INFORME SOBRE INSUFICIENCIA DE MEDIOS DEL CONTRATO DE SERVICIOS DENOMINADO *"SERVICIOS GESTIONADOS DE CIBERSEGURIDAD DE MADRID DIGITAL - 4 LOTES,* A ADJUDICAR MEDIANTE PROCEDIMIENTO ABIERTO MEDIANTE PLURALIDAD DE CRITERIOS.

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.

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*, 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.

Para el desempeño de las competencias que tiene encomendadas la Agencia, se precisa disponer de capacidades en ciberseguridad que acompañen a la organización en los procesos de digitalización y transformación de Madrid Digital y de los servicios ofrecidos por ésta a la Comunidad Madrid. Este contrato de **servicios gestionados de ciberseguridad**, permitirá:

- 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 externos 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 (ciberatacantes) de mayor riesgo en cada momento y de todo tipo, que permita simular estos ataques a fin de identificar vulnerabilidades y amenazas explotables de los servicios e

infraestructuras TIC, 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.

La Agencia para la Administración Digital de la Comunidad de Madrid 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 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