Metro de Madrid, S.A.

Memoria Justificativa y Solicitud de Contratación

OBJETO A CONTRATAR: SERVICIO DE PROTECCIÓN CONTRA ATAQUES VOLUMÉTRICOS DISTRIBUIDOS DE DENEGACIÓN DE SERVICIO (DDoS)

NÚMERO DE LA S.C: 6000010344

Dirección /Gerencia:	Explotación Ferroviaria Metro de Madrid, S.A.	**Área:**	Comunicaciones y Tecnologías de la Información.
División:	División de Instalaciones y Sistemas de Información	**Servicio:**	

Aprobado por: 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 de un servicio de protección ante ataques volumétricos distribuidos de denegación de servicio (DDoS).

2 DATOS DE LA LICITACIÓN

- **Objeto**

  El objeto que se contempla en la presente SC comprende la contratación de un servicio de protección ante ataques volumétricos distribuidos de denegación de servicio (DDoS).

- **Estamento responsable de la ejecución del contrato**

  Área de Comunicaciones y Tecnologías de la Información.

- **Valor estimado del contrato (artículo 101 LCSP)**

  Valor estimado: 210.000,00 euros (IVA no incluido).

- **Método de cálculo aplicado para determinar el valor estimado (artículo 101 LCSP)**

  ☒ En función de los precios del mercado sin incluir el IVA, teniendo en cuenta las posibles prórrogas (2 prorrogas de 6 meses).

- **Presupuesto base de Licitación (artículo 100 LCSP)**
  - Base imponible (BI): 140.000,00 euros
  - Importe del I.V.A.: 29.400,00 euros
  - Presupuesto base de licitación (PBL): 169.400,00 euros, IVA incluido

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

Costes Directos (98% del PE)	119.304,35 €
Costes Indirectos (2% del PE)	2.434,78 €
Presupuesto de Ejecución (PE): Costes Directos + Costes Indirectos	**121.739,13 €**
Gastos Generales (9% PE)	10.956,52 €

Beneficio Industrial (6% PE)	7.304,35 €

Base imponible	140.000,00 €

Presupuesto Base de Licitación (Base imponible + IVA)	**169.400,00 €**

- **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 servicio de protección ante ataques volumétricos distribuidos de denegación de servicio (DDOS) constituye un ámbito único de servicio que persigue un alto nivel de implicación y conocimiento de la realidad de Metro de Madrid. La realización independiente de diversas prestaciones en el marco del servicio sería una concepción errónea en tanto requeriría la coordinación de la ejecución de las diferentes prestaciones que, en la gran mayoría de los casos, requieren una respuesta inmediata, o están embebidas en el día a día de los procesos de negocio de la empresa, lo que se vería dificultado si existiese una pluralidad de contratistas. Por lo tanto, no procede la división en lotes.

- **Duración del contrato**

  - Plazo de duración/ejecución inicial del contrato: 24 meses

  - 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.

    - **Justificar los motivos** por los que este servicio/suministro precisa de un acta de inicio de los trabajos:

      Se precisa para establecer la forma de coordinar adecuadamente los trabajos de este servicio, 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 los sistemas y aplicaciones, en tanto es una exigencia de los fabricantes, en el caso que la siguiente licitación, o las licitaciones asociadas, se demorase en el tiempo para no incurrir en un proceso de regularización, asegurar que se sigue prestando el servicio, y, por último, conseguir un estado funcional óptimo de los sistemas y aplicaciones en caso de que, durante el período de vigencia del contrato, no se pueda acometer la evolución tecnológica de la plataforma que se ha determinado como necesaria, que daría lugar a una configuración diferente de sistemas y aplicaciones con sus propias particularidades en cuanto a soporte y mantenimiento.

    Las prórrogas se ejecutarán conforme a lo establecido en los pliegos de condiciones, siempre que el órgano de contratación los estime conveniente habiendo valorado por la situación del mercado o para dar coberturas en caso de no disponerse del nuevo contrato que dé continuidad.

- **Clasificación del contrato**

  ☒ Sujeto a LCSP (Ley 9/2017)

- **Naturaleza del contrato**

  ☒ Servicios

  - **Justificar** la insuficiencia de medios:

    Metro no dispone de medios para realizar la prestación; ya que, son servicios que requieren una altísima especialización técnica y la disponibilidad de equipamiento muy sofisticado para la prestación.

- **Procedimiento de licitación**

  ☒ Procedimiento Abierto

- **Justificación del procedimiento**:

- No es posible la aplicación del procedimiento abierto simplificado y simplificado abreviado, ya que el valor estimado del contrato es superior a los límites que establece la LCSP para estos procedimientos. 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.

- **<u>Criterio de adjudicación (artículos 145 y 146 LCSP)</u>**

☒ Pluralidad de criterios en base a la mejor relación **<u>calidad-precio</u>**

- Criterios cualitativos: 30,00 puntos

  Metodología y organización de los trabajos, 7,00 puntos

  Calidad del Servicio, 8,00 puntos

  Medios técnicos, 10,00 puntos

  Certificación ENS (Esquema Nacional de Seguridad), 5,00 puntos

  ¿Se aplicarán fórmulas de valoración de los criterios cualitativos? Si, para la "Certificación ENS"

  ¿Se evalúan criterios mediante juicios de valor dentro de la valoración de los criterios cualitativos?

  Sí, para los criterios: "Metodología y organización de los trabajos", "Calidad del Servicio" y "Medios técnicos".

  - **Justificación** de porqué se utilizan criterios de calidad evaluables mediante juicios de valor en lugar de criterios evaluables de forma automática mediante fórmulas automáticas**:**
    Al tratarse la naturaleza de este contrato de un servicio gestionado, resulta muy importante para el conocer el enfoque detallado de la prestación del servicio, metodología de seguimiento de los trabajos, organización de los trabajos y procedimientos previstos para asegurar la calidad del servicio. Estos aspectos son difícilmente valorables mediante la aplicación de fórmulas matemáticas, por ello se incluyen como aspectos cualitativos valorables mediante juicio de valor de acuerdo a las tablas detalladas en el PCP.

- Criterios económicos:

  ☒ Precio, 70,00 puntos

- ¿Se aplicarán fórmulas de valoración de los criterios económicos? Sí

- Se otorgará una puntuación económica de 0,00 puntos a las ofertas iguales al Presupuesto Base de licitación.
- Para el resto de casos se puntuará conforme a la siguiente fórmula:
- $C_i = C_{max} [1 - ((B_{max} - B_i)/B_{max})^{5/2}]$
-
- C_i = puntuación obtenida por el licitador i
-
- C_{max} = 70 puntos
-
- B_i = baja ofertada por el licitante i (%)
-
- B_{max} = Máxima baja ofertada admitida (%)
-
- Para el cálculo de las bajas ofertadas por los licitadores se aplicará la siguiente fórmula:
-
- $B_i = [1 – (Of_i/PBL)]*100$
-
- B_i = Baja (%) de la oferta económica "i"
-
- Of_i = Oferta económica "i"
-
- PBL = Presupuesto Base de Licitación

- **<u>Subcontratación (artículo 215 LCSP):</u>**

  ☒ Procede

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

- **<u>Procedimiento de subasta electrónica o petición sucesiva de ofertas</u>**

  ☒ NO

- **<u>Fondos FEDER</u>**

  ☒ Contrato no financiable con fondos FEDER

- **<u>Confidencialidad de los Pliegos de Prescripciones Técnicas</u>**

  ☒ SI

  ☒ En su totalidad

- **Justificar** las razones por las que se declara confidencial 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 y de la seguridad de las redes y sistemas de información.

- **Cesión de datos**

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

  ☒ NO

- **¿Ha participado alguna empresa externa a Metro de Madrid en la elaboración del pliego de prescripciones técnicas?**

  ☒ NO

3 JUSTIFICACIÓN DE LA NECESIDAD

La Coordinación de Seguridad Informática y Ciberseguridad, implanta, mantiene y gestiona 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, 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 la actualidad los ataques DDoS se distinguen en las siguientes categorías:

- Ataques volumétricos: son aquellos ataques que consiguen saturar el ancho de red. Son ataques que dejan inutilizables activos de red o activos publicados en internet por parte del cliente. **Este tipo de ataques no se pueden solventar por Metro de Madrid y requieren ser detenidos en un nivel de comunicaciones anterior, antes de llegar a la infraestructura de Metro.**
- Ataques de agotamiento de recursos: son los ataques que, sin saturar el enlace del cliente, consigue dejar indisponible a algún servicio generando suficiente tráfico para agotar la capacidad de procesamiento de los recursos de la infraestructura (firewall, balanceadores de carga, etc.).

- Ataques de Nivel de Aplicación: son los ataques que generan muy poco tráfico, que además suele aparecer como legítimo, pero que aprovecha fallos de diseño de las aplicaciones o de los servidores para sobrecargar los recursos computacionales del aplicativo.

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 aumentando 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 2022 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.

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

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, ya que se produce una pérdida de confianza en la marca, un daño reputacional y una afectación a los servicios que ofrecemos a nuestros usuarios.

Es por ello que Metro dispone de dos equipos Arbor Edge Defense 8100-1G, dimensionados al volumen de tráfico utilizado por los servicios que presta, 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. Su modo de funcionamiento es el siguiente:

- Analiza en tiempo real los paquetes de datos y volumen de tráfico que llega a nuestra red.
- Filtra el tráfico cuando se detectan comportamientos anómalos.
- Identifica las solicitudes de servicio legítimas de las generadas para saturar nuestra plataforma.

En los últimos meses, el grupo de ciberdelincuentes prorruso '*NoName057*', ha apuntado sus ataques contra instituciones y empresas danesas, alemanas, italianas, rumanas, noruegas, polacas, lituanas, suizas, holandesas o contra los parlamentos de Francia y Bulgaria. El pasado 16 de junio '*NoName057*' también incluyó a España entre sus objetivos, hackeando algunos operadores portuarios –junto a los de Italia, Alemania y Bulgaria–, y desde entonces ha lanzado una oleada de ataques DDoS, su especialidad, contra nuestro país que afectan incluso a la Casa Real.

En julio de este año se han producido ataques de DDos por dicho grupo contra países que apoyan a Ucrania en el conflicto, así como contra la propia nación ucraniana.

Este grupo de delincuentes ha reclamado estas ofensivas a través de su canal de Telegram, donde el pasado miércoles, 19 de julio de 2023, anunció que había conseguido bloquear las páginas web oficiales de la Casa Real, de la Moncloa, de los Ministerios de Justicia y de Política Territorial, del Tribunal Constitucional, de la Casa de la Moneda y de la empresa de consultoría e ingeniería Isdefe.

El jueves, 20 de julio de 2023 dicho grupo continuó con sus ataques contra empresas y organismos de España cometiendo nuevos ciberataques DDoS que estuvieron centrados en el sector bancario. Según informó en su cuenta de Telegram, esta vez sus víctimas fueron del sector bancario: ABANCA, Grupo Caja Rural, el Banco Cooperativo Español y Bankinter, cuyas páginas web quedaron inoperativas. En el caso de Bankinter, los piratas también deshabilitaron su aplicación.

El viernes, 21 de julio de 2023, dicho grupo publicaba en su cuenta de Telegram un mensaje en el que indicaba que continuaban su "viaje por España" y atacó las páginas web de puertos estatales y autoridades portuarias. Y posteriormente **se atribuyó más ofensivas que están centradas en el sector de transportes y que afectaron a Metro de Madrid**, a la EMT, a RENFE, a la red de tranvías de Barcelona, al servicio de metro y tranvías de Valencia, al Consorcio de Transporte de Mallorca y a la compañía de autobuses Avanza.

En el caso particular de Metro, el volumen del ataque bloqueó las comunicaciones de Metro durante 2 horas, tiempo que se tardó en encontrar las causas y proceder a la remediación, que consistió en que los técnicos de comunicaciones se pusieron en contacto con nuestros dos proveedores de servicios de internet -Telefónica y Globalia- para filtrar todo nuestro tráfico de internet en un nivel de comunicaciones anterior, antes de llegar a la infraestructura de Metro y sólo dejar que pasara el tráfico legítimo. **Esta acción la hicieron de forma gratuita, pero este servicio tiene un coste económico**.

Tuvo, además, diversas afecciones en los servicios de Metro durante más de 5 horas.

Posteriormente, el pasado jueves 21 de septiembre y el domingo 8 de octubre, Metro volvió a sufrir otro nuevo ataque durante más de 24 horas, pero de menor magnitud

que el anterior, en este caso, nuestros dos equipos Arbor Edge Defense 8100-1G fueron capaces de pararlo.

Los recientes ataques sufridos han puesto en evidencia la necesidad de dotarse, complementariamente, de una solución de protección ante ataques volumétricos. Si bien la solución instalada en el CPD no deja pasar hacia dentro los ataques volumétricos, nada puede hacer para evitar que, debido al ataque, el ancho de banda bajante se sature. Una protección completa requiere, por lo tanto, de una solución híbrida, con equipos «on-premises», como los Arbor Edge Defense ya desplegados en nuestros CPD, y una solución en la nube, en formato SaaS («Software as a Service») capaz de filtrar el tráfico del ataque antes de dirigirse hacia los enlaces de Internet de Metro de Madrid.

Todo ello hace que se proponga la contratación del servicio para que en futuros ataques, Metro sea capaz de proteger sus activos sin que tenga que estar sujeto a las decisiones de otras empresas de realizar favores de forma gratuita.

4 ANTECEDENTES

No existen contratos precedentes.

No se puede realizar comparación alguna pues es la primera vez que se contrata este tipo de servicio.

5 INFORMACIÓN PRESUPUESTARIA

PRESUPUESTO DE GASTO			
AÑO	**2024**	**2025**	**2026**
IMPORTE PERMITIDO	17.500,00 €	70.000,00 €	52.500,00 €
CECO	6740	6740	6740
CUENTA	629004	629004	629004