

**INFORME SOBRE INSUFICIENCIA DE MEDIOS PARA EL CONTRATO DE SERVICIOS
DENOMINADO “DISEÑO, IMPLEMENTACIÓN Y SUPERVISIÓN DE SERVICIOS DE
CIBERSEGURIDAD DE LA COMUNIDAD DE MADRID (2 LOTES)”, A ADJUDICAR POR
PROCEDIMIENTO ABIERTO CON PLURALIDAD DE CRITERIOS.**

OBJETO DEL CONTRATO

Este contrato tiene por objeto la prestación de servicios de diseño, implementación y supervisión de servicios de ciberseguridad de la Comunidad de Madrid, orientados a la mejora de la seguridad desde el diseño, y a la potenciación de las capacidades de seguridad en materia de prevención, detección, análisis y respuesta a incidentes de seguridad, dividido en dos lotes, Lote 1- Centro de Operaciones de Seguridad SOC-MD, y Lote 2- Soporte especializado en diseño seguro, SDS-MD, cuyas características se especifican en el pliego de prescripciones técnicas particulares.

JUSTIFICACIÓN DE LA INSUFICIENCIA DE MEDIOS

De conformidad con lo dispuesto en el *Artículo 116.4.f) de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP)*, se exponen a continuación los motivos relativos a la insuficiencia, falta de adecuación o no conveniencia de ampliación de los medios disponibles para cubrir las necesidades que se tratan de satisfacer a través del contrato de referencia.

La potenciación y mejora de las capacidades en ciberseguridad de los servicios TIC facilitados por Madrid Digital a la Comunidad de Madrid, objeto de este contrato, requiere de:

- Un alto conocimiento en materia de seguridad de todas las tecnologías e infraestructuras utilizadas por Madrid Digital, ya sean servidores, bases de datos, infraestructura de comunicaciones, infraestructura de seguridad, o software de negocio, para analizar las configuraciones y arquitectura de seguridad implantadas, y proponer mejoras de forma continua considerando la evolución de versiones de todas ellas.
- Una actualización 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 incidentes de seguridad.
- Tecnologías, herramientas y capacidades específicas en materia de prevención, detección temprana, monitorización y análisis de incidentes de seguridad. 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. Además, la instalación del sistema de gestión de eventos e información de seguridad (SIEM) en Madrid Digital, requiere personal experto en la parametrización de casos de uso que permita explotar de forma eficiente los eventos de seguridad recibidos de las distintas fuentes y correlados en el sistema.
- El alto grado de complejidad actual de los servicios TIC, la especialización de los ataques orientados a comprometer su seguridad, y el alto impacto que puede provocar la materialización de un ataque (indisponibilidad del servicio, fuga de información confidencial, pérdida de reputación, etc.) obligan a disponer de personal altamente capacitado y especializado en el análisis de los incidentes de seguridad, y en la evaluación de su impacto en los servicios, y en los protocolos de contención y recuperación de sistemas necesarios.

Además, la implantación de procesos y procedimientos operativos de seguridad comunes, implica el análisis y rediseño de todos los procesos TIC existentes, de forma que la seguridad se gestione de



forma centralizada, permitiendo un reporte y seguimiento efectivo del estado global de la seguridad de los servicios y una gestión de riesgos TIC.

Esta potenciación y mejora de las capacidades en ciberseguridad de Madrid Digital requieren de plataformas tecnológicas y herramientas específicas de fabricantes o empresas del sector especializadas en este tipo de servicios, así como de un conocimiento experto de las distintas soluciones de mercado que mejor se adapten al entorno TIC de Madrid Digital, y personal con amplio conocimiento en los productos comerciales seleccionados, que permitan la implantación, mantenimiento, soporte y evolución futura de las plataformas y herramientas solicitadas en ambos lotes, como son el sistema de monitorización de eventos (SIEM), analizadores de vulnerabilidades, herramientas de descubrimiento de activos o gestores de base de datos de conocimiento demandados en el lote I, o los gestores de configuraciones de seguridad y herramientas de revisión demandadas en el lote II.

Por otro lado, los servicios de ciberseguridad demandados, como los servicios de vigilancia digital, identificación de amenazas, asesoría o asistencia legal del lote I, o los servicios de consultoría de seguridad en la definición y diseño de los proyectos tecnológicos, en la mejora de las arquitecturas de seguridad o en la definición de políticas y controles específicos, del lote II, requieren de una alta capacitación en ciberseguridad, de un alto grado de especialización en los sistemas, y de una experiencia previa en su gestión, que sólo empresas especializadas del sector pueden ofrecer.

Madrid Digital no cuenta con personal en su propia plantilla, adecuado y suficiente para el desarrollo de estos servicios, al requerir capacidades técnicas y humanas especializadas en ciberseguridad. Todo esto lleva a la gestión de esta necesidad a través de la contratación con empresas especializadas en el sector de la seguridad.

Por lo anteriormente expuesto, se hace constar expresamente la insuficiencia de medios humanos y materiales para la prestación del servicio requerido.

La Subdirectora General de Infraestructuras y Operaciones

El Subdirector General de Recursos

Fdo.: Zaida Sampedro Préstamo

Fdo.: Antonio López-Fuensalida Sánchez-Paulete

