

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



RESOLUCIÓN DE INICIO DE EXPEDIENTE DE CONTATACIÓN

EXPEDIENTE AC-001-2025

RESOLUCIÓN DEL CONSEJERO DELEGADO DE LA
AGENCIA DE CIBERSEGURIDAD DE LA COMUNIDAD
DE MADRID POR LA QUE SE INICIA EL EXPEDIENTE
DE CONTRATACIÓN DENOMINADO

“SERVICIOS DE SOPORTE A LA OFICINA DE
GOBIERNO, RIESGO Y CUMPLIMIENTO DE LA
AGENCIA DE CIBERSEGURIDAD DE LA COMUNIDAD
DE MADRID”.

Control de Cambios

Autor	Versión	Fecha
Agencia de Ciberseguridad de la Comunidad de Madrid	0.1	31/01/2025

Resolución del Consejero Delegado de la Agencia de Ciberseguridad de la Comunidad de Madrid por la que se inicia el expediente de contratación denominado “SERVICIOS DE SOPORTE A LA OFICINA DE GOBIERNO, RIESGO Y CUMPLIMIENTO DE LA AGENCIA DE CIBERSEGURIDAD DE LA COMUNIDAD DE MADRID”.

De conformidad con lo que establece el Artículo 116 de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP), en uso de las atribuciones que me han sido conferidas de conformidad con lo dispuesto en Ley 14/2023, de 20 de diciembre, por la que se crea la Agencia de Ciberseguridad de la Comunidad de Madrid, y a la vista de la propuesta de contratación efectuada

RESUELVO

Autorizar el inicio y ordenar la tramitación del expediente de contratación del servicio denominado **“SERVICIOS DE SOPORTE A LA OFICINA DE GOBIERNO, RIESGO Y CUMPLIMIENTO DE LA AGENCIA DE CIBERSEGURIDAD DE LA COMUNIDAD DE MADRID”** cuyo presupuesto máximo de licitación asciende a **506.890,92 €** (quinientos seis mil ochocientos noventa euros con noventa y dos céntimos), IVA incluido, por anualidad.

La estimación del valor del contrato, incluyendo las posibles prórrogas, asciende a **1.256.754,34 €** (un millón doscientos cincuenta y seis mil setecientos cincuenta y cuatro euros con treinta y cuatro céntimos).

Motivación de la necesidad del contrato:

La ciberseguridad se ha convertido en un tema de importancia estratégica en nuestra sociedad, y la Comunidad de Madrid, como uno de los centros económicos y tecnológicos más destacados de España y Europa, debe reforzar y aumentar sus capacidades de ciberseguridad para mejorar la protección de todas sus instituciones y sus ciudadanos.

En este contexto, la **Agencia de Ciberseguridad de la Comunidad de Madrid**, creada mediante la Ley 14/2023, de 20 de diciembre, (en adelante, Agencia de Ciberseguridad o simplemente Agencia) se constituye como un organismo instrumental encargado de coordinar, dirigir y supervisar las políticas y estrategias de ciberseguridad en la Administración regional, sus organismos públicos y las entidades locales.

Este marco normativo define la ciberseguridad como un pilar esencial para garantizar la protección de los servicios esenciales, los activos críticos y los derechos de la ciudadanía.

Las funciones de la Agencia deben basarse en la implantación de medidas de prevención, detección y respuesta sobre la infraestructura pública y sus servicios, así como en la coordinación con los proveedores privados de servicios de la sociedad de la información para la consecución de sus objetivos, desarrollando así una política pública de ciberseguridad.

La Agencia tiene como objeto dirigir y coordinar la ciberseguridad y apoyar e impulsar la capacitación en ciberseguridad y el desarrollo digital seguro de la Región de Madrid, con arreglo al marco de competencias constitucional y estatutariamente establecido.

En consideración a lo anterior y para el mejor desempeño de las funciones mencionadas, la Agencia precisa disponer de los servicios externos de soporte a la Oficina de Gobierno, Riesgo y Cumplimiento (Oficina de GRC), organismo de la propia Agencia.

La contratación se sustenta en la necesidad de reforzar la supervisión y auditoría de las políticas y estrategias de ciberseguridad implementadas, abordando objetivos clave como:

- **Cumplimiento normativo integral:** Supervisar el alineamiento con los marcos legales aplicables, como el Esquema Nacional de Seguridad (ENS), la Directiva NIS2, el Reglamento General de Protección de Datos (RGPD), la Ley Orgánica 3/2018 (LOPDGDD) y otras normativas internacionales.
- **Protección de activos críticos y servicios esenciales:** Evaluar la seguridad de los sistemas y redes electrónicas que soportan servicios esenciales, asegurando su confidencialidad, integridad y disponibilidad frente a amenazas emergentes.
- **Mejora continua en los procesos de ciberseguridad:** Identificar áreas críticas de mejora a través de auditorías sistemáticas y recomendaciones accionables, promoviendo la sostenibilidad operativa y resiliencia de los sistemas.

La Oficina de GRC cumple un rol estratégico en la supervisión independiente y autónoma de las políticas y controles de ciberseguridad implementados por las entidades públicas. Este enfoque asegura:

1. **Eficacia y control normativo:** Validar la efectividad de los controles implementados para gestionar riesgos.
2. **Identificación de riesgos compartidos:** Priorizar medidas correctivas en entornos colaborativos y con sistemas interconectados.
3. **Fortalecimiento de la resiliencia regional:** Garantizar el cumplimiento de estándares alrededor de la seguridad de la información, y fomentar la mejora continua.

Ante la necesidad de garantizar la cobertura de las necesidades descritas, y siendo competencia de la Agencia proporcionar la solución que se pretende, atendiendo a la especificidad del servicio que constituye su objeto, y la necesidad de abordar el mismo de manera eficaz y con las garantías requeridas, **procede la tramitación del oportuno expediente de contratación**, mediante procedimiento abierto con pluralidad de criterios.

En Madrid, a fecha de firma

Firmado digitalmente por: ALEJANDRO LAS HERAS VÁZQUEZ
EL CONSEJERO DELEGADO DE LA AGENCIA DE CIBERSEGURIDAD DE LA COMUNIDAD DE
MADRID