Resolución reclamación art. 24 LTAIBG

S/REF: 001-066948

N/REF: R-0366-2022 / 100-006730 [Expte. 89-2023]

Fecha: La de firma

Reclamante: [redacted]

Dirección: [redacted]

Administración/Organismo: Ministerio de Asuntos Económicos y Transformación Digital

Información solicitada: Documentación relativa a un determinado procedimiento de contratación

Sentido de la resolución: Estimatoria parcial

I. ANTECEDENTES

1. Según se desprende de la documentación obrante en el expediente, el reclamante solicitó el 17 de marzo de 2022 al MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL, al amparo de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno[1] (en adelante, LTAIBG), la siguiente información:

   «En relación al expediente del asunto: Secretaría General de Administración Digital. Objeto: Construcción e implantación del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y Organismos Públicos (3988). Expediente: 2021NSP03988,

   Se pide:

   - Pliego de Prescripciones Técnicas Particulares y generales si se hubiesen aplicado.

[1] https://www.boe.es/buscar/doc.php?id=BOE-A-2013-12887

- Pliego de Cláusulas Administrativas Particulares y generales si se hubiesen aplicado.

- Memoria Justificativa de la necesidad.

- Informe favorable de la asesoría jurídica con particular referencia a la aplicabilidad del procedimiento negociado sin publicidad.»

2. Mediante resolución de 19 de abril de 2022, el Secretario General de Administración Digital contestó al solicitante en los siguientes términos:

«Una vez analizada la solicitud, esta Secretaría General de Administración Digital (SGAD) resuelve limitar el acceso a la información a que se refiere la solicitud de Don …, conforme a las previsiones del art 14.1 apartado a) de la Ley 19/2013.

El art 14.1 a) de la Ley dispone: "1. El derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para: a) La seguridad nacional".

Tal es el caso de este contrato, ya que el Centro de Operaciones va a ofrecer servicios de ciberseguridad de interés vital para la Administración General del Estado y sus Organismos Públicos.

Además, la naturaleza y contenido de los pliegos, así como de otros documentos, exigen la protección de intereses esenciales para la seguridad del Estado, y así se ha declarado conforme a lo previsto en el art 19.2 c) de la Ley 9/2017 de Contratos del Sector Público, y tiene por tanto este contrato una publicidad limitada de acuerdo a lo previsto en el art 168 a) 3º de la Ley de 9/2017 de Contratos del Sector Público, admitiéndose el uso del procedimiento negociado sin publicidad.

La información disponible sobre este contrato está accesible y disponible en la Plataforma de Contratación del Estado https://contrataciondelestado.es/ , si se utiliza el buscador de dicha URL y se introduce en el mismo el número de contrato, que es 2021NSP03988.»

3. Mediante escrito registrado el 20 de abril de 2022, el interesado interpuso una reclamación en aplicación del artículo 24[2] de la LTAIBG ante el Consejo de Transparencia y Buen Gobierno (en adelante, CTBG) en la que indica lo siguiente:

«La SGAD no aporta absolutamente ninguna razón para denegar el acceso a los documentos solicitados. Existe numerosa jurisprudencia a este respecto, en particular

[2] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&tn=1&p=20181206#a24

la Sentencia del Tribunal Supremo de 16 de octubre de 2017, recurso 75/2017: supondría un menoscabo injustificado y desproporcionado del derecho de acceso a la información pública cuando ni se ha intentado justificar en qué forma facilitar la información solicitada podría afectar al motivo de limitación invocado.

Es muy dudoso que los documentos solicitados tengan ningún efecto en la seguridad nacional. En el caso del informe del servicio jurídico y la memoria de justificación resulta muy difícil imaginar qué información pueden contener estos documentos que suponga ningún riesgo para la seguridad nacional. En el caso del PPT y PCAP, de existir datos que realmente pudiesen afectar a la seguridad nacional, éstos se podrían eliminar fácilmente. En todo caso, la práctica habitual y correcta sería incluir dichos datos sensibles en un anexo clasificado. En el mundo de la seguridad informática, del que este contrato es parte, la recomendación general es basar la seguridad en el diseño abierto y no en el secreto de la implementación o sus componentes, como queda reflejado en muchos de las normas y guías de buenas prácticas en esta materia. El prestigio de cualquier institución que defienda la seguridad (informática) basada en secretos se suele resentir en el corto plazo.»

4. Con fecha 22 de abril de 2022, el Consejo de Transparencia y Buen Gobierno remitió la reclamación al Ministerio de Asuntos Económicos y Transformación Digital, al objeto de que se formulasen las alegaciones que se considerasen oportunas. El 17 de mayo de 2022 se recibió respuesta de la Secretaría General de Administración Digital, en la que expone lo siguiente:

   «Alegación 1º. Objeto del Contrato
   El contrato celebrado tiene por objeto el diseño, construcción, implantación, migración e integración de entidades, operación, y apoyo a la gestión y dirección del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos (COCS).
   El alcance del contrato incluye la provisión de los medios necesarios para soportar la operativa del COCS de prestación de servicios de ciberseguridad a las más de 100 entidades de la AGE en el alcance del COCS.

   Alegación 2º. Contexto de la Contratación
   La creación del COCS responde a lo previsto en la Estrategia Nacional de Ciberseguridad 2019, medida 5 de la Línea de Acción 2 ("Garantizar la seguridad y resiliencia de los activos estratégicos para España").

Además, el COCS se encuentra recogido en la medida "17. Despliegue y operación del Centro de Operaciones de Ciberseguridad" del eje "4. Ciberseguridad" de la agenda España Digital 2025, adoptada el 23 de julio de 2020.
Posteriormente, el Plan de Digitalización de las Administraciones Públicas 2021–2025, presentado por el Presidente del Gobierno el 27 de enero de 2021, como instrumento para el fomento de las inversiones y reformas previstas en la citada agenda, incluye en el Eje 1 'Transformación digital de la Administración general del Estado', apartado 3.5 'Ciberseguridad', la Medida 9.
Dicha Medida 9 tiene como objetivo constituir el Centro de Operaciones de Ciberseguridad para toda la Administración General del Estado y sus Organismos Públicos para reforzar las capacidades de vigilancia, prevención, detección y respuesta ante incidentes de ciberseguridad, de un modo centralizado que mediante optimización y economías de escala permita una mejor eficacia y eficiencia, con los ahorros de dinero, esfuerzo y tiempo derivados. Se contempla también que además de ayudar a mejorar la ciberseguridad de las entidades en su alcance, este Centro contribuirá a facilitar el cumplimiento del Esquema Nacional de Seguridad.
La finalidad del COCS es la prestación de servicios horizontales de ciberseguridad que aumenten la capacidad de vigilancia y detección de amenazas en las operaciones diarias de los sistemas de información y comunicaciones de la AGE, así como la mejora de su capacidad de respuesta a ataques.

<u>Alegación 3º. Información que incluye el Pliego de Prescripciones Técnicas y en otros documentos.</u>
El Pliego de Prescripciones Técnicas (PPT) que rigió el procedimiento de adjudicación incluye información que, como se expondrá más adelante, no puede ser objeto de publicidad.
La información que incluyó dicho Pliego es la que sigue:
<u>3.1 Información sobre infraestructura y sobre mecanismos protección y detección en materia de seguridad de las entidades de la AGE.</u>
El COCS, una vez creado, ofrecerá servicios de prevención, protección, detección, respuesta, asesoramiento e información en materia de ciberseguridad a más de 100 entidades de la Administración General del Estado.

Con el objetivo de que las empresas seleccionadas pudieran realizar su mejor oferta y proponer una solución técnica válida para el COCS, era necesario que conocieran detalles del entorno tecnológico y de la infraestructura de seguridad de las entidades, lo que implicó facilitar información muy sensible sobre los siguientes puntos:

- Volumetrías de equipamiento y usuarios.

- Tipologías de servidores y sistemas operativos.

- Productos de antivirus y sistemas de detección y respuesta de punto final (EDR) instalados en puestos de trabajo.

- Productos y equipos especializados en seguridad de red, de diferentes tipologías: cortafuegos, productos de detección de fuga de información/control de accesos no autorizados (DLP/IRM), módulos de almacenamiento de claves criptográficas (HSM), elementos de detección/protección de intrusiones (IDS/IPS), elementos de inspección de tráfico cifrado, elementos de control de acceso a red local (NAC), sistemas de gestión de eventos e información de seguridad (SIEM), sistemas de protección de correo electrónico, sistemas de protección de la navegación, cortafuegos de aplicaciones (WAF), etc.

- Grado de cumplimiento del Esquema Nacional de Seguridad (ENS).

3.2 Información sobre infraestructura y sobre mecanismos protección y detección en materia de seguridad de la SGAD

El Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos (COCS) deberá instalarse en los Centros de Proceso de Datos (CPDs) de la SGAD, y ser compatible con la arquitectura normalizada de sistemas y comunicaciones de nube SARA, en todos sus aspectos, desde alimentación, refrigeración o ubicación en Racks de CPD, versiones y sistemas hardware, sistemas operativos, elementos de gestión, configuración de red, etc.

Además, en el PPT se requiere que "El Subsistema de Información de Protección de la Seguridad se construirá de forma que sea compatible con la arquitectura de referencia de nube SARA".

Por tanto, para que las empresas seleccionadas pudieran realizar su mejor oferta y proponer una solución técnica válida para el COCS, fue necesario que conocieran información de detalle sobre la infraestructura de la SGAD, y sobre la arquitectura de seguridad de referencia, lo que implicó facilitar información sensible sobre los siguientes puntos:

- Descripción de la plataforma nube SARA: servicios que ofrece, versiones de la plataforma de virtualización, sistemas operativos soportados, características de los servidores físicos, características de los sistemas de almacenamiento y de backup, etc.

- Descripción de la arquitectura de seguridad de referencia de nube SARA: esquemas de arquitectura de red, elementos que la componen y servicios de seguridad ofrecidos.

- Descripción de los elementos hardware y software que componen la citada arquitectura de seguridad de referencia, que incluye, para cada elemento: modelos de hardware, tipo de licencias existentes y funcionalidades de seguridad activas y soportadas.

3.3 Información sobre los mecanismos de prevención, protección, detección y respuesta que se van a implementar para la AGE

Como se ha indicado anteriormente, el COCS ofrecerá servicios de prevención, protección, detección, respuesta, asesoramiento e información en materia de Ciberseguridad a más de 100 entidades de la Administración General del Estado.

Por tanto, en el Pliego de Prescripciones Técnicas se describe con alto nivel de detalle, a través de los requisitos de obligado cumplimiento, cómo se deben prevenir, gestionar, contener y mitigar potenciales incidentes y problemas de seguridad, lo que implica facilitar información sensible sobre, entre otros, los siguientes puntos:

- Modelo de gestión de incidentes corporativos.

- Tipo y periodicidad de auditorías técnicas de seguridad.

- Elementos de protección requeridos.

Alegación 4º. Riesgos inherentes a la eventual publicidad del procedimiento de adjudicación

Como ya ha sido expuesto:

- El alcance del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y sus Organismos Públicos (COCS) que se va a construir mediante la contratación objeto de esta declaración abarca más de 100 entidades de la Administración General del Estado.

- Fue necesario proporcionar a los licitadores información sensible sobre infraestructura y sobre mecanismos de protección y detección en materia de seguridad de todas estas entidades.

- Un funcionamiento seguro que permita el cumplimiento de las competencias asignadas resulta crítico en el caso de muchas de las entidades incluidas en el alcance, ya que proporcionan servicios esenciales que son necesarios para el mantenimiento de la funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y las Administraciones Públicas.

Por otra parte, como también se ha indicado, fue necesario proporcionar a los licitadores información sobre infraestructura y sobre mecanismos protección y detección en materia de seguridad de la propia Secretaría General de Administración Digital (SGAD).

La SGAD, dada su naturaleza de prestador de servicios de Tecnologías de Información para las Administraciones Públicas, está expuesta, cada vez más, no sólo a las amenazas comunes a cualquier organización en Internet, sino también a la actividad maliciosa de mafias organizadas y grandes poderes de toda índole. Debido a ello, y dado el impacto en los servicios prestados e información manejada, así como el impacto mediático y reputacional que supondría un problema de seguridad interno, resulta imprescindible evitar la publicación total o parcial de aquellos expedientes que ofrezcan información relevante sobre los mecanismos de defensa utilizados y vectores de ataque a utilizar.

Además, el alcance de los servicios prestados y del riesgo asociado ha aumentado de forma significativa recientemente, debido a factores como los siguientes:

- *Aumento de competencias y responsabilidad de la SGAD al postularse como actor principal en la ejecución, control, supervisión y seguimiento del Plan de Digitalización de las Administraciones Públicas 2021 – 2025, presentado por el Presidente del gobierno el 27 de enero de 2021.*
- *Para la ejecución de lo anterior, un gran incremento de presupuesto anual a través de los fondos de recuperación europeos, que repercutirá enormemente en el número de proyectos a afrontar, en el nivel de exposición y en el interés y riesgo de intrusión por parte de ciberatacantes.*
- *Incremento de la importancia de la SGAD en el marco de la Ciberseguridad nacional con la puesta en marcha de la medida "17. Despliegue y operación del Centro de Operaciones de Ciberseguridad" del eje "4. Ciberseguridad" de la agenda España Digital 2025, adoptada el 23 de julio de 2020.*

Adicionalmente, el Plan de Digitalización de las Administraciones Públicas 2021 – 2025, que se constituye como instrumento para el fomento de las inversiones y reformas previstas en la citada agenda, incluye en el Eje 1 'Transformación digital de la Administración general del Estado', apartado 3.5 'Ciberseguridad', la Medida 9 "Centro de Operaciones de Seguridad".

- El COCS está incluido (medida 5) en la Línea de Acción 2 ("Garantizar la seguridad y resiliencia de los activos estratégicos para España") de la Estrategia Nacional de Ciberseguridad 2019.
- Situación de pandemia y teletrabajo que, si bien es coyuntural, establece un nuevo marco de trabajo y accesos remotos que implican reforzar aún más, si cabe, la seguridad interna de la organización.
- Crecimiento del conflicto geopolítico e incremento del número de ataques al sector público a través de fórmulas y herramientas cada vez más sofisticadas.

Por último, se significa que existe una alta probabilidad de que el COCS pueda ser declarado una de las infraestructuras críticas que contempla la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas y, según regula el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.
Por todo ello es imprescindible evitar la publicación total o parcial del pliego por ofrecer información relevante sobre los mecanismos de ciberseguridad utilizados y los posibles vectores de ataque.

Alegación 5º. Análisis del tipo de procedimiento de adjudicación aplicado
Hemos expuesto las razones por las cuales podría suponer un riesgo para la seguridad del Estado que la SGAD publicitara determinados datos sensibles de su sistema de seguridad a la hora de licitar este contrato.

Cuando se pretende limitar la publicidad de una licitación por razones de seguridad, como en el presente caso, la LCSP permite acudir a las figuras del contrato declarado secreto o reservado y a la del contrato en el que la protección de intereses esenciales para la seguridad del Estado exige limitar su publicidad.

Respecto de los contratos en que se limita la publicidad por exigirlo la protección de intereses esenciales para la seguridad del Estado esta declaración corresponde al titular del Departamento ministerial del que dependa el órgano de contratación en cuestión (según el artículo 19.2 c) de la LCSP).

Ambas figuras son idóneas para el fin buscado (limitar la publicidad de determinados aspectos sensibles) pero por las razones expuestas resulta más acorde al fin que se pretende la señalada en el artículo 19.2 c) de la LCSP.

Cabe recordar que la normativa no permite acudir a la adjudicación directa de los contratos secretos o reservados, ni en los que sea necesario proteger los intereses esenciales para la seguridad del Estado. Lo que permite la LCSP en estos dos casos es acudir al procedimiento negociado sin publicidad (artículo 168 a) 3º LCSP), esto es, un procedimiento sin publicar anuncio de licitación en el que las condiciones finales del contrato se negociarían con licitadores limitados e invitados por la SGAD a la negociación sobre la base de unos requisitos mínimos exigidos en los Pliegos.
También permite no publicar determinados datos en el anuncio de formalización del contrato (artículo 154.7).

Por todo ello, este tipo de procedimiento (Negociado sin publicidad previa declaración por el titular del Departamento ministerial de que concurre la circunstancia relativa a la protección de intereses esenciales para la seguridad del Estado) se ajusta perfectamente a lo perseguido por la SGAD para la adjudicación de este contrato salvaguardando determinados datos sensibles de su sistema de seguridad.

En el caso que nos ocupa, correspondió a la Ministra de Asuntos Económicos y Transformación Digital, como titular del Departamento ministerial (artículo 12. Ley 6/1997 de Organización y Funcionamiento de la Administración General del Estado), emitir, con fecha 27 de mayo de 2021, la declaración de que concurre la circunstancia relativa a la protección de intereses esenciales para la seguridad del Estado.

CONCLUSIÓN
Conforme a las argumentaciones y razonamientos anteriores, la SGAD estima que atender la petición del interesado en los términos que la ha formulado, podría comprometer gravemente la seguridad nacional y los intereses esenciales del Estado, por el carácter de alta sensibilidad que tienen los datos e informaciones contenidos en los documentos del expediente de contratación.»

5. El 18 de mayo de 2022, el CTBG comunicó al reclamante las alegaciones de la entidad requerida, concediéndole plazo para que alegase lo que estimase conveniente. Mediante escrito de 19 de mayo de 2022, el reclamante alega lo siguiente:

«En cuanto al razonamiento empleado, resulta sorprendente que la única información muy sensible a la que la SGAD se refiere que no es información pública es el grado de cumplimiento el Esquema Nacional de Seguridad en los distintos centros y organismos. Esta información se compila en documentos de USO OFICIAL y no es

accesible al público en general. Dado que estos documentos provienen del Centro Criptológico Nacional, es esperable que se hayan añadido al Pliego de Prescripciones Técnicas como anexos y sería, por tanto, bastante sencillo separarlos del resto en un anexo de USO OFICIAL accesible únicamente por los licitadores.

El resto de los datos que mencionan las alegaciones: volumetrías, tipologías de servidores, productos de seguridad, etcétera, se publican rutinariamente en la Plataforma de Contratación del Sector Público.

En cuanto a los detalles de la arquitectura de la nube SARA, los modelos de gestión de incidentes o la periodicidad de las auditorías, hay que conceder la posibilidad de que algunos de estos detalles no sean públicos pero es bastante razonable pensar que los organismos siguen las pautas a las que están obligados y cumplen las normas establecidas por el CCN al respecto. Estos detalles también son incluidos en multitud de pliegos de acceso público, siguiendo el razonamiento aquí empleado cualquier contrato en el que se desarrollen, modifiquen o mantengan sistemas de información debería ser declarado secreto o reservado, algo que no parece que esté ocurriendo.
Tampoco parece razonable que el elevado número de organismos en el alcance del futuro COCS sea una motivación particularmente acertada para justificar un potencial compromiso a la seguridad nacional. Si la información está disponible para cada organismo de forma individual no podemos esperar que al recopilarla en un único documento el riesgo aumente. ¿Estamos acaso basando la seguridad de la información en nuestras administraciones en la incapacidad de atacantes supuestamente sofisticados para localizar información disponible públicamente?

Ante la escasa motivación presentada por la SGAD y con los argumentos detallados en los párrafos anteriores, resulta evidente que el fondo del asunto va más allá de una petición de información, quedando en cuestión la validez de la modalidad empleada para este contrato. Sería deseable que en respuesta a mi petición se incluyera la declaración de que concurre la circunstancia relativa a la protección de intereses esenciales para la seguridad del Estado así como los informes completos elevados para justificar dicha circunstancia.»

II. FUNDAMENTOS JURÍDICOS

1. De conformidad con lo dispuesto en el artículo 38.2.c) de la LTAIBG[3] y en el artículo 8 del Real Decreto 919/2014, de 31 de octubre, por el que se aprueba el Estatuto del Consejo de Transparencia y Buen Gobierno[4], el Presidente de esta Autoridad Administrativa Independiente es competente para resolver las reclamaciones que, en aplicación del artículo 24 de la LTAIBG[5], se presenten frente a las resoluciones expresas o presuntas recaídas en materia de acceso a la información.

2. La LTAIBG reconoce en su artículo 12[6] el derecho de todas las personas a acceder a la información pública, entendiendo por tal, según dispone en el artículo 13, "*los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones*".

   De este modo, la LTAIBG delimita el ámbito material del derecho a partir de un concepto amplio de información, que abarca tanto documentos como contenidos específicos y se extiende a todo tipo de "*formato o soporte*". Al mismo tiempo, acota su alcance, exigiendo la concurrencia de dos requisitos que determinan la naturaleza "*pública*" de las informaciones: (a) que se encuentren "*en poder*" de alguno de los sujetos obligados, y (b) que hayan sido elaboradas u obtenidas "*en el ejercicio de sus funciones*".

   Cuando se dan estos presupuestos, el órgano competente debe conceder el acceso a la información solicitada, salvo que justifique de manera clara y suficiente la concurrencia de una causa de inadmisión o la aplicación de un límite legal.

3. La presente reclamación trae causa de una solicitud de acceso a determinada documentación relativa al expediente de un contrato cuyo objeto es la *Construcción e implantación del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y Organismos Públicos* (COCS) adjudicado por la Secretaría General de Administración Digital (SGAD), formulada en los términos que figuran en los antecedentes de hecho.

[3] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&p=20181206&tn=1#a24
[4] https://www.boe.es/buscar/act.php?id=BOE-A-2014-11410&tn=1&p=20141105#a8
[5] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&p=20181206&tn=1#a24
[6] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&tn=1&p=20181206#a12

El órgano requerido concede el acceso parcial a la documentación solicitada, invocando la aplicación del límite del artículo 14.1.a) LTAIBG y remitiendo a la información sobre el contrato publicada en la Plataforma de Contratación del Estado, para cuya localización facilita el enlace web y el número de contrato. El reclamante considera que no se ha justificado debidamente la aplicación del límite y considera muy dudoso que los documentos solicitados tengan incidencia en la seguridad nacional.

Posteriormente, en la fase de alegaciones de este procedimiento, la SGAD detalla el contenido de los documentos cuyo acceso se ha denegado y expone las razones por las que, a su juicio, la publicación de los mismos afectaría a la seguridad nacional. Asimismo, explicita los motivos por los que se ha optado por el procedimiento negociado sin publicidad previsto en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP). Y, finalmente, manifiesta que «*atender la petición del interesado en los términos que la ha formulado, podría comprometer gravemente la seguridad nacional y los intereses esenciales del Estado, por el carácter de alta sensibilidad que tienen los datos e informaciones contenidos en los documentos del expediente de contratación.*»

En trámite de audiencia el reclamante cuestiona que las razones aportadas justifiquen el carácter reservado de la información denegada y concluye precisando su solicitud manifestando que «*sería deseable que en respuesta a mi petición se incluyera la declaración de que concurre la circunstancia relativa a la protección de intereses esenciales para la seguridad del Estado así como los informes completos elevados para justificar dicha circunstancia.*»

4. Entrando en el examen del fondo del asunto, este Consejo ha verificado que, aplicando el número de expediente indicado en el formulario de búsqueda de la Plataforma de Contratación del Estado, se accede directamente a la siguiente información sobre el contrato de referencia: (i) el anuncio de adjudicación, y (ii) el anuncio de formalización junto con su publicación en el BOE, en ambos casos con la totalidad de los datos exigidos en al Anexo III de la LCSP. Por otra parte, a través de un enlace incluido en el anuncio de formalización se puede obtener (iii) el documento que contiene el propio contrato administrativo. En consecuencia el acceso concedido a esta parte de la información pública cumple con lo previsto en el art. 22.3 LTAIBG con arreglo al cual «*si la información ya ha sido publicada, la resolución podrá limitarse a indicar al*

solicitante cómo puede acceder a ella» y, con la doctrina establecida por este Consejo sobre los requisitos que se han observar en su aplicación.

El objeto de la controversia ha de circunscribirse por tanto al acceso a los pliegos de prescripciones técnicas y de cláusulas administrativas, por un lado, y a la memoria justificativa de la necesidad del contrato y el informe favorable de la asesoría jurídica sobre la aplicabilidad del procedimiento negociado sin publicidad, por otro.

5. La SGAD ha denegado el acceso a los pliegos de prescripciones técnicas y de cláusulas administrativas invocando la aplicación del límite previsto en la letra a) del artículo 14.1 LTAIBG según el cual el derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para «*la seguridad nacional*».

   En la aplicación de los límites legales al acceso a información pública es preciso tener presente que, como este Consejo ha señalado en múltiples resoluciones, el derecho de acceso a la información pública es un derecho de rango constitucional que goza de un amplio reconocimiento en nuestro ordenamiento, por lo que cualquier restricción de su eficacia ha de partir de una interpretación estricta de los límites y justificar de manera expresa la proporcionalidad de su aplicación. Así lo viene exigiendo también el Tribunal Supremo de manera constante en sus pronunciamientos, como él mismo se ha encargado de recordar en la Sentencia de 11 de junio de 2020 (ECLI: ES:TS:2020:1558) en la que se expresa en los siguientes términos:

   «La Exposición de Motivos de la Ley 9/2013, de diciembre, establece que el derecho de acceso a la información pública, del que son titulares todas las personas, solamente se verá limitado en aquellos casos en que así sea necesario por la propia naturaleza de la información o por su entrada en conflicto con otros intereses protegidos; y, en fin, que, en todo caso, los límites previstos se aplicarán atendiendo a un test de daño (del interés que se salvaguarda con el límite) y de interés público en la divulgación (que en el caso concreto no prevalezca el interés público en la divulgación de la información) y de forma proporcionada y limitada por su objeto y finalidad.

   Este Tribunal ha tenido ocasión de señalar -STS nº 1547/2017, de 16 de octubre de 2017 (rec. 75/2017) y STS 344/2020 10 de marzo de 2020 (rec. 8193/2018)- respecto a los límites oponibles frente al acceso a la información pública, que: "[...] La formulación amplia en el reconocimiento y en la regulación legal del derecho de acceso a la información obliga a interpretar de forma estricta, cuando no restrictiva,

tanto las limitaciones a ese derecho que se contemplan en el artículo 14.1 de la Ley 19/2013 como las causas de inadmisión de solicitudes de información que aparecen enumeradas en el artículo 18.1, sin que quepa aceptar limitaciones que supongan un menoscabo injustificado y desproporcionado del derecho de acceso a la información".

De manera que solo son aceptables las limitaciones que resulten justificadas y proporcionadas, así lo dispone el artículo 14.2 de la Ley 19/2013: «[...] 2. La aplicación de los límites será justificada y proporcionada a su objeto y finalidad de protección y atenderá a las circunstancias del caso concreto, especialmente a la concurrencia de un interés público o privado superior que justifique el acceso». Por tanto, la posibilidad de limitar el derecho de acceso a la información no constituye una potestad discrecional de la Administración y solo resulta posible cuando concurra uno de los supuestos legalmente establecido, que aparezca debidamente acreditado por quien lo invoca y resulte proporcionado y limitado por su objeto y finalidad.

[…]Tal y como hemos señalado anteriormente, la aplicación de los límites al acceso a la información requiere su justificación expresa y detallada que permita controlar la veracidad y proporcionalidad de la restricción establecida. (FJ. 3º)»

En consecuencia, la eventual aplicación de alguno de límites legales para denegar una solicitud de acceso a información pública sólo podrá considerarse conforme a derecho si se cumplen los requisitos de proporcionalidad y expresa justificación atendiendo a las circunstancias del caso concreto, tal y como exige nuestro ordenamiento y ha subrayado el Tribunal Supremo en los términos que se acaban de exponer.

En su resolución inicial, el órgano requerido se limitó a manifestar que el límite del artículo 14.1.a) LTAIBG aplica al contrato afectado porque el COCS «*va a ofrecer servicios de ciberseguridad de interés vital para la Administración General del Estado y sus Organismos Públicos»,* añadiendo que «*la naturaleza y contenido de los pliegos, así como de otros documentos, exigen la protección de intereses esenciales para la seguridad del Estado, y así se ha declarado conforme a lo previsto en el art 19.2 c) de la Ley 9/2017 de Contratos del Sector Público, y tiene por tanto este contrato una publicidad limitada de acuerdo a lo previsto en el art 168 a) 3º de la Ley de 9/2017 de Contratos del Sector Público, admitiéndose el uso del procedimiento negociado sin publicidad.»*

Sin embargo, en la fase de alegaciones de este procedimiento aporta una justificación más extensa y precisa de las razones por las que considera que la publicidad del pliego de prescripciones técnicas afecta a la protección de la seguridad nacional. En este sentido, se razona que dicho pliego contiene información sobre la infraestructura y sobre los mecanismos de protección y detección en materia de seguridad de las entidades de la AGE, información sensible sobre la infraestructura y la arquitectura de seguridad de la propia SGAD, e información sobre los mecanismos de prevención, protección, detección y respuesta que se van a implementar para la AGE, detallando los contenidos principales relativos a los tres ámbitos. A continuación, se explicitan los riesgos que se han tomado en consideración para excluir la publicidad del procedimiento de adjudicación, y se subraya que el alcance de los servicios que presta la SGAD y el riesgo asociado se han incrementado recientemente de forma significativa debido a una serie de factores que se relacionan.

A la vista de los datos y de las razones expresadas, este Consejo considera que ha quedado justificado de manera expresa y detallada que la divulgación del contenido del pliego de prescripciones técnicas es susceptible de causar un perjuicio real y no meramente hipotético a la seguridad informática de los órganos y organismos de la AGE y, por tanto, está fundada la invocación del límite del artículo 14.1.a) LTAIBG. A ello se añade que, en este caso, habida cuenta de que la información relativa a la adjudicación y formalización del contrato ha sido publicada íntegramente y se encuentra accesible, el valor añadido de la revelación de los detalles del pliego de prescripciones técnicas desde el punto de vista de la transparencia de la actuación de las administraciones públicas, no precipita un peso específico suficiente para conformar un interés público prevalente sobre la protección de la seguridad nacional en su dimensión de ciberseguridad.

En consecuencia, la reclamación ha de ser desestimada en este punto. No obstante, se considera pertinente recordar al órgano reclamado la necesidad de justificar debidamente —esto es, *de manera expresa y detallada* tal y como viene exigiendo este Consejo y el Tribunal Supremo—, la aplicación de los límites legales invocados en la resolución inicial sobre la solicitud de acceso, no siendo suficiente para cumplir con lo exigido por el art. 14.2 LTAIBG una motivación tan parca como la proporcionada en este caso.

6. A distinta conclusión se ha de llegar en relación con el acceso al pliego de cláusulas administrativas. En relación con este documento, nada se dice por parte del órgano

requerido sobre las razones que impiden su conocimiento público. Por otra parte, teniendo presente cuál es el contenido propio de estos pliegos, no se aprecia fundamento objetivo suficiente para aplicar restricciones en el acceso. De ahí que, dada su condición de información pública con arreglo al artículo 13 LTAIBG, el amplio grado de reconocimiento del derecho de acceso consagrado en nuestro ordenamiento y la necesaria interpretación restrictiva de sus límites conduzcan a estimar la reclamación en este punto.

7. Finalmente, el órgano requerido tampoco se pronuncia expresamente sobre la solicitud de acceso a la *memoria justificativa de la necesidad del contrato* y al *informe favorable de la asesoría jurídica con particular referencia a la aplicabilidad del procedimiento negociado sin publicidad*. No obstante, en sus alegaciones señala que las razones de protección de intereses esenciales para la seguridad del Estado concurrentes en este caso —y el marco en el que el contrato se ha celebrado— justifican que se hubiera acudido al procedimiento negociado sin publicidad previsto en el artículo 168. a) 3º LCSP, previa la declaración correspondiente con arreglo a lo previsto en el artículo 19.2.c) de la misma, señalando que «*correspondió a la Ministra de Asuntos Económicos y Transformación Digital, como titular del Departamento ministerial (artículo 12. Ley 6/1997 de Organización y Funcionamiento de la Administración General del Estado), emitir, con fecha 27 de mayo de 2021, la declaración de que concurre la circunstancia relativa a la protección de intereses esenciales para la seguridad del Estado».*

   Sin embargo, no se facilita al reclamante la mencionada declaración de que concurre la circunstancia relativa a la protección de intereses esenciales para la seguridad del Estado que de conformidad con lo dispuesto en el citado artículo 19.2 LCSP «*deberá hacerse de forma expresa en cada caso por el titular del Departamento ministerial*», ni los informes que eventualmente hubieran servido de base a la misma. Teniendo en cuenta que el acceso a estos documentos sirve claramente a los fines de control por la ciudadanía de la actuación de los poderes públicos en lo concerniente a la observancia de los presupuestos que permiten excepcionar las reglas generales de publicidad de la contratación pública contenidas en la LCSP, no se considera justificada la denegación del acceso y, en consecuencia, se ha de estimar la reclamación también este punto, recordando a la Administración que, en caso de que los documentos concernidos contuviesen aspectos cuyo conocimiento suponga un perjuicio real y efectivo para la seguridad nacional, lo procedente no es denegar el acceso en su totalidad sino otorgar el acceso parcial, de conformidad con lo dispuesto en el artículo 16 LTAIBG.

III. RESOLUCIÓN

En atención a los antecedentes y fundamentos jurídicos descritos, procede:

PRIMERO: ESTIMAR parcialmente la reclamación presentada por [redacted] frente a la resolución de 18 de abril de 2022, del MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL.

SEGUNDO: INSTAR al MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL a que, en el plazo máximo de 10 días hábiles, remita a la reclamante la siguiente información:

- *Pliego de Cláusulas Administrativas Particulares y generales si se hubiesen aplicado.*
- *Declaración de la Ministra de Asuntos Económicos y Transformación Digital emitida el 27 de mayo de 2021 sobre la concurrencia de la circunstancia relativa a la protección de intereses esenciales para la seguridad del Estado y los eventuales informes en los que se sustenta.*

  De esta información podrán excluirse, en su caso, aquellos aspectos que resulten afectados por el límite previsto en la letra a) del artículo 14.1 de la LTAIBG, cuya aplicación habrá de motivarse en los términos exigidos por el artículo 14.2 de la citada ley.

TERCERO: **INSTAR** al Ministerio de Asuntos Económicos y Transformación Digital a que, en el mismo plazo máximo, remita a este Consejo de Transparencia copia de la información enviada a la reclamante.

De acuerdo con el artículo 23.1[7], de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno, la reclamación prevista en el artículo 24 de la misma tiene la consideración de sustitutiva de los recursos administrativos, de conformidad con lo dispuesto en el artículo 112.2 de la Ley 39/2015, de 1 de octubre[8], de Procedimiento Administrativo Común de las Administraciones Públicas.

[7] https://www.boe.es/buscar/act.php?id=BOE-A-2013-12887&tn=1&p=20181206#a23
[8] https://www.boe.es/buscar/act.php?id=BOE-A-2015-10565&p=20151002&tn=1#a112

Contra la presente Resolución, que pone fin a la vía administrativa, se podrá interponer recurso contencioso-administrativo, en el plazo de dos meses, ante los Juzgados Centrales de lo Contencioso-Administrativo de Madrid, de conformidad con lo previsto en el artículo 9.1 c) de la Ley 29/1998, de 13 de julio, Reguladora de la Jurisdicción Contencioso-Administrativa[9].

EL PRESIDENTE DEL CTBG

Fdo.: José Luis Rodríguez Álvarez

[9] https://www.boe.es/buscar/act.php?id=BOE-A-1998-16718&tn=1&p=20181206#a9