

NÚMERO: 276 / 2025

Unidad Administrativa  
Área de Gestión de la Contratación

Exp. Núm.: ECON/000198/2024

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: **"MANTENIMIENTO, SERVICIOS DE SEGURIDAD AVANZADOS Y ADQUISICIÓN DE SOLUCIONES ANTIMALWARE CYTOMIC EPDR IMPLANTADAS EN 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 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 **"MANTENIMIENTO, SERVICIOS DE SEGURIDAD AVANZADOS Y ADQUISICIÓN DE SOLUCIONES ANTIMALWARE CYTOMIC EPDR IMPLANTADAS EN LA COMUNIDAD DE MADRID"**, cuyo presupuesto máximo de licitación asciende a **4.867.956,77 euros (IVA incluido)**.

#### **Motivación de la necesidad del contrato:**

La 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.

En este sentido, 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) como la propia INTERPOL informó en su último informe global de tendencias de criminalidad de octubre de 2022.

Para el adecuado desempeño de las funciones que tiene atribuidas la Agencia, actualmente se encuentra en ejecución el contrato de servicios denominado **"DISEÑO, MANTENIMIENTO, SOPORTE TÉCNICO Y ADQUISICIÓN DE SOLUCIONES DE SEGURIDAD ANTIMALWARE PANDA, INSTALADAS EN LOS DIFERENTES PUESTOS Y SERVIDORES WINDOWS EXISTENTES EN LOS CENTROS DEPENDIENTES DE LA COMUNIDAD DE MADRID"**, expediente ECON/000045/2020, tramitado mediante negociado sin publicidad a la empresa PANDA SECURITY S.L.U.

Dicha solución EPDR **se encuentra adaptada e integrada en todas las maquetas ofimáticas desplegadas en los puestos de usuario**, ya sean fijos en modalidad sobremesa o móviles en modalidad portátil, Tablet o smartphone, **y en todos los servidores Windows y servidores Linux**, mediante procesos específicos de integración y homologación establecidos al efecto para asegurar la completa compatibilidad del servicio antimalware.

Por otro lado, en la actualidad, se dispone del servicio de **Threat Hunting ("caza de amenazas")**, de búsqueda proactiva de nuevas amenazas avanzadas y ataques, a través del análisis mediante IA (Inteligencia Artificial) de la información generada por los endpoints, facilitado por analistas expertos, que añade la detección de amenazas avanzadas capaces de evadir la seguridad del EPDR. El análisis de métricas y la creación de reglas de comportamiento e indicadores de ataque (IoA) realizado en este

servicio, proporciona una defensa más eficiente y una detección de amenazas en fase temprana.

En la actualidad, el **servicio de protección antimalware Cytomic EPDR** (Endpoint Protection Detection Response) **se encuentra desplegado en 104.676 máquinas**, entre puestos de usuario, servidores Windows y servidores Linux, y **457 licencias** del producto para protección de dispositivos móviles, denominado **Endpoint Protection Plus**.

En el ejercicio de las funciones mencionadas con anterioridad, ante el actual panorama de ciberataques, donde éstos se vuelven cada vez más sofisticados y dirigidos, es imprescindible contar un **servicio integral de detección y respuesta** que combine una **herramienta eficaz** y permanentemente actualizada con **servicios especializados de monitorización** que garanticen un sistema efectivo contra amenazas avanzadas.

Resulta imprescindible proceder a la contratación de un sistema de seguridad para garantizar la seguridad de nuestra organización que **integre, de forma conjunta**, un sistema **EPDR** (Endpoint Protection, Detection and Response), producto que combina la tecnología de protección de Endpoint (**EPP**), con capacidades automatizadas de detección y respuesta (**EDR**), junto con su mantenimiento y un **servicio de soporte técnico avanzado y especializado** compuesto por un equipo altamente cualificado, dedicado para Madrid Digital, responsable de la explotación y mantenimiento de la solución antimalware en toda la planta instalada, teniendo entre sus actividades fundamentales, la monitorización, identificación, aislamiento, desinfección y recuperación de servicios afectados por incidentes de seguridad relacionados con malware.

Por otro lado, en relación con la necesidad de adquirir nuevas licencias de producto para endpoints o servidores que requieran protección antimalware, y dado que **no es factible incorporar soluciones distintas a la desplegada en toda la planta protegida**, se requiere articular una **partida variable para la adquisición de licencias adicionales**, tanto de licencias EPDR, licencias Endpoint Protection Plus como de licencias de la plataforma Cytomic ORION, que se abonará sólo si se materializa la necesidad dentro del periodo de ejecución del contrato.

Con la adquisición de **Cytomic ORION**, se obtendrán capacidades avanzadas de protección, prevención, detección y respuesta, que permitan mejorar la detección temprana de amenazas, la investigación de actividades anómalas, y la respuesta automatizada, aprovechando las capacidades de modelado de comportamiento mediante aprendizaje automático e información de amenazas mediante IA que ofrece la solución.

Por los motivos expuestos, en la actualidad se requiere contar con los servicios de **mantenimiento y actualización de la solución Endpoint Protection, Detection & Response (Cytomic EPDR)** instalada en los puestos, servidores y dispositivos móviles (Endpoint Protección Plus para Móviles-Android e IOS), así como el **soporte técnico avanzado y especializado, y el servicio de "Threat Hunting"** (caza de amenazas). Además, es objeto del contrato la **adquisición de nuevas licencias bajo demanda** de los productos Cytomic EPDR, Endpoint Protección Plus para Móviles (Android e IOS) y Cytomic ORION (Plataforma para detección, búsqueda, investigación y respuesta ante incidentes,) para cubrir las nuevas necesidades que puedan surgir durante la totalidad de la vigencia del contrato.

Ante la necesidad de garantizar la cobertura de las necesidades descritas, y siendo competencia de la Agencia proporcionar los servicios/suministros 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.

Madrid, a fecha de firma  
LA CONSEJERA DELEGADA

Firmado digitalmente por: ELENA LIRIA FERNÁNDEZ - \*\*\*6106\*\*  
Fecha: 2025.07.18 12:37