**Recurso nº 462/2025**
**Resolución nº 704/2025**
**Sección 1ª**

# RESOLUCIÓN DEL TRIBUNAL ADMINISTRATIVO CENTRAL DE RECURSOS CONTRACTUALES

En Madrid, a 08 de mayo de 2025.

**VISTO** el recurso especial en materia de contratación interpuesto por D. F.H.A., en representación de ORANGE ESPAGNE, S.A.U., contra los pliegos del procedimiento "*Implantación de una red 5G Stand Alone privada y de un Operador Móvil Virtual en el Centro de Adiestramiento de San Gregorio (Zaragoza)",* con expediente 2024/SP03032001/00000748, convocado por la Subdirección General de Gestión Económica del Ministerio de Defensa, susceptible de financiación con cargo a Fondos EU NextGeneration del Plan de Recuperación, Transformación y Resiliencia; este Tribunal, en sesión del día de la fecha, ha adoptado la siguiente Resolución:

## ANTECEDENTES DE HECHO

**Primero.** Aprobado el expediente de contratación para la licitación del contrato mixto de suministros y servicios para la implantación de una red 5G Stand Alone privada y de un Operador Móvil Virtual en el Centro de Adiestramiento de San Gregorio (Zaragoza), tramitado por la vía de urgencia se remitió para su anuncio en el DOUE. El anuncio de licitación y los pliegos fueron publicados en la Plataforma de Contratación del Sector Público los días 22 y 24 de marzo de 2025, respectivamente.

El valor estimado se fijó en 8.016.528,92 € (sin impuestos), con los siguientes códigos de clasificación CPV:

32400000 - Redes.

32500000 - Equipo y material para telecomunicaciones.

32510000 - Sistema inalámbrico de telecomunicaciones.

32523000 - Instalaciones de telecomunicaciones.

48200000 - Paquetes de software de conexión en red, Internet e intranet.

La fecha para la presentación de las ofertas quedó señalada hasta las 9:00 horas del día 21 de abril de 2025.

**Segundo.** La licitación del contrato, que se considera de suministros, por procedimiento abierto está sujeta a la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014 (LCSP, en adelante).

**Tercero.** El 3 de abril de 2025, se formaliza en sede electrónica recurso especial en materia de contratación por parte de la mercantil ORANGE ESPAGNE, S.A.U., contra los pliegos de este procedimiento abierto dirigido a obtener su anulación por considerar que las prescripciones técnicas resultan restrictivas y que únicamente pueden ser ofertadas por la entidad TELEFÓNICA ESPAÑA (en adelante, TELEFÓNICA).

**Cuarto.** Con fecha 22 de abril de 2025 el Subdirector General de Gestión Económica de la Dirección General de Asuntos Económicos del Ministerio de Defensa certifica que, a la fecha fin del plazo de presentación de ofertas ha presentado oferta UTE TSOL TME TIS SAN GREGORIO, cuyos miembros son Telefónica Soluciones de Informática y Comunicaciones de España, S.A.U. (74%), Telefónica Ingeniería de Seguridad S.A.U. (25%) y Telefónica Móviles España S.A.U. (1%).

**Quinto.** En la tramitación de este recurso, se han observado todos los trámites legal y reglamentariamente establecidos, esto es, lo prescrito por la LCSP, así como por el Real Decreto 814/2015, de 11 de septiembre, por el que se prueba el Reglamento de los procedimientos especiales de revisión en materia contractual y de organización del Tribunal Administrativo Central de Recursos Contractuales (en adelante, RPERMC).

Este recurso se ha tramitado con preferencia y urgencia en esta sede por así venir exigido en el artículo 58.2 del Real Decreto –Ley 36/2020, introducido por el apartado cinco de la

disposición final trigésima primera del R.D.-Ley 6/2022, de 29 de marzo, por el que se adoptan medidas urgentes en el marco del Plan Nacional de respuesta a las consecuencias económicas y sociales de la guerra en Ucrania.

Tras el requerimiento efectuado por este Tribunal, al amparo del artículo 56.2 de la LCSP, el órgano de contratación remite, con el expediente, informe al recurso, de 8 de abril de 2025, acompañado de Informe técnico, de 7 de abril de 2025, solicitando la desestimación del recurso.

**Sexto.** Por Acuerdo de este Tribunal de 10 de abril de 2025 dictado al amparo del artículo 58.1 b) Real Decreto-Ley 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, se aprecia que *prima facie* no concurren causas de inadmisibilidad del recurso y se acuerda conceder la medida cautelar consistente en suspender el procedimiento de contratación, sin que esta afecte al plazo de presentación de ofertas ni impida su finalización de conformidad con lo establecido en los artículos 49 y 56 de la LCSP, de forma que según lo establecido en el artículo 57.3 del mismo cuerpo legal, será la resolución del recurso la que acuerde el levantamiento de la medida adoptada.

**FUNDAMENTOS DE DERECHO**

**Primero.** Este Tribunal es competente para conocer del recurso interpuesto, de conformidad con lo dispuesto en el artículo 45 de la LCSP.

**Segundo.** La recurrente interpone recurso contra los pliegos que rigen una licitación en la que no ha presentado oferta.

Respecto del interés que puede ostentar quien no es licitador, traemos a colación la Sentencia del Tribunal Constitucional, Sala Segunda, 52/2007, de 12 de marzo; Sentencia del Tribunal Supremo, Sala III, de 20 de mayo de 2008 –Roj STS 2176/2008–), la regla es que solo los operadores económicos que han presentado su oferta al procedimiento están legitimados para impugnar los pliegos, pues sólo quienes se encuentran en esa situación están en condiciones de alzarse con el contrato. Sin embargo, esta regla quiebra en los

casos en los que el operador económico impugna una cláusula del Pliego que le impide participar en la licitación en condiciones de igualdad (cfr., por todas, Sentencia del Tribunal Supremo, Sala III, 5 de julio de 2005 –Roj STS 4465/2005–).

Esta doctrina es coherente con el Ordenamiento Comunitario, en el que el artículo 1.3 de la Directiva 89/665/CEE requiere que los procedimientos de recurso sean accesibles a cualquier persona que *"tenga o haya tenido interés en obtener un determinado contrato".*

En ese sentido, la Sentencia del TJCE, Sala Sexta, de 12 de febrero de 2004 (asunto C-230/02), señaló: «*27 En este sentido, como ha señalado la Comisión en sus observaciones escritas, la participación en el procedimiento de adjudicación de un contrato puede constituir en principio válidamente, con arreglo al artículo 1, apartado 3, de la Directiva 89/665, un requisito cuyo cumplimiento se exija para determinar que la persona afectada tiene un interés en obtener el contrato de que se trate o puede verse perjudicada por el carácter supuestamente ilegal de la decisión de adjudicación de dicho contrato. Si no ha presentado una oferta, esta persona difícilmente puede demostrar que tiene interés en oponerse a esta decisión o que se ha visto perjudicada o puede verse perjudicada como consecuencia de dicha adjudicación.*

*No obstante, en el supuesto de que una empresa no haya presentado una oferta debido a la existencia de características supuestamente discriminatorias en la documentación relativa a la licitación o en el pliego de cláusulas administrativas, que le hayan impedido precisamente estar en condiciones de prestar todos los servicios solicitados, tendría derecho a ejercitar un recurso directamente contra dichas características, incluso antes de que concluya el procedimiento de adjudicación del contrato público de que se trate»".*

En esta línea se inscribe la doctrina de este Tribunal que se recoge, entre otras muchas, en la Resolución nº 200/2023, de 17 de febrero, según la que para recurrir los pliegos de una licitación, el empresario: (i) debe haber presentado proposición, en tanto solo en este caso adquiere la expectativa de resultar adjudicatario del contrato que conforma el interés legítimo fundante de la legitimación o (ii) no ha podido presentarla como consecuencia de condiciones discriminatorias incluidas en los pliegos, condiciones que son precisamente las que censura en su recurso.

Más recientemente, en la Resolución nº 230/2024 dijimos:

*"Siendo ello así y dado que en modo alguno el recurrente justifica mínimamente que las cláusulas que impugna le hayan impedido presentar oferta en condiciones de igualdad, este Tribunal considera que carece de legitimación para interponer el recurso, al no reunir los requisitos exigidos por el artículo 48 de la LCSP, tal y como se ha interpretado, entre otras, en nuestra Resolución nº 843/2023 y las que en ella se citan.*

*En efecto, en nuestra Resolución nº 843/2023 se señalaba: «Sobre la legitimación para la impugnación de pliegos, distinguiendo que se presente o no proposición, hemos indicado, entre otras, en la resolución nº 3/2023, de 13 de enero de 2023, cuanto sigue: "Tal como hemos expuesto en nuestra Resolución n° 1512/2022, de 1 de diciembre (Recurso n° 1451/2022) la doctrina de este Tribunal en relación con la legitimación activa de los recurrentes que no han presentado oferta en el procedimiento de contratación puede resumirse en dos consideraciones: "para recurrir los pliegos de una licitación, el empresario debe – como regla general con arreglo al artículo 50.1.b) de la LCSP– haber presentado proposición, pues sólo en este caso adquiere la expectativa de resultar adjudicatario del contrato que conforma el interés fundante de su legitimación; sin perjuicio de lo anterior, es preciso reconocer –excepcionalmente– tal legitimación al empresario que no haya concurrido a la licitación como consecuencia de condiciones discriminatorias incluidas en los pliegos que la rigen de cara a su admisión en ella, condiciones que son precisamente las que combata en su recurso."*

En definitiva, la doctrina establecida por este Tribunal para analizar la legitimación del recurrente que no presenta oferta puede sintetizarse, señalando que el recurso solo será admisible cuando el recurrente alegue y mínimamente pruebe que la cláusula o cláusulas del pliego que impugna son nulas, discriminatorias y le impiden presentar oferta en condiciones de igualdad. La sentencia de 26 de enero de 2022 del TGUE, Sala novena ampliada, en el asunto Leonardo SpA contra Agencia Europea de la Guardia de Fronteras y Costas, confirma el criterio que este Tribunal viene manteniendo al analizar la legitimación del recurrente que no presenta oferta.

El objeto social de la recurrente es afín a las prestaciones del servicio que se licita y sostiene en su recurso que algunos de los requisitos que se exigen en el PPT solamente los puede ofrecer TELEFÓNICA, por lo que debe entenderse que ostenta legitimación para recurrir los pliegos ex artículo 48 de la LCSP.

**Tercero.** Los pliegos que rigen la presente licitación de un contrato de suministros, cuyo valor estimado se eleva a 8.016.528,92 €, son susceptibles de recurso especial en materia de contratación, de acuerdo con los artículos 44.1 a) y 44.2 a) de la LCSP.

**Cuarto.** El recurso se ha interpuesto dentro del plazo legalmente establecido al efecto en el artículo 50.1 b) de la LCSP, habiéndose cumplido también con el resto de las formalidades. A pesar de que se trata de un contrato financiado con fondos del Plan de Recuperación, Transformación y Resiliencia, no es de aplicación el plazo especial de diez días naturales del artículo 58.1 del Real Decreto Ley 36/2020 porque no se trata de la impugnación del acuerdo de adjudicación, sino de los pliegos rectores de este procedimiento abierto.

**Quinto.** La defensa de la recurrente centra la impugnación de los pliegos en lo tocante a las prescripciones técnicas pues, a su juicio, resultan restrictivas de la concurrencia y vulneran el principio de igualdad de trato entre licitadores, pues exigen una serie de características técnicas que únicamente pueden ser ofertadas por la entidad TELEFÓNICA, sin tan siquiera permitir que otras mercantiles, como es la recurrente, puedan ofrecer una solución de características análogas o similares a las ofrecidas por TELEFÓNICA a través de su producto.

En concreto, la recurrente ORANGE ESPAGNE, S.A.U., impugna el apartado 5.2 del PPT por vulneración del artículo 126 de la LCSP y así a lo largo de su recurso, tras la cita de la doctrina de este Tribunal y de la propia Jurisprudencia del Tribunal de Justicia de la Unión Europea, advierte que:

"*En consecuencia, aplicada esta doctrina al caso que nos ocupa, basta con comparar las especificaciones del PPT objeto del presente recurso, con las del catálogo de servicios de TELÉFONICA, para darse cuenta de que, el poder adjudicador pretende favorecer a dicha*

*empresa, conculcando así, tanto el principio de igualdad de trato como el de libre concurrencia:*

*Nos referimos concretamente al apartado 5.2. del PPT (Página 33) en el que se indican los requisitos técnicos a cumplir como OMV, solicitando un sistema de comunicaciones seguras, con certificación del Centro Criptológico Nacional (en adelante CCN) para el manejo de información hasta el nivel "Confidencial". Los requisitos, que mostramos a continuación, se corresponden con soluciones externas a los propios operadores, por lo que, podrían ser ofertados por cualquier operador, en cumplimiento de lo solicitado en la presente licitación.*

- *OMV_OB01: El Operador Móvil Virtual (OMV) deberá emplear la arquitectura definida en la CCN-STIC 496, siguiendo el esquema de referencia del CCN para comunicaciones seguras móviles.*

- *OMV_OB02: El OMV permitirá un sistema de comunicaciones seguras especializado en comunicaciones tácticas y deberá integrarse sobre la infraestructura 5G, con certificación del CCN para el manejo de información hasta el nivel "Confidencial". El candidato deberá presentar en su oferta evidencia del certificado del CCN para el manejo de información hasta el nivel "Confidencial".*

- *OMV_OB03: El sistema deberá ser desplegable on-premise en las instalaciones del cliente y bajo completo control del administrador asignado, asegurando total independencia de proveedores externos.*

- *OMV_OB04: El servidor que ejecuta las funciones de OMV deberá estar completamente integrado en la red privada 5G y ofrecer servicio de comunicaciones seguras a los terminales 5G entregados.*

- *OMV_OB05: Se deberá desarrollar una aplicación compatible con dispositivos 5G que permita la conexión a través de la red privada del OMV.*

- *OMV_OB07: El sistema deberá ser capaz de manejar aplicaciones de banda ancha, empleando esquemas avanzados de modulación del sistema 5G para maximizar las tasas de bit-rate.*

- *OMV_OB09: La aplicación de Comunicaciones Seguras deberá contar con una agenda cifrada, oculta y exclusiva, independiente de la agenda del sistema operativo.*

- *OMV_OB10: La aplicación de Comunicaciones Seguras dispondrá de autorización de uso expedido por el Centro Criptológico Nacional para manejar información hasta nivel "Confidencial" en burbuja 5G Stand Alone. El candidato deberá presentar en su oferta un certificado del CCN estableciendo autorización de uso para manejar información hasta nivel "Confidencial" en burbuja 5G SA.*

- *OMV_OB11: La aplicación de Comunicaciones Seguras entre los terminales se basará en una infraestructura cliente-servidor descentralizada, de forma que no existan puntos únicos de fallo, incluso si uno de los nodos queda completamente aislado.*

- *OMV_OB12: La aplicación de Comunicaciones Seguras entre los terminales dispondrá de funcionalidad de posicionamiento, tracking, chat, llamada de voz y video llamada.*

- *OMV_OB16: La aplicación deberá permitir la copia de seguridad y restauración de la información de usuario y configuración, con las debidas medidas de seguridad.*

- *OMV_OB17: La aplicación deberá permitir chats individuales y grupales (hasta 256 usuarios), con funciones avanzadas de envío de ficheros, notas de voz, imágenes, videos, ubicación y contactos.*

*Sin embargo, existen otra serie de **requisitos que solamente puede ofrecer TELEFÓNICA y, que no dotan de mayor seguridad al servicio**, respecto de lo que pudieran ofrecer otros posibles licitadores, concretamente:*

- *OMV_OB06: El sistema deberá ser capaz de gestionar comunicaciones IoT, permitiendo la conexión de una gran cantidad de terminales de baja velocidad, optimizando el uso del espectro y garantizando la eficiencia.*

- *OMV_OB08: La infraestructura del OMV deberá ser capaz de adaptar dinámicamente las formas de onda, utilizando una única forma de onda flexible y programable (software defined waveform), que permita optimizar el rendimiento para múltiples casos de uso.*

- *OMV_OB13: La aplicación de Comunicaciones Seguras sobre ordenadores funcionará en Windows, Linux y Android.*

- *OMV_OB14: La aplicación de Comunicaciones Seguras sobre ordenadores permitirá la comunicación con sensores IP.*

- *OMV_OB15: La aplicación de Comunicaciones Seguras sobre ordenadores permitirá la comunicación IP con carga de pago y mando y control de robótica terrestre y aérea.*

- *OMV_OB18: La aplicación deberá permitir la edición y destrucción de mensajes enviados, tanto de forma local como remota, sin dejar rastro en el dispositivo receptor.*

- *OMV_OB19: La aplicación deberá permitir llamadas individuales y grupales (hasta 8 usuarios) con multivideoconferencia de alta calidad (configurable por el usuario).*

- *OMV_OP01: Se valorará la funcionalidad Push to Video (PTV) que permitirá el envío de videos de alta calidad en tiempo real, con la posibilidad de activar esta función automáticamente desde el OMV, incluida la desactivación de la funcionalidad.*

- *OMV_OB20: La aplicación deberá contar con la funcionalidad Push to Talk (PTT), permitiendo comunicación en grupos de hasta 256 usuarios, con control y priorización de canales.*

- *OMV_OB21: El administrador del OMV deberá tener control total sobre la activación y desactivación de funcionalidades PTT para los usuarios.*

- *OMV_OB22: Todas las comunicaciones deberán contar con seguridad de cifrado extremo-extremo real, con claves generadas y negociadas directamente entre los extremos.*

- *OMV_OB23: El sistema deberá ser multicifra e interoperable, permitiendo el uso de diferentes cifrados simultáneamente (ENS-Alto, Difusión Limitada, Confidencial).*

- *OMV_OB24: El sistema deberá implementar separación de zonas Roja/Negra, con un módulo de cifra independiente (Módulo Crypto).*

- *OMV_OB25: La aplicación deberá utilizar siempre el teclado en "modo incógnito" y el micrófono de forma exclusiva para evitar accesos no autorizados por parte de otras aplicaciones.*

- *OMV_OB26: El sistema deberá comprobar la integridad de la plataforma en el arranque y durante la ejecución, detectando intentos de acceso no autorizados o depuración".*

Además la recurrente en defensa de dicha restricción de la concurrencia competitiva y considerando que solo dichas prescripciones las puede cumplir TELEFONICA, expresa que ha realizado consultas a CCN que es el organismo certificador de soluciones para manejar información clasificada y, por tanto, quien acredita y certifica soluciones en un catálogo denominado CPSTIC (Catálogo de Productos de Seguridad, TIC), adjuntando varias capturas de pantalla en las que se refleja las consultas y la respuestas obtenidas. Y manifiesta:

*"Con esta respuesta del CCN, organismo ajeno totalmente a este procedimiento de contratación, queda claro que únicamente existen en el mercado dos (2) soluciones que cumplan con el requisito exigido de confidencialidad: COMSec de Indra y Secret.T de Telefónica. Pero, también queda claro que, en el PPT se exigen requisitos adicionales, los transcritos en páginas anteriores, que la solución de Indra no cumple, lo que evidencia, sin lugar a duda, la tesis sostenida por mi representada a lo largo de este recurso, esto es, que el pliego se ha redactado favoreciendo a determinada entidad, por lo que claramente, se está restringiendo artificialmente la competencia".*

Tras transcribir de manera parcial el Informe Razonado de la Necesidad para la contratación, indica que *"**en ningún momento en el Informe de Necesidad, se hace referencia a ninguna necesidad específica y concreta de securización.***

*Pero es que a mayor abundamiento en todo lo expuesto hasta ahora, no es la primera vez en los últimos meses, que esta parte ha observado, que unos pliegos van directamente dirigidos a TELEFÓNICA, como ha sucedido, sin ir más lejos el pasado mes de febrero , en Licitación de la D.G. de la Guardia Civil muy similar a la del presente expediente, cuyo objeto consistía en la "Adquisición de una burbuja móvil 5G para despliegue de comunicaciones tácticas para su uso con distintas unidades de la Guardia Civil"8 , en la que, los requisitos establecidos en los pliegos eran prácticamente idénticos a los que se impugnan ahora. Como resultas de dicho proceso, al no poder ser de otra manera, sólo presentó oferta TELEFÓNICA".*

Y como resumen de sus tesis anulatorias del apartado 5.2 del PPT puntualiza:

"*Concluyendo todo lo expuesto hasta ahora:*

- *De acuerdo con lo establecido en la vigente LCSP (Art. 126) las prescripciones técnicas de una licitación deben facilitar a las empresas licitadoras el acceso al expediente de contratación en condiciones de igualdad, estando obligados los órganos de contratación a dar a los licitadores un tratamiento igualitario y no discriminatorio.*

- *Las especificaciones técnicas no podrán, en ningún caso, mencionar una fabricación o una procedencia determinada o un procedimiento concreto, ni hacer referencia a una marca, a una patente o a un tipo, a un origen o a una procedencia determinada con la finalidad de favorecer o descartar ciertas empresas o productos, dando la oportunidad a los licitadores de ofrecer productos o servicios de carácter equivalente.*

- *En el caso que nos ocupa, el Ministerio de Defensa, dicho sea con todos los respetos y en términos de estricta defensa, ha redactado unos pliegos sesgados que van totalmente dirigidos a que sea TELEFÓNICA la única licitadora que se adjudique el proyecto. Hecho éste que, en los últimos meses, curiosamente desde que el accionariado del operador de telecomunicaciones ha experimentado variaciones por todos conocidas, ya se ha producido en otras licitaciones como la reseñada anteriormente de la Guardia Civil.*

*Por consiguiente, no cabe sino concluir que el apartado 5.2 del PPT es contrario a Derecho por cuanto vulnera la vigente normativa de Derecho de la Competencia, procediendo declarar su nulidad".*

En fin, suplica la estimación del recurso con anulación del apartado 5.2. del PPT por cuanto se ha demostrado que dichas prescripciones reproducen literalmente las descripciones del servicio ofrecido por TELEFÓNICA, vulnerando así los principios de igualdad de trato entre licitadores y de libre concurrencia que deben presidir la contratación pública.

**Sexto.** Por su parte, el órgano de contratación en un informe elevado a este Tribunal junto con el expediente, suscrito por el Subdirector General de Gestión Económica de fecha 8 de abril de 2025, se opone a las tesis anulatorias del PPT instada de contrario y se apoya en un informe técnico firmado por Capitán Ingeniero de la Subdirección de Sistemas de Información y Telecomunicaciones de Ejército de Tierra.

Dado el carácter eminentemente técnico de esta discusión, que afecta a la legalidad de las exigencias del PPT, hemos de estar al contenido de este informe de carácter técnico y que afirma:

"*Respecto a las alegaciones de índole jurídico-material que se manifiestan en lo que el técnico responsable de la redacción del PPT entiende, cabe decir:*

- *El PPT para la contratación, no se ha concebido con la intención de exclusión según el ámbito de aplicación de la Directiva 2014/24/UE del Parlamento Europeo y del Consejo de 26 de febrero de 2014, ni de restringir artificialmente la competencia.*

- *El PPT para la contratación, en ningún caso introduce condiciones contrarias al ordenamiento jurídico, primando lo normativo sobre lo contractual, y todos los criterios técnicos en dicho PPT han sido determinados con arreglo a las instrucciones y buenas prácticas de orden técnico para ejecutar la prestación licitada por parte de la entidad adjudicadora dentro de los límites definidos en la LCSP para el establecimiento de prescripciones técnicas.*

- *Todas las prescripciones técnicas incluidas proporcionan a posibles licitantes la posibilidad de cumplirlas en condiciones de igualdad, pero siendo que los productos y servicios que ofrecen son distintos de unos empresarios respecto a los de otros, salvo que se provean de los mismos fabricantes, ofreciendo exactamente lo mismo en aspectos materiales y técnicos, unas ofertas se ajustarán cumpliendo las prescripciones técnicas y otras no, y en todo caso las prescripciones no crean obstáculos injustificados pues cada una ha sido objeto de un minucioso análisis técnico sobre su conveniencia y viabilidad justificando así su necesidad y proporcionalidad técnica.*

- *Sobre el objeto del contrato, se ha dado mucha información y publicidad conociéndose por parte de las empresas interesadas del sector (que pudieran licitar o no) la intención de publicar el expediente de contratación. Siendo así, se ha tratado con equidad a todas, y concretamente se han mantenido varias reuniones presenciales y por videoconferencia con ORANGE, e incluso se tiene constancia de que han realizado un reconocimiento sobre el terreno (en el CENAD de San Gregorio, en Zaragoza) acompañado por personal militar para recabar datos útiles de cara a la preparación de su oferta. Cabe destacar que, en los mismos términos*

*anteriores, se han tratado a varias empresas que se han interesado por el asunto, por ejemplo, Accenture, Vodafone, Telefónica, COMSA, Ericsson. Nunca se han ocultado a las empresas las necesidades del Ejército de Tierra sobre todo en materia de la seguridad que se requeriría.*

- *Al establecer las prescripciones técnicas, debidamente justificadas, se han tenido en cuenta que están presentes en productos del mercado, o que en todo caso están completamente abiertos a la producción de otros más que quieran fabricarlo; en el PPT se han eludido formas de presentación determinada, marcas o nombres de productos exclusivos y/o patentados, y solo se manifiestan necesidades a satisfacer, y que cualquiera puede cumplir adaptando su producción a lo requerido, máxime teniendo en cuenta que se trata de un producto software, precisamente por la precaución de no limitar la pública y libre concurrencia.*

- *La Administración no ha requerido en ningún caso, a los licitadores, ajustarse a ninguna forma de presentación que libremente ha elegido cada productor y que así queda reflejado en el conjunto de los requisitos del PPT; sí se ha exigido que los componentes en la oferta sea ajustada a sus necesidades, y son estos, los licitadores o productores, los que libremente, si quieren participar en la licitación, han de ajustarse a cumplir lo exigido en las prescripciones técnicas, algo que pueden hacer si modifican su forma de producción y/o lo ajustan a lo solicitado, previa adquisición al productor, sin que nada se lo impida. Tampoco puede responsabilizarse a la Administración de que un determinado empresario pretenda licitar y no se encuentre en el mercado su producto, o tampoco encuentre quien se lo venda a través de acuerdos libres de mercado, ajustado a los requisitos, mientras otros si lo encuentran. Además, podrían recurrir a una U.T.E. para la licitación. En definitiva, la Administración, no es responsable de los acuerdos a los que lleguen los licitadores dentro del mercado.*

- *Ninguno de los requisitos especificados y que se recurren, refieren a productos fabricados con un "material" concreto o único bajo una determinada marca, y por tanto, no se excluye cualquier otro que fuera equivalente por sus propiedades.*

*Además, el OMV es un producto software. En los requisitos se aluden características de productos que son estrictamente necesarias, pues solo así pueden garantizar su ajuste a los requisitos y que se asegure el cumplimiento de la función para lo que se desean usar"*

En lo tocante a los motivos de seguridad y las respuestas dadas por el CCN a VODAFONE, el informe técnico adjunto al jurídico matiza que:

*"ORANGE continúa su recurso alegando que de acuerdo con la respuesta del CCN, organismo ajeno totalmente a este procedimiento de contratación, únicamente existen en el mercado dos (2) soluciones que cumplan con el requisito exigido de confidencialidad: COMSec de Indra y Secret.T de Telefónica, y que en el PPT se exigen requisitos adicionales que la solución de Indra no cumple, lo que evidencia que el PPT se ha redactado favoreciendo a determinada entidad, por lo que claramente, se está restringiendo artificialmente la competencia.* ***Ante esta afirmación el técnico responsable de la redacción del PPT manifiesta que absolutamente todos los requisitos obedecen a una necesidad operativa, consistente en que la red sirva para un propósito militar, permitiendo ejecutar las funcionalidades previstas. Por tanto, no debe buscarse más relación en cada requisito que el que lo liga al cumplimiento de un objetivo operativo. No hay forma de manejar la situación aludida de que los requisitos no pueden formularse, si juntos, determinados licitadores, no son capaces de cumplirlos. Los requisitos permiten el filtrado de las ofertas determinando inequívocamente cuales las cumplen****. Por ejemplo, los requisitos R5G_OB13 y R5G_OB14 "Cesión de uso de espectro durante la ejecución del proyecto y posterior periodo de garantía" y "Cesión anual del uso del espectro previo canon" podrían ser argumentados por empresas del sector que no son operadores de telecomunicaciones con licencia de uso del espectro (como podría ser el caso de Indra o Accenture), como imposibles de cumplir porque los operadores también licitantes se negarían a proporcionarlo, es lo mismo que refiere ORANGE respecto a Telefónica cuando dice en su correo al CCN que no puede ofrecer la solución de Telefónica por ser de otro operador, (es decir, se interpreta que Telefónica se negaría a proporcionarle la aplicación que ha fabricado).*

A continuación el informe técnico pasa a refutar cada una de las exigencias técnicas que a juicio de la recurrente limitan la concurrencia competitiva dirigiendo el contrato a una única licitadora, y así:

*"**OMV_OB06:** El sistema deberá ser capaz de gestionar comunicaciones IoT, permitiendo la conexión de una gran cantidad de terminales de baja velocidad, optimizando el uso del espectro y garantizando la eficiencia.*

- *Para el caso de comunicar sensores y maquinaria entre sí para aplicaciones IoT, (Internet de las Cosas), se involucra a multitud de terminales de baja velocidad. Para este caso, respecto al proyecto que nos ocupa, en cuanto acceso al medio, es muy importante tener en cuenta que el número de usuarios simultáneo que permite un sistema 5G es muy superior al permitido en un sistema 4G y anteriores, ya que multiplica por 100 el número de dispositivos conectados por unidad de área respecto a la anterior generación.*

- *En el CENAD SG se pondrán en marcha sendos sistemas "de vigilancia perimetral y de zonas sensibles", "de vigilancia medioambiental", "de mando y control de plataformas autónomas" así como las unidades militares durante sus maniobras portarán numerosos sensores conectables a la red, esperándose alcanzar densidades extremas de dispositivos conectados simultáneamente. **Por tanto, la de dicha conectividad, es una necesidad operativa acuciante que el Ejército de Tierra espera resolver con la red 5G SA objeto del proyecto.***

***OMV_OB08:** La infraestructura del OMV deberá ser capaz de adaptar dinámicamente las formas de onda, utilizando una única forma de onda flexible y programable (software defined waveform), que permita optimizar el rendimiento para múltiples casos de uso.*

- *La selección de las formas de onda adecuadas a cada caso de uso se considera como una de las decisiones más críticas en el desarrollo de la 5G. Idealmente se desea contar con una sola forma de onda flexible, capaz de ser reconfigurada para múltiples aplicaciones y que pudiera definirse por programación (software defined*

*waveform) y generarse en una plataforma hardware. Este requisito busca la escalabilidad futura de la red.*

- *En el Ejército de Tierra se está estudiando la posibilidad de adquirir una forma de onda específica para el uso militar que dificulte, entre otras, la vulnerabilidad de las redes 5G que se construyan con propósitos militares ante la guerra electrónica (EW) de un potencial adversario. Dicha forma de onda se estudia en compatibilidad con el estándar 3GPP por lo que* ***el Ejército de Tierra estima que la capacidad de la infraestructura del OMV de adaptar dinámicamente las formas de onda es una necesidad operativa.***

***OMV_OB13****: La Aplicación de Comunicaciones Seguras sobre ordenadores funcionará en Windows, Linux y Android.*

- *Estos son los tres sistemas operativos predominantes en el mercado de los ordenadores y de los dispositivos móviles por lo que la Aplicación de Comunicaciones Seguras debe funcionar en ellos. Se trata de una capacidad técnica que cumplen la compilación de muchísimas aplicaciones informáticas y que da libertad al Ejército de poder decidir donde la instala sin preocuparse de lo que disponen sus unidades.* ***Es una capacidad técnica no solo oportuna, afecta o puede afectar a la interoperabilidad de sistemas con dicha Aplicación, lo que la convierte en una necesidad operativa.***

***OMV_OB14****: La aplicación de Comunicaciones Seguras sobre ordenadores permitirá la comunicación con sensores IP.*

- *Ya se ha argumentado que en el CENAD SG, las unidades militares durante sus maniobras portarán numerosos sensores conectados a la red.*
- *Los sensores embarcados, así como los dispuestos en el perímetro o en todo el campo de batalla (que se simula en el CENAD SG) y los que portan en sus vehículos y los material de las unidades de combate, establecerán comunicaciones con el CORE 5G mediante este protocolo (Internet Protocol -IP-) de la capa de red, por lo que el OMV se debe conectar a ellos mediante este protocolo, y deben poder*

*gestionarse las comunicaciones seguras con todos aquellos dispositivos susceptibles de conectarse a la red 5G, como pueden ser terminales móviles, cámaras, sensores y demás, que puedan ser gestionados desde un ordenador con sistemas operativos de uso común como Windows, Linux y Android, véase requisito anterior.*

- ***Todo lo anterior obedece a la necesidad operativa de enviar y recibir información actualizada y en tiempo real en los centros de control y los puestos de mando que se establezcan mediante el protocolo estándar IP.***

***OMV_OB15:*** *La aplicación de Comunicaciones Seguras sobre ordenadores permitirá la comunicación IP con carga de pago y mando y control de robótica terrestre y aérea.*

- *Ya se ha argumentado que en el CENAD SG se pondrán en marcha varios sistemas "de vigilancia perimetral y de zonas sensibles", "de vigilancia medioambiental", y "de mando y control de plataformas autónomas".*

- *Los sensores embarcados como carga de pago de plataformas no tripuladas establecerán comunicaciones con el CORE 5G mediante este protocolo (Internet Protocol -IP-) de la capa de red, por lo que el OMV se debe conectar a ellos mediante este protocolo, y deben poder gestionarse las comunicaciones seguras con todos aquellos dispositivos susceptibles de conectarse a la red 5G, como pueden ser los sensores de carga de pago de AGV,s y UAV,s, que puedan ser gestionados desde un ordenador con sistemas operativos de uso común como Windows, Linux y Android, véanse requisitos anteriores.*
- ***Todo lo anterior obedece a la necesidad operativa de enviar y recibir información actualizada y en tiempo real en los centros de control y los puestos de mando que se establezcan mediante el protocolo estándar IP.***

***OMV_OB18:*** *La aplicación deberá permitir la edición y destrucción de mensajes enviados, tanto de forma local como remota, sin dejar rastro en el dispositivo receptor.*

- *Estas funcionalidades propias de aplicativos de mensajería más extendidas, incluso de WhatsApp, satisfacen la necesidad de que los mensajes enviados puedan ser editados con la finalidad de ofuscarlos tanto en su contenido como en su envío que pudiera ser en modo confirmación de lectura, y garantizando la confidencialidad entre los corresponsales con autodestrucción por tiempo o visualización.*

- *La destrucción local y remota de mensajes enviados sin dejar rastro, es otra de las funciones deseables para mantener el secreto de las comunicaciones y la confidencialidad (sanitización) de emisores y receptores de los mensajes, así como en su caso ofuscar potenciales fuentes de información ante presuntos atacantes.*

- ***Es una necesidad operativa del ET relacionada con la seguridad de las operaciones militares, así como con la instrucción y adiestramiento.***

***OMV_OB19:*** *La aplicación deberá permitir llamadas individuales y grupales (hasta 8 usuarios) con multivideoconferencia de alta calidad (configurable por el usuario).*

- *Se consideran funcionalidades imprescindibles poder realizar llamadas individuales, con posibilidad de añadir nuevos usuarios sin cortar la llamada, realizar llamadas grupales de hasta 8 usuarios y realizar multivideoconferencia de hasta 8 usuarios. Se aclara que los 8 usuarios sería el número que marca la esfera de control de un Jefe de una Unidad.*

- ***Es una necesidad operativa del ET relacionada con el mando y control de las unidades militares, así como con su instrucción y adiestramiento.***

***OMV_OP01:*** *Se valorará la funcionalidad Push To Video (PTV) que permitirá el envío de videos de alta calidad en tiempo real, con la posibilidad de activar esta función automáticamente desde el OMV, incluida la desactivación de la funcionalidad.*

- *Push To Video es otra innovación de comunicación crítica que se encontrará disponible gracias a la mayor velocidad de datos y baja latencia de la red 5G, incluso en entorno degradado de las comunicaciones. Sin embargo, no se han encontrado*

*muchas referencias de productores o fabricantes, por lo que en este caso se decidió, a pesar de la notable función que resulta para la operatividad de la red, considerar este requisito OPCIONAL, precisamente para evitar la falta de concurrencia al expediente.*

- *Esta aplicación permitirá con solo presionar un botón en un terminal, o activándolo automáticamente desde el OMV, que se envíe un video a un destinatario o grupo de destinatarios designados.*

- *El Administrador deberá poder activar y desactivar estos servicios a los usuarios desde el Operador Móvil Virtual (OMV).*

- *Permitirá la puesta en contacto de operadores de los diversos sistemas de vigilancia (proyectos basados en sensores y relacionados con la red 5G SA) con los sensores que operan. En un extremo, el sensor dotado de cámara transmitirá un video cada vez que detecte un evento programado. Por otro lado, la aplicación en el teléfono inteligente del operador recibirá el video y podrá monitorear e interactuar a través de la aplicación.*

- *Los dispositivos integrados para esta funcionalidad deberán cumplir las especificaciones IP68 y Mil-Std-810H.*

- ***En una instalación donde se dispara munición real y se utilizan artefactos explosivos todo lo relacionado con la seguridad y la comunicación de eventos críticos así como asociados a obtener mayor conciencia situacional son funcionalidades absolutamente necesarias en el contexto militar.***

***OMV_OB20****: La aplicación deberá contar con la funcionalidad Push To Talk (PTT), permitiendo comunicación en grupos de hasta 256 usuarios, con control y priorización de canales.*

- *La comunicación mediante Push To Talk (PTT) en grupos de hasta 256 usuarios permiten que estos utilicen sus dispositivos móviles en una red tipo MESH, como*

*si se tratara de radios en lugar de teléfonos utilizando como botón de transmisión PTT un botón software mostrado en pantalla o el botón auxiliar integrado en el teléfono (de haberlo).*

- *El sistema permitirá (mediante la priorización y control de canales) la creación de canales de comunicación entre varios usuarios, asignando prioridades a cada uno de ellos y dando al usuario la opción de "pisar" al hablante actual si tiene una prioridad mayor. La aplicación posibilitará el uso simultáneo de varios de estos canales en recepción, pudiéndose establecer la prioridad de cada uno de ellos de manera que el audio recibido dependa de esta priorización. El usuario podrá elegir dinámicamente por cuál de ellos transmitir en cada momento, estableciendo también un canal de transmisión por defecto cuando pulse el botón PTT.*

- *Dentro de los diferentes canales, se mostrará la localización de cada uno de los integrantes (estos mandan su posición con cifrado extremo a extremo con la frecuencia configurada), proporcionando conciencia situacional (Situational Awareness) a través de una interfaz adaptativa que permite su uso tanto en terminales móviles como tablets, a modo de Centro de Mando y Control Táctico para su utilización sobre el terreno.*

- ***En una instalación donde se dispara munición real y se utilizan artefactos explosivos todo lo relacionado con la seguridad y la comunicación de eventos críticos así como asociados a obtener mayor conciencia situacional son funcionalidades absolutamente necesarias en el contexto militar.***

***OMV_OB21:*** *El administrador del OMV deberá tener control total sobre la activación y desactivación de funcionalidades PTT para los usuarios.*

- *Este requisito no puede entenderse sin el anterior. Permite al administrador de la red activar y desactivar estos servicios a los usuarios desde el Operador Móvil Virtual (OMV) porque no es deseable que todos los usuarios de la red, incluidos dispositivos autónomos tengan acceso a esta funcionalidad.*

- ***Mantener el control sobre esta funcionalidad, en función de dispositivos y usuarios, es esencial para la seguridad de las operaciones militares”****.*

Por lo que concierne a las prescripciones específicas de seguridad, el informe técnico de la Subdirección de Sistemas de Información y Telecomunicaciones del Ejército de Tierra, defiende su inclusión en el PPT por los siguientes motivos sin que ello implique restricciones a la concurrencia competitiva como alega ORANGE:

*“**OMV_OB22**: Todas las comunicaciones deberán contar con seguridad de cifrado extremo-extremo real, con claves generadas y negociadas directamente entre los extremos.*

- *No es poco característico solicitar el cumplimiento de este requisito. Aplicaciones como WhatsApp o Telegram, así como otras muchas de mensajería actualmente ofrecen esta funcionalidad y no son específicamente diseñadas para el ámbito militar.*

- *La aplicación dispondrá de cifrado extremo-extremo real, con negociación entre los extremos, en chats, envío de ficheros, llamadas y video llamadas. En todas las comunicaciones grupales, las claves no las generará el OMV, sino que se negociarán entre los extremos, manteniéndose una cifra independiente con cada miembro del grupo.*

- *Respecto a las funcionalidades de mensajería, deberá presentar, además, las siguientes características:*

    - *El envío de mensajes en chats tanto individuales como grupales deberá realizarse siempre con cifrado de extremo a extremo.*

    - *El emisor podrá saber cuándo se ha entregado el mensaje al servidor, cuándo se ha entregado a cada destinatario, cuándo lo ha visto cada receptor e incluso cuándo lo ha leído cada uno. El mismo emisor del mensaje podrá también eliminar o editar un mensaje ya enviado, notificando al receptor.*

- *El emisor tendrá control sobre la información enviada, pudiendo enviarla bajo diferentes modos que le permitirían pedir la confirmación de recepción del mensaje antes de que el receptor pueda leerlo, evitar que salga del círculo de confianza, hacer que se destruya en el receptor después de su visualización o en un tiempo determinado, de forma segura y sin dejar rastro.*

- *En el caso de mensajes seguros, la aplicación, además, impedirá la captura de pantalla, copia de texto o cualquier otro método que permita reproducir de alguna manera el mensaje seguro recibido que pueda disponer de manera nativa el terminal receptor.*

- *El sistema permitirá el envío de ficheros, tanto en conversaciones individuales como grupales, siempre con cifrado de extremo a extremo. La aplicación permite el envío de imágenes, fotos capturadas con la cámara en el momento, envío de cualquier tipo de documento, notas de audio, contactos y ubicación (se podrá compartir la ubicación actual y en tiempo real). El emisor podrá saber cuándo se ha entregado el fichero al servidor, cuándo se ha entregado a cada destinatario, cuándo lo ha visto cada receptor e incluso cuándo lo ha abierto cada uno. Este también podrá eliminar un fichero ya enviado.*

- *Los ficheros enviados y/o recibidos se almacenarán de forma segura, cifrados dentro de la memoria interna de la aplicación, lo que garantizará que nadie, salvo el usuario, pueda acceder a ellos. Como medida de seguridad adicional, los ficheros solo se podrán visualizar desde dentro de la aplicación, con el visor integrado del que dispone el sistema, y para ello el usuario habrá tenido que autenticarse ante la aplicación.*

- *En cuanto a las funcionalidades de llamadas de voz y video llamadas la aplicación permitirá el establecimiento de los siguientes tipos de llamadas:*

    - *Llamadas de voz: tanto individuales como grupales. Se podrán añadir nuevos participantes a una llamada individual ya iniciada sin salir de ella,*

*estableciendo una llamada a tres sin necesidad de realizar una multiconferencia desde el principio. También se podrán establecer llamadas con todos los participantes de un grupo (llamadas en grupo) o llamadas a una lista de usuarios (meetings en tiempo real) de hasta ocho usuarios.*

- *Video llamadas: tanto individuales como grupales. Al igual que para las llamadas de voz, se podrán añadir usuarios a una video llamada ya iniciada. Se permitirán video llamadas a tres, video llamadas en grupo y meetings con vídeo en tiempo real. o Se establecerán canales cifrados independientes (con distinta cifra) con cada participante en la llamada, teniendo el canal de audio y video (en el caso de las video llamadas) un cifrado extremo-extremo con cada uno de los participantes.*

- ***Todo lo anterior se corresponde con las exigencias de seguridad de las operaciones militares en cuanto a seguridad de las comunicaciones COMSEC, por tanto, es un requisito fundamentado operativamente.***

***OMV_OB23:*** *El sistema deberá ser multicifra e interoperable, permitiendo el uso de diferentes cifrados simultáneamente (ENS-Alto, Difusión Limitada, Confidencial).*

- *El sistema será multicifrado e interoperable, pudiéndose utilizar, por ejemplo, una cifra ENS Alto, otra Difusión Limitada y otra Confidencial de manera simultánea. La aplicación será capaz de dar servicio a todos los dominios.*

- *Normalmente los niveles de confidencialidad de diferentes comunicaciones serán diferentes y lo que se preceptúa es disponer de cifrado independiente de cada uno de ellos, por ejemplo, los declarados, de los cuales uno de ellos (ENS-Alto) es propio de uso civil, y los otros dos son los niveles inferiores dispuestos en la Política de Seguridad de la Información del Ministerio de Defensa.* ***Por tanto, nuevamente el fundamento del requisito es operativo y adecuado al uso previsto del sistema en el futuro.***

***OMV_OB24**: El sistema deberá implementar separación de zonas Roja/Negra, con un módulo de cifra independiente (Módulo Crypto).*

- *El sistema incorporará separación de zonas Roja/Negra, incluyendo un Módulo de Cifra (Módulo Crypto) independiente.*

- *Todo sistema de comunicaciones seguras debe cumplir como se especifica en otro requisito con la Guía CCN-STIC-496 que establece en la arquitectura que en los sistemas de comunicaciones móviles deben diseñarse con una clara separación lógica y física entre la parte roja y la parte negra.*

- ***Este requisito se vincula por tanto a las estrictas medidas de seguridad que se requieren para la red pretendida precisamente por su carácter operativo.***

***OMV_OB25:** La aplicación deberá utilizar siempre el teclado en "modo incógnito" y el micrófono de forma exclusiva para evitar accesos no autorizados por parte de otras aplicaciones.*

- *La aplicación utilizará siempre el teclado en “modo incógnito” y el micrófono en modo exclusivo para evitar que ningún otro aplicativo pueda tener acceso al micrófono mientras que esté en uso por la aplicación.*

- ***Esto es una medida de ciberseguridad ante la posibilidad de que un atacante instalara un malware capaz de manipular el micrófono o el teclado, lo cual es una característica absolutamente necesaria desde el punto de vista de la seguridad y la operatividad.***

***OMV_OB26:** El sistema deberá comprobar la integridad de la plataforma en el arranque y durante la ejecución, detectando intentos de acceso no autorizados o depuración.*

- *Se comprobará siempre la integridad de la plataforma, tanto en arranque (detectando un jailbreak o root) como en tiempo de ejecución con la detección de intentos de acceso o depuración por parte de debuggers.*

- *Esto es una medida de ciberseguridad ante la posibilidad de que un atacante instalara un malware capaz de manipular el micrófono o el teclado,* ***lo cual es una característica absolutamente necesaria desde el punto de vista de la seguridad y la operatividad".***

De esta forma, se contra argumentan las versiones dadas por ORANGE sobre el carácter restrictivo de estas exigencias técnicas del OMV y de las medidas de seguridad motivadas por el Ejército de Tierra y con ello se extraen las siguientes conclusiones:

*"1). Los requisitos técnicos del PPT están fundamentados en la MEMORIA TECNICA DE SUBPROYECTO UNICO SECTORIAL 5G, arriba mencionado, siendo estos definidos internamente por el propio ET.*

*2). Una vez analizados, uno por uno, los requisitos que se pretenden impugnar, y a la vista del exhaustivo análisis arriba reflejado, queda claro que estos no mencionan una fabricación o una procedencia determinada o un procedimiento concreto, desarrollo técnico exclusivo, ni hacen referencia a una marca, a una patente o a un tipo, a un origen o a una procedencia determinada con la finalidad de favorecer o descartar ciertas empresas o productos. Además, tampoco limitan la libre participación ni tampoco adjudican automáticamente el expediente a una empresa concreta, considerando por tanto que estos requisitos técnicos son alcanzables por las entidades del sector de las telecomunicaciones, desarrollando esta solución o estableciendo alianzas estratégicas con proveedores tecnológicos especializados para implementar una solución equivalente.*

*3). La capacidad de cumplir con los requisitos del PPT depende de la voluntad, capacidad inversora y técnica de cada licitador interesado para cumplir en plazo, lo cual reafirma el principio de libre competencia.*

*4). Se considera que el Pliego de Prescripciones Técnicas cumple con los principios y requisitos legales, y que los apartados impugnados no vulneran la normativa contractual ni suponen una restricción ilegítima de la concurrencia.*

*5). Todo lo descrito anteriormente refleja que la seguridad del OMV no ha sido únicamente el requisito principal, sino que ha habido otros requisitos operáticos relacionados con el uso*

*que solo el propio ET puede definir, y así se han tenido en cuenta en el PPT, todo ello derivado de la experiencia en maniobras y ejercicios, y alineados con el objetivo de dotar al sistema de una capacidad operativa integral.*

*6). Los requisitos técnicos que se pretenden impugnar en el recurso, se justifican en términos de necesidad, proporcionalidad y adecuación a las finalidades perseguidas por el contrato, de conformidad con lo dispuesto en:*

- *El artículo 116 de la Ley 9/2017, de Contratos del Sector Público.*

- *Los principios de libre concurrencia y eficiencia en la contratación pública.*

- *Las buenas prácticas técnicas y la experiencia acumulada por la Subdirección de Sistemas de Información y Telecomunicaciones (SUBCIS) de la Jefatura del Ciberespacio y de los Servicios de Asistencia Técnica (JCISAT) del Ejército de Tierra".*

Por todo ello y con apoyo en este informe técnico, el Subdirector General de Gestión Económica del Ministerio de Defensa suplica a este Tribunal la desestimación del recurso ya que "*no se ha cometido ninguna irregularidad y declara que no se han vulnerado los principios de libre concurrencia e igualdad de trato entre licitadores en el aparatado 5.2 del PPT, y tan solo se pretende en la redacción de dicho PPT se manifiesta que absolutamente todos los requisitos obedecen a una necesidad operativa, consistente en que la red sirva para un propósito militar, permitiendo ejecutar las funcionalidades previstas y siempre cumpliendo los requisitos de seguridad requeridos".*

**Séptimo.** Los términos de la discusión se centran en el apartado 5.2 del PPT y si en concreto, las especificaciones técnicas requeridas para el OMV y sus normas de seguridad contravienen o no los principios de igualdad, no discriminación y concurrencia competitiva que han de presidir los procedimientos de contratación en el sector público (artículos 1 y 132 de la LCSP).

Para ello, hemos de partir del artículo 126 de la LCSP, norma que la recurrente considera vulnerada por el órgano de contratación, y cuyo tenor literal en su apartado 6 advierte:

*"6. Salvo que lo justifique el objeto del contrato, las prescripciones técnicas no harán referencia a una fabricación o una procedencia determinada, o a un procedimiento concreto que caracterice a los productos o servicios ofrecidos por un empresario determinado, o a marcas, patentes o tipos, o a un origen o a una producción determinados, con la finalidad de favorecer o descartar ciertas empresas o ciertos productos. Tal referencia se autorizará, con carácter excepcional, en el caso en que no sea posible hacer una descripción lo bastante precisa e inteligible del objeto del contrato en aplicación del apartado 5, en cuyo caso irá acompañada de la mención «o equivalente»".*

En aplicación del citado artículo, la Resolución 874/2019, de 25 de julio, citaba la Resolución 584/2014, donde se decía "*debe partirse de la existencia de un amplio margen de discrecionalidad para el órgano de contratación a la hora de definir los requisitos técnicos que han de exigirse. Cabe citar en este sentido el informe de la Junta Consultiva de Navarra 2/2009: "La determinación de los criterios técnicos en los pliegos, así como su aplicación concreta por la mesa de contratación, son libremente establecidos por las entidades adjudicadoras de contratos públicos, dentro de los límites de la ciencia y la técnica, por ser ellas las que mejor conocen las necesidades públicas que deben cubrir y los medios de los que disponen y que no son susceptibles de impugnación, salvo en los casos de error patente o irracionalidad". También se citaba en la misma resolución 837/2015, que indicaba a este respecto que "el principio de neutralidad tecnológica se concibe como un principio que debe inspirar la actividad reguladora y que supone que la regulación tecnológica debe prestar atención a los efectos de las acciones y no a las acciones y a los medios por ellos mismos. Así concebido, y como se señala en la tan mencionada resolución de la Comisión del Mercado de las telecomunicaciones de 29 de abril de 2013 'Su objetivo consiste en evitar que, a través de la imposición de una determinada tecnología, se pueda influir en las condiciones de libre competencia en que debe desarrollarse el sector de las comunicaciones electrónicas. La aplicación concreta de este principio en el marco de la contratación administrativa se traduce en que los pliegos de cláusulas administrativas aseguren a los operadores económicos el libre acceso a la prestación del servicio, de tal modo que la Administración, al elaborar los mismos, debe evitar imponer condiciones restrictivas, como puede ser el uso de determinadas tecnologías, que dificulten al libre acceso e imposibiliten la efectividad del principio mencionado. La normativa postula, de este modo, la conveniencia de ofrecer a los*

*operadores, prestadores de servicios, adjudicatarios en concursos públicos, etc., la posibilidad de ofrecer los servicios a través de las tecnologías o infraestructuras que consideren más convenientes, sin limitaciones en la introducción y desarrollo de una tecnología concreta. (…) Este principio inspirador de la actuación de las Administraciones Públicas no puede sin embargo ser incondicionado. En particular, deberá atenderse a la posible existencia de justificaciones objetivas, que podrían hacer decaer la plena aplicación de este principio, tal y como ha señalado el Tribunal Supremo en la Sentencia de 18 de noviembre de 2009 (recurso contencioso administrativo núm. 54/2006) en la que expresamente se indica lo siguiente: 'La flexibilidad con la que se recoge este principio evidencia de que no se trata de un mandato inexorable, sino que el legislador, por supuesto, pero también el Gobierno, podrían adoptar medidas en las que no fuera posible mantener una absoluta neutralidad entre las distintas tecnologías que concurren en este ámbito. Ahora bien, no cabe duda de que en tal caso dicha medida tecnológicamente no neutral debe estar sólidamente justificada, sin que fuese posible adoptar otra equivalente y respetuosa con el referido principio, y ser proporcionada en relación con los objetivos perseguidos.' En definitiva, puede de nuevo concluirse que el principio de neutralidad tecnológica es parte esencial del ordenamiento regulador del sector de las comunicaciones electrónicas, sin perjuicio de que las Administraciones públicas en el marco de su actuación puedan en caso de que esté justificado de manera objetiva hacer uso de la necesaria flexibilidad que reconoce la normativa sectorial a la hora de aplicar el citado principio.'* ***De acuerdo con la citada resolución, el principio de neutralidad tecnológica puede decaer frente a la existencia de justificaciones objetivas que aconsejen el uso de una tecnología determinada."***

Las posiciones enfrentadas han de ser evaluadas al amparo del referido artículo 126.6 de la LCSP y de la doctrina de este Tribunal con relación al establecimiento de las prescripciones técnicas por el órgano de contratación y el principio de discrecionalidad técnica.

En la reciente Resolución nº 9/2025, de 9 de enero de 2025, que a su vez se remite a la Resolución n.º 27/2022, de 20 de enero, con cita de la Resolución 1590/2021, de 12 de noviembre de 2021, señalamos a este respecto lo siguiente:

*"Conviene recordar así, por último, que esta discrecionalidad técnica reconocida en favor del órgano de contratación viene siendo reiterada por este Tribunal. Al efecto puede citarse la Resolución nº 263/2019, de 25 de marzo del mismo año, y las que en ella se citan: «El artículo 1.1 de la LCSP establece, en similares términos al artículo 1 del derogado TRLCSP, que 'La presente Ley tiene por objeto regular la contratación del sector público, a fin de garantizar que la misma se ajusta a los principios de libertad de acceso a las licitaciones, publicidad y transparencia de los procedimientos, y no discriminación e igualdad de trato entre los licitadores; y de asegurar, en conexión con el objetivo de estabilidad presupuestaria y control del gasto, y el principio de integridad, una eficiente utilización de los fondos destinados a la realización de obras, la adquisición de bienes y la contratación de servicios mediante la exigencia de la definición previa de las necesidades a satisfacer, la salvaguarda de la libre competencia y la selección de la oferta económicamente más ventajosa'. Es por ello que continúa siendo totalmente válido el criterio seguido por este Tribunal en la Resolución 220/2017, de 24 de febrero, que con cita a la Resolución 250/2015, de 23 de marzo, y, la Resolución 756/2014, afirma que 'pues bien, debe tenerse presente (...) lo dispuesto en los artículos 86 y 117.2 del TRLCSP, con arreglo a los cuales el contrato debe ajustarse a los objetivos que la Administración contratante persigue para la consecución de sus fines, correspondiendo a ésta apreciar las necesidades a satisfacer con el contrato y siendo la determinación del objeto del contrato una facultad discrecional de la misma, sometida a la justificación de la necesidad de la contratación y a las limitaciones de los artículos 22 y 86 del TRLCSP. Por ello, como ha reconocido este Tribunal en las Resoluciones, 156/2013, de 18 de abril y 194/2013, de 23 de mayo, la pretensión de la recurrente no puede sustituir a la voluntad de la Administración'."*

Expuesta la anterior doctrina, debemos traer a colación, por ser especialmente ilustrativo lo dispuesto por el órgano de contratación, con remisión al informe técnico que acompaña y que expone que el apartado 5.2 del PPT impugnado por ORANGE, en lo referido a los requisitos técnicos del OMV y sus normas de seguridad, no responde a una marca concreta ni se han definido pensando en las soluciones técnicas de una empresa, sino en las necesidades del Ministerio de Defensa para la implantación de una RED 5G y de un OMV en el Centro de Adiestramiento de San Gregorio (Zaragoza) y todo ello, presidido por las estrictas medidas de seguridad que se requieren para la red pretendida precisamente por su carácter operativo.

Pues bien, habida cuenta del objeto del contrato, y considerando el Ministerio de Defensa ha motivado las necesidades técnicas para la implementación de tecnologías avanzadas en defensa, incluyendo las políticas de ciberseguridad y la actualización constante de los sistemas de información, no se aprecia la infracción que invoca la recurrente por este Tribunal, siguiendo la doctrina reiterada en numerosas resoluciones, en la que se reconoce al órgano de contratación, en aras del interés general que subyace en la licitación, un amplio margen de discrecionalidad en la determinación del objeto del contrato y de los requisitos técnicos exigidos en las licitaciones pública, a fin de garantizar, en conexión con el objetivo de estabilidad presupuestaria y control del gasto, una eficiente utilización de los fondos públicos.

Y así, desde un punto de vista formal, estos requisitos satisfacen plenamente lo descrito en el artículo 126 LCSP. Respecto al listado de requisitos impugnados, por una parte, están descritos en términos funcionales, sin referencia a marcas ni fabricantes.

Hay algunas referencias tecnológicas, como la compatibilidad con sistemas operativos Windows, Linux y Android, pero estos son de amplio uso, con lo cual no parece algo restrictivo. Otras referencias como PPT (Push to Talk) o PPV (Push to Video) y otras del estilo, no se refieren a soluciones de marcas concretas ni patentes, sino a tecnologías genéricas, por lo que tampoco parece que estén limitando la competencia en este sentido.

Se infiere del recurso que la solución de ORANGE no cumpliría algunos de los requisitos exigidos en el apartado 5.2 del PPT, pero eso no quiere decir no correspondan a necesidades reales del Ministerio de Defensa. Por ejemplo, no parece desproporcionado que el Ministerio de Defensa quiera poder comunicar con sensores en campo, o que no sea útil la función de “pulsar y verse” (Push to Video) o “pulsar para hablar” (Push to Talk). En general, desde el punto de vista del artículo 126 de la LCSP el informe del órgano de contratación justifica todos los requisitos muy razonadamente.

Por otro lado, la argumentación más poderosa de ORANGE parece construirse sobre el hecho de que no dispone en su cartera de productos de una aplicación de comunicaciones seguras. Es decir, ORANGE ataca principalmente la aplicación de comunicaciones seguras y por ello impugna el apartado 5.2 del PPT, que contiene la descripción de dicha aplicación.

Pues bien, en aplicación de la Guía CCN-STIC 496 y otras como la Guía CCN-STIC-101, el CCN está legitimado para elaborar estas guías en virtud de la Disposición Adicional Segunda del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. En concreto, el CCN realiza la acreditación mediante el procedimiento descrito en la Guía CCN-STIC-101 a la que se refiere la 496. Dado que la Guía 496 establece que los sistemas de cifra deben tener una certificación nacional, el Ministerio de Defensa está legitimado para exigir este certificado y no admitir otros, como por ejemplo uno equivalente de Francia o uno de la OTAN (que también habrían podido ser válidos). En la medida en que la restricción a la concurrencia responde a una exigencia contenida en la Guía 496 del CCN, no resulta injustificada.

Por todo lo anteriormente expuesto, dado que la posible discriminación no radica en que el cumplimiento de una prescripción recaiga en un número limitado de empresas, sino en que dicha prescripción pudiera haberse establecido de manera injustificada o innecesaria, se considera que las exigencias que prevé el PPT denunciadas por la recurrente, a la vista del informe técnico que se adjunta al informe al recurso, no adolecen de aquella característica, pues se encuentran adecuadamente justificadas por el órgano de contratación, con base en su discrecionalidad técnica y sin que la recurrente haya conseguido rebatir dicha necesidad. Además, de acuerdo con la información aportada por ella misma en el recurso, habría otra empresa, además de TELEFÓNICA, que cumpliría el requisito de confidencialidad, por lo que debe descartarse que exista un único licitador que pueda cumplir con esa parte del contrato. A pesar de que, según apunta la recurrente -si bien de esta afirmación no aporta ninguna prueba, ni realiza una argumentación detallada que pudiera soportar la misma-, la solución de la otra empresa distinta de TELEFÓNICA no cumpliría requisitos adicionales exigidos en el PPT, ello no obsta para que pudiera concurrir en UTE con otro/s licitador/es que sí que los cumplan.

En consecuencia, procede desestimar el recurso.

Por todo lo cual,

**VISTOS** los preceptos legales de aplicación,

**ESTE TRIBUNAL**, en sesión celebrada en el día de la fecha **ACUERDA:**

**Primero.** Desestimar el recurso especial en materia de contratación interpuesto por D. F.H.A., en representación de ORANGE ESPAGNE, S.A.U., contra los pliegos del procedimiento *"Implantación de una red 5G Stand Alone privada y de un Operador Móvil Virtual en el Centro de Adiestramiento de San Gregorio (Zaragoza)",* con expediente 2024/SP03032001/00000748, convocado por la Subdirección General de Gestión Económica del Ministerio de Defensa.

**Segundo.** Levantar la suspensión del procedimiento de contratación conforme a lo dispuesto por 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.

Esta resolución es definitiva en la vía administrativa y contra la misma cabe interponer recurso contencioso-administrativo ante la Sala de lo Contencioso Administrativo de la Audiencia Nacional, 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 11.1 letra f) y 46.1 de la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso Administrativa.

LA PRESIDENTA
LOS VOCALES