

**RESOLUCIÓN DEL TRIBUNAL ADMINISTRATIVO DE CONTRATACIÓN
PÚBLICA DE LA COMUNIDAD DE MADRID**

En Madrid, a 18 de diciembre de 2025

VISTO el recurso especial en materia de contratación interpuesto por la representación legal de FIBRATEL, S.L. contra el Acuerdo de fecha 17 de noviembre de 2025 del Consejero Delegado de la Agencia de Ciberseguridad de la Comunidad de Madrid por el que se adjudica el contrato específico denominado: *“Licenciamiento de una solución de arquitectura de ciberseguridad SASE”*, correspondiente al expediente ACR-035-2025 (SDA 25/2022 – Lote 4), licitado por la Dirección General de Racionalización y Centralización de la Contratación dada la condición de la Agencia de Ciberseguridad de la Comunidad de Madrid de entidad adherida al SDA 25/2022, este Tribunal, en sesión celebrada el día de la fecha, ha dictado la siguiente.

RESOLUCIÓN

ANTECEDENTES DE HECHO

Primero. - Mediante invitaciones cursadas a los adjudicatarios del Lote 4 del Sistema de Adquisición Centralizada 25/2022 se convocó la licitación del contrato específico de referencia.

El valor estimado del contrato específico asciende a 2.022.673,99 euros y su plazo de

entrega será de 30 días y de ejecución de 7 meses.

A la presente licitación se han presentado 5 licitadores, entre los que se encuentra el recurrente.

Segundo. - Con fecha 15 de octubre se remiten las invitaciones a participar en el contrato específico que nos ocupa a los licitadores que figuran el listado del SDA 25/2022, concretamente al Lote 4 y siendo objeto de la contratación el *“licenciamiento de solución de arquitectura de ciberseguridad en la nube Secure Access Service Edge- SASE”*.

Con carácter previo a la valoración económica, el 3 de noviembre de 2025 se encomendó a la unidad técnica de la Agencia un informe con la finalidad de verificar la adecuación de las soluciones propuestas por los licitadores a los requisitos mínimos establecidos en el documento de invitación y el pliego de condiciones que a ella se anexa.

Dado que la propia licitación exige que las soluciones ofertadas garanticen la compatibilidad y el cumplimiento de los requisitos técnicos de la solución SASE del fabricante Zscaler, los licitadores incorporaron a sus ofertas la relación de programas incluidos y la modalidad de licenciamiento correspondiente, proporcionando así a la unidad técnica de valoración de la Agencia, la información necesaria para llevar a cabo un análisis completo y debidamente fundamentado de las soluciones ofertadas.

Con fecha 14 de noviembre de 2025, la Agencia de Ciberseguridad emitió el citado informe técnico, del cual se concluye que las propuestas presentadas por ORANGE ESPAGNE, S.A. y FIBRATEL no resultan susceptibles de admisión. Dicho informe determina que, además de basarse en una solución distinta de la requerida en la licitación, las ofertas analizadas presentan diversas insuficiencias técnicas que impiden su adecuación a los requisitos mínimos establecidos. Tales insuficiencias son consecuencia directa de la distinta arquitectura y capacidades inherentes a la solución

ofertada, propias de un fabricante diferente, lo que impide alcanzar los niveles funcionales requeridos.

Con fecha 17 de noviembre de 2025, el Consejero Delegado de la Agencia de Ciberseguridad adjudica el contrato específico a CONSULTORIA, INTEGRACIÓN Y VIRTUALIZACIÓN S.L. y se notifica el mismo día a todos los licitadores.

El recurrente solicita al órgano de contratación información sobre las puntuaciones y demás actuaciones del procedimiento, que son atendidas por correo electrónico desde la Agencia de Ciberseguridad y donde se informa que su oferta ha sido excluida.

Tercero. - El 3 de diciembre de 2025 la representación legal de FIBRATEL S.L. (FIBRATEL), presenta en el Registro General de la Consejería de Economía, Hacienda y Empleo, con entrada en este Tribunal el mismo día, recurso especial en materia de contratación en el que solicita la anulación de la adjudicación y de la exclusión de su oferta.

El 9 de diciembre de 2025 el órgano de contratación remitió a este Tribunal el expediente de contratación y el informe a que se refiere el artículo 56.2 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP).

Cuarto. - La tramitación del expediente de contratación se encuentra suspendida en virtud del Acuerdo adoptado por este Tribunal el 28 de noviembre de 2024 sobre el mantenimiento de la suspensión en los supuestos de recursos sobre los acuerdos de adjudicación.

Quinto. - La Secretaría del Tribunal dio traslado del recurso a los interesados en cumplimiento de la previsión contenida en el artículo 56.3 de la LCSP, concediéndole un plazo, de cinco días hábiles, para formular alegaciones. En el plazo otorgado, se han presentado alegaciones por parte de la adjudicataria de cuyo contenido se dará cuenta en el fundamento quinto de derecho de esta Resolución.

FUNDAMENTOS DE DERECHO

Primero. - Este Tribunal resulta competente para resolver en virtud de lo establecido en el artículo 46.1 de la LCSP y el artículo 3 de la Ley 9/2010, de 23 de diciembre, de Medidas Fiscales, Administrativas y Racionalización del Sector Público de la Comunidad de Madrid.

Segundo. - El recurso ha sido interpuesto por persona legitimada para ello, al tratarse de un licitador excluido del procedimiento de adjudicación, por tanto, cuyos derechos e intereses legítimos individuales o colectivos se han visto perjudicados o puedan resultar afectados de manera directa o indirectamente por las decisiones objeto del recurso (Artículo 48 de la LCSP).

Asimismo, se acredita la representación del firmante del recurso.

Tercero. - El recurso especial se interpuso en tiempo y forma, pues el acuerdo de adjudicación fue adoptado y notificado el 17 de noviembre de 2025 e interpuesto el recurso, en este Tribunal, el 3 de diciembre de 2025, dentro del plazo de quince días hábiles, de conformidad con el pie de recurso que figura en el acuerdo de adjudicación, que prevalece frente a la reducción de plazos establecida en el artículo 58 del RD 36/2020, de 30 de diciembre, por el que se aprueban medidas urgentes para la modernización de la Administración Pública y para la ejecución del Plan de Recuperación, Transformación y Resiliencia.

Cuarto. - El recurso se interpuso contra el acto de adjudicación en el marco de un contrato específico de un SDA de suministro cuyo valor estimado es superior a 100.000 euros. El acto es recurrible, de acuerdo con el artículo 44.1.a) y 2 c) de la LCSP.

Quinto.- Fondo del asunto. Alegaciones de las partes.

1. Alegaciones de la recurrente.

La recurrente acude a NESTKOPE como fabricante del producto para aclarar y demostrar de forma técnica, precisa y verificable, que la solución propuesta se ajusta a las especificaciones técnicas y funcionales descritas en el expediente y que las observaciones recogidas en el informe no se corresponden con las capacidades reales, actuales y públicamente documentadas de la plataforma.

Así manifiesta:

“En un contexto donde la seguridad en la nube y el modelo SASE son pilares fundamentales para la protección de los servicios digitales de la Comunidad de Madrid, Netskope aporta una arquitectura madura, probada y diseñada desde sus fundamentos bajo el principio de Zero Trust, garantizando seguridad, control, visibilidad y rendimiento para usuarios remotos, sedes, aplicaciones internas y servicios en la nube.

Todas las alegaciones descritas en el informe —incluyendo RBI, Browser Isolation para aplicaciones privadas, acceso seguro sin instalación de software en el endpoint, capacidades de ZTNA, segmentación futura, disponibilidad global, DLP avanzado, sandboxing, hardware propio para acceso a sedes y analítica de amenazas— forman parte de la solución de Netskope.

La plataforma SASE y Zero Trust Network Access permite a Madrid Digital disponer de una seguridad unificada y adaptativa, con visibilidad completa del tráfico, control granular de acciones, protección en tiempo real frente a amenazas y una infraestructura de nube de seguridad altamente redundante. Netskope ofrece una aproximación coherente, flexible y moderna, alineada con los objetivos del expediente ACR-035-2025 y plenamente capaz de soportar las necesidades técnicas, operativas y de protección del dato de la Comunidad de Madrid.

En conjunto, Netskope reafirma su condición de solución apta, completa y conforme con los requerimientos del pliego, aportando claridad técnica y desmontando, punto por punto, cada una de las impugnaciones recogidas en el informe”.

A partir de dicho informe, el recurrente da cuenta de las conclusiones de cumplimiento según informe técnico de adjudicación efectuado por la Agencia de Ciberseguridad:

“●Punto 1

○Descripción: *“La solución ofertada debe estar homologada en el Catálogo 105 de Productos y ser STIC del CCN en, al menos, nivel medio”:*

○Conclusión: *El propio pliego (epígrafe 11) declara que la guía CCN aplicable a SaaSno existe, por lo que este requisito es no exigible.*

No existe categoría SaaS en el Catálogo STIC, por lo que ningún fabricante puede cumplirlo (imposibilidad técnica no imputable al licitador).

El pliego reconoce que el sistema aún no está categorizado ENS, lo que impide exigir cualificación.

Se solicita su inaplicabilidad o admisión de equivalencia funcional.

●Punto 2

○Descripción: *“Que la solución identifique y detecte ataques a Active Directory. Mejore la seguridad de su Active Directory inspeccionando el tráfico y detectando comportamientos relacionados con ataques a Active Directory, como elkerberoasting y la enumeración de usuarios”:*

○Conclusión: *La solución de Netskope cumple plenamente con el requisito gracias a su arquitectura de protección multicapa, diseñada para ofrecer una defensa integral tanto a nivel de tráfico como de identidad. Este enfoque permite identificar y bloquear ataques dirigidos al Directorio Activo —incluyendo técnicas comokerberoasting, enumeración de usuarios o intentos de elevación de privilegios— mediante la combinación de firmas específicas en su motor IPS, inspección avanzada del tráfico y controles Zero Trust aplicados al acceso a servicios internos, además de aplicar análisis de comportamiento para detectar anomalías.*

●Punto 3

○Descripción: *“En el Documento de Invitación se establecen como requisito que el fabricante proporcione un “Servicio Cloud en arquitectura multitenant con más de 160 nodos en distribución mundial con alta redundancia”:*

○Conclusión: *Netskope da cumplimiento a este requisito apoyándose en su infraestructura global, compuesta actualmente por 205 nodos diseñados con una arquitectura de alta redundancia.*

●Punto 4

○Descripción: *“La solución debe ofrecer capacidad de Browser Isolation en acceso a aplicaciones privadas, sin requerir la instalación de ningún software ni plugin en el puesto del usuario, y con control completo de la sesión, permitiendo o bloqueando acciones como copiar/pegar, subir o descargar archivos, imprimir, e incluso insertando una marca de agua que permita identificar el usuario, marca de tiempo y mensaje personalizable”:*

○ **Conclusión:** Netskope cumple con el requisito de acceso a aplicaciones privadas, sin requerir la instalación de ningún software ni plugin en el puesto del usuario, y con control completo de la sesión, permitiendo o bloqueando acciones como copiar/pegar, subir o descargar archivos, imprimir, e incluso insertando una marca de agua que permita identificar el usuario, marca de tiempo y mensaje personalizable.

● **Punto 5**

○ **Descripción:** “En el Documento de Invitación se establecen como requisito que: “La solución debe ofrecer protección de aplicaciones a nivel 7, con capacidad para bloquear los ataques conocidos OWASP-10 y las vulnerabilidades conocidas (CVE) en los accesos a los servicios web publicados en modo Zero Trust.”

○ **Conclusión:** Netskope proporciona capacidades completas para detectar y bloquear OWASP-10, apoyándose en su IPS avanzado, firmas específicas de SQL injection (por ejemplo) y análisis en tiempo real en los accesos a los servicios web publicados en modo Zero Trust.” Además, Netskope incluye en la propuesta toda la potencia de UEBA y de CCI, evaluando el comportamiento de los usuarios y además dotando de capacidades de bloqueo a las aplicaciones en base a sus vulnerabilidades.

● **Punto 6**

○ **Adicionalmente, la solución debe proveer un HW propio del fabricante que se conecte al servicio en nube y permita el acceso a servicios ubicados en sedes remotas o ayuntamientos a los usuarios que estén en remoto. Estos appliances hardware deben estar disponibles en varios formatos y además deben permitir extender a futuro la segmentación sobre la red interna de la sede”:**

○ **Conclusión:** La solución ofertada incorpora hardware propio del fabricante, concretamente el modelo NSG-500, y habilita tanto la conectividad remota hacia sedes y ayuntamientos como el acceso desde estas ubicaciones hacia los usuarios. El equipamiento se encuentra disponible en formatos físicos y virtuales, garantizándola escalabilidad y adaptación a distintos escenarios técnicos. Asimismo, la arquitectura propuesta permite extender la segmentación interna de la red en el futuro y, adicionalmente, integra capacidades Zero Trust mediante ZTNA sin necesidad de publicar servicios en internet ni exponer direccionamientos pertenecientes a la Agencia de Ciberseguridad de la Comunidad de Madrid. Estas características acreditan el cumplimiento pleno del requisito, ajustándose al marco técnico y de seguridad establecido en el pliego.

● **Punto 7**

○ **Descripción:** “La solución debe permitir a futuro la incorporación de funcionalidades adicionales sobre el acceso a las aplicaciones privadas como Data Protection o análisis de ficheros mediante Sandboxing. Estas funcionalidades deben estar disponibles a día de hoy en la solución; no son válidas soluciones que plantean estas opciones como parte de su roadmap de evolución tecnológica”

○ **Conclusión:** Tras analizar el requisito y la funcionalidad incluida en la oferta, queda acreditado que Netskope cumple plenamente con la exigencia de disponer, en el momento actual, de capacidades operativas de protección de datos y análisis avanzado de ficheros —incluyendo sandboxing e inspección profunda— aplicables a

aplicaciones privadas. Estas capacidades forman parte del catálogo oficial y están disponibles sin depender de desarrollos futuros, lo que satisface estrictamente lo requerido por la Agencia de Ciberseguridad de la Comunidad de Madrid.

Asimismo, con el fin de aportar un mayor nivel de cobertura funcional y asegurar que el alcance del contrato responda con holgura a los escenarios planteados por el órgano de contratación, Netskope ha incorporado de manera explícita dichas funcionalidades dentro de las licencias propuestas. Esta inclusión garantiza que el adjudicatario dispone desde el inicio de todos los mecanismos necesarios para la protección del dato y el análisis seguro de contenidos, alineándose con el principio de suficiencia técnica exigido en los procesos de contratación pública.

Por tanto, conforme a la interpretación objetiva del pliego y la documentación acreditada, la propuesta de Netskope satisface de forma completa y verificable el requisito técnico analizado.

● **Punto 8**

○ *Descripción: “El documento de invitación indica que: “No se admitirán exclusiones en los acuerdos de nivel de servicio SLA como, por ejemplo: Excluir el tiempo necesario para analizar un contenido desde un punto de vista de ciber amenazas(Threat scanning) y control de fuga de información (DLP). Excluir upgrades no planeados. Excluir de los resultados request o respuestas más grandes de 1MB.”*

○ *Conclusión: El “mantenimiento de emergencia” no es un upgrade ni produce cambios funcionales, sino una medida crítica de seguridad aceptada por el sector. Netskope no realiza upgrades no planificados que generen indisponibilidad. Se cumple el requisito del pliego”.*

Junto a estas alegaciones técnicas incluye un detallado estudio en el que va demostrando punto por punto, siguiendo el informe técnico de la Agencia de Ciberseguridad, su cumplimiento de las prescripciones técnicas exigidas.

Así mismo incluye junto al recurso nueva documentación que probaría la compatibilidad de soluciones.

Considera en conclusión que su oferta cumple con todas las condiciones exigibles y su exclusión vulnera los principios básicos de la contratación pública, solicitando en consecuencia su admisión al procedimiento de adjudicación.

2. Alegaciones del órgano de contratación.

La Agencia de Ciberseguridad considera que lo fundamental del presente recurso se centra en la justificación de la contratación específica, ya que representa el eje central de la controversia y constituye el elemento clave para comprender y valorar el desarrollo del procedimiento seguido.

Así, manifiesta que de conformidad con el documento de invitación estandarizado del SDA 25/2022 disponible en el Portal de Contratación Centralizada, para la elaboración del expediente ACR-035-2025 *“Licenciamiento de solución de arquitectura de ciberseguridad en la nube “Secure Access Service Edge – SASE”*, la Agencia de Ciberseguridad marcó expresamente la casilla que exige el suministro de soluciones determinadas a fin de garantizar la compatibilidad con las funcionalidades existentes.

En concreto, en el apartado 2.2 *“Características principales de las prestaciones”* del documento de invitación, se indica expresamente que:

“☒ Se exige el suministro de soluciones concretas a fin de garantizar la compatibilidad con las funcionalidades existentes. Se incluye justificación en el Anexo IV de este documento”.

Considera que resulta esencial sobre este asunto, señalar además que, a la hora de completar la información perteneciente al Anexo IV del documento de invitación, la Agencia de Ciberseguridad siguió las instrucciones expresamente previstas por la Dirección General de Racionalización y Centralización de la Contratación (DGRCC) en el propio documento, cuyo tenor literal es el siguiente:

“Se deberá aportar la justificación de la instalación existente y de la necesidad de compatibilidad con la misma, que haga técnicamente inviable el uso de otras soluciones; o, en su defecto, la justificación de costes desproporcionados que se generarían en caso de cambio de producto.”

En cumplimiento de esta instrucción, la Agencia de Ciberseguridad hizo constar en el Anexo IV que dispone de un contrato vigente adjudicado a fecha 28 de enero de 2025 cuyo objeto es el servicio de suscripción a bases de datos para la seguridad de acceso a internet en Entidades Locales basado en el software del fabricante Zscaler (ZIA y ZPA) en régimen de cesión de derecho de uso para dar cobertura de seguridad a diferentes Entidades Locales de menos de 20.000 habitantes.

Añade que, precisamente, por tratarse de un sistema crítico para la seguridad de las entidades locales, la Agencia indicó en el Anexo IV que la adopción de una nueva solución implicaría una brecha de seguridad que podría afectar a la integridad, disponibilidad y confidencialidad de los datos ya que la arquitectura actual de la Agencia de Ciberseguridad, tal y como se justifica en el citado Anexo IV, se construyó, probó y optimizó específicamente para funcionar con las licencias y el software Zscaler actual.

De este modo, la Agencia de Ciberseguridad justificó que la necesidad de contratar el software del fabricante Zscaler no responde a una preferencia arbitraria, sino a un requisito técnico objetivo imprescindible para proteger la inversión tecnológica ya realizada, resultando técnicamente inviable de conformidad con el Anexo IV del documento de invitación, el uso de otras soluciones.

En definitiva, la exigencia de compatibilidad plena no constituye una restricción injustificada de la competencia, sino una condición derivada de las especificaciones técnicas del sistema vigente y plenamente amparada por las instrucciones del propio SDA 25/2022.

Con anterioridad al envío de las invitaciones a licitar la DGRCC emitió informe favorable sobre el expediente y concretamente sobre las invitaciones.

Asimismo, con el fin de despejar cualquier duda acerca de la necesidad de la contratación específica, la Agencia de Ciberseguridad remitió a todos los licitadores

que solicitaron participar en el expediente —*en estricto cumplimiento de los principios de igualdad y transparencia*— una memoria justificativa que acompañaba al Documento de Invitación, cuya finalidad fue acreditar de manera expresa la procedencia técnica de acudir a un fabricante concreto.

En dicha memoria además de exponerse los antecedentes de la arquitectura tecnológica actualmente implantada, basada en la solución SASE del fabricante Zscaler, se incorpora un cuarto apartado titulado “*Motivaciones para adquirir el suministro a un fabricante concreto*”.

Este apartado reviste una importancia fundamental ya que detalla los condicionantes tecnológicos que motivan la necesidad de contratar una solución concreta (SASE). Del mismo modo, se hace constar que se trata de una tecnología ya homologada en la Agencia de Ciberseguridad, habiéndose adaptado a la misma todos los procesos de administración, desarrollo, despliegue, operación y explotación. Por tanto, la interoperabilidad de esta tecnología con otros sistemas está ya probada, habiéndose realizado la homologación con todos los servicios relacionados.

En consecuencia, la adquisición de licencias con características técnicas distintas generaría incompatibilidades, dificultades de uso y mantenimiento, con el consiguiente incremento significativo de costes.

No obstante, en cumplimiento de lo especificado en el artículo 12.6 de la LCSP, a la descripción de la licencia se unió el término “o equivalente”.

Considera la Agencia de Ciberseguridad competencia propia elegir el suministro licitado y así continuar con la misma arquitectura existente, pues cambiar a un producto alternativo, como el ofertado por FIBRATEL, que no responde a las exigencias técnicas, no supone únicamente la instalación de un nuevo software. Implicaría la reestructuración de la infraestructura crítica de las EELL y el

reentrenamiento del personal encargado de la gestión y operación de los sistemas, con el riesgo añadido de generar vulnerabilidades temporales durante la transición.

Así mismo considera que en aras al principio de discrecionalidad técnica y una vez justificada la necesidad y demostrado que el producto no es único o exclusivo de un proveedor la opción seguida es conforme a las normas de contratación pública.

Indica que con carácter previo al análisis pormenorizado de los ocho motivos invocados por FIBRATEL en su recurso, ha de recordarse que la oferta presentada por cada licitador debe ser completa, autosuficiente y cerrada en el momento de la finalización del plazo de presentación de propuestas, no siendo admisible que en fase de recurso se aporte información técnica nueva que no figuraba en su oferta.

Tal y como se desprende del propio escrito de recurso de FIBRATEL, la mercantil introduce ahora múltiples referencias, enlaces, descripciones de funcionalidades, capturas y documentación técnica adicional que no constan en los términos resumidos en el informe técnico de valoración ni se deducen de forma clara de la respuesta original. Se trata, por tanto, de información extemporánea que no puede tenerse en cuenta para revisar la decisión de exclusión

Concretando en los incumplimientos de la oferta presentada por FABRITEL resume sus posiciones y que responden a:

- Falta de homologación en el Catálogo 105 CCN-STIC.
- Deficiencias en detección de ataques a Active Directory.
- Número insuficiente de nodos cloud.
- Requisitos que implican instalación de software en el endpoint.
- Cumplimiento parcial o inexistente en OWASP Top-10, sandboxing, ZTNA y SLA.
- Aportación de documentación técnica nueva en fase de recurso, no admisible conforme a la LCSP.

En relación a la vulneración del principio de igualdad de los licitadores destaca que junto con la adjudicataria se han presentado dos ofertas más que cumplen con los requisitos exigidos, por lo que el producto no es exclusivo, pudiendo ser distribuido por varias empresas.

Por todo ello solicita la desestimación del recurso.

3.- Alegaciones de los interesados.

La adjudicataria considera que centrar la defensa de este recurso en una información de NETSKOPE, no es admisible, pues carece de legitimación al no ser parte en la licitación.

Considera así mismo que en esta fase procesal no se puede ni reinterpretar la oferta ni aportar nueva documentación, considera que el recurso pretende reconstruir la oferta de forma extemporánea.

Entrando ya en el fondo del recurso se evidencian determinados puntos donde la oferta de FIBRATEL no cumple el PPT:

- Homologación CPSTIC en Catálogo 105: la solución no estaba homologada en el momento de la oferta.
- Detección de ataques a Active Directory: la oferta reconoció cumplimiento parcial.
- Infraestructura con más de 160 nodos: Netskope solo dispone de 120+ data centers.
- Browser Isolation sin instalación: la solución requiere instalación de software.
- Protección OWASP-10 y CVE: no acreditada de forma completa.
- Hardware propio para ZTNA: la arquitectura se basa en SD-WAN, no en ZTNA puro.

- Funcionalidades adicionales (DLP, sandboxing): cumplimiento parcial y fragmentado.
- SLA sin exclusiones: los términos de Netskope permiten excluir mantenimientos no programados.

Por todo ello considera que la exclusión de la oferta efectuada por el órgano de contratación es conforme a Derecho, solicitando la desestimación del recurso.

Sexto.- Consideraciones del Tribunal.

Vistas las alegaciones de las partes el Tribunal debe recordar que los Pliegos constituyen la base del contrato y sus determinaciones las reglas conforme a las cuales debe ser cumplido al determinar el contenido de la relación contractual.

Igualmente, las características técnicas correspondientes a los productos objeto de suministro corresponde determinarlas al órgano de contratación de acuerdo con lo establecido en el artículo 28 de la LCSP y no cabe relativizarlas, ni obviarlas durante el proceso de licitación.

A la vista de las manifestaciones de la recurrente, del órgano de contratación y de la adjudicataria debe señalarse que nos encontramos ante un debate técnico respecto del que este Tribunal no puede decidir, por lo que ha de prevalecer sin duda el criterio técnico del órgano de contratación sobre la correcta configuración de las prescripciones técnicas a exigir.

Como ha señalado el Tribunal en diversas Resoluciones, baste citar la Resolución 306/2020 de 13 de noviembre o la más reciente 396/2025 de 25 de septiembre, “cabe traer a colación lo señalado por el Tribunal Administrativo Central de Recursos Contractuales en su Resolución 545/2014, de 11 de julio, nos encontramos ante una calificación que tiene una componente de carácter eminentemente técnico, para el que este Tribunal carece de la competencia adecuada al no tratarse de una cuestión

susceptible de ser enjuiciada bajo la óptica de conceptos estrictamente jurídicos. Es decir, se trata de una cuestión plenamente incurso en el ámbito de lo que tradicionalmente se viene denominando discrecionalidad técnica de la Administración, doctrina Jurisprudencial reiteradamente expuesta y plenamente asumida por este Tribunal en multitud de resoluciones entre las que por vía de ejemplo podemos citar la 139/2023 de 13 de abril (para justificar puntuaciones) Resoluciones n.º 435/2023 de 21 de diciembre, (para justificar cumplimiento de prescripciones)

Como hemos abundantemente reiterado, es de plena aplicación a los criterios evaluables en función de juicios de valor la jurisprudencia del Tribunal Supremo respecto de la denominada discrecionalidad técnica de la Administración. Ello supone que tratándose de cuestiones que se evalúan aplicando criterios estrictamente técnicos, el Tribunal no puede corregirlos aplicando criterios jurídicos. No se quiere decir con ello, sin embargo, que el resultado de estas valoraciones no puedan ser objeto de análisis por parte de este Tribunal, sino que este análisis debe quedar limitado de forma exclusiva a los aspectos formales de la valoración, tales como las normas de competencia o procedimiento, a que en la valoración no se hayan aplicado criterios de arbitrariedad o discriminatorios, o que finalmente no se haya recurrido en error material al efectuarla. Fuera de estos casos, el Tribunal debe respetar los resultados de dicha valoración.

El Tribunal Supremo en la Sentencia 813/2017, de 10 de mayo de 2017, delimitando más el ámbito de la discrecionalidad afirma que “la discrecionalidad técnica de la que, ciertamente, están dotados los órganos de contratación para resolver cuál es la oferta más ventajosa no ampara cualquier decisión que pretenda fundarse en ella ni se proyecta sobre todos los elementos en cuya virtud deba producirse la adjudicación. Jugará, por el contrario, solamente en aquellos que, por su naturaleza, requieran un juicio propiamente técnico para el cual sean necesarios conocimientos especializados’ tal y como ocurre por analogía en el caso concreto que nos ocupa”.

Más recientemente la Sentencia de la Sala Tercera del Tribunal Supremo 897/2024

de 23 de mayo de 2024 (rec.2999/2022) en línea con la STS de 25 de abril de 2024 ha considerado que la *“si la decisión de discrecionalidad técnica está insuficientemente motivada es suficiente para su admisión”*.

Asimismo, Tribunal Constitucional ya desde su sentencia 34/1995 estableció la discrecionalidad técnica como herramienta de la administración, de esa manera ha delimitado más el ámbito de la discrecionalidad afirma que *“la discrecionalidad técnica de la que, ciertamente, están dotados los órganos de contratación para resolver cuál es la oferta más ventajosa no ampara cualquier decisión que pretenda fundarse en ella ni se proyecta sobre todos los elementos en cuya virtud deba producirse la adjudicación. Jugará solo en aquellos que, por su naturaleza, requieran un juicio técnico para el que se necesiten conocimientos especializados’ tal y como ocurre por analogía en el caso concreto que nos ocupa”*.

Si la adopción del criterio de elección discrecional esté justificado, motivado y no es arbitrario, se podrá o no estar de acuerdo con sus razonamientos; esa valoración, que se presume imparcial, no puede sustituirse por otra, y menos por la de uno de los postores.

Todos los Tribunales de Recursos Contractuales asumen la doctrina de la discrecionalidad técnica tal y como aquí se ha manifestado, a modo de ejemplo podemos nombrar la Resolución 458/2022 de 22 de septiembre del TARCJA, la Resolución 1187/2022, de 6 de octubre del TACRC, la Resolución 20/2024 de 30 de octubre del OARCE, la Resolución 430/2024, de 20 de noviembre del TCCSP, la Resolución 25/2024 de 8 de marzo del TACPA, la Resolución 108/2024 del TRCCyL, la Resolución 78/2024 de 31 de mayo de TACGal y la Resolución 15/2023 de 18 de enero de TACP Canarias

En el presente caso, la exigencia de utilizar licencias *de solución de arquitectura de ciberseguridad en la nube “Secure Access Service Edge – SASE* , responde a la exigencia de compatibilidad con las funcionalidades existentes.

Se podrá o no estar de acuerdo con sus razonamientos, pero siempre que la adopción del criterio de elección discrecional esté justificado, motivado y no sea arbitrario, dicha valoración, que se presume imparcial, no puede ser sustituida por otra, y menos por la de uno de los licitadores.

En definitiva, no se aprecia por este Tribunal *“arbitrariedad”* en el juicio técnico, en la valoración realizada a la oferta del adjudicatario, ni falta de motivación, por lo que el motivo debe ser desestimado.

Por tanto, procede la desestimación del recurso

Por lo expuesto, vistos los preceptos legales de aplicación, este Tribunal

ACUERDA

Primero. - Desestimar el recurso especial en materia de contratación interpuesto por la representación legal de FIBRATEL, S.L. contra el acuerdo de fecha 17 de noviembre de 2025 del Consejero Delegado de la Agencia de Ciberseguridad de la Comunidad de Madrid por el que se adjudica el contrato específico denominado: *“Licenciamiento de una solución de arquitectura de ciberseguridad SASE”*, correspondiente al expediente ACR-035-2025 (SDA 25/2022 – Lote 4), licitado por la Dirección General de Racionalización y Centralización de la Contratación dada la condición de la Agencia de Ciberseguridad de la Comunidad de Madrid de entidad adherida al SDA 25/2022,

Segundo. - Levantar la suspensión del procedimiento de adjudicación de conformidad con lo estipulado en el artículo 57.3 de la LCSP.

Tercero. - Declarar que no se aprecia la concurrencia de mala fe o temeridad en la interposición del recurso por lo que no procede la imposición de la multa prevista en

el artículo 58 de la LCSP.

NOTIFÍQUESE la presente resolución a las personas interesadas en el procedimiento.

Esta resolución es definitiva en la vía administrativa, será directamente ejecutiva y contra la misma cabe interponer recurso contencioso-administrativo ante el Tribunal Superior de Justicia de la Comunidad de Madrid, en el plazo de dos meses, a contar desde el día siguiente a la recepción de esta notificación, de conformidad con lo dispuesto en los artículos 10, letra k) y 46.1 de la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso Administrativa, todo ello de conformidad con el artículo 59 de la LCSP.

EL TRIBUNAL