



Memoria Justificativa y Solicitud de Contratación

**OBJETO A CONTRATAR: RENOVACIÓN TECNOLÓGICA DE
EQUIPO PARA LA PROTECCIÓN ANTE ATAQUES DE
DENEGACIÓN DE SERVICIOS (DoS)**

SolCon 2000003265

**Dirección
/Gerencia:**

Explotación Ferroviaria

Área:

Sistemas de Información

Metro de Madrid, S.A.

División:

Ingeniería y Mantenimiento

Servicio:

Explotación de Sistemas y
Seguridad Informática

Aprobado por: Juan Pablo 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 la renovación tecnológica del equipo existente para la protección ante ataques de denegación de servicios (DoS) en tanto se encuentra en fin de mantenimiento, lo que significa que desde dicha fecha no se producen actualizaciones software para el modelo instalado, y con un fin de vida próximo previsto a partir de cual ya no tendrá mantenimiento hardware.

En un equipo de esta tipología no disponer de actualizaciones software hace que ante el avance en los temas derivados de la ciberseguridad que sea fácilmente atacable y parcialmente útil para su cometido.

2 DATOS DE LA LICITACIÓN

▪ Objeto

Contratación consistente en la renovación tecnológica de un (1) equipo para la protección ante ataques de denegación de servicios (DoS) que actualmente se encuentra protegiendo la conexión a Internet.

El equipo a renovar es de propósito específico, y de última generación¹, con la capacidad de detección, prevención y protección en el caso de ataques de denegación de servicios (DoS), distribuidos o no, que, simulando el comportamiento normal de un usuario que accede a los servicios publicados, genera un muy elevado número de peticiones que intentan afectar la capacidad para seguir ofreciendo el servicio en los términos óptimos para los usuarios. Igualmente, incorporan software y/o suscripciones a servicios de inteligencia que permiten precisamente evitar los ataques en base al conocimiento global.

El suministro consistirá en la adquisición de un (1) equipo para la renovación tecnológica del existente para la protección del nodo de red frontera de conexión con Internet, con su correspondiente software embebido y soporte técnico y mantenimiento, y los servicios profesionales mínimos para su instalación y configuración inicial.

▪ Servicio responsable de la ejecución del contrato

Servicio de Explotación de Sistemas y Seguridad Informática.

▪ Valor estimado del contrato (artículo 101)

¹ A su vez, sería exactamente igual al modelo de equipo para la protección ante ataques de denegación de servicios (DoS) que se ha propuesto adquirir para dotar al 2º nodo de red frontera de los mismos controles de seguridad que el nodo primario. La unificación de tecnologías permite también una gestión más eficiente en cuanto a la configuración y administración de las reglas.

Valor estimado: 70.000,00 euros (IVA no incluido)

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

☒ El valor real del contrato precedente, ajustado en función de los precios de mercado y de los cambios en el número de unidades de materiales a suministrar

▪ **Presupuesto base de Licitación (Art. 100)**

- Base imponible (BI): 70.000,00 euros
- Importe del I.V.A.: 14.700,00 euros
- Presupuesto base de licitación (PBL): 84.700,00 euros, IVA incluido

▪ **Desglose del presupuesto base de licitación (Art. 100.2)**

Costes Directos (98%)	59.652,18 €
Costes Indirectos (2%)	1.217,39 €
PRESUPUESTO DE EJECUCIÓN	60.869,57 €
Gastos Generales (9%)	5.478,26 €
Beneficio Industrial (6%)	3.652,17 €
BI	70.000,00 €
IVA	14.700,00 €
PBL	84.700,00 €

▪ **Modificación del contrato**

☒ No procede

▪ **División en lotes:**

☒ NO se divide en lotes (Art. 99.3)

- **Justificar los motivos** de la no división en lotes: La adquisición del equipo para la protección ante ataques de denegación de servicios (DoS) constituye un ámbito único de suministro que incluye todos los aspectos requeridos como son la adquisición, el respectivo soporte y mantenimiento anual, y los servicios profesionales mínimos para su instalación y configuración inicial, siendo elementos inseparables. Por lo tanto, no procede la división en lotes.

▪ **Duración del contrato**

- Plazo de duración/ejecución inicial del contrato: 1 año, 1 mes y 15 días.
- Hito a partir del cual comienza la duración/ejecución del contrato:
 - ☒ A partir del día siguiente a la formalización del contrato
- Prórrogas:
 - ☒ NO

▪ **Clasificación del contrato**

- ☒ Sujeto a LCSP (Ley 9/2017)

▪ **Naturaleza del contrato**

- ☒ Suministros

▪ **Procedimiento de licitación**

- ☒ Procedimiento Abierto Simplificado

Se propone la contratación mediante procedimiento abierto con el fin de asegurar los principios de igualdad, transparencia y libre competencia. Además, no se reúnen los requisitos necesarios que exige la LCSP para la aplicación de un procedimiento negociado. En consecuencia con lo anterior, se va a utilizar el procedimiento abierto simplificado al tratarse de un contrato que cumple con las dos condiciones previstas en el artículo 159.1 de la LCSP.

▪ **Criterio de adjudicación (Arts. 145 y 146)**

- ☒ Único criterio (precio o criterio basado en rentabilidad)

- **Justificar las razones** por el que se propone este criterio de adjudicación: El criterio de adjudicación será el precio más bajo. La razón es que los productos a adquirir están perfectamente definidos - técnica y económicamente - por cada uno de los fabricantes no siendo posible introducir modificaciones de ninguna clase respecto de sus funcionalidades, prestaciones y/o características técnicas. Igualmente, el soporte y mantenimiento de los productos 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, incluyendo los servicios profesionales de instalación y puesta en marcha.

En consecuencia, no es posible que los licitadores presenten propuestas con variaciones ni en los productos ni en sus condiciones de soporte y mantenimiento, ni es susceptible de introducirse ninguna modificación en el contrato. Las propuestas de los licitadores solo podrán diferenciarse en el precio ofertado.

▪ **Subcontratación**

☒ Procede

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

▪ **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 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 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 ANTECEDENTES Y JUSTIFICACIÓN DE LA NECESIDAD

Desde el Área de Comunicaciones y Tecnologías de la Información (en lo sucesivo, ACTI) se implanta y mantiene una gran cantidad de servicios informáticos corporativos, desarrollados y/o soportados en tecnologías variadas y que operan 24 horas al día, los 7 días a la semana, los 365 días del año. Entre dichos servicios se encuentran aquellos que se publican hacia Internet que, por tal razón, tienen un mayor nivel de exposición al riesgo con origen en la probabilidad de materialización de diferentes tipos de ataques, por lo que requieren de garantías de seguridad y disponibilidad específicas. Son ejemplo de estos tipos de ataques los denominados de denegación de servicio (DoS), distribuidos o no, que muestran una tendencia creciente en los últimos años.

En términos de seguridad, se dispone de una infraestructura tecnológica cuyo objetivo principal es evitar y/o mitigar el efecto de los diferentes tipos de ataques que podrían materializarse, y que se muestra efectiva principalmente en aquellos casos que responden a patrones conocidos o identificables. Dicha infraestructura está constituida por diferentes elementos, cada uno con un propósito específico, que protegen la red corporativa en general, y los servicios publicados en particular, frente a los ataques provenientes de Internet.

La infraestructura de seguridad implementada requiere, entre otros, tener capacidad de detección, prevención y protección en el caso de ataques de denegación de servicios (DoS), distribuidos o no; ya que, se trata de formas de ataque muy específicas

y que, en algunos casos, llegan a simular un comportamiento normal de un usuario que accede a los servicios publicados, aunque generando un muy elevado número de peticiones que intentan afectar la capacidad para seguir ofreciendo el servicio en los términos óptimos para los usuarios, haciendo mucho más difícil su reconocimiento, para lo que se requiere de equipos especialmente preparados a tal fin.

A tales efectos, se dispone de un (1) equipo Arbor, modelo Pravail APS 2104 del fabricante NetScout, que se encarga de la detección, prevención y protección en el caso de ataques de denegación de servicios (DoS) en el nodo de la red frontera de conexión con Internet que se encuentra activo, con su correspondiente soporte técnico y mantenimiento, y suscripción de servicios y software hasta el mes de abril de 2021.

Dicho modelo, según comunicado del fabricante NetScout, se encuentra en fin de mantenimiento desde el pasado 31.12.2019, lo que significa que, desde dicha fecha, aunque se sigue dando asistencia técnica y mantenimiento de software para las últimas versiones desarrolladas para dichos modelos, no se producen actualizaciones de software para el modelo instalado, lo que significa que cualquier problema de seguridad o de funcionamiento que se resuelva con nuevas versiones de software no estará disponible para este modelo. Por otro lado, tiene fin de vida previsto para el 31.12.2021 momento a partir del cual ya no contará con ningún tipo de asistencia técnica y/o mantenimiento ni hardware ni software. La evolución tecnológica del modelo Pravail APS 2104 es el modelo Arbor Edge Defense 2600 que, adicionalmente, posibilita la migración de todas las configuraciones y reglas de seguridad actualmente implementadas según las necesidades de los servicios informáticos de Metro de Madrid.

Por ello, el objeto de la presente acción es la adquisición de un (1) equipo de propósito específico para la detección, prevención y protección contra ataques de denegación de servicios (DoS), con su respectivo soporte técnico y mantenimiento, así como las tareas de instalación, configuración, prueba y puesta en producción, todo ello según los términos establecidos en los pliegos de la licitación, para la renovación tecnológica del existente.

En el caso de no acometer la acción, no se dispondrá de equipo de propósito específico para la detección, prevención y protección en el caso de ataques de denegación de servicios (DoS) para la conexión a Internet, con la consecuente imposibilidad de ofrecer niveles de ciberseguridad acordes a las necesidades de Metro de Madrid, ni disponer de una infraestructura de servicios de seguridad homogénea.

La adquisición de equipos para la protección ante ataques de denegación de servicios (DoS) tiene asociados contratos ejecutados anteriormente, a saber:

Empresa	Contrato N°	Período	Importe Contrato
Sistemas Avanzados de Tecnología, S.A. (SATEC)	7716000041	marzo 2016	70.950,97 €

4 INFORMACIÓN PRESUPUESTARIA

PRESUPUESTO DE INVERSIÓN

AÑO	2021
IMPORTE PERMITIDO	70.000,00 €
PEP	08.058
EXPEDIENTE	N2516