Resolución 187/2022

S/REF: 001-066956

N/REF: R/0365/2022; 100-006727

Fecha: La de firma

Reclamante: [redacted]

Dirección: [redacted]

Administración/Organismo: Ministerio de Asuntos Económicos Y Transformación Digital

Información solicitada: Contrato para la construcción e implantación del Centro de Operaciones de Ciberseguridad de la Administración General del Estado

Sentido de la resolución: Archivo

I. ANTECEDENTES

1. Según se desprende de la documentación obrante en el expediente, el 17 de marzo de 2022 el reclamante solicitó 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:

   «Copia de la memoria justificativa, presupuestos de licitadores, informe de valoración de ofertas y resto de documentación que integra el expediente administrativo relativo al contrato para la construcción e implantación del Centro de Operaciones de Ciberseguridad de la Administración General del Estado y Organismos Públicos (licitado por la Secretaría General de Administración Digital), dado que en la Plataforma de Contratación del Sector Público sólo consta anuncio de adjudicación y la formalización del acuerdo con la UTE ganadora (Telefónica-Indra) en el momento en que se formaliza esta solicitud de acceso a la información pública.»

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

2. Mediante resolución de fecha 19 de abril de 2022, el MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL contestó al solicitante lo siguiente:

   «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 solicitante interpuso una reclamación, en aplicación del artículo 24[2] de la LTAIBG, ante el Consejo de Transparencia y Buen Gobierno (en adelante, CTBG) con el siguiente contenido resumido:

   «(…)La Secretaría General de Administración Digital defiende que concurre en el caso uno de los límites previstos en el artículo 14 de la ley (la seguridad nacional) para no facilitar la documentación requerida.

   No puedo estar de acuerdo con dicha tesis y no puede estarlo tampoco el Consejo de Transparencia y Buen Gobierno si se repara en la argumentación expuesta en múltiples resoluciones ya dictadas. Entiendo que determinados pasajes de un documento concreto puedan ocultarse para no perjudicar la defensa nacional, pero ¿todo debe ser protegido? ¿De la primera letra a la última? ¿Todo debe quedar bajo el velo de la confidencialidad? ¿Qué hay que proteger en un informe de valoración de ofertas o en los presupuestos presentados por los distintos licitadores? Es evidente que ahí no puede operar el límite esgrimido por la Administración y que, tratándose de información pública, no existe ningún obstáculo para que se facilite.

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

[redacted]

Pero es que además no se motiva suficientemente en la resolución cuál sería el perjuicio objetivable en caso de divulgación de la información, como exige la doctrina de este Consejo y la jurisprudencia. No basta con hacer una invocación genérica, sino que hay que aportar argumentos al caso.

Por las razones expuestas, ruego al CTBG que se declare competente, admita a trámite esta reclamación y dicte resolución estimatoria.»

4. Con fecha 22 de abril de 2022, el Consejo de Transparencia y Buen Gobierno remitió el expediente al MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL al objeto de que pudiera hacer las alegaciones que considerase oportunas; lo que efectuó mediante escrito recibido el 17 de mayo de 2022 en el que se pone de manifiesto lo siguiente:

«(…)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.

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.

[redacted]

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.

3º. Información que se incluye el Pliego de Prescripciones Técnicas y en otros Documentos. 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:

3.1 Información sobre infraestructura y sobre mecanismos protección y detección en materia de seguridad de las entidades de la AGE. 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

[redacted]

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 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. 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.*

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

[redacted]

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

[redacted]

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.

5º. Análisis del tipo de procedimiento de adjudicación aplicado. 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.

[redacted]

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, se concedió audiencia al reclamante para que presentase las alegaciones que estimara pertinentes. El 18 de mayo de 2022, se recibió escrito con el siguiente contenido:

   «Es evidente que la Administración aporta en el trámite de alegaciones una explicación y motivación huérfana en la resolución que dio pie a esta reclamación. Considerando razonables los motivos aducidos por el Ministerio de Asuntos Económicos y Transformación Digital, por medio del presente escrito formalizo mi desistimiento a este expediente para evitar trabajo innecesario a este Consejo de Transparencia y Buen Gobierno. Ruego que se archive, posibilidad que prevé la ley.»

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*».

[3] https://boe.es/buscar/act.php?id=BOE-A-2013-12887&p=20181206&tn=1#a38
[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

[redacted]

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 por la ley, 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 en relación con el contenido del contrato para la construcción e implantación del Centro de Operaciones de Ciberseguridad de la Administración General del Estado, formulada en los términos que figuran en los antecedentes de hecho.

   El Ministerio requerido dictó resolución facilitando parte de la información solicitada y, en fase de reclamaciones, argumenta con mayor profundidad por qué resulta procedente la entrega parcial de la información, y no su totalidad, manifestando el reclamante su voluntad de desistir de esta reclamación al considerar razonables las explicaciones ofrecidas.

4. Teniendo en cuenta lo anterior, resulta de aplicación lo dispuesto en el artículo 94 de la Ley 39/2015, de 1 de octubre, de Procedimiento Administrativo Común de las Administraciones Públicas, según cuyo tenor:

   «1. Todo interesado podrá desistir de su solicitud o, cuando ello no esté prohibido por el ordenamiento jurídico, renunciar a sus derechos.

   2. Si el escrito de iniciación se hubiera formulado por dos o más interesados, el desistimiento o la renuncia sólo afectará a aquellos que la hubiesen formulado.

   3. Tanto el desistimiento como la renuncia podrán hacerse por cualquier medio que permita su constancia, siempre que incorpore las firmas que correspondan de acuerdo con lo previsto en la normativa aplicable.

   4. La Administración aceptará de plano el desistimiento o la renuncia, y declarará concluso el procedimiento salvo que, habiéndose personado en el mismo terceros interesados, instasen éstos su continuación en el plazo de diez días desde que fueron notificados del desistimiento o renuncia.

[redacted]

5. Si la cuestión suscitada por la incoación del procedimiento entrañase interés general o fuera conveniente sustanciarla para su definición y esclarecimiento, la Administración podrá limitar los efectos del desistimiento o la renuncia al interesado y seguirá el procedimiento.»

En consecuencia, recibido en el Consejo de Transparencia el desistimiento expreso del reclamante y no habiéndose personado en el procedimiento terceros interesados que insten su continuación, ni existir causas que permitan limitar sus efectos, debe darse por finalizado el actual procedimiento de reclamación, con el consiguiente archivo de actuaciones.

III. RESOLUCIÓN

En atención a los antecedentes y fundamentos jurídicos descritos, procede **ARCHIVAR** la reclamación presentada por [redacted] frente al MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL.

De acuerdo con el artículo 23, número 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.

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

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

[redacted]