pública podrán ser sustentados con carta del fabricante y/o link impreso.*

*(...)"*

- **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:*
> *(...)*
> - *El Postor deberá presentar un listado de los componentes que formarán parte de la solución ofertada y una matriz para el cumplimiento técnico punto por punto de cada servicio solicitado, adjuntando adicionalmente los datasheets, manuales, ficha técnica u otro documento similar, adicionalmente los puntos que no puedan ser sustentados con información pública podrán ser sustentados con carta del fabricante y/o link impreso.*

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

**Cuestionamiento N° 9:** **Respecto al *"Servicio de interconexión de datos con las 12 sedes de Lima y 22 sedes en provincias a nivel nacional".***

El participante **AMÉRICA MÓVIL PERÚ S.A.C.** cuestionó la absolución de la consulta y/u observación Nº 327 del pliego, alegando que la respuesta emitida por el Comité de Selección vulneraría el Principio de Libertad de Concurrencia, en la medida que las Bases de la convocatoria no establecen, en ninguno de sus extremos, condición o requisito relacionado con el local o locales donde deben alojarse los servidores DNS. Pues, el único requerimiento consignado era la redundancia del servicio DNS, exigencia que, por sí sola, garantiza el cumplimiento del servicio. No obstante, en la absolución realizada, y sin que se haya brindado una justificación técnica o normativa, el Comité de Selección incorporó una condición adicional no prevista en las Bases, al señalar que, al menos un local en el que se encuentre uno de los servidores DNS, deberá encontrarse en un Data Center propio o tercerizado que alojará el DNS de propiedad del Contratista, y que dicho Data Center deberá estar certificado en ANSI/TIA y/o EPIS de Diseño y/o Construcción y/u Operación.

Por lo tanto, la pretensión del recurrente consiste en que la Entidad **confirme que no será exigible contar con el certificado en ANSI/TIA y/o EPIS de Diseño y/o Construcción y/u Operación.**

**Pronunciamiento**

Sobre el particular, de la revisión del acápite 4.1 y 4.4 del numeral 3.1 del Capítulo III de la Sección Específica de las Bases de la convocatoria, se aprecia lo siguiente:

| | |
|---|---|
| *"4.1 SERVICIO DE ACCESO A INTERNET SEDE CENTRAL*<br><br>*(...)*<br>● ***Redundancia en los servicios DNS en el mismo local o locales diferentes.***<br><br>*(...)"* | *"4.4 SERVICIO DE INTERCONEXIÓN DE DATOS CON LAS 12 SEDES DE LIMA Y 22 SEDES EN PROVINCIAS A NIVEL NACIONAL*<br><br>*(...)*<br>● ***El Contratista deberá poseer servidores DNS redundantes y distribuidos en locales distintos.***<br>*(...)"* |

(El subrayado y resaltado es agregado)

Es así que, mediante la consulta y/u observación N° 327 del pliego, se solicitó confirmar que al menos uno de los locales en los que se encuentre instalado un servidor DNS deberá ubicarse en un Data Center, ya sea propio o tercerizado, que aloje dicho servicio y sea de propiedad del Contratista. Asimismo, se requirió que dicho Data Center cuente con certificación ANSI/TIA y/o EPIS de Diseño y/o Construcción y/u Operación. Ante lo cual, el Comité de Selección acogió la solicitud presentada por el participante.

En consecuencia, de la revisión del acápite 4.4 del numeral 3.1 del Capítulo III, correspondientes a la Sección Específica de las Bases de la convocatoria, se aprecia que la Entidad implementó lo absuelto, conforme a lo siguiente:

> ***"4.4 <u>SERVICIO DE INTERCONEXIÓN DE DATOS CON LAS 12 SEDES DE LIMA Y 22 SEDES EN PROVINCIAS A NIVEL NACIONAL</u>***
>
> *(...)*
> - *El Contratista deberá poseer servidores DNS redundantes y distribuidos en locales distintos **<u>y/o al menos un local en el que se encuentre uno de los servidores DNS, deberá encontrarse en un Data Center propio o tercerizado que alojará el DNS de propiedad del contratista. Dicho Data Center deberá estar certificado en ANSI/TIA y/o EPIS de Diseño y/o Construcción y/o Operación</u>***

*(...)"*

(El subrayado y resaltado es agregado)

En relación con ello, y en atención al cuestionamiento formulado por el participante, mediante INFORME N° 000020-2025-OIT-OGETIC-SG-HPS/MC[21], la Entidad señaló lo siguiente:

> ***"(...)** la incorporación de este requerimiento técnico responde a una legítima **<u>mejora de los términos técnicos y no constituye una alteración intempestiva del procedimiento.</u>***
>
> *Asimismo, **<u>no se han realizado modificaciones a fin de restringir el presente concurso público ni a los proveedores que participaron en la indagación de mercado</u>**, cabe precisar que la empresa AMERICA MOVIL PERU S.A.C. no se presentó en dicho estudio de mercado, por lo que en la presente consulta se amplió la característica con una expresión de adición que se utiliza para indicar la posibilidad de elegir entre la suma o la alternativa de opciones mencionando que ..."y/o que al menos un local en el que se encuentre uno de los servidores DNS, deberá encontrarse en un Data Center propio o tercerizado que alojará el DNS de propiedad del contratista. Dicho Data Center deberá estar certificado en ANSI/TIA y/o EPIS de Diseño y/o Construcción y/o Operación."*
> *(...)"*

(El subrayado y resaltado es agregado)

Adicionalmente, mediante el INFORME N° 000022-2025-OIT-OGETIC-SG-HPS/MC[22], la Entidad indicó lo siguiente:

> ***"(...)** Al respecto en calidad de área usuaria se informa lo siguiente:*
>
> *• La característica inicial de los términos de referencia mencionaba lo siguiente: "El Contratista deberá poseer servidores DNS redundantes y distribuidos en locales distintos."*
> *• Luego de la absolución de consultas y observaciones se apertura la característica adicionando: "...y/o que al menos un local en el que se encuentre uno de los servidores DNS, deberá encontrarse en un Data Center propio o tercerizado que alojará el DNS de propiedad del contratista. Dicho Data Center deberá estar certificado en ANSI/TIA y/o EPIS de Diseño y/o Construcción y/o Operación".*
> *• Por ende, se aprecia **<u>que no se ha restringido la participación de postores</u>**, sino que además*

[21] Remitido mediante el Expediente N° 2025-0015186, de fecha 27 de mayo de 2025.
[22] Remitido mediante el Expediente N° 2025-0023633, de fecha 10 de junio de 2025.

*se ha aperturado para aumentar dicha pluralidad a más postores potenciales.*
*(...)*
*• Los servicios DNS son esenciales para el funcionamiento de la aplicaciones y comunicaciones de las organizaciones, la disponibilidad continua del servicio es crucial y los Data Centers certificados en estándares de ANSI/TIA (Institute of Electrical and Electronics Engineers - Telecommunications Industry Association) y EPIS (International Standards for the Performance of Data Centers) garantizan que el alojamiento y operación de los servidores DNS cumple con los más altos estándares internacionales de diseño, construcción y operación.*
*• La Certificación ANSI/TIA es un estándar de calidad reconocido globalmente para el diseño, construcción y operación de infraestructuras de telecomunicaciones y data centers, los Data Centers certificados ANSI/TIA aseguran una estructura fiable, con estándares de redundancia, capacidad eléctrica, protección ante desastres y gestión eficiente de la infraestructura tecnológica, lo que asegura la continuidad del servicio DNS. Esto es fundamental para garantizar que los servidores DNS funcionen de manera estable y sin interrupciones.*
*• Al igual que ANSI/TIA, la certificación EPIS asegura que el Data Center cumple con normas internacionales de operación y tiene un plan robusto de contingencia y redundancia de equipos, lo que minimiza riesgos de fallos en el servicio.*
*• Por lo tanto, la exigencia de contar con un Data Center certificado en ANSI/TIA y/o EPIS no constituye una barrera para la participación de proveedores, ya que existen múltiples opciones tanto en Data Centers propios como tercerizados que cumplen con estos estándares. Además, no es necesario que el Data Center sea propio, sino que el contratista puede optar por utilizar un Data Center tercerizado, lo que amplía las posibilidades de cumplir con este requisito sin generar restricciones.*
*(...)*
*• Por último, se precisa que **no se han pedido nuevas obligaciones y/o condiciones para los proveedores** por lo que el párrafo final se mantendría (...).”*

(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 a lo cuestionado por el recurrente, el Comité de Selección en coordinación con el área usuaria de la Entidad, siendo la responsable de la determinación de su requerimiento y, por ende, la mejor conocedora de sus necesidades, a través del citado informe, ratificó su requerimiento, argumentando que los servicios DNS son fundamentales para el correcto funcionamiento de las aplicaciones y las comunicaciones dentro de una organización. En ese sentido, la utilización de Data Centers que cuenten con certificaciones conforme a los estándares ANSI/TIA (Institute of Electrical and Electronics Engineers - Telecommunications Industry Association) y EPIS (International Standards for the Performance of Data Centers) garantiza que la infraestructura destinada al alojamiento y operación de los servidores DNS, cumple con los más altos niveles de exigencia en términos de diseño, construcción y operación, alineándose con las mejores prácticas reconocidas a nivel internacional.

Por lo tanto, considerando el análisis de los párrafos precedentes, y en tanto la pretensión del recurrente se encuentra orientada a que la Entidad confirme que no será exigible contar con el certificado en ANSI/TIA y/o EPIS de Diseño y/o Construcción y/u Operación; y en la medida que, a través del informe técnico correspondiente, la Entidad ha denegado el extremo solicitado por el recurrente, este Organismo Técnico Especializado ha decidido **NO ACOGER** el presente cuestionamiento.

**Cuestionamiento N° 10:** **Respecto a las *"Características técnicas del Anexo A: Punto 01".***

El participante **AMERICA MOVIL PERU S.A.C.** cuestionó la absolución de la consulta y/u observación N° 362 del pliego, alegando que la respuesta emitida por el Comité de Selección vulneraría el Principio de Libertad de Concurrencia, al introducir un nuevo requerimiento técnico no contemplado originalmente en los términos de referencia, referido a las características del sistema operativo y/o firmware del equipamiento. Señaló que dicha exigencia constituye una modificación sustancial al requerimiento inicial y que, además, omite considerar las distintas políticas de divulgación de vulnerabilidades adoptadas por los diversos fabricantes de dispositivos firewall, centrándose únicamente en los lineamientos seguidos por un proveedor específico.

Por lo tanto, la pretensión del recurrente consiste en que la Entidad **deje sin efecto la respuesta emitida en la consulta y/u observación Nº 362 del pliego.**

**Pronunciamiento**

Sobre el particular, de la revisión del Anexo A: Punto N° 01 del numeral 3.1 del Capítulo III de la Sección Específica de las Bases de la convocatoria, se aprecia lo siguiente:

> *"**ANEXO A: PUNTO N° 01***
>
> ***SERVICIO DE SEGURIDAD PERIMETRAL GESTIONADA EQUIPO DE SEGURIDAD PERIMETRAL FIREWALL DE SIGUIENTE GENERACIÓN (02)***
>
> ***Características Técnicas***
>
> ***Descripción***
> - *Adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la red empresarial.*
> - *La solución tiene que ser ofrecida en alta disponibilidad, se entiende por alta disponibilidad, es decir por lo menos 02 (dos) appliances con las mismas características mínimas mencionadas en estas especificaciones y funcionar de manera activo/pasivo o activo/activo.*
> - *El fabricante debe estar como líder en el último informe de Forrester Wave Automated Malware Analysis y/o el reporte de Forrester Wave Enterprise Firewall Solution.*
> - *El fabricante debe estar certificado por USGv6 para trabajar IPv6 tanto en Firewall como en IPS.*
> - *La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7.*

***(…)"***

Es así que, mediante consulta y/u observación N° 362 del pliego, se solicitó confirmar que los equipos NGFW ofertados, como parte del servicio de seguridad perimetral gestionada, no deberán registrar más de diez (10) vulnerabilidades (CVE) anunciadas y/o publicadas en sus SO y/o firmware, acumuladas en sus distintas versiones durante los doce (12) meses previos a la fecha de presentación de propuestas. Ante lo cual, el Comité de Selección acogió la petición formulada por el participante, considerando que dicha medida contribuye a mitigar los riesgos de seguridad asociados a vulnerabilidades potenciales en el marco del servicio requerido.

En consecuencia, de la revisión del Anexo A: Punto N° 01 del numeral 3.1 del Capítulo III, correspondientes a la Sección Específica de las Bases de la convocatoria, se aprecia que la Entidad implementó lo absuelto, conforme a lo siguiente:

*"**<u>ANEXO A: PUNTO N° 01</u>***

***SERVICIO DE SEGURIDAD PERIMETRAL GESTIONADA EQUIPO DE SEGURIDAD PERIMETRAL FIREWALL DE SIGUIENTE GENERACIÓN (02)***

***Características Técnicas***

***Descripción***

- *Adquisición de una solución de protección de redes con características de Next Generation Firewall (NGFW) para la seguridad de la red empresarial.*
- *La solución tiene que ser ofrecida en alta disponibilidad, se entiende por alta disponibilidad, es decir por lo menos 02 (dos) appliances con las mismas características mínimas mencionadas en estas especificaciones y funcionar de manera activo/pasivo o activo/activo.*
- *El fabricante debe estar como líder en el último informe de Forrester Wave Automated Malware Analysis y/o el reporte de Forrester Wave Enterprise Firewall Solution.*
- *El fabricante debe estar certificado por USGv6 para trabajar IPv6 tanto en Firewall como en IPS.*
- *La plataforma debe ser optimizada para análisis de contenido de aplicaciones en capa 7.*
- ***<u>Los equipos firewall ofertados que conforman el servicio de seguridad perimetral gestionada, no deberán tener en sus respectivos sistemas operativos y/o firmware, más de diez (10) vulnerabilidades (CVE) anunciadas y/o publicadas, acumuladas entre sus diferentes versiones durante los últimos 12 meses anteriores a la fecha de presentación de propuestas</u>***

***(…)"***

(El subrayado y resaltado es agregado)

En relación con ello, y en atención al cuestionamiento formulado por el participante, mediante INFORME N° 000020-2025-OIT-OGETIC-SG-HPS/MC[23], la Entidad señaló lo siguiente:

***"(...)** el sustento técnico adoptado por el área usuaria en relación a dicha pregunta fue que el requerimiento de limitar a diez (10) el número de CVEs conocidas en los últimos 12 meses **<u>es</u>***

[23] Remitido mediante el Expediente N° 2025-0015186, de fecha 27 de mayo de 2025.

***una práctica aceptada en evaluaciones de riesgo tecnológico**, y responde a los siguientes principios:*

*• Prevención proactiva de exposición a amenazas conocidas.*
*• Reducción del vector de ataque mediante software con historial probado de seguridad.*
*• Alineamiento con buenas prácticas de gestión de activos TIC, conforme a ISO/IEC 27001, NIST 800-53 y al Esquema Nacional de Seguridad Digital en Perú.*

*Asimismo, contrario a lo alegado, esta restricción **no está enfocada en un fabricante en particular.** Todos los fabricantes de nivel empresarial cuentan con mecanismos de control de calidad y gestión de vulnerabilidades, además que tienen mecanismos PSIRT y publican CVEs bajo políticas internacionales.*

*Si un equipo acumula más de 10 CVEs en 12 meses, esto no se debe a la "transparencia del fabricante", sino a deficiencias estructurales o debilidad en el ciclo de desarrollo seguro.*
*(...)"*

(El subrayado y resaltado es agregado)

Adicionalmente, mediante el INFORME N° 000022-2025-OIT-OGETIC-SG-HPS/MC[24], la Entidad indicó lo siguiente:

***"(...)** Al respecto en calidad de área usuaria se informa lo siguiente:*

*• Al respecto se indica que, la exigencia incluida con respecto a las vulnerabilidades presentes en los equipos firewall ofertados como parte del requerimiento, **no modifica el alcance de los términos de referencia en el sentido que no adiciona nuevas capacidades y/o componentes adicionales necesarios para poder tener una menor cantidad de vulnerabilidad y/o brindar el servicio**, dado que, el hecho de contar con un producto con sistemas operativos y/o firmware de mayor seguridad, el cual tenga una cantidad prudente o reducida de vulnerabilidades no debería exigir un mayor costo en la elaboración de la propuesta técnica u económica requerida, esta es una capacidad inherente de seguridad propia de los equipos firewalls.*
*• Sin embargo, como área usuaria, **se señala que dicha característica no se ha pedido en la etapa inicial, por ende, a fin de no restringir la participación de potenciales postores y continuar con el proceso de manera óptima y eficiente se considerará la expresión como opcional** quedando de la siguiente manera: "Los equipos firewall ofertados que conforman el servicio de seguridad perimetral gestionada, no deberán tener en sus respectivos sistemas operativos y/o firmware, más de diez (10) vulnerabilidades (CVE) anunciadas y/o publicadas, acumuladas entre sus diferentes versiones durante los últimos 12 meses anteriores a la fecha de presentación de propuestas (opcional)"*
*(...)"*

(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.

[24] Remitido mediante el Expediente N° 2025-0023633, de fecha 10 de junio de 2025.

Ahora bien, en atención a lo cuestionado por el recurrente, el Comité de Selección en coordinación con el área usuaria de la Entidad, siendo la responsable de la determinación de su requerimiento y, por ende, la mejor conocedora de sus necesidades, a través del citado informe, se rectifica de lo absuelto, argumentando que el requerimiento que limita a diez (10) el número de vulnerabilidades conocidas (CVE) en los últimos doce meses, se enmarca dentro de prácticas reconocidas en evaluaciones de riesgo tecnológico, y tiene como finalidad prevenir de forma proactiva la exposición a amenazas conocidas, así como reducir la superficie de ataque, mediante el uso de software con historial de seguridad comprobado, y alinearse con estándares internacionales como la ISO/IEC 27001, el NIST 800-53 y el Esquema Nacional de Seguridad Digital del Perú.

Asimismo, la Entidad agrega que, contrario a lo afirmado por el participante, dicha exigencia no está orientada a favorecer a un fabricante en particular, toda vez que, todos los proveedores de nivel empresarial cuentan con mecanismos de calidad, gestión de vulnerabilidades y áreas PSIRT, que publican CVE's bajo estándares internacionales. En ese sentido, la acumulación de más de diez vulnerabilidades no obedece necesariamente a políticas de transparencia, sino que puede reflejar debilidades estructurales o deficiencias en el ciclo de desarrollo seguro del producto.

Aunado a ello, se precisa que la exigencia referida al número de vulnerabilidades presentes en los equipos firewall ofertados no altera el alcance establecido en los términos de referencia, en tanto no implica la incorporación de nuevas funcionalidades ni componentes adicionales que incrementen el nivel de complejidad técnica o el costo del servicio, toda vez que disponer de un sistema operativo y/o firmware con un menor número de vulnerabilidades constituye una característica inherente a la arquitectura de seguridad de los firewalls empresariales. No obstante, a lo afirmado, la Entidad reconoce que dicha condición no fue contemplada en la versión inicial del requerimiento, por lo que, a fin de no restringir la participación de posibles postores y asegurar el desarrollo eficiente del proceso de contratación, se ha dispuesto que dicho criterio sea considerado únicamente como opcional.

Por lo tanto, considerando el análisis de los párrafos precedentes, y en tanto la pretensión del recurrente se encuentra orientada a que la Entidad deje sin efecto la respuesta emitida en la consulta y/u observación Nº 362 del pliego; y en la medida que, mediante informe técnico, la Entidad admite la petición formulada por el recurrente, precisando que será únicamente opcional, este Organismo Técnico Especializado ha decidido **ACOGER** el presente cuestionamiento. Por lo que, con ocasión de la integración definitiva de las Bases, se implementará la siguiente disposición:

- **Se dejará sin efecto** lo absuelto en la consulta y/u observación N° 362 del pliego, y se deberá considerar la siguiente absolución: *"Los equipos firewall ofertados que conforman el servicio de seguridad perimetral gestionada, no deberán tener en sus respectivos sistemas operativos y/o firmware, más de diez (10) vulnerabilidades (CVE) anunciadas y/o publicadas, acumuladas entre sus diferentes versiones durante los últimos 12 meses anteriores a la fecha de presentación de propuestas (opcional)."*

- **<u>Se adecuará</u>** el contenido del Anexo A: Punto N° 01 del numeral 3.1 del Capítulo III correspondiente a la Sección Específica de las Bases Integradas Definitivas, conforme a lo siguiente:

> *"**<u>ANEXO A: PUNTO N° 01</u>***
>
> ***SERVICIO DE SEGURIDAD PERIMETRAL GESTIONADA EQUIPO DE SEGURIDAD PERIMETRAL FIREWALL DE SIGUIENTE GENERACIÓN (02)***
>
> ***Características Técnicas***
>
> ***Descripción***
> ***(…)***
> - *Los equipos firewall ofertados que conforman el servicio de seguridad perimetral gestionada, no deberán tener en sus respectivos sistemas operativos y/o firmware, más de diez (10) vulnerabilidades (CVE) anunciadas y/o publicadas, acumuladas entre sus diferentes versiones durante los últimos 12 meses anteriores a la fecha de presentación de propuestas (opcional)*

***(…)"***

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

## 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 al plazo de prestación del servicio

De la revisión al numeral 1.8 del Capítulo I y los acápites 13 y 14 del numeral 3.1 del Capítulo III pertenecientes a la Sección Específica de las Bases Integradas, se aprecia lo siguiente:

| ***1.8. PLAZO DE PRESTACIÓN DEL SERVICIO*** | ***13. PLAZO DE PRESTACIÓN DEL SERVICIO*** | ***14. PLAZO DE IMPLEMENTACIÓN DEL SERVICIO*** |
|---|---|---|
| *Los servicios materia de la presente convocatoria se prestarán en el plazo de 1,096 (Mil noventa seis días calendario) lo que equivale a treinta y seis (36) meses y deberá iniciar el 08 de agosto del 2025 y luego de suscrita el Acta de Implementación del servicio por parte del contratista y el área usuaria que es la Oficina General de Estadísticas y Tecnologías de* | *El plazo de prestación del servicio deberá ser de 1.096 (Mil noventa seis días calendario) lo que equivale a treinta y seis (36) meses y deberá iniciar el 08 de agosto del 2025 y luego de suscrita el Acta de* | *El plazo de entrega para realizar la instalación, configuración y puesta en marcha del servicio será de hasta ciento veinte (120) días calendario que se computaran a partir del día siguiente de la suscripción* |

| | | |
|---|---|---|
| *Información y Comunicaciones OGETIC, en caso de no coincidir con el plazo de implementación, se respetará el nuevo inicio dentro de los tiempos establecidos en concordancia con lo establecido en el expediente de contratación y según el siguiente detalle:*<br><br>***PLAZO DE IMPLEMENTACIÓN DEL SERVICIO***<br><br>*El plazo de entrega para realizar la instalación, configuración y puesta en marcha del servicio será de hasta ciento veinte (120) días calendario que se computarán a partir del día siguiente de la suscripción del contrato.*<br><br>***PLAZO DE PRESTACIÓN DE SERVICIO***<br><br>*El plazo de prestación del servicio deberá ser de 1.096 (Mil noventa seis días calendario) lo que equivale a treinta y seis (36) meses y deberá iniciar el 08 de agosto del 2025 y luego de suscrita el Acta de implementación del servicio por parte del contratista y el área usuaria que es la Oficina General de Estadísticas y Tecnologías de Información y Comunicaciones OGETIC, en caso de no coincidir con el plazo de implementación, se respetará el nuevo inicio dentro de los tiempos establecidos.* | *implementación del servicio por parte del contratista y el área usuaria que es la Oficina General de Estadísticas y Tecnologías de Información y Comunicaciones OGETIC, en caso de no coincidir con el plazo de implementación, se respetará el nuevo inicio dentro de los tiempos establecidos* ***tomando como base las gestiones anticipadas que correspondan*** | *del contrato.*<br><br>***La Entidad garantizará los accesos y autorizaciones necesarias para la ejecución de los respectivos trabajos de implementación del servicio dentro de sus instalaciones.***<br><br>***La ausencia de facilidades de acceso y/o autorizaciones y/o facilidades técnicas requeridas imputables a la Entidad, determinará la suspensión del plazo de implementación previsto en las bases hasta que se encuentre subsanado el inconveniente, sin generar penalidad alguna al contratista.***<br><br>***El plazo de prestación del servicio será computado desde la fecha de la suscripción del Acta de Activación (Acta de Implementación del servicio) y no desde la fecha del contrato.*** |

(El subrayado y resaltado es agregado)

De lo anterior, se advierte que, la información contenida en el numeral 1.8 del Capítulo I y los acápites 13 y 14 del numeral 3.1 del Capítulo III, correspondientes a la Sección Específica de las Bases integradas, no guardaría congruencia entre sí.

En relación con ello, mediante el INFORME N° 000022-2025-OIT-OGETIC-SG-HPS/MC[25], la Entidad señaló lo siguiente:

> ***"(…)*** *se remite el párrafo que debería ir según la último precisión adecuada luego de la absolución de consultas y observaciones:*
>
> ***PLAZO DE IMPLEMENTACIÓN DEL SERVICIO***

[25] Remitido mediante el Expediente N° 2025-0023633, de fecha 10 de junio de 2025.

*El plazo de entrega para realizar la instalación, configuración y puesta en marcha del servicio será de hasta ciento veinte (120) días calendario que se computarán a partir del día siguiente de la suscripción del contrato.*

*La Entidad garantizará los accesos y autorizaciones necesarias para la ejecución de los respectivos trabajos de implementación del servicio dentro de sus instalaciones.*

*La ausencia de facilidades de acceso y/o autorizaciones y/o facilidades técnicas requeridas imputables a la Entidad, determinará la suspensión del plazo de implementación previsto en las bases hasta que se encuentre subsanado el inconveniente, sin generar penalidad alguna al contratista.*

*El plazo de prestación del servicio será computado desde la fecha de la suscripción del Acta de Activación (Acta de Implementación del servicio) y no desde la fecha del contrato.*

***PLAZO DE PRESTACIÓN DEL SERVICIO***
*El plazo de prestación del servicio deberá ser de 1.096 (Mil noventa seis días calendario) lo que equivale a treinta y seis (36) meses y deberá iniciar el 08 de agosto del 2025 y luego de suscrita el Acta de implementación del servicio por parte del contratista y el área usuaria que es la Oficina General de Estadísticas y Tecnologías de Información y Comunicaciones OGETIC, en caso de no coincidir con el plazo de implementación, se respetará el nuevo inicio dentro de los tiempos establecidos tomando como base las gestiones anticipadas que correspondan.*
***(...)"***

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

- **Se adecuará** el numeral 1.8 del Capítulo I de la Sección Específica de las Bases Integradas Definitivas, conforme al siguiente detalle:

***"1.8. PLAZO DE PRESTACIÓN DEL SERVICIO***

~~*Los servicios materia de la presente convocatoria se prestarán en el plazo de 1,096 (Mil noventa seis días calendario) lo que equivale a treinta y seis (36) meses y deberá iniciar el 08 de agosto del 2025 y luego de suscrita el Acta de Implementación del servicio por parte del contratista y el área usuaria que es la Oficina General de Estadísticas y Tecnologías de Información y Comunicaciones OGETIC, en caso de no coincidir con el plazo de implementación, se respetará el nuevo inicio dentro de los tiempos establecidos en concordancia con lo establecido en el expediente de contratación y según el siguiente detalle:*~~

***PLAZO DE IMPLEMENTACIÓN DEL SERVICIO***

*El plazo de entrega para realizar la instalación, configuración y puesta en marcha del servicio será de hasta ciento veinte (120) días calendario que se computarán a partir del día siguiente de la suscripción del contrato.*

*La Entidad garantizará los accesos y autorizaciones necesarias para la ejecución de los respectivos trabajos de implementación del servicio dentro de sus instalaciones.*

*La ausencia de facilidades de acceso y/o autorizaciones y/o facilidades técnicas requeridas imputables a la Entidad, determinará la suspensión del plazo de implementación previsto en las bases hasta que se encuentre subsanado el*

*inconveniente, sin generar penalidad alguna al contratista.*

*El plazo de prestación del servicio será computado desde la fecha de la suscripción del Acta de Activación (Acta de Implementación del servicio) y no desde la fecha del contrato.*

***PLAZO DE PRESTACIÓN DEL SERVICIO***

*El plazo de prestación del servicio deberá ser de 1.096 (Mil noventa seis días calendario) lo que equivale a treinta y seis (36) meses y deberá iniciar el 08 de agosto del 2025 y luego de suscrita el Acta de implementación del servicio por parte del contratista y el área usuaria que es la Oficina General de Estadísticas y Tecnologías de Información y Comunicaciones OGETIC, en caso de no coincidir con el plazo de implementación, se respetará el nuevo inicio dentro de los tiempos establecidos tomando como base las gestiones anticipadas que correspondan.*

*(...)"*

- Se **adecuará** la Cláusula Quinta del Capítulo V de la Sección Específica de las Bases Integradas Definitivas, conforme al siguiente detalle:

***"CLÁUSULA QUINTA: DEL PLAZO DE LA EJECUCIÓN DE LA PRESTACIÓN***

~~*El plazo de prestación del servicio será de acuerdo al siguiente detalle:*~~

- ***Plazo de Implementación de Servicio***

*El plazo de entrega para realizar la instalación, configuración y puesta en marcha del servicio será de hasta ciento veinte (120) días calendario que se computaran a partir del día siguiente de la suscripción del contrato.*

*La Entidad garantizará los accesos y autorizaciones necesarias para la ejecución de los respectivos trabajos de implementación del servicio dentro de sus instalaciones.*

*La ausencia de facilidades de acceso y/o autorizaciones y/o facilidades técnicas requeridas imputables a la Entidad, determinará la suspensión del plazo de implementación previsto en las bases hasta que se encuentre subsanado el inconveniente, sin generar penalidad alguna al contratista.*

*El plazo de prestación del servicio será computado desde la fecha de la suscripción del Acta de Activación (Acta de Implementación del servicio) y no desde la fecha del contrato.*

- ***Plazo de Prestación del Servicio***

*El plazo de prestación del servicio deberá ser de 1.096 (Mil noventa seis días calendario) lo que equivale a treinta y seis (36) meses y deberá iniciar el 08 de agosto del 2025 y luego de suscrita el Acta de implementación del servicio por parte del contratista y el área usuaria que es la Oficina General de Estadísticas y Tecnologías de Información y Comunicaciones OGETIC, en caso de no coincidir con el plazo de implementación, se respetará el nuevo inicio dentro de los tiempos establecidos tomando como base las gestiones anticipadas que correspondan.*

*(...)"*

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

### 3.2 Respecto a la documentación de presentación facultativa

De la revisión a los anexos que forman parte de las Bases Integradas, se aprecia lo siguiente:

> *"(…)*
>
> **ANEXO Nº 7**
>
> **DECLARACIÓN JURADA DE CUMPLIMIENTO DE CONDICIONES PARA LA APLICACIÓN DE LA EXONERACIÓN DEL IGV**
>
> Señores
> **COMITÉ DE SELECCIÓN**
> **CONCURSO PÚBLICO Nº 05-2025/MC**
> Presente.-
>
> Mediante el presente el suscrito, postor y/o Representante Legal de [CONSIGNAR EN CASO DE SER PERSONA JURÍDICA], declaro bajo juramento que gozo del beneficio de la exoneración del IGV previsto en la Ley Nº 27037, Ley de Promoción de la Inversión en la Amazonía, dado que cumplo con las condiciones siguientes:
>
> 1.- Que el domicilio fiscal de la empresa[146] se encuentra ubicada en la Amazonía y coincide con el lugar establecido como sede central (donde tiene su administración y lleva su contabilidad);
>
> 2.- Que la empresa se encuentra inscrita en las Oficinas Registrales de la Amazonía (exigible en caso de personas jurídicas);
>
> 3.- Que, al menos el setenta por ciento (70%) de los activos fijos de la empresa se encuentran en la Amazonía; y
>
> 4.- Que la empresa no presta servicios fuera de la Amazonía.
>
> [CONSIGNAR CIUDAD Y FECHA]
>
> *(...)"*

De lo expuesto, se advierte que la Entidad ha incluido dentro de las Bases, un anexo relativo a la "Declaración jurada de cumplimiento de condiciones para la aplicación de la exoneración del IGV"; siendo de notar que, dentro de la misma, el postor se declara que *"la empresa no presta servicios fuera de la Amazonía"*, a efecto de gozar el beneficio previsto en la Ley N° 27037 - Ley de Promoción de la Inversión en la Amazonía.

Sin embargo, de la revisión del objeto de contratación se aprecia que el presente tiene como finalidad la contratación del Servicio de acceso a internet, seguridad perimetral gestionada, telefonía e interconexión de datos, para el Ministerio de Cultura; el cual es una entidad del gobierno central. De lo que se colige que, dicho servicio no podría ser prestado exclusivamente dentro de la Amazonía; por lo que, dicho beneficio no podría ser aplicable a la presente contratación.

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 suprimirá** el Anexo N° 7 - Declaración jurada de cumplimiento de condiciones para la aplicación de la exoneración del IGV, de las Bases Integradas Definitivas.

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

**3.3. Respecto a los requisitos para perfeccionar el contrato**

De la revisión del numeral 2.3 del Capítulo II pertenecientes 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:*
>
> *a)* ***<u>Carta Fianza</u>*** *de fiel cumplimiento del contrato.*
>
> *(...)"*

(El subrayado y resaltado es agregado)

Al respecto, se advierte que las Bases estarían restringiendo la forma de presentación de la garantía de fiel cumplimiento, al exigir exclusivamente la carta fianza como medio de acreditación. Ello contraviene lo dispuesto en el artículo 148 del Reglamento de la Ley de Contrataciones del Estado, el cual establece que dicha garantía puede ser materializada mediante carta fianza y/o póliza de caución, emitidas por entidades supervisadas por la Superintendencia de Banca, Seguros y AFP, que cuenten con clasificación de riesgo B o superior.

Por lo tanto, corresponde al Contratista determinar el tipo de documento que presentará para acreditar la garantía de fiel cumplimiento, pudiendo optar por una carta fianza o una póliza de caución, conforme a lo previsto en la normativa aplicable al presente procedimiento de selección.

En ese sentido, considerando lo señalado en los párrafos precedentes y con ocasión de la integración definitiva de las Bases, se implementarán las siguientes disposiciones:

- **<u>Se adecuará</u>** el numeral 2.3 del Capítulo II de la Sección Específica de las Bases Integradas Definitivas, conforme al siguiente detalle:

> ***"2.3 REQUISITOS PARA PERFECCIONAR EL CONTRATO***
>
> *El postor ganador de la buena pro debe presentar los siguientes documentos para perfeccionar el contrato:*
>
> *a)* ~~*Carta Fianza*~~ *Garantía de fiel cumplimiento del contrato.*
>
> *(...)"*

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

### 3.4. Respecto a la conformidad de la prestación del servicio

De la revisión al acápite 16 del numeral 3.1 del Capítulo III y a la cláusula novena del Capítulo V, correspondientes a la Sección Específica de las Bases integradas, se aprecia lo siguiente:

| | |
|---|---|
| ***"16. CONFORMIDAD***<br>*• La conformidad del Servicio de Implementación será emitida por la Oficina General de Estadísticas y Tecnologías de la Información y Comunicaciones, previo informe de la Oficina de Informática y Telecomunicaciones quien verificará el cumplimiento del servicio y el entregable* ***<u>indicado en el ítem 12.</u>***<br>*• La conformidad mensual del servicio será emitida por la Oficina General de Estadísticas y Tecnologías de la Información y Comunicaciones previa presentación de la factura del Contratista,* ***<u>así como un informe del entregable según lo indicado en el ítem 13.</u>***<br>***(…)"*** | ***"CLÁUSULA NOVENA: CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO***<br>***(…)***<br><br>*La conformidad del Servicio de Implementación será emitida por la Oficina General de Estadísticas y Tecnologías de la Información y Comunicaciones, previo informe de la Oficina de Informática y Telecomunicaciones quien verificará el cumplimiento del servicio y el entregable* ***<u>indicado líneas arriba.</u>***<br>*La conformidad mensual del servicio será emitida por la Oficina General de Estadísticas y Tecnologías de la Información y Comunicaciones previa presentación de la factura del Contratista,* ***<u>así como un informe con el registro de incidencias, requerimientos, eventos del servicio internet, eventos de seguridad en general, clasificándolos en controlados, mitigados y/o aceptados.</u>***<br>*(…)"* |

(El subrayado y resaltado es agregado)

De lo anterior, se advierte que, la información contenida en el acápite 16 del numeral 3.1 del Capítulo III y a la cláusula novena del Capítulo V, correspondientes a la Sección Específica de las Bases integradas, <u>no guardaría congruencia entre sí.</u>

En relación con ello, mediante el CARTA N.º 001-2025-CS-CP Nº 05-2025/MC-1[26], la Entidad señaló lo siguiente:

> ***"(…)*** *ante ello este colegiado precisa la misma como deberá quedar redactado dicho extremo en la cláusula novena del capítulo V, correspondientes a la sección específica de las bases integradas no definitivas, a fin de que guarden congruencia:*
> *(...)*
>
> *- La conformidad del servicio de implementación será emitida por la Oficina General de Estadísticas y Tecnologías de la Información y Comunicaciones, previo informe de la Oficina de Informática y Telecomunicaciones quien verificará el cumplimiento del servicio y el entregable indicado en el ítem 12 de los términos de referencia.*

[26] Remitido mediante el Expediente N° 2025-0023633, de fecha 10 de junio de 2025.

*- La conformidad mensual del servicio será emitida por la Oficina General de Estadísticas y Tecnologías de la Información y Comunicaciones previa presentación de la factura del contratista, así como un informe del entregable según lo indicado en el ítem 13 de los términos de referencia.*
*(...)"*

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 adecuará** la Cláusula Novena del Capítulo V de la Sección Específica de las Bases Integradas Definitivas, conforme al siguiente detalle:

> ***"CLÁUSULA NOVENA: CONFORMIDAD DE LA PRESTACIÓN DEL SERVICIO***
> *(...)*
>
> - *La conformidad del Servicio de Implementación será emitida por la Oficina General de Estadísticas y Tecnologías de la Información y Comunicaciones, previo informe de la Oficina de Informática y Telecomunicaciones quien verificará el cumplimiento del servicio y el entregable indicado ~~líneas arriba.~~ en el ítem 12 de los términos de referencia.*
>
> - *La conformidad mensual del servicio será emitida por la Oficina General de Estadísticas y Tecnologías de la Información y Comunicaciones previa presentación de la factura del Contratista, ~~así como un informe con el registro de incidencias, requerimientos, eventos del servicio internet, eventos de seguridad en general, clasificándolos en controlados, mitigados y/o aceptados.~~ así como un informe del entregable según lo indicado en el ítem 13 de los términos de referencia.*
>
> *(...)"*

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

Firmado digitalmente por LAURA SILVA Anthony David FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 25.06.2025 19:45:06 -05:00

## 4. CONCLUSIONES

Firmado digitalmente por CHAMOCHUMBI CHERRE Carlos Ernesto FAU 20419026809 soft
Motivo: Doy V° B°
Fecha: 25.06.2025 19:37:32 -05:00

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 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, 25 de junio del 2025

*Código: 6.1*

Firmado digitalmente por FLORES BAZAN Miguel Angel FAU 20419026809 soft
Motivo: Soy el autor del documento
Fecha: 25.06.2025 20:12:33 -05:00