Expediente:12577/2023

INFORME – PROPUESTA DE INICIACIÓN DE UN PROCEDIMIENTO DE ADJUDICACIÓN

CONTRATACIÓN: SERVICIO DE "AUDITORÍAS TÉCNICAS DE CIBERSEGURIDAD".

A los efectos previstos en la Disposición Adicional 5ª del Real Decreto-ley 3/2020, de 4 de febrero, de medidas urgentes por el que se incorporan al ordenamiento jurídico español diversas directivas de la Unión Europea en el ámbito de la contratación pública en determinados sectores; de seguros privados; de planes y fondos de pensiones; del ámbito tributario y de litigios fiscales, en conexión con la Disposición Adicional 8ª de 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 del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, se elabora el presente Informe Justificativo de la Necesidad de la contratación de referencia:

1.- MEMORIA JUSTIFICATIVA DEL CONTRATO:

1.1.- Necesidad: La Autoridad Portuaria de Bilbao (en adelante, A.P.B.), en desarrollo de las competencias y funciones que se asignan en virtud del artículo 25 del Real Decreto Legislativo 2/2011, de 5 de septiembre, por el que se aprueba el texto refundido de la Ley de Puertos del Estado y de la Marina Mercante, planifica, desarrolla y mantiene unos servicios de seguridad informática necesarios para dar soporte a sus aplicaciones de gestión, como medio para la prestación de las actividades y los servicios que legalmente le corresponden, y que resultan necesarios para la correcta explotación y funcionamiento de los organismos portuarios, lo que se realiza a través de la división de Tecnologías de Información de la Autoridad Portuaria de Bilbao (en adelante APB), dado que tiene la responsabilidad de la seguridad de la información de la Entidad.

En este sentido, si bien durante los últimos años la APB ha intensificado la protección sobre sus activos realizando varios proyectos de seguridad tecnológica, con el objetivo de mejorar el nivel global de ciber resiliencia de forma acorde con la evolución del contexto de la ciberseguridad con un aumento exponencial en los últimos años de los casos conocidos de ciberataques a nivel nacional y mundial, resulta necesaria la contratación específica de un servicio de auditoría técnica en ciberseguridad, que permita la identificación de las de acciones y/o medidas eficaces a implementar frente a los ataques tecnológicos, mejorando y reforzando las capacidades de prevención y vigilancia en el ámbito portuario.

1.2.- Alcance del contrato: El presente servicio tiene por objeto la contratación del servicio de

auditorías técnicas de todos los servicios y sistemas de información de la Entidad, con el objeto último de dar cumplimiento a la obligatoriedad del Esquema Nacional de Seguridad. A tal efecto, el ámbito de las auditorías de seguridad comprende: (i) Una auditoria de seguridad de los servicios (negocio e infraestructura), con periodicidad CUATRIMESTRAL (3 al año), de toda la plataforma tecnológica de la Entidad (infraestructura, sistemas, aplicaciones y servicios), (ii) Un (1) ejercicio ANUAL de RED TEAM.

1.3.- Justificación insuficiencia de medios: La realización del referido servicio requiere ejecutar una serie de prestaciones para las cuales se precisa la contratación de una empresa externa a esta entidad, al tratarse de funciones específicas, y técnicas muy concretas, que no entran dentro del ámbito competencial reservado a la autoridad portuaria, y que sólo se pueden prestar por una entidad dotada de personal especializado y formado a tal efecto. De este modo, externalizar la prestación del servicio es la fórmula más adecuada para proporcionar una solución integrada a las necesidades expuestas.

2.- OBJETO DEL CONTRATO:

El objeto del presente contrato viene dado por la prestación del servicio requerido, tal y como se recoge en el Pliego de Prescripciones Técnicas.

3.- DIVISIÓN DEL OBJETO DEL CONTRATO EN LOTES:

El objeto del contrato no es susceptible de su división en lotes, al no permitirlo así la naturaleza de este servicio. En este sentido, todas las actividades constituyen una unidad funcional y técnica que se engloba dentro del mismo ámbito material de las auditorías técnicas de ciberseguridad, y que, además, se ejecutarán sobre el mismo entorno tecnológico. De tal manera que la ejecución de estas debe hacerse de forma homogénea y coordinada por la misma empresa, en aras de conseguir una mayor eficacia en la prestación del servicio. El ejercicio de las prestaciones puede verse imposibilitado si se dividen en lotes y se adjudican a una pluralidad de contratistas, dado que las especificidades técnicas del servicio, requiere de su ejecución por un solo contratista para garantizar la eficiencia, garantía de calidad y reducción de costes que ello supone.

4.- PRESUPUESTO BASE DE LICITACIÓN:

El presupuesto base de licitación del contrato asciende a TRESCIENTOS CINCUENTA Y CUATRO MIL EUROS (354.000 €) I.V.A. excluido, para el plazo de ejecución del contrato de tres (3) años.

En relación con los costes considerados para la determinación del presupuesto base de licitación, I.V.A. excluido, procede indicar que éste es adecuado a los precios de mercado, tal y como se indica en el Pliego de Prescripciones Técnicas, y que comprende el desglose de los costes directos e indirectos precisos para la ejecución del contrato, así como otros gastos eventuales calculados para su determinación, de conformidad con lo dispuesto en el artículo 100.2 LCSP.

COSTES DIRECTOS	287.805 €
COSTES INDIRECTOS	34.537 €
OTROS GASTOS	31.658 €
- Gastos Generales	14.390 €
- Beneficio	17.268 €
PRESUPUESTO BASE LICITACIÓN (3 AÑOS) I.V.A. EXCLUIDO	354.000 €

En cuanto a la estimación de los costes directos de todo el equipo de trabajo a adscribir al contrato para el plazo de ejecución del contrato (3 años) se ha efectuado tomando como base a efectos orientativos el “Convenio Colectivo de Oficinas y Despachos de Bizkaia (Código de Convenio número 48001755011981)”, de conformidad con las tablas salariales vigentes y publicadas en el sector de ingeniería e informática, en atención al objeto del contrato, sin que ello suponga prejuzgar el ámbito efectivo de aplicación de este o de otros convenios colectivos sectoriales o de empresas que pudieran ser de aplicación.

5.- VALOR ESTIMADO DEL CONTRATO:

El valor estimado del contrato asciende a QUINIENTOS NOVENTA MIL EUROS (590.000 €) I.V.A. excluido, quedando incluido en el citado importe cualquier forma de opción eventual, y la eventual prórroga anual del contrato, así como el resto de los costes referidos en el artículo 101 de la LCSP. Este valor estimado se desglosa conforme se indica a continuación:

Presupuesto base de licitación (I.V.A excluido €)	354.000 €
Importe de las modificaciones previstas (I.V.A. excluido).	No aplica.
Prórrogas previstas.	Si, posibilidad de prórrogas anuales, hasta un máximo de dos (2): por importe máximo de 118.000 euros, I.V.A. excluido anuales para cada una.
TOTAL, VALOR ESTIMADO DEL CONTRATO (I.V.A excluido).	590.000 €

6.- PROCEDIMIENTO DE ADJUDICACIÓN Y CONTENIDO DEL PLIEGO DE CONDICIONES PARTICULARES:

Se trata de un contrato de servicios cuyo objeto entra dentro del ámbito de aplicación de la Ley 9/2017 de Contratos del sector público (Disposición Adicional 8ª, apartado tercero), que, por razón de su cuantía, está sujeto a regulación armonizada (SARA). En este sentido, la licitación exige su publicación en el perfil del contratante y en el Diario Oficial de la Unión Europea (DOUE).

Se propone como procedimiento de adjudicación el procedimiento abierto, previsto en el artículo 156 a 158 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, con utilización de varios criterios de adjudicación.

Los criterios de solvencia económica y financiera y técnica y profesional exigidos para concurrir a la presente contratación cumplen con los requisitos establecidos por los artículos 87 y 90 de la Ley 9/2017.

Así mismo, se exigen como criterio adicional de solvencia, el cumplimiento y acreditación documental de las condiciones de seguridad de la información que se exigen como estándares de calidad en este ámbito. A tal efecto, se exige que los licitadores dispongan de la siguiente documentación:

- Declaraciones y/o Certificaciones de Conformidad con el Esquema Nacional de Seguridad (ENS) con al menos, un nivel MEDIO, expedido por un Organismo Certificador Autorizado, y específicamente en la realización de auditorías técnicas de ciberseguridad, debiendo mantener la conformidad vigente durante la duración del contrato.

  Así mismo, los productos o servicios de ciberseguridad con los que el adjudicatario preste el servicio deberán estar certificados para al menos nivel MEDIO en el ENS o equivalente, en cuyo caso, deberá proporcionar toda la información relativa a la seguridad de las soluciones empleadas que le habiliten para su utilización, sin incumplir en nivel ENS MEDIO.

En este sentido, la exigencia y acreditación de las referidas declaraciones y/o certificaciones, resulta procedente, proporcional y adecuado al objeto de este servicio, dado que el Esquema Nacional de Seguridad (ENS) es una norma de obligado cumplimiento para todos los sistemas de las Administraciones Públicas, por lo que hay que exigir su cumplimiento, no solo a los sistemas de información operados por personal de dichas administraciones, y/o en sus

dependencias, sino también a aquellos otros que, estando operados por terceros e, incluso, en dependencias de terceros, desarrollan funciones, misiones, cometidos o prestan servicios para dichas administraciones, aplicando las mismas medidas de seguridad del sistema de información de la Administración Pública que se trate, destacando que, si los sistemas concernidos son de categoría MEDIA, es imprescindible que el proveedor posea la correspondiente Certificación de Conformidad con el ENS para tales sistemas, en una categoría igual o superior, es decir MEDIA o ALTA, nunca inferior, para evitar el incumplimiento de las exigencias establecidas en el Real Decreto mencionado.

Igualmente, respecto a la solicitud de que la categoría exigida sea MEDIA, hay que indicar que la categoría de un sistema de información, en materia de seguridad, debe modular el equilibrio entre la importancia de la información que maneja, los servicios que presta y el esfuerzo de seguridad requerido, en función de los riesgos a los que está expuesto, bajo el criterio del principio de proporcionalidad marcado por el artículo 43 del Real Decreto 3/2010, indicado anteriormente. Por tanto, la categoría vendrá determinada en función del impacto que tendría un incidente que afectase a la seguridad de la información, o de los servicios, con perjuicio para la disponibilidad, autenticidad, integridad, confidencialidad o trazabilidad, como dimensiones de seguridad, siguiendo el procedimiento establecido en el Anexo I del Real Decreto indicado y tomando como referencia la guía de seguridad de las TIC del Centro Criptológico Nacional.

De tal manera que, tras la valoración de los diferentes tipos de información que se manejan y dado que se trata de auditorías técnicas de ciberseguridad, queda establecido en categoría MEDIA, teniendo en cuenta las dimensiones de seguridad de disponibilidad, autenticidad, integridad, confidencialidad y trazabilidad.

En cuanto a la solvencia técnica y profesional, no se precisa adscripción de medios materiales concretos, en los términos previstos en el artículo 76 de la Ley 9/2017. Si bien, dada la especificidad técnica del servicio, se prevé la adscripción de los siguientes medios personales:

- **Un Responsable del Servicio**, de perfil gestor técnico, y que será el interlocutor válido para la ejecución y seguimiento del día a día del servicio. Dicho Responsable del Servicio deberá tener titulación universitaria en ingeniería informáticas o telecomunicaciones, o equivalente, y una experiencia profesional mínima acreditada de TRES (3) años como Responsable de Servicios de Auditorías Técnicas de Ciberseguridad, y disponer al menos una de las siguientes certificaciones en vigor: ISACA-CISM, ISC2-CISSP, ISC2-ISSMP o EC-C|CISO.

- **Equipo técnico**: Deberá estar compuesto por el número de personas que a juicio de la empresa licitante sean necesarias para dar una adecuada cobertura y prestación del

servicio, teniendo en cuenta que no habrá asignación de recursos dedicados en exclusividad a este contrato. En todo caso, cada uno de los integrantes del equipo de trabajo deberán tener una experiencia mínima acreditada de DOS (2) años, en la prestación de servicios de Auditorías Técnicas de ciberseguridad.

- Al menos dos (2) miembros del equipo ofertado, deberán contar con dicha experiencia mínima (2 años) en cada tipo de servicio de auditoria técnica de ciberseguridad descritas. Además, al menos el 50% del equipo que se oferte para la ejecución del contrato, tendrá, al menos, una certificación en Ciberseguridad, en vigor, emitida por ISACA, ISC2 o EC-Council.

Así mismo, se indica que la adscripción de todos los indicados medios humanos, con el número y características de la oferta, así como -en su caso- las mejoras ofertadas, quedará integrada en el contrato y se configura como condición especial de ejecución, cuyo incumplimiento por parte del adjudicatario podrá dar lugar a la imposición de las penalizaciones establecidas en la cláusula 38 del presente Pliego de Condiciones Particulares.

Los criterios de adjudicación del Pliego de Condiciones Particulares incluyen criterios cualitativos y criterios relativos al precio (de evaluación automática), cumpliendo con los requisitos establecidos por los artículos 145 y 146 de la Ley 9/2017.

Criterios evaluables de forma automática (60 puntos) comprenden:

- **Precio** (Proposición Económica PE: 40 puntos) para determinar la oferta más ventajosa en términos más económicos.

- **Criterios cualitativos evaluables de forma automática** (PCCEA: 20 puntos), distribuidos de forma excluyente en 5, 10, 15 y 20 puntos, en atención al porcentaje ofertado de Nivel de Cobertura de la Matriz MITRE ATT&CK®, con respecto al mínimo del 10% establecido en el PPT.

Criterios cualitativos sujetos a juicio de valor: (40 puntos) Que están directamente relacionados con el objeto del contrato, dado que se refieren nivel de calidad de la prestación y el de los medios ofertados para su ejecución. Y se han formulado de manera clara, objetiva y proporcionada, con respeto a los principios de igualdad, no discriminación, transparencia, y no limitación de la concurrencia, en cuanto se garantiza la posibilidad de que las ofertas sean evaluadas en condiciones de competencia efectiva. En concreto, se refieren a:

- **CALIDAD DE LA MEMORIA TÉCNICA PARA LA EJECUCIÓN DEL SERVICIO**, con particular atención a los siguientes extremos:

Auditorías de seguridad de los servicios: Se valorará la descripción del procedimiento de ejecución y el nivel de profundidad de las auditorías de seguridad de los servicios descrita en el PPT, así como, las mejoras sobre los requisitos mínimos descritos en dicho epígrafe.

Ejercicio de Red TEAM: Se valorará la descripción del procedimiento de ejecución y el nivel de profundidad del ejercicio de RED TEAM descrito en el PPT, así como, las mejoras sobre los requisitos mínimos descritos en dicho epígrafe.

Metodología: Se valorará la metodología, técnicas y herramientas de ejecución de la prestación de los servicios, planificación en plazos y esfuerzos, seguimiento de la ejecución del contrato, así como los modelos propuestos para cada uno de los entregables.

Criterios, todos ellos, vinculados con el objeto del contrato, dado que se refieren al detalle y calidad de las prestaciones objeto del contrato, así como, a la metodología a emplear en la ejecución de éstas con la adecuación y seguridad que requiere este tipo de entorno tecnológico.

Por su parte, en el anexo nº 1 de normas específicas del PCP, en relación con lo previsto en el PPT, se determinan los distintos Acuerdos de Nivel de Servicio (ANS), como parte fundamental de la presente licitación, relacionadas con los siguientes aspectos:

- Cumplimiento de los plazos de entrega de los entregables especificados en el PPT.
- Cumplimiento de la calidad de los informes en términos de forma (sin errores ortográficos, gramaticales, de formato).
- Detección de todas las vulnerabilidades de seguridad catalogadas. Las auditorías y los test deben identificar más vulnerabilidades en componentes, protocolos, etc. que las que se encuentren en catálogos públicos, pero sí o sí, deben detectar inexcusablemente todas las vulnerabilidades en componentes, protocolos, etc. que se encuentren en dichos catálogos públicos.

Los referidos ANS tendrán carácter contractual y su cumplimiento es una condición especial de ejecución del contrato, en la medida que se deberán cumplir con ellos y garantizar durante toda la ejecución del contrato, y en caso de incumplimiento darán lugar a las correspondientes penalidades, en los términos establecidos en el PCP.

Igualmente, se prevé una condición especial de ejecución de carácter social, de conformidad con el artículo 202 de la Ley 9/2017, consistente en que la empresa adjudicataria adopte durante la

ejecución de los trabajos objeto del contrato, todas aquellas medidas que resulten de aplicación y vayan encaminadas a promover la igualdad de hombres y mujeres en el trabajo, de conformidad con lo establecido en la cláusula 38 del PCP. Dicha condición persigue la presencia equilibrada de mujeres y hombres en el equipo que preste los servicios de seguridad, es decir, los servicios contratados. La vinculación del criterio social y en este caso, de igualdad de género, con el objeto del contrato, debe ser entendida en términos amplios, en aspectos relativos a la calidad de la contratación. En ese sentido, queremos justificar cómo, para este órgano de contratación, el establecimiento de medidas que fomenten la igualdad de género en el empleo, en la contratación administrativa, es un mandato legal, un compromiso político y un objetivo de gestión.

Lo que hago constar a efectos de la tramitación del expediente de contratación, como requisito previo a la aprobación del expediente de contratación por parte del Órgano de Contratación de la Entidad.

En Santurtzi, a 18 de enero de 2024.

FDO. LA JEFA DE TECNOLOGÍAS DE LA INFORMACIÓN

Vº Bº EL SECRETARIO GENERAL,