

PRONUNCIAMIENTO N° 456-2024/OSCE-DGR

Entidad : Ministerio de Relaciones Exteriores

Referencia : Concurso Público N° 17-2024-RE-1, convocado para la “Contratación del servicio de seguridad gestionada para el Ministerio de Relaciones Exteriores”.

1. ANTECEDENTES

Mediante el formulario de solicitud de emisión de pronunciamiento recibido el 31 de julio¹ de 2024 y subsanado el 13² de agosto de 2024, el presidente del comité de selección a cargo del procedimiento de selección de la referencia remitió al Organismo Supervisor de las Contrataciones del Estado (OSCE) la solicitud de elevación de cuestionamientos al pliego absolutorio de consultas y observaciones e integración de Bases presentada por el participante **AGGITY PERU S.A.C.**, en cumplimiento de lo dispuesto por el artículo 21 de la Ley de Contrataciones del Estado, aprobada mediante la Ley N° 30225, en adelante la “Ley”, y el artículo 72 de su Reglamento, aprobado por el Decreto Supremo N° 344-2018-EF, en adelante el “Reglamento”.

Ahora bien, cabe precisar que en la emisión del presente pronunciamiento se utilizó el orden establecido por el comité de selección en el pliego absolutorio³ y los temas materia de cuestionamientos de los mencionados participantes, conforme al siguiente detalle:

- **Cuestionamiento N° 1** : Respecto a la absolución de la consulta y/u observación N° 75, referida al “**Nivel de madurez**”.
- **Cuestionamiento N° 2** : Respecto a la absolución de la consulta y/u observación N° 37, referida a la “**Mitigación de ataques**”.
- **Cuestionamiento N° 3** : Respecto a la absolución de la consulta y/u observación N° 39, referida al “**Monitoreo gráfico**”.
- **Cuestionamiento N° 4** : Respecto a la absolución de la consulta y/u observación N° 41, referida a la “**Capacidad mínima de nuevas sesiones o conexiones por segundo**”.

¹ Mediante Expediente N° 2024-0100494.

² Mediante Expediente N° 2024-0106771.

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

- **Cuestionamiento N° 5** : Respecto a la absolución de las consultas y/u observaciones N° 40 y N° 42, referida al **“Throughput de los Firewalls Externos - Firewall Internos”**.
- **Cuestionamiento N° 6** : Respecto a la absolución de la consulta y/u observación N° 56, referida a la **“Integración al Active Directory”**.

Por otro lado, cabe señalar que de la revisión de la solicitud de elevación del participante **AGGITY PERU S.A.C.**, se aprecia lo siguiente:

- Se aprecia que cuestiona la absolución de la consulta y/u observación N° 9 y N° 10, mediante la cual en su solicitud de elevación requiere lo siguiente: *“respecto al requerimiento de que el contratista deba estar registrado como miembro de FIRST (Forum of Incident Response and Security Teams)(...) en relación a la consulta N° 9 y N° 10 se formuló a fin de solicitar a la entidad que acepte la acreditación opcional, sin embargo, nuestra consulta no fue aceptada. Por ello solicitamos que este requerimiento también pueda ser sustentada mediante la contratación de una entidad especializada que cumpla con este requerimiento (...) se solicita que el OSCE o suprima esta exigencia o que señale la opción de acreditar ello mediante la contratación de una entidad especializada que cumpla con este requerimiento”*.

Asimismo, de la revisión del pliego absolutorio, se advierte que las consultas y/u observaciones N° 9 y N° 10, no versa sobre solicitar que el equipo de respuesta antes incidentes del contratista pueda ser sustentada mediante la contratación de una entidad especializada o a que se suprima dicho requisito; sino a solicitar que se acepte que el equipo de respuesta ante incidentes del contratista puedan estar opcionalmente registrado como miembro de FIRST y que se acepte que el postor puedan ser opcionalmente miembro registrado de FIRST.

- Además, se aprecia que cuestiona la absolución de la consulta y/u observación N° 65, mediante la cual en su solicitud de elevación requiere lo siguiente: *“solicitamos que se modifiquen los requisitos de la siguiente manera: 1) indicar que el soporte para PSV y TSV sea opcional, manteniendo CSV como obligatorio (...), 2) Permitir que el soporte sea para CEF o LEEF sin requerir ambos, 3) aceptar que el soporte sea para uno de los protocolos de transferencia mencionados (FTP, SFTP o FTPS) en lugar de todos ellos (...)”*

Asimismo, de la revisión del pliego absolutorio, se advierte que la consulta y/u observación N° 65, no versa sobre solicitar que el soporte para PSV y TSV sea opcional y el soporte CSV sea obligatorio, el soporte sea para CEF o LEEF sin requerir ambos y que el soporte sea para uno de los protocolos de transferencia FTP, SFTP o FTPS y no todos ellos; sino a solicitar que se modifique las especificación técnica de la siguiente manera CSV, PSV, TSV, texto plano, archivos en formato CEF/LEEF y JSON. Estos pueden estar alojados en

servidores FTP/SFTP/FTPS y en carpetas compartidas de equipos Windows y Linux.

En ese sentido, los aspectos indicados por el recurrente en su solicitud de elevación no fueron abordados en la etapa de formulación de consultas y/u observaciones; por lo que al tratarse de pretensiones adicionales que debieron ser presentadas en la etapa pertinente, estas devienen en extemporáneas; razón por la cual, **este Organismo Técnico Especializado no se pronunciará al respecto.**

2. CUESTIONAMIENTOS

De manera previa, cabe señalar que el OSCE no ostenta la calidad de perito técnico dirimente respecto a las posiciones de determinados aspectos del requerimiento (especificaciones técnicas, términos de referencia y expediente técnico de obra, según corresponda); sin embargo, puede requerir a la Entidad informes que contengan la posición técnica al respecto⁴, considerando que el área usuaria es la dependencia que cuenta con los conocimientos técnicos necesarios para definir las características técnicas de los bienes, servicios y obras que se habrán de contratar.

Cuestionamiento N° 1

Respecto al “Nivel de madurez”.

El participante **AGGITY PERU S.A.C.**, cuestionó la absolución de la consulta y/u observación N° 75, señalando que mediante la citada consulta y/u observación se solicitó que la madurez de un Centro de Operaciones y Seguridad (SOC) sea acreditada con la presentación del Certificado ISO 27001, no obstante, si bien la Entidad decidió no aceptar la solicitud, ésta no fundamenta dicha decisión, pues solo indica que el área usuaria es la responsable de formular su requerimiento y que además se realizó un estudio de mercado. En relación a ello, cabe indicar que la ISO 27001 es una certificación internacional que establece los requisitos para la implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI). Por lo tanto, la pretensión del recurrente consiste en **que se acepte que el nivel de madurez de nivel 3 de un total de 5 sea acreditado con el certificado ISO 27001.**

Pronunciamiento

Al respecto, de la revisión del acápite 4.1.6 del numeral 3.1 del Capítulo III de la sección específica de las Bases de la convocatoria, la Entidad consignó lo siguiente:

“4.1.6. Calidad de servicio

(...)

Asimismo, el contratista será responsable de la actualización oportuna de parches y de hacer las copias de respaldo de la configuración y políticas de los productos

⁴ Ver el Comunicado N° 011-2013-OSCE/PRE.

*propuestos, para esto **deberá demostrar que el Centro de Operaciones y Seguridad (SOC) cuenta con procedimientos que han logrado un nivel de madurez de nivel 3 de un total de 5, los cuales deberán acreditar con documento emitido por una entidad auditora internacional.***

(...)” (El subrayado y resaltado es nuestro).

Así, mediante la consulta y/u observación N° 75, se solicitó aceptar como “madurez” que el proveedor pueda demostrar su madurez si cuenta con el certificado ISO27001 por más de 5 años o para una pluralidad de proveedores se considere este punto como opcional.

Ante lo cual, el comité de selección no confirmó lo solicitado, bajo los argumentos de que: i) en la indagación de mercado se determinó existencia de pluralidad de proveedores, quienes remitieron sus cotizaciones y manifestaron que cumplen con las condiciones establecidas en el requerimiento; y que, ii) las características técnicas del servicio buscan atender las necesidades de la institución.

En ese contexto y teniendo en cuenta lo cuestionado por el recurrente, respecto a la absolución señalada en los párrafos precedentes, el área usuaria de la Entidad mediante el INFORME N° 34-2024-MRE/OGI/OTI-RRB ⁵, indicó lo siguiente:

“(...

*Al respecto, no se puede tomar en cuenta como equivalencia una certificación ISO 27001 como si fuera nivel de madurez de un Centro de Operaciones y Seguridad (SOC), porque son temas totalmente distintos. **La certificación ISO 27001 garantiza a las empresas gestionar adecuadamente sus propios riesgos de seguridad de la información y en un marco de mejora continua corporativa, garantizando la continuidad del negocio y principalmente del servicio brindado.***

***En cambio, un nivel 3 de madurez de un SOC, garantiza que, en una escala CMM (Capability Maturity Model - Modelo de Madurez de Capacidades), dicho SOC ya cuenta con procesos de atención y ejecución no solo documentados sino estandarizados, los cuales otorga rapidez y fiabilidad en la atención.** Se debe tener en cuenta también que existen empresas que certifican el nivel de madurez de un SOC, como por ejemplo NRD Cyber Security o SOC-CMM, así mismo; **lo establecido en el TDR es un requerimiento que se ha venido solicitando desde nuestro servicio anterior, y debido a que esta institución maneja información del Estado altamente sensible, se exige estándares y marcos de referencias de la industria, además mencionar que lo requerido lo vienen cumpliendo a nivel nacional más de 2 proveedores de servicio de seguridad gestionada.** Teniendo en cuenta lo mencionado, se evidencia que no se vulnera la normativa de contrataciones ni se vulnera la pluralidad de postores y libre participación”*

(El subrayado y resaltado es nuestro).

Adicionalmente, mediante INFORME N° 35-2024-MRE/OGI/OTI-RRB⁶, la Entidad precisó lo siguiente:

⁵ Remitido mediante Expediente N° 2024-0100494, de fecha 31 de julio de 2024.

⁶ Remitido mediante Expediente N° 2024-0106771, de fecha 13 de agosto de 2024.

“(…)

La respuesta a la consulta es la siguiente:

Sustento Técnico:

A nivel internacional lo que se conoce como Modelo de Capa de Madurez (CMM por sus siglas en inglés), lo cual como lo indica su nombre es un marco de niveles de madurez para la mejora continua de las actividades de los procesos en los que se pueda medir, comúnmente en 5 escalas (más detalle en https://en.wikipedia.org/wiki/Capability_Maturity_Model). Si bien este CMM nació para los procesos de desarrollo de Software, actualmente es aplicado a muchas áreas de procesos y servicios, y en el caso de los Centros de Operaciones y Seguridad (SOC por sus siglas en inglés), se tiene varias metodologías para medir, pero una de las más utilizadas es la SOC-CMM cuyo análisis se evalúa bajo la gestión óptima de sus 5 áreas de conocimiento (más detalle en <https://www.soc-cmm.com/introduction/>). La obtención de una certificación en nivel de madurez garantiza a los clientes de un proveedor que los servicios brindados están realizándose bajo un enfoque metodológico y de cumplimiento de un estándar.

Sustento Legal:

Siendo el Modelo de Capa de Madurez un punto de índole técnico para centros de SOC u CyberSoc (SOC-CMM), no se ha encontrado aspectos legales al cual poder sustentar, sin embargo, existe varios componentes resolutivos a nivel ministerial que mencionan a la norma internacional ISO/IEC 27001, como la RESOLUCIÓN DE SECRETARÍA DE GOBIERNO Y TRANSFORMACIÓN DIGITAL N° 003-2023-PCM/SGTD, donde establece la implementación y mantenimiento del sistema de gestión de seguridad de la información en las entidades públicas y por consiguiente, es importante contar con servicios cuyos proveedores también cumplan dicha norma.

Es preciso indicar que, la certificación ISO 27001 que menciona el postor, si bien es una certificación reconocida mundialmente en el ámbito de la seguridad de la información (específicamente los Sistemas de Gestión de Seguridad de la Información), está enfocada en gestionar riesgos de seguridad de la información, para garantizar la confidencialidad, integridad y disponibilidad de la información, sin embargo no está enfocada a medición de nivel de madurez de procesos (más detalles en <https://www.iso.org/standard/27001>).

Justamente se solicita que el potencial proveedor para el Servicio de Seguridad Gestiona pueda tener la certificación de al menos nivel 3 (de 5 niveles) de madurez en SOC-CMM ya que esto garantizará que los servicios que brinde dicho proveedor cumplan con la mencionada metodología, esto sobre todo para la atención de incidentes, y no solo al ámbito de protección de la información.

Como se mencionó en el informe anterior, no se puede tomar en cuenta como equivalencia una certificación ISO 27001 como si fuera nivel de madurez de un Centro de Operaciones y Seguridad (SOC), porque son temas totalmente distintos. La certificación ISO 27001 garantiza a las empresas gestionar adecuadamente sus propios riesgos de seguridad de la información y en un marco de mejora continua corporativa, garantizando la continuidad del negocio y principalmente del servicio brindado. En cambio, un nivel 3 de madurez de un SOC, garantiza que, en una escala CMM (Capability Maturity Model Modelo de Madurez de Capacidades), dicho SOC ya cuente con procesos de atención y ejecución no solo documentados sino estandarizados, los cuales otorga rapidez y fiabilidad en la atención. Se debe tener en cuenta también que existen empresas que certifican el nivel de madurez de un SOC, como por ejemplo NRD Cyber Security o SOC-CMM, así mismo; lo establecido en el TDR es un requerimiento que se ha venido solicitando desde nuestro

servicio anterior, y debido a que esta institución maneja información del Estado altamente sensible, se exige estándares y marcos de referencias de la industria, además mencionar que lo requerido lo vienen cumpliendo a nivel nacional más de 2 proveedores de servicio de seguridad gestionada. Teniendo en cuenta lo mencionado, se evidencia que no se vulnera la normativa de contrataciones ni se vulnera la pluralidad de postores y libre participación. Por lo tanto dejamos a juicio de este Organismo Superior de Contrataciones del Estado (OSCE) la decisión mantener o quitar este requerimiento en la calidad del servicio”.

(El subrayado y resaltado es nuestro).

Sobre el particular, cabe señalar que el artículo 16 de la Ley y el artículo 29 del Reglamento, establece que las especificaciones técnicas, los términos de referencia o el expediente técnico, que integran el requerimiento, contienen la descripción objetiva y precisa de las características y/o requisitos funcionales relevantes para cumplir la finalidad pública de la contratación, siendo que, el área usuaria es responsable de la adecuada formulación del requerimiento, debiendo asegurar la calidad técnica y reducir la necesidad de su reformulación por errores o deficiencias técnicas que repercutan en el proceso de contratación.

En relación a ello, cabe precisar que, conforme al Principio de Competencia, los procesos de contratación incluyen disposiciones que permiten establecer condiciones de competencia efectiva y obtener la propuesta más ventajosa para satisfacer el interés público que subyace a la contratación, encontrándose prohibida la adopción de prácticas que restrinjan o afecten la competencia.

Ahora bien, en atención a los aspectos cuestionados por el recurrente, se aprecia que la Entidad, como mejor conocedora de las necesidades que desea satisfacer mediante los citados informes ratificó su requerimiento referido a solicitar que el nivel de madurez requerido para el Centro de Operaciones y Seguridad (SOC) sea acreditado con documento emitido por una entidad auditora internacional y no con la presentación del ISO 27000, argumentando que si bien la certificación ISO 27001 garantiza a las empresas gestionar adecuadamente sus propios riesgos de seguridad de la información garantizando la continuidad del negocio del servicio brindado, el nivel de madurez requerido para el SOC genera que el mismo cuente con procesos de atención y ejecución no solo documentados sino estandarizados, los cuales otorga rapidez y fiabilidad en la atención de incidentes y no solo está referido al ámbito de protección de la información, por lo que existe diferencia entre lo que regula y brinda el certificado ISO 27001 y el grado de madurez requerido por la Entidad el cual debe ser acreditado mediante documento emitido por una entidad auditora internacional.

De otro lado precisó que el requerimiento del grado de madurez requerido para el Centro de Operaciones y Seguridad (SOC) así como su forma de acreditación cuenta con más de dos 2 empresas a nivel nacional, por lo que no se vulnera la norma de contrataciones ni se afecta la pluralidad de postores y libre concurrencia.

De lo expuesto en los párrafos precedentes se puede colegir que la Entidad mediante su informe señaló los aspectos por los cuales ratifica la forma de acreditación del

grado de madurez requerido para el Centro de Operaciones y Seguridad (SOC), lo cual tiene carácter de declaración jurada y está sujeto a rendiciones de cuentas.

De otro lado, cabe señalar que, de la revisión del numeral 4.2 del formato de “Resumen Ejecutivo de Actuaciones Preparatorias (servicios)” se aprecia que la Entidad declaró la existencia de pluralidad de proveedores en la capacidad de cumplir con la totalidad del requerimiento, lo cual incluye el grado de madurez requerido para el Centro de Operaciones y Seguridad (SOC) así como su forma de acreditación.

En ese sentido, considerando el análisis de los párrafos precedentes y dado que la pretensión del recurrente, se encuentra orientada a se acepte que el nivel de madurez de nivel 3 de un total de 5 sea acreditado con el certificado ISO 27001, y en tanto la Entidad mediante su informe señaló los aspectos que consideró para no admitir dicha pretensión, ratificando su requerimiento; este Organismo Técnico Especializado ha decidido **NO ACOGER** el presente cuestionamiento, máxime si existe pluralidad de proveedores en la capacidad de cumplir con la totalidad del requerimiento, lo cual incluye el grado de madurez requerido para el Centro de Operaciones y Seguridad (SOC) así como su forma de acreditación.

Finalmente, cabe precisar que, de conformidad con el artículo 9 de la Ley, los funcionarios y servidores que intervienen en el proceso de contratación encargados de elaborar el requerimiento, indagación de mercado, el pliego absolutorio y **el Informe Técnico, así como la atención de los pedidos de información requeridos,** en virtud a la emisión del presente pronunciamiento, con independencia del régimen jurídico que los vincule a la Entidad, **son responsables de la información que obra en los actuados para la adecuada realización de la contratación.**

Cuestionamiento N° 2

Respecto a la “Mitigación de ataques”.

El participante **AGGITY PERU S.A.C.**, cuestionó la absolución de la consulta y/u observación N° 37, señalando que la Entidad no motivó su absolución, puesto que no tuvo presente que las soluciones de mitigación basada en la capa de red y la capa de aplicación cada una tiene su lugar, además no consideró que el análisis de comportamiento adaptativo ofrece una ventaja en término de adaptabilidad, precisión y capacidad para manera ataques DDoS modernos y sofisticados además de identificar y mitigar amenazas en tiempo real. Por lo tanto, la pretensión del recurrente consiste en que **se acepte que las funcionalidades de mitigación de ataques de la solución Anti-DDoS tenga la capacidad de detección y mitigación por comportamiento.**

Pronunciamiento

Al respecto, de la revisión del acápite 4.1.1 del numeral 3.1 del Capítulo III de la sección específica de las Bases de la convocatoria, la Entidad consignó lo siguiente:

<i>“4.1 CARACTERÍSTICAS DEL SERVICIO</i>
--

(...)
 4.1.1 Seguridad Gestionada
 (...) *b) Solución Anti-DDoS*
 (...) **Funcionalidades de mitigación de ataques**
 (...) **• Mitigación de ataques basados en aplicación / Prevención L3-L4: paquetes inválidos, detección inundación ICMP /TCP SYN, expresión regular de carga útil, tasa basada en bloqueo, asignación de tráfico o Mitigación de ataques basados en aplicación / Prevención L3-L4: paquetes inválidos, detección inundación ICMP /TCP SYN, expresión regular de carga útil, tasa basada en bloqueo, asignación de tráfico.**
 (...)”

(El subrayado y resaltado es nuestro).

Así, mediante la consulta y/u observación N° 37, se solicitó confirmar que se aceptará tener la capacidad de detección y mitigación por comportamiento, por lo que, la solución realizará una estimación automática de umbrales adaptativos para parámetros críticos L3, L4 y L7, sugiriendo que el citado texto quede de la siguiente forma: “Mitigación de ataques basados en aplicación / Prevención L3-L4: paquetes inválidos, detección inundación ICMP /TCP SYN, expresión regular de carga útil, tasa basada en bloqueo, asignación de tráfico "o" tener la capacidad de detección y mitigación por comportamiento, en ese sentido la solución realizara una estimación automática de umbrales adaptativos para parámetros críticos L3, L4 y L7”.

Ante lo cual, el comité de selección entre otros aspectos aclaró que mantiene las características técnicas de acuerdo al término de referencia, los cuales indican L3-L4 y como opcional se considerará L7.

En razón a la absolución de la consulta y/u observación N° 37, la Entidad decidió modificar el acápite 4.1.1 del numeral 3.1 de las Bases integradas, según el siguiente detalle:

“4.1 CARACTERÍSTICAS DEL SERVICIO
 (...) *4.1.1 Seguridad Gestionada*
 (...) *b) Solución Anti-DDoS*
 (...) **Funcionalidades de mitigación de ataques**
 (...) **• Mitigación de ataques basados en aplicación / Prevención L3-L4, L7 (opcional): paquetes inválidos, detección inundación ICMP /TCP SYN, expresión regular de carga útil, tasa basada en bloqueo, asignación de tráfico o Mitigación de ataques basados en aplicación / Prevención L3-L4, L7 (opcional): paquetes inválidos, detección inundación ICMP /TCP SYN, expresión regular de carga útil, tasa basada en bloqueo, asignación de tráfico.**
 (...)”

(El subrayado y resaltado es nuestro).

En ese contexto y teniendo en cuenta lo cuestionado por el recurrente, respecto a la absolución señalada en los párrafos precedentes, el área usuaria de la Entidad mediante el INFORME N° 34-2024-MRE/OGI/OTI-RRB ⁷, indicó lo siguiente:

“(…)

Con respecto al presente cuestionamiento, se debe tener en consideración que los requisitos técnicos que se hacen mención en este punto del TDR, corresponden a la solución del anti DDoS (Ataque de denegación de servicio distribuido - Distributed Denial- of-Service), el cual impide principalmente que un atacante inunde uno o más servidores con tráfico de Internet para evitar que los usuarios accedan a servicios y sitios en línea conectados.

En tal sentido, teniendo en cuenta que es la primera defensa que se configura y se antepone en una red de datos, debe de tener como capacidades la mitigación de ataques basados principalmente en la capa L3 y L4, y también pueda asegurar la capa L7 (motivo por el cual se puso como opcional). Luego del anti DDoS, la segunda defensa de la red es el Firewall y posteriormente un WAF; en ese contexto, **no es correcto indicar que se genera redundancias de funcionalidades ya que cada solución tiene un fin específico, y es motivo que también se solicitan cada una de dichas soluciones de ciberseguridad por separado**, que en algunos casos pueden tener ciertas funcionalidades avanzadas que se sobreponen, por las nuevas tecnologías actuales que tienen ciertas marcas, lo que evidencia que para evitar vulnerar el principio de contrataciones es que se solicita las soluciones por separado y no en conjunto o unificadas” (El subrayado y resaltado es nuestro).

Al respecto cabe señalar que a través de la Opinión N° 002-2020/DTN se indicó que el área usuaria es la dependencia que cuenta con los conocimientos técnicos necesarios para definir las características técnicas de los bienes, servicios y obras que se habrán de contratar.

Ahora bien, en atención a los aspectos cuestionados por el recurrente, se aprecia que la Entidad, como mejor conocedora de las necesidades que desea satisfacer mediante el citado informe ratificó su requerimiento referido a las funcionalidades de mitigación de ataques requeridas para la solución del anti DDoS puesto que dicha solución al ser la primera defensa que se configura y se antepone en una red de datos, debe tener la capacidades la mitigación de ataques basados principalmente en la capa L3 y L4 y opcionalmente en la capa L7, lo que impide principalmente que un atacante inunde uno o más servidores con tráfico de Internet a fin de evitar que los usuarios accedan a servicios y sitios en línea conectados.

De lo expuesto en los párrafos precedentes se puede colegir que la Entidad mediante su informe señaló los aspectos por los cuales ratifica las funcionalidades requeridas para la solución del anti DDoS, considerando no modificar el aspecto relacionado a la mitigación de ataques y que dicha condición cuente con la capacidad de detección y mitigación por comportamiento.

En ese sentido, considerando el análisis de los párrafos precedentes y dado que la pretensión del recurrente, se encuentra orientada a que se acepte que las

⁷ Remitido mediante Expediente N° 2024-0100494, de fecha 31 de julio de 2024.

Funcionalidades de mitigación de ataques de la solución Anti-DDoS tenga la capacidad de detección y mitigación por comportamiento, y en tanto la Entidad mediante su informe señaló los aspectos que consideró para no admitir dicha pretensión, ratificando su requerimiento; este Organismo Técnico Especializado ha decidido **NO ACOGER** el presente cuestionamiento.

Finalmente, cabe precisar que, de conformidad con el artículo 9 de la Ley, los funcionarios y servidores que intervienen en el proceso de contratación encargados de elaborar el requerimiento, indagación de mercado, el pliego absolutorio y **el Informe Técnico, así como la atención de los pedidos de información requeridos**, en virtud a la emisión del presente pronunciamiento, con independencia del régimen jurídico que los vincule a la Entidad, **son responsables de la información que obra en los actuados para la adecuada realización de la contratación**.

Cuestionamiento N° 3

Respecto al “Monitoreo gráfico”.

El participante **AGGITY PERU S.A.C.**, cuestionó la absolución de la consulta y/u observación N° 39, señalando que la Entidad no brindó una absolución clara y motivada, al exigir que se presente un monitoreo gráfico de paquetes descartado por firma, pues dicho requerimiento es infundado y se contradice con el requerimiento relacionado a la “mitigación de ataques basados en aplicación/Web Servers-HTTP incorporar firmas o anomalías, expresión regular de la carga útil”. Por lo tanto, la pretensión del recurrente consiste en **que la funcionalidad de reportes de la Solución Anti-DDoS acepte el monitoreo por firmas o anomalías**.

Pronunciamiento

Al respecto, de la revisión del acápite 4.1.1 del numeral 3.1 del Capítulo III de la sección específica de las Bases de la convocatoria, la Entidad consignó lo siguiente:

“4.1 CARACTERÍSTICAS DEL SERVICIO

(...)

4.1.1 Seguridad Gestionada

(...)

b) Solución Anti-DDoS

(...)

Funcionalidades de Reportes

(...)

• Debe contar con un monitoreo gráfico que muestra las estadísticas del rendimiento de todos los paquetes descartados por inundaciones, firmas, anomalías y otras amenazas.

(...)”

(El subrayado y resaltado es nuestro)

Así, mediante la consulta y/u observación N° 39, se solicitó confirmar que también se aceptará tener la capacidad de detección y mitigación por comportamiento, por lo que, la solución realizará una estimación automática de umbrales adaptativos para parámetros críticos L3, L4 y L7, sugiriendo que el citado texto quede de la siguiente

manera: “Debe contar con un monitoreo gráfico que muestre las estadísticas del rendimiento de todos los paquetes descartados por inundaciones, firmas “o” anomalías y otras amenazas”.

Ante lo cual, el comité de selección no confirmó lo solicitado, bajo los argumentos de que: i) en la indagación de mercado se determinó existencia de pluralidad de proveedores, quienes remitieron sus cotizaciones y manifestaron que cumplen con las condiciones establecidas en el requerimiento; y que, ii) las características técnicas del servicio buscan atender las necesidades de la institución, debido a que la Entidad está en proceso de diseño y mejora de su infraestructura de red.

En ese contexto y teniendo en cuenta lo cuestionado por el recurrente, respecto a la absolución señalada en los párrafos precedentes, el área usuaria de la Entidad mediante INFORME N° 35-2024-MRE/OGI/OTI-RRB⁸, precisó lo siguiente:

“(…)

La respuesta a la consulta 39, es la siguiente

Sustento Técnico:

Al respecto, es necesario aclarar que a nivel de **mitigación de ataque** se había aceptado en una etapa anterior de consultas y observaciones que sea por firmas o anomalías, es por ello, que, **para tener un alineamiento lógico y no contradictorio, quedará de la siguiente forma, dentro de la funcionalidad de reporte (...):**

“Debe contar con un monitoreo gráfico que muestre las estadísticas del rendimiento de todos los paquetes descartados por inundaciones, firmas o anomalías”.

(El subrayado y resaltado es nuestro)

Al respecto cabe señalar que a través de la Opinión N° 002-2020/DTN se indicó que el área usuaria es la dependencia que cuenta con los conocimientos técnicos necesarios para definir las características técnicas de los bienes, servicios y obras que se habrán de contratar.

Ahora bien, en atención a los aspectos cuestionados por el recurrente, se aprecia que la Entidad, como mejor conocedora de las necesidades que desea satisfacer mediante el citado informe decidió aceptar lo solicitado por el recurrente modificando la funcionalidad de reporte de la Solución Anti-DDoS y que el monitoreo gráfico sea por “inundaciones, firmas o anomalías”.

De lo expuesto en los párrafos precedentes se puede colegir que la Entidad recién mediante su informe decidió aceptar que el monitoreo gráfico de la Solución Anti-DDoS sea por “inundaciones, firmas o anomalías”.

En ese sentido, considerando el análisis de los párrafos precedentes y dado que la pretensión del recurrente, se encuentra orientada a que la funcionalidad de reportes de la Solución Anti-DDoS acepte el monitoreo por firmas o anomalías, y en tanto la Entidad mediante su informe decidió aceptar dicha pretensión; este Organismo

⁸ Remitido mediante Expediente N°2024-0106771, de fecha 13 de agosto de 2024.

Técnico Especializado ha decidido **ACOGER** el presente cuestionamiento, por lo que, se emitirá las siguientes disposiciones:

- **Se adecuará** el acápite 4.1.1 del numeral 3.1 de la Sección Específica de las Bases integradas definitivas, según el siguiente detalle:

4.1 CARACTERÍSTICAS DEL SERVICIO

(...)

4.1.1 Seguridad Gestionada

(...)

b) Solución Anti-DDoS

(...)

Funcionalidades de Reportes

(...)

- Debe contar con un monitoreo gráfico que muestra las estadísticas del rendimiento de todos los paquetes descartados por inundaciones, firmas, o anomalías ~~y otras amenazas~~.

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

Finalmente, cabe precisar que, de conformidad con el artículo 9 de la Ley, los funcionarios y servidores que intervienen en el proceso de contratación encargados de elaborar el requerimiento, indagación de mercado, el pliego absolutorio y **el Informe Técnico, así como la atención de los pedidos de información requeridos**, en virtud a la emisión del presente pronunciamiento, con independencia del régimen jurídico que los vincule a la Entidad, **son responsables de la información que obra en los actuados para la adecuada realización de la contratación**.

Cuestionamiento N° 4

Respecto a la “Capacidad mínima de nuevas sesiones o conexiones por segundo”.

El participante **AGGITY PERU S.A.C.**, cuestionó la absolución de la consulta y/u observación N° 41, señalando que requerir que la característica “*Capacidad mínima de nuevas sesiones o conexiones por segundo*” sea medida en “HTTP” resulta restrictiva dado que no todos los fabricantes presentan este valor en sus hojas de datos, dado que presentan mediciones con transacciones TCP. Por lo tanto, la pretensión del recurrente consiste en que **se acepte equipo que soporten 140,000 nuevas sesiones o conexiones por segundo medido en HTTP o TCP**.

Pronunciamiento

Al respecto, de la revisión del acápite 4.1.1 del numeral 3.1 de las Bases de la convocatoria, la Entidad consignó lo siguiente:

“4.1 CARACTERÍSTICAS DEL SERVICIO

(...)
4.1.1 Seguridad Gestionada
(...)
c) Seguridad Perimetral
(...)
Los componentes para los Firewalls Externos deberán contar con las siguientes características mínimas:
(...)
• Capacidad mínima de nuevas sesiones o conexiones por segundo de 140,000 medidos en HTTP.
(...)”

(El subrayado y resaltado es nuestro).

Así, mediante la consulta y/u observación N° 41, se solicitó aceptar al menos mediciones en HTTP “o” TCP.

Ante lo cual, el comité de selección decidido no aceptar lo solicitado, bajo los argumentos de que: i) en la indagación de mercado se determinó existencia de pluralidad de proveedores, quienes remitieron sus cotizaciones y manifestaron que cumplen con las condiciones establecidas en el requerimiento; y que, ii) las características técnicas del servicio buscan atender las necesidades de la institución.

En ese contexto y teniendo en cuenta lo cuestionado por el recurrente, respecto a la absolución señalada en los párrafos precedentes, el área usuaria de la Entidad mediante el Informe N° 35-2024-MRE/OGI/OTI-RRB⁹, indicó lo siguiente:

“(...)
La respuesta a la consulta 41, es la siguiente

Sustento Técnico:
Al respecto, es necesario aclarar que los protocolos como HTTP y TCP, son protocolos básicos y comunes que cualquier equipamiento de seguridad perimetral de gama media a gama alta cumplen diversos fabricantes, según en su información pública como también en sus hojas técnicas.

Así mismo, el MRE solicita que la medición de nuevas sesiones o conexiones por segundo sea por HTTP por ser la medición más efectiva y precisa, las cuales se pueden verificar en la información técnica de los fabricantes, Palo Alto y Hillstone

Sin embargo, existen otros fabricantes que no tienen tal información en sus hojas técnicas ni como información pública, pero esta información podría ser obtenida mediante una carta de fabricante. En vista que algunos postores solicitan la apertura y con el objetivo de una mayor pluralidad y al ver que el requisito no restringe ni vulnera la necesidad del MRE, **se da por aceptado el requerimiento del postor que ha elevado la consulta.**

Por lo tanto, se aceptará equipos que soporten 140,000 nuevas sesiones o conexiones por segundo medido en HTTP o TCP (ver detalle en Anexo N° 2)”.

⁹ Remitido mediante Expediente N°2024-0106771, de fecha 13 de agosto de 2024.

Al respecto cabe señalar que a través de la Opinión N° 002-2020/DTN se indicó que el área usuaria es la dependencia que cuenta con los conocimientos técnicos necesarios para definir las características técnicas de los bienes, servicios y obras que se habrán de contratar.

Ahora bien, en atención a los aspectos cuestionados por el recurrente, se aprecia que la Entidad, como mejor conocedora de las necesidades que desea satisfacer recién mediante el citado informe decidió aceptar lo solicitado por el recurrente modificando la Capacidad mínima de nuevas sesiones o conexiones por segundo requerida para los Firewalls Externos y es esta sean medidas en “HTTP o TCP”.

De lo expuesto en los párrafos precedentes se puede colegir que la Entidad recién mediante su informe decidió aceptar que la Capacidad mínima de nuevas sesiones o conexiones por segundo también sea medidas en “TCP”.

En ese sentido, considerando el análisis de los párrafos precedentes y dado que la pretensión del recurrente, se encuentra orientada a que se acepte equipo que soporten 140,000 nuevas sesiones o conexiones por segundo medido en HTTP o TCP, y en tanto la Entidad mediante su informe decidió aceptar dicha pretensión; este Organismo Técnico Especializado ha decidido **ACOGER** el presente cuestionamiento, por lo que, se emitirá las siguientes disposiciones:

- **Se adecuará** el acápite 4.1.1 del numeral 3.1 de la Sección Específica de las Bases integradas definitivas, según el siguiente detalle:

<p>4.1 CARACTERÍSTICAS DEL SERVICIO (...) 4.1.1 Seguridad Gestionada (...) c) Seguridad Perimetral (...) Los componentes para los Firewalls Externos deberán contar con las siguientes características mínimas: (...) • Capacidad mínima de nuevas sesiones o conexiones por segundo de 140,000 medidos en HTTP o TCP.</p>

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

Finalmente, cabe precisar que, de conformidad con el artículo 9 de la Ley, los funcionarios y servidores que intervienen en el proceso de contratación encargados de elaborar el requerimiento, indagación de mercado, el pliego absolutorio y **el Informe Técnico, así como la atención de los pedidos de información requeridos**, en virtud a la emisión del presente pronunciamiento, con independencia del régimen jurídico que los vincule a la Entidad, **son responsables de la información que obra en los actuados para la adecuada realización de la contratación**.

Cuestionamiento N° 5

Respecto al “Throughput de los Firewalls Externos - Firewall Internos”.

El participante **AGGITY PERU S.A.C.**, cuestionó la absolución de la consulta y/u observación N° 40, señalando que la especificación que indica “(...) Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el modo más alto de inspección de seguridad (...)”, en particular “con el modo más alto de inspección de seguridad” es relativo, impreciso y no objetivo. Por lo tanto, la pretensión del recurrente consiste en que; **i) se suprima el término “con el modo más alto de inspección de seguridad” y ii) se acepte los valores de throughput indicado en las hojas de datos de cada fabricante.**

Asimismo, cuestionó la absolución de la consulta y/u observación N° 42, señalando que la especificación que indica “(...) Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el modo más alto de inspección de seguridad (...)”, en particular “con el modo más alto de inspección de seguridad” es relativo, impreciso y no objetivo. Por lo tanto, la pretensión del recurrente consiste en que; **i) se suprima el término “con el modo más alto de inspección de seguridad” y ii) se acepte los valores de throughput indicado en las hojas de datos de cada fabricante.**

Pronunciamiento

Al respecto, de la revisión del acápite 4.1.1 del numeral 3.1 del Capítulo III de las Bases de la convocatoria, la Entidad consignó lo siguiente:

“4.1 CARACTERÍSTICAS DEL SERVICIO

(...)

4.1.1 Seguridad Gestionada

(...)

c) Seguridad Perimetral

(...)

Los componentes para los Firewalls Externos deberán contar con las siguientes características mínimas:

(...)

• Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el modo más alto de inspección de seguridad y este deberá estar público en su hoja de datos. Se debe garantizar que el equipo no degrade su rendimiento por debajo de lo requerido al habilitar los módulos de seguridad

(...)

Los dos (2) Firewall Internos, deberán cumplir técnicamente las siguientes características:

(...)

• El throughput de prevención de amenazas (Control de aplicaciones, IPS, antivirus y antimalware, deberá ser de 15 Gbps como mínimo, medido con transacciones HTTP de

64K o tráfico mixto o mixto empresarial (presentar carta de fabricante, en caso requiera el sustento). Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el modo más alto de inspección de seguridad y este deberá estar público en su hoja de datos. Se debe garantizar que el equipo no degrade su rendimiento por debajo de lo requerido al habilitar los módulos de seguridad.
(...)”

(El subrayado y resaltado es nuestro)

Así, mediante la consulta y/u observación N° 40 y N° 42, se solicitó confirmar que se aceptaran los valores publicados en la hoja de datos de cada fabricante como validados para los parámetros de rendimiento solicitados.

Ante lo cual, el comité de selección no confirmó lo solicitado, ya que, a parte de la hoja de datos, se podrá acreditar mediante una carta del fabricante.

En ese contexto y teniendo en cuenta lo cuestionado por el recurrente, respecto a la absolución señalada en los párrafos precedentes, el área usuaria de la Entidad mediante el INFORME N° 35-2024-MRE/OGI/OTI-RRB¹⁰, indicó lo siguiente:

“respecto a los diferentes niveles o modos de inspección de seguridad
(...)”

La respuesta a la consulta es la siguiente:

Según la solicitud de precisar el alcance de los términos "con el modo más alto de inspección de seguridad" en la presente contratación se aclara lo siguiente:

Dice:

Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el modo más alto de inspección de seguridad y este deberá estar público en su hoja de datos o acreditado mediante Carta del Fabricante. Se debe garantizar que el equipo no degrade su rendimiento por debajo de lo requerido al habilitar los módulos de seguridad.

Deberá decir:

Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido (10 Gbps como mínimo, medido con transacciones HTTP de 64K o tráfico mixto o mixto empresarial) con el nivel o modo que no degrade su rendimiento por debajo de lo solicitado al habilitar los módulos de seguridad, y este deberá estar público en su hoja de datos o acreditado mediante Carta del Fabricante (en la etapa de perfeccionamiento del contrato).
(...)

La respuesta a la consulta es la siguiente:

Según la solicitud de precisar el alcance de los términos "con el modo más alto de inspección de seguridad" en la presente contratación se aclara lo siguiente:

Dice:

El throughput de prevención de amenazas (Control de aplicaciones, IPS, antivirus y

¹⁰ Remitido mediante Expediente N°2024-0106771, de fecha 13 de agosto de 2024.

antimalware, deberá ser de 15 Gbps como mínimo, medido con transacciones HTTP de 64K o tráfico mixto o mixto empresarial (presentar carta de fabricante, en caso requiera el sustento). Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el modo más alto de inspección de seguridad y este deberá estar público en su hoja de datos. Se debe garantizar que el equipo no degrade su rendimiento por debajo de lo requerido al habilitar los módulos de seguridad

Deberá decir:

El throughput de prevención de amenazas (Control de aplicaciones, IPS, antivirus y antimalware, deberá ser de 15 Gbps como mínimo, medido con transacciones HTTP de 64K o tráfico mixto o mixto empresarial, si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el modo que no degrade su rendimiento por debajo de lo requerido al habilitar los módulos de seguridad y este deberá estar público en su hoja de datos (en caso requiera el sustento, deberá presentar carta de fabricante en la etapa de perfeccionamiento del contrato).

Ver detalle en el Anexo N° 7”.

Al respecto cabe señalar que a través de la Opinión N° 002-2020/DTN se indicó que el área usuaria es la dependencia que cuenta con los conocimientos técnicos necesarios para definir las características técnicas de los bienes, servicios y obras que se habrán de contratar.

Ahora bien, en atención a los aspectos cuestionados por el recurrente, se aprecia que la Entidad, como mejor conocedora de las necesidades que desea satisfacer recién mediante el citado informe decidió modificar su requerimiento y suprimir el texto “con el modo más alto de inspección de seguridad” y precisar que, si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido tanto para los Firewalls Externos e Internos.

De lo expuesto en los párrafos precedentes se puede colegir que la Entidad recién mediante su informe decidió suprimir el texto “con el modo más alto de inspección de seguridad” a fin de evitar que el requerimiento cuente con condiciones imprecisas y precisar que el equipo ofertado deberá soportar el throughput requerido, tanto para los Firewalls Externos e Internos.

En ese sentido, considerando el análisis de los párrafos precedentes y dado que la pretensión del recurrente, se encuentra orientada a que i) se suprima el término “con el modo más alto de inspección de seguridad” y ii) se acepte los valores de throughput indicado en las hojas de datos de cada fabricante, y en tanto la Entidad mediante su informe decidió suprimir el texto “con el modo más alto de inspección de seguridad” y precisó que el throughput requerido tanto para los Firewalls Externos e Internos será el precisado en el requerimiento para cada componente; este Organismo Técnico Especializado ha decidido **ACOGER PARCIALMENTE** el presente cuestionamiento, por lo que, se emitirán las siguientes disposiciones:

- **Se adecuará** el acápite 4.1.1 del numeral 3.1 de la Sección Específica de las Bases integradas definitivas, según el siguiente detalle:

“4.1 CARACTERÍSTICAS DEL SERVICIO

(...)

4.1.1 Seguridad Gestionada

(...)

c) Seguridad Perimetral

(...)

Los componentes para los Firewalls Externos deberán contar con las siguientes características mínimas:

(...)

• Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido ~~con el modo más alto de inspección de seguridad~~ (10 Gbps como mínimo, medido con transacciones HTTP de 64K o tráfico mixto o mixto empresarial) con el nivel o modo que no degrade su rendimiento por debajo de lo solicitado al habilitar los módulos de seguridad y este deberá estar público en su hoja de datos o acreditado mediante Carta del Fabricante (en la etapa de perfeccionamiento del contrato). ~~Se debe garantizar que el equipo no degrade su rendimiento por debajo de lo requerido al habilitar los módulos de seguridad.~~

(...)

Los dos (2) Firewall Internos, deberán cumplir técnicamente las siguientes características:

(...)

• El throughput de prevención de amenazas (Control de aplicaciones, IPS, antivirus y antimalware, deberá ser de 15 Gbps como mínimo, medido con transacciones HTTP de 64K o tráfico mixto o mixto empresarial ~~(presentar carta de fabricante, en caso requiera el sustento)~~. Si el fabricante tuviese diferentes niveles o modos de inspección de seguridad, el equipo ofertado deberá soportar el throughput requerido con el modo ~~más alto de inspección de seguridad~~ que no degrade su rendimiento por debajo de lo requerido al habilitar los módulos de seguridad y este deberá estar público en su hoja de datos o acreditado mediante Carta del Fabricante (en caso requiera el sustento, deberá presentar carta de fabricante en la etapa de perfeccionamiento del contrato). ~~Se debe garantizar que el equipo no degrade su rendimiento por debajo de lo requerido al habilitar los módulos de seguridad.~~

(...)”

- **Se incluirá** en el numeral 2.3 del Capítulo II de la de la Sección Específica de las Bases integradas definitivas, según el siguiente detalle:

- Hoja de datos o Carta del Fabricante mediante el cual se acredite el throughput de prevención de amenazas requerido para el Firewalls Externos y Firewall Internos

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

Finalmente, cabe precisar que, de conformidad con el artículo 9 de la Ley, los funcionarios y servidores que intervienen en el proceso de contratación encargados de elaborar el requerimiento, indagación de mercado, el pliego absolutorio y el

Informe Técnico, así como la atención de los pedidos de información requeridos, en virtud a la emisión del presente pronunciamiento, con independencia del régimen jurídico que los vincule a la Entidad, **son responsables de la información que obra en los actuados para la adecuada realización de la contratación.**

Cuestionamiento N° 6

Respecto a la “Integración al Active Directory”.

El participante **AGGITY PERU S.A.C.**, cuestionó la absolución de la consulta y/u observación N° 56, señalando que, el solicitar que la extracción de información contextual del “*Active Directory*” se realice exclusivamente a través de la Solución de Detección y Respuesta Endpoint (EDR) direcciona el requerimiento a una sola empresa, restringiendo la participación de otros proveedores, y así limitando la pluralidad y competencia. Por lo tanto, la pretensión del recurrente consiste en **que se acepte que la información contextual y atributos del “Active Directory” también se extraída del SIEM.**

Pronunciamiento

Al respecto, de la revisión del acápite 4.1.1 del numeral 3.1 del Capítulo III de la sección específica de las Bases de la convocatoria, la Entidad consignó lo siguiente:

“4.1 CARACTERÍSTICAS DEL SERVICIO
(...)
4.1.1 Seguridad Gestionada
(...)
f) Solución de Detección y Respuesta Endpoint (EDR)
(...)
Análítica de comportamiento de Usuario:
(...)
• Deberá contar con integración al Active Directory para extraer información contextual del usuario, incluyendo el departamento en el cual labora, número de teléfono, última fecha de autenticación.
(...)”

(El subrayado y resaltado es nuestro).

Así, mediante la consulta y/u observación N° 56, se solicitó confirmar que se aceptará como mínimo brindar la información desde la solución SIEM, donde se puedan definir umbrales para detectar excesos, la cual pueda procesar los datos para brindar el detalle solicitado.

Ante lo cual, el comité de selección no confirmó lo solicitado, bajo los argumentos de que: i) en la indagación de mercado se determinó existencia de pluralidad de proveedores, quienes remitieron sus cotizaciones y manifestaron que cumplen con las condiciones establecidas en el requerimiento; y que, ii) las características técnicas del servicio buscan atender las necesidades de la institución.

En ese contexto y teniendo en cuenta lo cuestionado por el recurrente, respecto a la absolución señalada en los párrafos precedentes, el área usuaria de la Entidad mediante el Informe N° 35-2024-MRE/OGI/OTI-RRB¹¹, indicó lo siguiente:

“(…) La respuesta a la consulta 56, es la siguiente

Sustento Técnico:

Si bien en el estudio de mercado, más de un proveedor cotizó y manifestaron bajo declaración jurada que cumplen con los requisitos del TDR, en la etapa de estudio de mercado se evidenció que se cumplía la pluralidad de postores.

Sin embargo, en el procedimiento de selección en vista que algunos postores solicitan mayor apertura y con el objetivo de una mayor pluralidad y al ver que el requisito no restringe ni vulnera la necesidad del MRE, se podría aceptar la característica del participante. (ver detalle en Anexo N° 3)

DICE: Deberá contar con integración al Active Directory para extraer información contextual del usuario, incluyendo el departamento en el cual labora, número de teléfono, última fecha de autenticación.

*DEBE DECIR: Deberá contar con integración al Active Directory para extraer información contextual del usuario, incluyendo el departamento en el cual labora, número de teléfono, última fecha de autenticación, **en caso esta información contextual del usuario no pueda ser extraída por el EDR se aceptará que esta información sea brindada desde la solución SIEM**”.*

(El subrayado y resaltado es nuestro).

Al respecto cabe señalar que a través de la Opinión N° 002-2020/DTN se indicó que el área usuaria es la dependencia que cuenta con los conocimientos técnicos necesarios para definir las características técnicas de los bienes, servicios y obras que se habrán de contratar.

Ahora bien, en atención a los aspectos cuestionados por el recurrente, se aprecia que la Entidad, como mejor conocedora de las necesidades que desea satisfacer recién mediante el citado informe decidió aceptar lo solicitado por el recurrente señalando que en caso la información contextual del usuario no pueda ser extraída por el EDR se aceptará que esta información sea brindada desde la solución SIEM.

De lo expuesto en los párrafos precedentes se puede colegir que la Entidad recién mediante su informe decidió aceptar que adicionalmente información contextual del usuario de la Solución de Detección y Respuesta Endpoint (EDR), también pueda ser extraída desde la solución SIEM

En ese sentido, considerando el análisis de los párrafos precedentes y dado que la pretensión del recurrente, se encuentra orientada a que se acepte que la información contextual y atributos del “Active Directory” también se extraída del SIEM, y en tanto la Entidad mediante su informe decidió aceptar dicha pretensión; este Organismo Técnico Especializado ha decidido **ACOGER** el presente cuestionamiento, por lo que, se emitirá las siguientes disposiciones:

¹¹ Remitido mediante Expediente N°2024-0106771, de fecha 13 de agosto de 2024.

- **Se adecuará** el acápite 4.1.1 del numeral 3.1 de la Sección Específica de las Bases integradas definitivas, según el siguiente detalle:

4.1 CARACTERÍSTICAS DEL SERVICIO

(...)

4.1.1 Seguridad Gestionada

(...)

f) Solución de Detección y Respuesta Endpoint (EDR)

(...)

Análítica de comportamiento de Usuario:

(...)

- Deberá contar con integración al Active Directory para extraer información contextual del usuario, incluyendo el departamento en el cual labora, número de teléfono, última fecha de autenticación *en caso esta información contextual del usuario no pueda ser extraída por el EDR se aceptará que esta información sea brindada desde la solución SIEM.*

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

Finalmente, cabe precisar que, de conformidad con el artículo 9 de la Ley, los funcionarios y servidores que intervienen en el proceso de contratación encargados de elaborar el requerimiento, indagación de mercado, el pliego absolutorio y **el Informe Técnico, así como la atención de los pedidos de información requeridos**, en virtud a la emisión del presente pronunciamiento, con independencia del régimen jurídico que los vincule a la Entidad, **son responsables de la información que obra en los actuados para la adecuada realización de la contratación.**

3. ASPECTOS REVISADOS DE OFICIO

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

3.1. Características técnicas mínimas

Al respecto, de la revisión del literal 1) del numeral 2.3 del Capítulo II de la sección específica de las Bases integradas, la Entidad consignó lo siguiente:

*“1) **Ficha Técnica del fabricante** en donde señale la marca y modelo (en caso de software, se podrá colocar el nombre de la solución o software) **de los appliance o componentes ofrecidos en calidad de alquiler**, acompañado de la **información técnica del fabricante y/o documento del mismo**, donde **se detalle las características técnicas mínimas solicitadas**, en idioma español o en su defecto acompañado de la traducción respectiva, emitida por*

traductor público juramentado o traductor colegiado certificado, según corresponda ().*

**Se precisa que las especificaciones técnicas de las soluciones serán evidenciadas con documentación del fabricante. Cuando existan características técnicas que no se encuentren en la documentación del fabricante podrá acreditarse mediante una carta del fabricante”.*

Al respecto, se advierte que la Entidad no precisó las características técnicas mínimas que requiere que se acrediten con la información técnica del fabricante y/o documento del mismo.

En relación a ello, la Entidad mediante INFORME TÉCNICO CS N° 001/CP-SM-17-2024-RE-1¹², señaló que el numeral 4.1.2 del requerimiento, hace referencia a las características técnicas indicadas en el literal 4.1.1 Seguridad Gestionada del numeral 4.1 Características del servicio de los términos de referencia, por lo que el literal l) del numeral 2.3 de las Bases integradas está relacionado a lo indicado en el el literal 4.1.1 Seguridad Gestionada del numeral 4.1 de las Bases.

En ese sentido con ocasión de la integración definitivas de las Bases, se implementarán las siguientes disposiciones:

- **Se adecuará** el numeral 2.3 del Capítulo II de la sección específica de las Bases integradas definitivas, según el siguiente detalle:

“l) Ficha Técnica del fabricante en donde señale la marca y modelo (en caso de software, se podrá colocar el nombre de la solución o software) de los appliance o componentes ofrecidos en calidad de alquiler, acompañado de la información técnica del fabricante y/o documento del mismo, donde se detalle las características técnicas mínimas solicitadas en el literal 4.1.1 Seguridad Gestionada del numeral 4.1 Características del servicio de los términos de referencia, en idioma español o en su defecto acompañado de la traducción respectiva, emitida por traductor público juramentado o traductor colegiado certificado, según corresponda ().
(...)”*

- **Se dejará sin efecto y/o ajustará** todo extremo del pliego absolutorio, las bases o Informe Técnico que se oponga a la disposición prevista en el párrafo anterior.

3.2. Certificación del líder del servicio

Al respecto, de la revisión del literal s) del numeral 2.3 del Capítulo II y del acápite 5.1.2 del numeral 3.1 del Capítulo III, ambos de sección específica de las Bases integradas, se aprecia lo siguiente:

<i>Capítulo II</i>	<i>Capítulo III</i>
<i>“2.3 REQUISITOS PARA PERFECCIONAR</i>	<i>“3.1 TERMINOS DE REFERENCIA</i>

<p><i>EL CONTRATO</i> (...) s) <i>Certificación de Lead Cybersecurity Manager o Certificación Certified Information Systems Security Professional - CISSP del Líder del Servicio, en idioma español o en su defecto acompañado de la traducción respectiva, emitida por traductor público juramentado o traductor colegiado certificado, según corresponda.</i></p> <p><i>CONSULTA 143</i> <i>Respuesta a Consulta 143 del participante THINK NETWORKS PERU S.A.C.: Se aceptará también la certificación CISSP para la firma de contrato, lo cual se incluye en el término de referencia”.</i></p>	<p>(...) 5.1.2. <i>Un (1) Líder del Servicio</i> (...) <i>Certificaciones:</i> <i>El Líder del Servicio deberá contar con certificación de ISO/IEC 27032 Lead Cybersecurity Manager vigente o Certificación Certified Information Systems Security Professional - CISSP vigente o Certificación Certified Information Systems Security Professional - CISSP vigente.</i></p> <p><i>Importante: El ganador de la buena pro deberá presentar para la suscripción del contrato la certificación de Lead Cybersecurity Manager o Certificación Certified Information Systems Security Professional - CISSP en idioma español, o en su defecto acompañado de la traducción respectiva, emitido por traductor público juramentado o traductor colegiado certificado, según corresponda.</i></p> <p><i>CONSULTA 15</i> <i>Respuesta a Consulta 15 del participante AGGITY PERU S.A.C.: No se confirma lo consulta. Como bien lo señala en la nota Importante del numeral 5.1.2. del TDR: El ganador de la buena pro deberá presentar para la suscripción del contrato la certificación de Lead Cybersecurity Manager en idioma español, o en su defecto acompañado de la traducción respectiva, emitido por traductor público juramentado o traductor colegiado certificado, según corresponda.</i></p> <p><i>CONSULTA 136</i> <i>Respuesta a Consulta 136 del participante IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.: No se acepta, debido a que la certificación LCSPC es una certificación básica de ciberseguridad y la certificación SDLPC no es similar al servicio solicitado.</i></p> <p><i>CONSULTA 154</i> <i>Respuesta a Consulta 154 del participante THINK NETWORKS PERU S.A.C.: Se aceptará también la certificación CISSP para la firma de contrato”.</i></p>
--	--

Al respecto, se aprecian incongruencias en el tipo de certificaciones solicitadas al Líder del Servicio, puesto que en los requisitos para perfeccionar el contrato se

solicita certificaciones en “Lead Cybersecurity Manager o Certificación Certified Information Systems Security Professional - CISSP”, mientras que, en los términos de referencia se solicita certificaciones en “ISO/IEC 27032 Lead Cybersecurity Manager vigente o Certificación Certified Information Systems Security Professional - CISSP vigente o Certificación Certified Information Systems Security Professional - CISSP vigente”.

En relación a ello, la Entidad mediante INFORME N° 35-2024-MRE/OGI/OTI-RRB¹³, señaló que las certificaciones que se solicitan para el Líder del servicio son; ISO/IEC 27032 Lead Cybersecurity Manager vigente o Certificación Certified Information Systems Security Professional - CISSP vigente.

En ese sentido con ocasión de la integración definitivas de las Bases, se implementarán las siguientes disposiciones:

- **Se adecuará** el literal s) del numeral 2.3 del Capítulo II y del acápite 5.1.2 del numeral 3.1 del Capítulo III, ambos de sección específica de las Bases integradas definitivas, según el siguiente detalle:

Capítulo II	Capítulo III
<p>“2.3 REQUISITOS PARA PERFECCIONAR EL CONTRATO (...)</p> <p>s) Certificación de ISO/IEC 27032 Lead Cybersecurity Manager vigente o Certificación Certified Information Systems Security Professional - CISSP vigente del Líder del Servicio, en idioma español o en su defecto acompañado de la traducción respectiva, emitida por traductor público juramentado o traductor colegiado certificado, según corresponda.</p> <p>CONSULTA 143</p> <p>Respuesta a Consulta 143 del participante THINK NETWORKS PERU S.A.C.: Se aceptará también la certificación Certified Information Systems Security Professional – CISSP vigente para la firma de contrato, lo cual se incluye en el término de referencia”.</p>	<p>“3.1 TERMINOS DE REFERENCIA (...)</p> <p>5.1.2. Un (1) Líder del Servicio (...)</p> <p>Certificaciones:</p> <p>El Líder del Servicio deberá contar con certificación de ISO/IEC 27032 Lead Cybersecurity Manager vigente o Certificación Certified Information Systems Security Professional - CISSP vigente o Certificación Certified Information Systems Security Professional - CISSP vigente.</p> <p>Importante: El ganador de la buena pro deberá presentar para la suscripción del contrato la certificación de ISO/IEC 27032 Lead Cybersecurity Manager vigente o Certificación Certified Information Systems Security Professional - CISSP vigente en idioma español, o en su defecto acompañado de la traducción respectiva, emitido por traductor público juramentado o traductor colegiado certificado, según corresponda.</p> <p>CONSULTA 15</p> <p>Respuesta a Consulta 15 del</p>

¹³ Remitido mediante Expediente N°2024-0106771, de fecha 13 de agosto de 2024.

	<p>participante AGGITY PERU S.A.C.: No se confirma lo consulta. Como bien lo señala en la nota Importante del numeral 5.1.2. del TDR: El ganador de la buena pro deberá presentar para la suscripción del contrato la certificación de ISO/IEC 27032 Lead Cybersecurity Manager vigente en idioma español, o en su defecto acompañado de la traducción respectiva, emitido por traductor público juramentado o traductor colegiado certificado, según corresponda.</p> <p>CONSULTA 136 Respuesta a Consulta 136 del participante IMPERIA SOLUCIONES TECNOLOGICAS S.A.C.: No se acepta, debido a que la certificación LCSPC es una certificación básica de ciberseguridad y la certificación SDLPC no es similar al servicio solicitado.</p> <p>CONSULTA 154 Respuesta a Consulta 154 del participante THINK NETWORKS PERU S.A.C.: Se aceptará también la certificación Certified Information Systems Security Professional – CISSP vigente para la firma de contrato”.</p>
--	---

- Se dejará sin efecto y/o ajustará todo extremo del pliego absolutorio, las bases o Informe Técnico que se oponga a la disposición prevista en el párrafo anterior.

3.3. Respecto a la Seguridad Gestionada

Al respecto, de la revisión del acápite 4.1.1 del numeral 3.1 del Capítulo III de la sección específica de las Bases integradas, la Entidad consignó lo siguiente:

“4.1 CARACTERÍSTICAS DEL SERVICIO
(...)
4.1.1 Seguridad Gestionada
(...)
i) Servicio del Sistema de Analítica, Eventos de Seguridad Informática y correlación (SIEM)
(...)
La plataforma, en su conjunto, deberá cumplir como mínimo con las siguientes características:
(...)”

• *La plataforma de correlación deberá realizar la colección de fuentes en formato o protocolos: CSV, PSV, TSV, texto plano, Archivos en formato CEF/LEEF, JSON; alojados Servidores FTP/SFTP/FTPS y en carpetas compartidas de equipos Windows y Linux.*
 (...)” (El subrayado y resaltado es nuestro).

De lo expuesto se aprecia que la Entidad requiere que la plataforma de correlación deberá realizar la colección de fuentes en formato o protocolos: CSV, PSV, TSV, texto plano, Archivos en formato CEF/LEEF, JSON; alojados Servidores FTP/SFTP/FTPS y en carpetas compartidas de equipos Windows y Linux., no obstante, se advierte que no se tiene la certeza si, necesariamente la información requerida deben ser en todos los formatos o protocolos detallados: CSV, PSV, TSV, texto plano, Archivos en formato CEF/LEEF, JSON alojados Servidores FTP/SFTP/FTPS o en cualquiera de ellos.

En atención a ello, la Entidad mediante el Informe N° 35-2024-MRE/OGI/OTI-RRB¹⁴, la entidad a fin de brindar información clara precisó que el texto observado quedará de la siguiente manera: “*La plataforma de correlación deberá realizar la colección de fuentes en formato o protocolos: CSV o PSV o TSV o texto plano o Archivos en formato (CEF o LEEF o JSON); alojados Servidores FTP, SFTP y FTPS; y en carpetas compartidas de equipos Windows y Linux*”

En ese sentido con ocasión de la integración definitivas de las Bases, se implementarán las siguientes disposiciones:

- **Se adecuará** el acápite 4.1.1 del numeral 3.1 del Capítulo III de la sección específica de las Bases integradas definitivas, según el siguiente detalle:

“4.1 CARACTERÍSTICAS DEL SERVICIO
 (...)
 4.1.1 Seguridad Gestionada
 (...)
 i) **Servicio del Sistema de Analítica, Eventos de Seguridad Informática y correlación (SIEM)**
 (...)
 La plataforma, en su conjunto, deberá cumplir como mínimo con las siguientes características:
 (...)
 • La plataforma de correlación deberá realizar la colección de fuentes en formato o protocolos: ~~CSV, PSV, TSV, texto plano, Archivos en formato CEF/LEEF, JSON; alojados Servidores FTP/SFTP/FTPS~~ *CSV o PSV o TSV o texto plano o Archivos en formato (CEF o LEEF o JSON); alojados Servidores FTP, SFTP y FTPS y en carpetas compartidas de equipos Windows y Linux.*
 (...)”

¹⁴ Remitido mediante Expediente N°2024-0106771, de fecha 13 de agosto de 2024.

- **Se dejará sin efecto y/o ajustará** todo extremo del pliego absolutorio, las bases o Informe Técnico que se oponga a la disposición prevista en el párrafo anterior.

3.4. Causales de Resolución de Contrato

Al respecto, cabe indicar que, de la revisión del acápite 6 del numeral 3.1 del Capítulo III, de la Sección Específica de las Bases, la Entidad estableció lo siguiente:

“RESOLUCIÓN DEL CONTRATO (artículo 8 de la Ley N° 31564, Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio Público).

Son causales de resolución del contrato la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, en caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, bajo cualquier modalidad. (...).”

Al respecto, cabe señalar que las causales de resolución del contrato se encuentran establecidas expresamente en la normativa de contratación pública, en tal sentido, no corresponde establecer supuestos adicionales.

En ese sentido, con ocasión de la integración definitiva de las Bases, se implementarán las siguientes disposiciones:

- **Se suprimirá** la lista de supuesto de resolución de contrato consignada en el acápite 6 del numeral 3.1 del Capítulo III de la Sección Específica de las Bases Integradas Definitivas.
- **Se dejará sin efecto y/o ajustará** todo extremo del pliego absolutorio, las bases o Informe Técnico que se oponga a la disposición prevista en el párrafo anterior.

3.5. Respecto al Anexo N° 11

De la revisión de la Sección Anexos, la Entidad ha consignado el Anexo N° 11 “Solicitud de bonificación del cinco por ciento (5%) por tener la condición de micro y pequeña empresa”, en caso haya un ítem o ítems cuyo valor estimado corresponde a una Adjudicación Simplificada.

No obstante, de la revisión del numeral 1.2 “Objeto de la convocatoria” del Capítulo I de las Bases integradas, se aprecia que la presente contratación está conformada por un ítem “servicio de seguridad gestionada para el Ministerio de Relaciones Exteriores”, cuyo valor estimado corresponde a un Concurso público; por lo tanto, no corresponde la solicitud de bonificación del cinco por ciento (5%) sobre el puntaje total obtenido, por tener la condición de micro y pequeña empresa (Anexo N°11).

En ese sentido, con ocasión de la integración definitiva de Bases, se implementarán las siguientes disposiciones:

- **Se suprimirá** el Anexo N° 11 “Solicitud de bonificación del cinco por ciento (5%) por tener la condición de micro y pequeña empresa” de la Sección “Anexos” de la Sección Específica de las Bases integradas definitivas.
- **Se dejará sin efecto y/o ajustará** todo extremo del pliego absolutorio, las bases o Informe Técnico que se oponga a la disposición prevista en el párrafo anterior.

4. CONCLUSIONES

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

4.1 Se procederá a la integración definitiva de las Bases a través del SEACE, en atención a lo establecido en el artículo 72 del Reglamento.

4.2 Es preciso indicar que contra el pronunciamiento emitido por el OSCE no cabe interposición de recurso administrativo alguno, siendo de obligatorio cumplimiento para la Entidad y los proveedores que participan en el procedimiento de selección.

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

4.3 Una vez emitido el pronunciamiento y registrada la integración de Bases definitivas por el OSCE, corresponderá al comité de selección **modificar** en el cronograma del procedimiento, las fechas del registro de participantes, presentación de ofertas y otorgamiento de la buena pro, teniendo en cuenta que, entre la integración de Bases y la presentación de propuestas no podrá mediar menos de siete (7) días hábiles, computados a partir del día siguiente de la publicación de las Bases integradas en el SEACE, conforme a lo dispuesto en el artículo 70 del Reglamento.

4.4 Finalmente, se recuerda al Titular de la Entidad que el presente pronunciamiento no convalida extremo alguno del procedimiento de selección.

Jesús María, 28 de agosto de 2024