

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

NÚMERO 337/ 2024

Unidad Administrativa
Área de Gestión de la Contratación

Exp.: ECON/000237/2023

Resolución de la *Consejera Delegada de la Agencia para la Administración Digital de la Comunidad de Madrid*, por la que se inicia el expediente de contratación denominado: **"SERVICIOS GESTIONADOS DE CIBERSEGURIDAD DE MADRID DIGITAL - 4 LOTES"**

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 el *Artículo 10.8.2 b) de la Ley 7/2005, de 23 de diciembre, de Medidas Fiscales y Administrativas*, y a la vista de la propuesta de contratación efectuada por la *Subdirección General de Ciberseguridad, Protección de Datos y Privacidad*

RESUELVO

Autorizar el inicio y ordenar la tramitación del expediente de contratación del servicio denominado **"SERVICIOS GESTIONADOS DE CIBERSEGURIDAD DE MADRID DIGITAL - 4 LOTES"**, cuyo presupuesto máximo de licitación asciende a 15.643.329,15 €, IVA incluido.

Motivación de la necesidad del contrato:

Uno de los cinco objetivos del Plan Estratégico 2022-26 de Madrid Digital es el desarrollo de las competencias de seguridad de la información y ciberseguridad. Este objetivo se desarrolla 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.

Según va 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 alta sobre todo tipo de ciberdelitos (sobre todo el ransomware, el phishing y las estafas por Internet).

El reto en materia de seguridad de la información y ciberseguridad para la Comunidad de Madrid y Madrid Digital es evidente, 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 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.

Para ello, es necesario acometer, a través del presente expediente, este proyecto transformador, encaminado a 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.

El expediente de contratación está formado por 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).

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

En Madrid, a fecha de firma
LA CONSEJERA- DELEGADA

Firmado digitalmente por: LIRIA FERNANDEZ ELENA
Fecha: 2024 06 25 09:42