

Este documento se ha obtenido directamente del original que contenía todas las firmas auténticas y se han ocultado los datos personales protegidos y los códigos que permitirían acceder al original

# Memoria Justificativa de la Necesidad

---

---

***“SERVICIOS GESTIONADOS DE CIBERSEGURIDAD DE MADRID DIGITAL - 4 LOTES”***

---

---



## MEMORIA JUSTIFICATIVA DE LA NECESIDAD DEL CONTRATO DE SERVICIOS DENOMINADO “SERVICIOS GESTIONADOS DE CIBERSEGURIDAD DE MADRID DIGITAL - 4 LOTES” A ADJUDICAR MEDIANTE PROCEDIMIENTO ABIERTO CON PLURALIDAD DE CRITERIOS.

### ANTECEDENTES Y JUSTIFICACIÓN DE LA NECESIDAD.

De acuerdo con lo establecido en el artículo 10 de la Ley 7/2005, de 23 de diciembre, de Medidas Fiscales y Administrativas (B.O.C.M. núm. 311, de 30 de diciembre de 2005), modificada parcialmente por la Ley 9/2015, de 28 de diciembre, de Medidas Fiscales y Administrativas (B.O.C.M. núm. 311, de 31 de diciembre de 2015), y por de la Ley 11/2022, de 21 de diciembre, de Medidas Urgentes para el Impulso de la Actividad Económica y la Modernización de la Administración de la Comunidad de Madrid –artículo 26–la (B.O.C.M. núm. 304, de 22 de diciembre de 2022), la **Agencia para la Administración Digital de la Comunidad de Madrid** (en adelante, la **Agencia** o **Madrid Digital**), en el ejercicio de sus competencias, obra con plena autonomía financiera y de gestión, y opera bajo los objetivos de horizontalidad y centralización en la gestión de los servicios de informática y comunicaciones de la Administración de la Comunidad de Madrid, de modo que se garantice el mejor equilibrio técnico-económico entre las soluciones aplicadas y los servicios prestados, todo ello sin perjuicio de la necesaria atención a las peculiaridades propias de los servicios públicos que se prestan a los ciudadanos.

Entre las competencias que, conforme al apartado tercero del referido precepto, se atribuyen a la Agencia para el cumplimiento de sus objetivos se recoge/n, en concreto, la/s siguiente/s:

*a) La dirección, planificación, impulso, desarrollo y ejecución de planes y proyectos de tecnología, de comunicación electrónica y de seguridad de la información de la Administración General e Institucional de la Comunidad de Madrid, garantizando la interoperabilidad, escalabilidad, compatibilidad, suministro e intercambio de información.*

*d) La adquisición, el diseño, desarrollo, implantación, mantenimiento, gestión y evolución de la infraestructura tecnológica, sistemas de información y de comunicaciones electrónicas y seguridad de la información de titularidad de la Agencia, así como la ejecución de las actuaciones para su consolidación y racionalización, incluyéndose en particular el puesto de trabajo, las infraestructuras de almacenamiento, los centros de procesos de datos, incluido el uso de nubes públicas y privadas de la Comunidad de Madrid y el archivo electrónico único de los expedientes y documentos electrónicos.*

*j) Elaboración y aprobación de las políticas de seguridad de los sistemas de información y comunicación electrónicas de titularidad de la Agencia y la gestión de los recursos comunes para la prevención, detección y respuesta a los incidentes y amenazas de ciberseguridad en el ámbito de sus funciones.*

El desarrollo de estas competencias de seguridad de la información y ciberseguridad es uno de los cinco objetivos del Plan Estratégico 2022-26 de Madrid Digital, cuyo propósito es: Hacer de la Comunidad de Madrid una Administración más segura, confiable y resiliente. Este objetivo se desarrolla en dicho plan a través de cuatro líneas de actuación, dos de ellas dedicadas a la prevención, cibervigilancia y detección de amenazas y vulnerabilidades de forma proactiva y

temprana, con el fin de eliminarlas, neutralizarlas, minimizando las consecuencias de materialización de incidente de seguridad, y otra de respuesta y recuperación ante incidentes de seguridad que permitan gestionar el riesgo, minimizando el impacto del incidente e identificando sus causas.

Hay que tener en cuenta que, según va avanzando y aumentando la digitalización de la Comunidad de Madrid y, por tanto, el número y diversidad de servicios digitales y sistemas de información que utilizan los ciudadanos y los empleados públicos, mayor es la necesidad de ciberseguridad que garantice de forma transversal e integradora que la información y los datos personales están protegidos. Y más aún si consideramos que cualquier Administración se relaciona de forma continua con el ciudadano, con otras Administraciones y con las empresas por Internet, red abierta a todo el mundo, en la que se detecta una tendencia al alza sobre todo tipo de ciberdelitos (sobre todo el ransomware, el phishing y las estafas por Internet).

Es evidente, por tanto, el importante reto en materia de seguridad de la información y ciberseguridad para la Comunidad de Madrid y Madrid Digital, que obliga a reforzar y aumentar de forma constante y proactiva las capacidades de personal especializado, procesos y tecnologías de ciberseguridad, necesarias para asegurar la disponibilidad, confidencialidad e integridad de la información y de los servicios digitales, todo ello bajo un enfoque de identificación y gestión de riesgos.

La Agencia en ejercicio de sus competencias, y a razón de las necesidades descritas anteriormente, ya en 2019, adjudicó el contrato ECON/000079/2018 denominado: “*Diseño, implementación y supervisión de servicios de ciberseguridad de la Comunidad de Madrid (2 lotes)*”, cuyo Lote 1 fue suscrito con la empresa SISTEMAS INFORMATICOS ABIERTOS, S.A. y el Lote 2 con la empresa ATOS SPAIN, S.A.

Con la presente contratación, se pretende:

- Aumentar y mejorar las capacidades humanas, organizativas y tecnológicas en materia de prevención, detección, análisis y respuesta.
- Disponer de más flexibilidad y capacidad ante los riesgos y amenazas actuales y futuras.
- Reforzar las capacidades avanzadas de respuesta y resiliencia en caso de incidentes o ataques premeditados, que permitan reducir los tiempos de detección, identificar la causa raíz y minimizar el impacto de los incidentes de seguridad.
- Poder realizar simulacros, ejercicios de ataque y defensa que permitan evidenciar riesgos y debilidades para mejorar las defensas.
- Impulsar la mejora de la seguridad desde el diseño y el refuerzo de las medidas y controles de ciberseguridad aplicados en las protecciones para evitar los daños que puedan producir las distintas amenazas y vectores de ataque.
- Mejorar la conciencia, comprensión y compromiso con la ciberseguridad en toda la organización.

La consecución de los objetivos fijados en materia de ciberseguridad requiere de:

- Detección y evaluación continua de las vulnerabilidades técnicas conocidas asociadas a cada tecnología, y de los nuevos métodos de ataque y explotación de estas vulnerabilidades, así como de las medidas preventivas recomendadas por organizaciones

gubernamentales de seguridad (CCN-CERT, INCIBE, CNPIC, etc.), fabricantes y empresas de seguridad, para minimizar los riesgos de materialización de ciberincidentes.

- Tecnologías, herramientas y capacidades específicas avanzadas en materia de prevención y detección temprana de amenazas, y monitorización, detección y análisis de ciberincidentes. El amplio abanico de herramientas existentes añade una alta complejidad a su implantación, parametrización y adaptación a las tecnologías con las que deben interactuar, requiriendo un conocimiento muy especializado de las mismas. La instalación de los nuevos sistemas previstos (sistema de gestión de eventos e información de seguridad, SIEM, y sistema de análisis avanzado de tráfico NDR) en nube, requiere personal experto en la parametrización de fuentes de eventos, casos de uso de monitorización, e integraciones con servicios de inteligencia de amenazas, que permita explotar de forma eficiente los eventos de seguridad e identificar los incidentes de seguridad.
- Disponer de personal altamente capacitado y especializado en la búsqueda proactiva de amenazas persistentes (Threat Hunting) en el análisis de los incidentes de seguridad, en la evaluación de su impacto en los servicios, en la determinación de la causa raíz y en los protocolos de contención y recuperación de sistemas necesarios. Todo ello se ha visto exponencialmente incrementado por el cada vez mayor número y alto grado de complejidad actual de los servicios e infraestructuras TIC, y por el incremento y especialización de los ataques orientados a comprometer su seguridad, y el alto impacto que puede provocar la materialización de un ataque en la información y servicios digitales que presta Madrid Digital (indisponibilidad del servicio, fuga de información confidencial, pérdida de reputación, etc.).
- Un alto conocimiento en materia de seguridad de todas las tecnologías e infraestructuras utilizadas por Madrid Digital, ya sean servidores, bases de datos, comunicaciones, software de negocio o soluciones específicas de seguridad, para analizar las configuraciones y las arquitecturas de seguridad implantadas, y proponer mejoras de forma continua sobre estas arquitecturas, y sobre los procesos de revisión y control de medidas de seguridad establecidos en Madrid Digital.
- Conocimiento experto en las técnicas de ataque y actores de amenazas activos más utilizados en cada momento, que permita simular estos ataques a fin de identificar vulnerabilidades y amenazas explotables de los sistemas, mejorar los procedimientos operativos de monitorización y control, y las protecciones actuales.
- Un equipo especializado en el seguimiento y control de servicios gestionados de ciberseguridad, que apoye a la Subdirección de General de Ciberseguridad en el gobierno de cada servicio.

Ante la necesidad de garantizar la continuidad y cobertura de las necesidades descritas, y siendo competencia de la Agencia proporcionar el servicio que se pretende, atendiendo a la especificidad de los servicios que constituyen su objeto, y la necesidad de abordar los mismos de manera eficaz y con las garantías requeridas, procede la tramitación del oportuno expediente de contratación.

Por lo tanto, en base al valor estimado del contrato, con la pretensión de recibir el mayor número de proposiciones, a fin de obtener un criterio de selección objetivo, y en base a la mejor relación calidad-precio, esta Subdirección General propone su tramitación mediante **procedimiento abierto con pluralidad de criterios**, en virtud de lo establecido en los Artículos 131.2, 145 y 156 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP).

## OBJETO DEL CONTRATO

El objeto del presente contrato es la prestación de los servicios de ciberseguridad necesarios para dotar a Madrid Digital de: capacidades en materia prevención, detección y análisis de amenazas, ciberataques y vulnerabilidades; de capacidades de respuesta y recuperación ante incidentes de seguridad; de capacidades de simulacros y ejercicios de ataque y defensa; de prescripción y asesoramiento de medidas y controles de ciberseguridad que fortalezcan las arquitecturas tecnológicas existentes o las que nuevas que se requieren implantar; y de apoyo a Madrid Digital para el seguimiento y control de la prestación de los servicios.

Se divide en los siguientes lotes:

- LOTE 1: Centro de Operaciones de Ciberseguridad (SOC-MD).
- LOTE 2: Servicios de Supervisión y Control de las Protecciones (SSCP-MD).
- LOTE 3: Servicio de Ciberseguridad Ofensiva (SCO-MD).
- LOTE 4: Oficina Técnica de Seguimiento y Control de los Servicios Gestionados de Ciberseguridad (OTSC-Ciber).

Todo ello, dentro del ámbito de competencia de la Agencia, de conformidad con lo establecido en el pliego prescripciones técnicas.

## PLAZO DE EJECUCIÓN

El plazo de duración del contrato será de **24 MESES**, desde el 1 de julio de 2024 hasta el 30 de junio de 2026.

## IMPORTE DEL CONTRATO

El importe máximo del contrato será de **QUINCE MILLONES SEISCIENTOS CUARENTA Y TRES MIL TRESCIENTOS VEINTINUEVE EUROS CON QUINCE CÉNTIMOS, IVA incluido, 15.643.329,15 €, IVA incluido, según el siguiente desglose:**

**TABLA CONJUNTA DE TODOS LOS LOTES CON PRESUPUESTO AL COMPLETO:**

	LOTE 1	LOTE 2	LOTE 3	LOTE 4	TOTAL
<b>CUOTA FIJA</b>	11.171.499,20 €	738.816,00 €	0,00 €	519.168,00 €	12.429.483,20 €
<b>CUOTA VARIABLE</b>	234.624,00 €	34.632,00 €	229.632,00 €	0,00 €	498.888,00 €
<b>TOTAL BASE IMPONIBLE</b>	11.406.123,20 €	773.448,00 €	229.632,00 €	519.168,00 €	12.928.371,20 €
<b>IVA</b>	2.395.285,87 €	162.424,08 €	48.222,72 €	109.025,28 €	2.714.957,95 €
<b>TOTAL CON IVA</b>	13.801.409,07 €	935.872,08 €	277.854,72 €	628.193,28 €	15.643.329,15 €

LOTES	AÑO 2024	AÑO 2025	AÑO 2026	TOTALES
<b>Lote 1: Centro Operaciones Ciberseguridad - SOC</b>				
Cuota fija - servicios	599.204,80 €	1.289.529,60 €	644.764,80 €	2.533.499,20
Cuota fija - subscripciones	2.159.500,00 €	4.319.000,00 €	2.159.500,00 €	8.638.000,00
<b>Total Cuota Fija</b>	<b>2.758.704,80 €</b>	<b>5.608.529,60 €</b>	<b>2.804.264,80 €</b>	<b>11.171.499,20</b>
Cuota variable - servicios	58.656,00 €	117.312,00 €	58.656,00 €	234.624,00
<b>Base Imponible</b>	<b>2.817.360,80 €</b>	<b>5.725.841,60 €</b>	<b>2.862.920,80 €</b>	<b>11.406.123,20</b>
<b>21% IVA</b>	<b>591.645,76 €</b>	<b>1.202.426,74 €</b>	<b>601.213,37 €</b>	<b>2.395.285,87</b>
<b>Importe Total , IVA Incluido</b>	<b>3.409.006,56 €</b>	<b>6.928.268,34 €</b>	<b>3.464.134,17 €</b>	<b>13.801.409,07</b>
<b>Lote 2: Supervisión y Control de las Protecciones - SCP</b>				
Cuota fija - servicios	184.704,00 €	369.408,00 €	184.704,00 €	738.816,00
Cuota variable - servicios	0,00 €	23.088,00 €	11.544,00 €	34.632,00
<b>Base Imponible</b>	<b>184.704,00 €</b>	<b>392.496,00 €</b>	<b>196.248,00 €</b>	<b>773.448,00</b>
<b>21% IVA</b>	<b>38.787,84 €</b>	<b>82.424,16 €</b>	<b>41.212,08 €</b>	<b>162.424,08 €</b>
<b>Importe Total , IVA Incluido</b>	<b>223.491,84 €</b>	<b>474.920,16 €</b>	<b>237.460,08 €</b>	<b>935.872,08 €</b>
<b>Lote 3: Ciberseguridad Ofensiva - SCO</b>				
Cuota variable - servicios	57.408,00 €	114.816,00 €	57.408,00 €	229.632,00 €
<b>Base Imponible</b>	<b>57.408,00 €</b>	<b>114.816,00 €</b>	<b>57.408,00 €</b>	<b>229.632,00 €</b>
<b>21% IVA</b>	<b>12.055,68 €</b>	<b>24.111,36 €</b>	<b>12.055,68 €</b>	<b>48.222,72 €</b>
<b>Importe Total , IVA Incluido</b>	<b>69.463,68 €</b>	<b>138.927,36 €</b>	<b>69.463,68 €</b>	<b>277.854,72 €</b>
<b>Lote 4: Oficina Técnica Seguimiento y Control - OTSGC</b>				
Cuota fija - servicios	129.792,00 €	259.584,00 €	129.792,00 €	519.168,00 €
<b>Base Imponible</b>	<b>129.792,00 €</b>	<b>259.584,00 €</b>	<b>129.792,00 €</b>	<b>519.168,00 €</b>
<b>21% IVA</b>	<b>27.256,32 €</b>	<b>54.512,64 €</b>	<b>27.256,32 €</b>	<b>109.025,28 €</b>
<b>Importe Total , IVA Incluido</b>	<b>157.048,32 €</b>	<b>314.096,64 €</b>	<b>157.048,32 €</b>	<b>628.193,28 €</b>



LOTES	AÑO 2024	AÑO 2025	AÑO 2026	TOTALES
Importes Totales sin IVA	3.189.264,80 €	6.492.737,60 €	3.246.368,80 €	12.928.371,20 €
21% IVA	669.745,60 €	1.363.474,90 €	681.737,45 €	2.714.957,95 €
Importes Totales con IVA	3.859.010,40 €	7.856.212,50 €	3.928.106,25 €	15.643.329,15 €

Por lo anteriormente expuesto, esta Subdirección propone el inicio de los trámites oportunos para proceder a la contratación de los servicios referenciados.

**La Subdirectora de la Subdirección General de Ciberseguridad, Protección de Datos y Privacidad**

Firmado digitalmente por: MUÑOZ FUENTES ESTHER  
Fecha: 2024 06 12 12:32

**Fdo.: Esther Muñoz Fuentes**