



Memoria Justificativa y Solicitud de Contratación para contratos de la LCSP

**OBJETO A CONTRATAR: SERVICIO DE MANTENIMIENTO Y
SOPORTE DE DOS EQUIPOS PARA LA PROTECCIÓN ANTE
ATAQUES DE DENEGACIÓN DE SERVICIOS (DoS)**

NÚMERO. DE LA SC: 6000010221

**Dirección
/Gerencia:**

Explotación Ferroviaria

Área:

Comunicaciones y
Tecnologías de la
Información

División:

Instalaciones y Sistemas
de Información

Servicio:

No procede

Aprobado:

Juan Tébar

1 OBJETO DE LA SOLICITUD DE CONTRATACIÓN:

El presente documento tiene por objeto elevar a la aprobación del correspondiente órgano de contratación de Metro de Madrid, S.A., la autorización para el inicio de un proceso de licitación que tiene por objeto la contratación del mantenimiento, soporte y suscripción de servicios del equipamiento para la protección ante ataques de denegación de servicio (DoS) gestionados por el Área de Comunicaciones y Tecnologías de la Información.

2 DATOS DE LA LICITACIÓN

▪ Objeto:

El objeto de esta licitación es la contratación del soporte técnico, mantenimiento, y suscripciones de software del equipamiento (2 equipos AED 8100) para la protección ante ataques de denegación de servicio (DoS), basados en tecnología del fabricante NetScout, incluyendo componentes hardware, así como componentes software y servicios de seguridad incorporados en los equipos.

La contratación de los servicios de mantenimiento y soporte técnico, y la suscripción de software es condición indispensable, por un lado, para no incurrir en una situación de ilegalidad al utilizar productos sin la debida licencia de uso otorgada por el fabricante en las condiciones establecidas y, por otro lado, para para disponer de un soporte técnico especializado para la resolución de incidencias, tanto del hardware como del software, la sustitución / reemplazo en caso de averías o roturas, y el derecho de uso del software y los servicios incorporados a los equipos, tal que garanticen la completa operatividad de los mismos; así como disponer de nuevas versiones, actualizaciones y parches, y acceso a bases de datos y documentación del fabricante. Igualmente, permite que los sistemas de ciberseguridad se encuentren en un estado funcional óptimo.

▪ Estamento responsable de la ejecución del contrato

Área de Comunicaciones y Tecnologías de la Información.

▪ Valor estimado del contrato (artículo 101 LCSP):

Valor estimado: 145.600,00 euros (IVA no incluido).

▪ Método de cálculo aplicado para determinar el valor estimado:

El valor real de los distintos contratos análogos adjudicados, ajustado en función de los precios habituales en el mercado, teniendo en cuenta las posibles prórrogas (2 prórrogas de 6 meses cada una).

- **Presupuesto base de licitación (artículo 100 LCSP):**
 - Base imponible (BI): **109.200,00** euros
 - Importe del I.V.A.: **22.932,00** euros
 - Presupuesto Base de Licitación (PBL): **132.132,00** euros, IVA incluido

- **Desglose del presupuesto base de licitación: (artículo. 100.2 LCSP)**

COSTE ENDÓGENOS Son los generados por el contrato y están formados por los Costes Directos e Indirectos.		
Presupuesto de ejecución (PE)	Costes Directos 98%	93.057,39 €
	Costes Indirectos 2%	1.899,13 €
T O T A L Presupuesto de Ejecución (PE)		94.956,52 €
COSTE EXÓGENOS Son los relacionados con las actividades de la empresa y están formados por los gastos de estructura (GG+BI).		
Gastos Generales (GG)	9% del PE	8.546,09 €
Beneficio Industrial (BI)	6% del PE	5.697,39 €
Base Imponible		109.200,00 €
IVA (21 %)	21%	22.932,00 €
Presupuesto base de licitación (PBL)		132.132,00 €

- **Modificación del contrato (artículo 204 LCSP)**

☒ No Procede

- **División en lotes:**

☒ **NO se divide en lotes (artículo. 99.3 LCSP)**

- **Justificar los motivos** de la no división en lotes:

El riesgo para la correcta ejecución del contrato procede de la naturaleza del objeto del mismo, al implicar la necesidad de coordinar la ejecución de las diferentes prestaciones, cuestión que podría verse imposibilitada

por su división en lotes y ejecución por una pluralidad de contratistas diferentes

▪ **Duración del contrato:**

- Plazo de duración/ejecución inicial del contrato: 36 meses y 24 días.

- Hito a partir del cual comienza la duración/ejecución del contrato:

☒ A partir del día siguiente a la firma del acta de inicio de los trabajos o en la fecha de inicio que se indique en la propia acta no comenzado antes del 20 de noviembre de 2022

- **Justificar los motivos** por los que este servicio precisa de un acta de inicio de los trabajos: Se precisa para establecer la forma de coordinar adecuadamente los trabajos de mantenimiento, así como para explicitar los puntos principales del contrato, forma de pago, penalizaciones y ajustar la fecha de inicio.

- Prórrogas:

☒ SI

- N° de prórrogas: 2

- Duración de cada prórroga: 6 meses

- **Justificación** de la necesidad de prórrogas: La prórroga del contrato se concibe, por un lado, para asegurar la continuidad de los servicios de soporte y mantenimiento y suscripciones de software de los sistemas y aplicaciones, en tanto es una exigencia de los fabricantes, en el caso que la siguiente licitación se demorase en el tiempo para no incurrir en un proceso de regularización. Además, analizado el mercado se considera oportuno por el órgano de contratación

▪ **Clasificación del contrato:**

☒ Sujeto a LCSP (Ley 9/2017)

▪ **Naturaleza del contrato:**

☒ Mixto (servicios)

- **Justificar** la insuficiencia de medios:

Los servicios de mantenimiento, soporte técnico y de suscripción de licencias de software y/o de servicios de seguridad incluidos en equipamiento de propósito específico que componen esta acción solamente pueden ser prestados o bien por el fabricante del software y/o hardware o bien por empresas acreditadas o certificadas por el fabricante para la prestación de dichos servicios.

El contrato asociado a este servicio es una pieza fundamental para proporcionar un servicio de acuerdo a los parámetros habituales de calidad, disponibilidad y seguridad que requiere el servicio público que presta Metro de Madrid, y que desde el Área de Comunicaciones y Tecnologías de la Información se presta a los diferentes estamentos para poder proporcionar, en su conjunto, un servicio de calidad a los clientes.

Algunas de las razones por las que es necesaria realizar esta contratación es:

- Derecho de uso del software y suscripciones de software y de servicios de seguridad que se configuran en los sistemas o en el equipamiento hardware.
- Reparación de averías hardware.
- Reparación de errores software.
- Asistencia en las peticiones de servicio las 24 horas del día y 7 días a la semana (24x7) o en horario laboral de lunes a viernes, según las condiciones contratadas, con un tiempo de respuesta adaptado a la criticidad de cada servicio.
- Actualizaciones de firmware, corrección de errores de software, alertas de seguridad y actualizaciones de parches críticos.
- Actualizaciones fiscales, legales y normativas
- Acceso a la web del fabricante, incluida la posibilidad de realizar consultas ante las dudas y aclaraciones de carácter técnico, que se puedan plantear con cualquiera de sus productos.
- Versiones mayores de productos y tecnología, que incluyen versiones generales de mantenimiento, versiones de funcionalidad seleccionada y actualizaciones de documentación, acceso a foros, etc.

Si no se dispusiera de este tipo de servicios, cuando se produjese una avería/incidencia, la parada en el servicio se prolongaría durante un tiempo que sería la suma del tiempo de detección, del tiempo de diagnóstico y del tiempo de corrección y esto podría ser cuestión de minutos, de horas o incluso de días, dependiendo de la severidad de la misma; por lo cual, es que para cierto tipo de sistemas de ciberseguridad se considera un riesgo no asumible, principalmente porque suponen perder la capacidad de ofrecer seguridad a los diferentes sistemas, aplicaciones, servicios y plataformas tecnológicas que ofrecen servicios a los diferentes procesos de negocio y estamentos de Metro de Madrid.

No disponer de este soporte y mantenimiento, suscripción de servicios y derecho de uso / suscripción de licencias supondría, por un lado, que ante un problema en los mencionados elementos daría lugar a largas indisponibilidades que afectaría a diferentes aplicaciones y, por otro lado, incurrir en una situación de ilegalidad al utilizar productos sin la debida licencia de uso otorgada por el fabricante en las condiciones establecidas.

La paralización de dichas aplicaciones afectaría directamente a la gestión de la empresa. Dependiendo de la severidad de la incidencia, esta afectación a la operativa de los departamentos de Metro tendría una duración que no se

puede calcular, y que incluso podría ser indefinida al no disponerse del remedio que aplica el fabricante al problema que pudiese ocurrir.

▪ **Procedimiento de licitación:**

☒ Procedimiento Abierto

▪ **Justificación del procedimiento:**

No es posible la aplicación del procedimiento abierto simplificado y super-simplificado, ya que el valor estimado del contrato es superior a los límites que establece la LCSP para estos procedimientos. Además, no se reúnen los requisitos necesarios que exige la LCSP para la aplicación de un procedimiento negociado. Por todo lo anterior, y con el fin de asegurar los principios de igualdad, transparencia y libre competencia, se propone la contratación mediante procedimiento abierto.

▪ **Criterio de adjudicación (artículos 145 y 146 LCSP):**

☒ Único criterio (precio)

▪ **Justificar las razones** por el que se propone este criterio de adjudicación:

- Los servicios de soporte técnico y mantenimiento, así como los derechos de uso y/o las suscripciones de software, se prestan en las condiciones técnicas y económicas establecidas por el fabricante bien sea de forma directa o a través del canal de empresas certificadas o acreditadas. Es el fabricante quien establece niveles de soporte, canales de comunicación y atención, condiciones de uso del software y el hardware, etc., no existiendo ninguna característica por la que se pueda valorar la calidad de las ofertas más allá del precio de los servicios a prestar acorde a las condiciones establecidas y, en caso de incumplimiento, aplicar las penalidades establecidas.

▪ **Subcontratación (artículo 215 LCSP):**

☒ Procede

- Indicar las tareas críticas que no podrán ser objeto de subcontratación: ninguna

▪ **Procedimiento de subasta electrónica o petición sucesiva de ofertas:**

☒ NO

▪ **Fondos FEDER:**

☒ Contrato no financiable con fondos FEDER

▪ **Confidencialidad de los Pliegos de Prescripciones Técnicas:**

☒ SI

☒ En su totalidad

- **Justificar las razones** por las que se declara confidencial (en su totalidad o en parte del contenido) el pliego de prescripciones técnicas:

En el pliego de prescripciones técnicas se incluye información técnica de detalle de arquitecturas, elementos y servicios de ciberseguridad, que protegen los servicios informáticos de Metro de Madrid, incluyendo aquellos que sirven para la prestación del servicio esencial en el ámbito de la protección de infraestructuras críticas y de la seguridad de las redes y los sistemas, y la publicación del contenido del pliego técnico podría suponer un grave riesgos para la ciberseguridad en tanto ofrecería información que posibilitaría diseñar ataques concretos para vulnerar los sistemas de ciberseguridad.

▪ **Cesión de datos**

¿La ejecución de este contrato requiere la cesión de datos por parte de Metro de Madrid, S.A. al contratista?

☒ NO

3 JUSTIFICACIÓN DE LA NECESIDAD

En primer lugar, es importante destacar que, en consideración a los costes administrativos y el tiempo necesario para realizar sucesivas licitaciones anuales, se ha planteado la licitación con una vigencia de 36 meses y 24 días, y 2 posibles prórrogas de 6 meses.

La Coordinación de Seguridad Informática y Ciberseguridad, implanta y mantiene una gran cantidad de servicios informáticos corporativos, desarrollados y/o soportados en tecnologías variadas y que operan las 24 horas al día, los 7 días a la semana, los 365 días del año. Entre estos destacan aquellos que se publican hacia Internet (como pueden ser el correo electrónico, la Web corporativa, los servicios de navegación Web, Andén Central, el correo electrónico y el sistema de relación con proveedores utilizado para la publicación de licitaciones y la presentación de ofertas, por destacar algunos de los más representativos), que requieren de garantías de seguridad y disponibilidad.

Los servicios que están publicados hacia Internet, por esta misma razón, tienen un mayor nivel de exposición al riesgo con origen en diferentes tipologías de ataques, como son los denominados ataques de denegación de servicio (DoS) y/o ataques distribuidos de denegación de servicios (DDoS), como variante de los primeros, que muestran una tendencia creciente en los últimos años.

En términos de seguridad, a finales del año pasado, 2021, la infraestructura tecnológica asociada a funciones de seguridad, cuyo objetivo principal es evitar y/o mitigar el efecto de los diferentes tipos de ataques que responden a patrones conocidos o identificables, se actualizó con unos equipos de propósito específico de mayor capacidad y prestaciones para afrontar eficaz y eficientemente los ataques de denegación de servicio que, en la gran mayoría de los casos, simulan un comportamiento normal de un usuario que accede a los servicios publicados, pero generando un muy elevado número de peticiones que intentan afectar la capacidad de los servidores para responder adecuadamente a las peticiones legítimas.

Durante 2020 hubo más ataques que nunca a clientes de diversos sectores, así como la campaña de extorsión DDoS más grande, que afectó a miles de empresas a nivel mundial. Por lo tanto, no sorprendió que, en 2021, los atacantes continuaran reforzando los ataques DDoS.

Los atacantes aceleran el ritmo y suben el listón y los ataques DDoS son cada vez peores. Tres de los seis peores ataques DDoS volumétricos que la empresa Akamai ha registrado y mitigado se han producido en abril de 2021, incluidos los dos mayores ataques de extorsión DDoS conocidos hasta la fecha.

Los atacantes siguen ampliando sus objetivos. El número de ataques a clientes al mes continuó a lo largo de 2021 hasta alcanzar un volumen sin precedentes y se ha seguido viendo la diversificación de los ataques en zonas geográficas y sectores. Un análisis reciente anunció un aumento del 57 % en la cantidad de clientes diferentes que han sufrido ataques año tras año.

En lo que llevamos de año, Andorra ha sufrido 3 ciberataques. Uno de ellos multiplicó por casi treinta el tráfico habitual de la red de telecomunicaciones de Andorra generando problemas de conexión intermitentes durante cuatro días a los clientes de fibra y móvil de Andorra Telecom, el único operador estatal. El portavoz de esta empresa, Carles Casadevall, explicó que, si bien el tráfico nacional habitual es de unos 35GB por segundo, el ataque hizo llegar la red a picos de 1TB. Tras la denuncia del operador, la unidad de delitos tecnológicos de la Policía de Andorra está investigando el origen del ataque. Carles Casadevall detalla que la agresión cibernética, del tipo de denegación de servicio (DDoS), llegó de 50 países diferentes, entre ellos Rusia, Corea del Sur, China o Brasil.

Los motivos de estos ataques pueden ser diversos, afán de notoriedad, guerra sucia, sabotajes, aunque el principal objetivo es la consecución de réditos económicos.

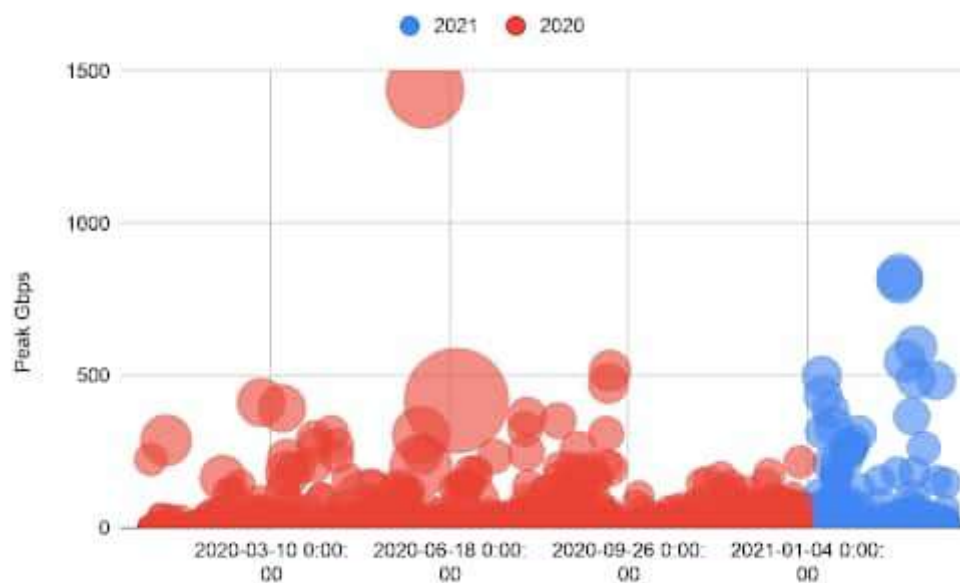
Al parecer, los cibercriminales se están aferrando a la esperanza de obtener importantes ganancias en bitcoins, así que han comenzado a redoblar sus esfuerzos y su ancho de banda de ataque, dejando atrás cualquier expectativa de que la extorsión DDoS se haya acabado.

Sin embargo, el tamaño del ataque de extorsión no ha sido la única característica notable del modus operandi de los atacantes. Tal como informó el equipo de respuesta a incidentes e inteligencia en seguridad (SIRT) de la empresa Akamai en la advertencia publicada el 23 de marzo de 2021, los cibercriminales utilizaban un vector de ataque DDoS nunca visto que aprovechaba un protocolo de red conocido como el protocolo 33 o el protocolo de control de congestión de datagramas (DCCP)

Conclusión: los atacantes escudriñan constantemente maneras nuevas y creativas de lanzar ataques DDoS, y la explotación del protocolo DCCP es el ejemplo más reciente de tales actividades delictivas.

Al mirar hacia el futuro, el pronóstico de ataques DDoS prevé el crecimiento de los ataques en cuatro frentes:

1. Número de ataques DDoS
2. Número de ataques DDoS de gran tamaño (> 50 Gbps)
3. Número de sectores a los que se dirigen los ataques DDoS
4. Número de organizaciones a los que se dirigen los ataques DDoS



Fig, 1: Ataques DDoS desde 2020 hasta el presente. Tamaño de las burbujas = Mpps; color = año.

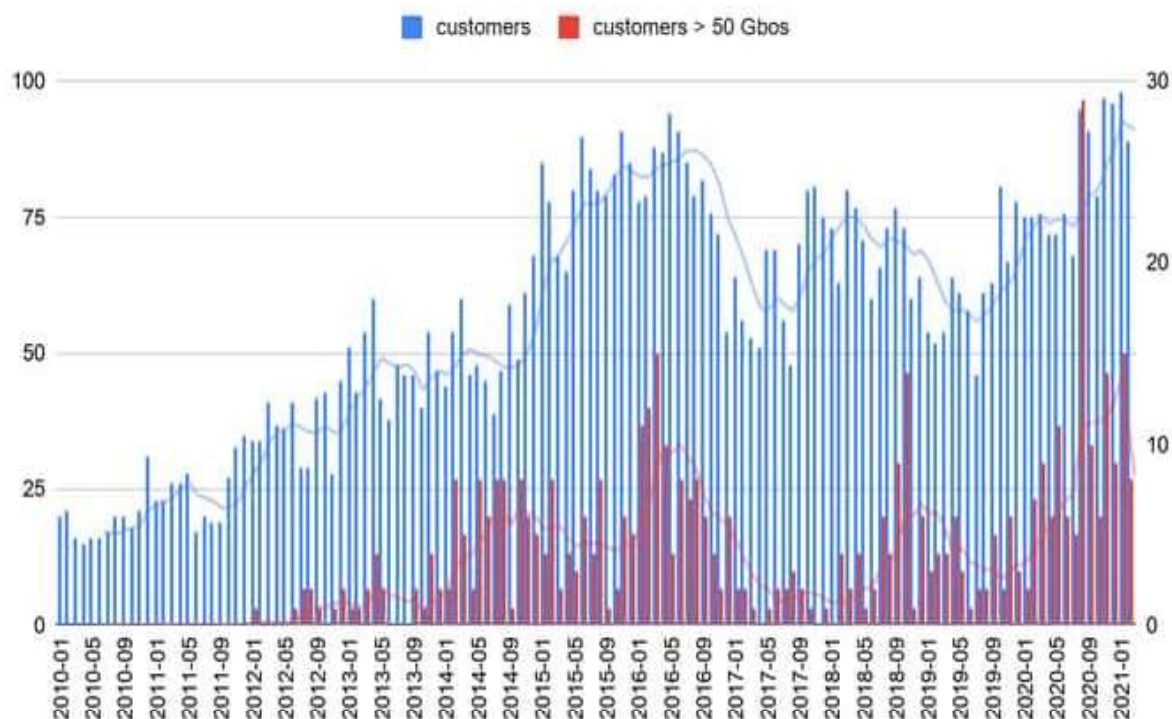


Fig. 2: Tendencias de ataques a clientes desde 2010 hasta el presente. Azul = total; rojo > 50 Gbps.

Fuente: Akamai Technologies (<https://www.akamai.com/es/es/> y <https://www.akamai.com/es/blog/security/2021-los-ataques-ddos-volumetricos-aumentan-con-rapidez>) empresa especializada en servicios de redes de distribución de contenido, rendimiento web avanzado y móvil, y seguridad en la nube, que publica informes trimestrales en cuanto al “Estado de Internet / Seguridad”.

En este contexto Metro de Madrid no puede ser ajeno a la realidad de los vectores de riesgo relativos a ataques de esta naturaleza que se producen en un mundo interconectado a través de Internet.

Es por ello que se dispone de dos equipos de propósito específico para la detección y protección contra ataques de denegación de servicios (DoS), distribuidos o no, respondiendo a las necesidades de protección de los servicios informáticos publicados hacia Internet, y permitiendo prever medidas de protección de forma anticipada y proactiva. Dichos equipos, Arbour Edge Defense 8100-1G, fueron adquiridos en las siguientes SCs:

- 2000003161, denominada “Adquisición de equipo para la protección ante ataques de denegación de servicios (DoS)” dio lugar al pedido 7721000041.
- 2000003265, denominada “Renovación tecnológica de un equipo para la protección ante ataques de denegación de servicios (DoS)” dio lugar al pedido 7721000172.

Para asegurar el correcto funcionamiento y la actualización permanente de los equipos de protección contra ataques de denegación de servicio, es necesario disponer del soporte y mantenimiento, tanto del hardware, como del software que lleva incorporado, incluyendo suscripciones de servicios y derechos de uso, así como, la

sustitución o reemplazo del equipamiento en caso de fin de vida, obsolescencia, rotura o daño irreparable.

Por ello, el objeto de la presente acción es la contratación del servicio de mantenimiento, soporte y suscripción de servicios del equipamiento para la protección ante ataques de denegación de servicios según los términos establecidos en los Pliegos de la Licitación.

Es necesario destacar que en el caso de no acometer la acción, la pérdida de soporte y mantenimiento del equipamiento ocasionaría la obsolescencia progresiva del mismo, la posibilidad de quedar fuera de servicio por un plazo indefinido en cualquier momento por cuestiones técnicas imprevistas, la imposibilidad de acceder a soporte técnico especializado, y una situación de ilegalidad en cuanto al uso del software y los servicios embebidos en el equipamiento; todo ello, impidiendo que se pueda garantizar la seguridad, el rendimiento y la disponibilidad de servicios críticos publicados en Internet; así como, la posibilidad de incurrir en costes mayores si no se contrata el soporte y mantenimiento, y posteriormente se quisiese regularizar la situación de los contratos.

4 ANTECEDENTES

a) *Contratos precedentes:*

	CONTRATACIONES ANTERIORES						CONTRATACIÓN ACTUAL
SOLICITUD DE CONTRATACIÓN N° CONTRATO	2000001121	6000005850	6000006834	6000007102	2000003161	2000003265	600000xxxx
OBJETO DEL CONTRATO	ADQ. EQUIPO PROTECCIÓN DoS	MANT EQUIPOS ANTIDoS	MANT PROTECCIÓN ANTE ATAQUES DENEG SERV	MANT. SISTEMAS SEGURIDAD INFORM. 2019-20 (Lote 9 - Mantenimiento, soporte y suscripción de servicios del equipamiento para la protección ante ataques de denegación de servicios	ADQ. EQUIPOS PROTECCIÓN ATAQUES DoS	RENOVAR PROTEC. ATAQUES DENEGACIÓN DoS	

				(DDoS))			
DURACIÓN INICIAL DEL CONTRATO	1 año	1 año	1 año	2 años	1 año	1 año	3 años y 24 días
PRÓRROGAS PREVISTAS	NO	NO	NO	NO	NO	NO	2 de 6 meses
MODIFICADOS PREVISTOS	NO	NO	NO	NO	NO	NO	NO
LOTES	NO	NO	NO	SI (Lote 9)	NO	NO	NO
PRESUPUESTO BASE LICITACIÓN (SIN IVA)	90.000,00 €	19.439,77 €	19.272,54 €	1.235.419,00 €	70.000,00 €	70.000,00 €	109.200,00
VALOR ESTIMADO	90.000,00 €	19.439,77 €	19.272,54 €	1.235.419,00 €	70.000,00 €	70.000,00 €	145.600,00 €
IMPTE SOPORTE, MTO y SUSCRIPCIÓN	22.510,52 €	19.439,77 €	19.272,54 €	31.143,36 €	14.068,83 €	14.068,83 €	

Nota: Algunos de estos contratos corresponden al suministro del equipamiento, el soporte, mantenimiento y suscripción de servicios por un año, y los servicios profesionales para la instalación, configuración y puesta en marcha del equipo. Por tal razón, se ha distinguido en esta fila las partidas económicas equivalentes al presente.

b) Comparación de los alcances del contrato precedente y el del objeto de la nueva licitación.

Los alcances entre el contrato precedentes en lo que respecta al soporte, mantenimiento y suscripción de servicios y el de esta nueva licitación son los mismos. Los alcances de las Solicitudes de Contratación, 2000003161 y 2000003265 son diferentes a la de esta Solicitud. En las SCs antes citadas se contemplaba el suministro de hardware (un equipo), servicios profesionales de instalación y el mantenimiento, el soporte técnico y suscripción de software, todo por un año, mientras que, en esta solicitud, se pide sólo el mantenimiento, el soporte técnico y la suscripción de software de los dos equipos, por 3 años y 24 días.

Con respecto al importe inicial con el que se lanzó la solicitud de contratación, en ésta se han realizado dos modificaciones:

- se ha aumentado la vigencia del contrato de 2 a 3 años, según recomendaciones del Gabinete del Director.
- Se han modificado las partidas anuales a la baja. Con respecto a la partida correspondiente al año 2024, se observa que es ligeramente superior a la de los años anteriores, esto es debido a los 24 días de más que incluye, para tener alineados el fin del soporte de los 2 equipos.

Se hace notar que el pago de cada anualidad se realiza por adelantado, de ahí que para el año 2025 no haya presupuestada cantidad alguna.

5 INFORMACIÓN PRESUPUESTARIA

PRESUPUESTO DE GASTO			
AÑO	2022	2023	2024
IMPORTE PERMITIDO	36.000,00 €	36.000,00 €	37.200,00 €
CECO	6740	6740	6740
CUENTA	622226	622226	622226

El presente documento, emitido a efectos de cumplimiento de obligaciones en materia de transparencia, es copia fiel del original, en el que constan las firmas auténticas y completas de las personas firmantes.

En cumplimiento de las obligaciones de protección de datos personales, no constan en esta copia datos identificativos adicionales a nombre y apellidos.