

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

Memoria Justificativa de la Necesidad

“MANTENIMIENTO, SERVICIOS DE SEGURIDAD AVANZADOS Y ADQUISICIÓN DE LAS SOLUCIONES ANTIMALWARE CYTOMIC EPDR IMPLANTADAS EN LA COMUNIDAD DE MADRID”

MEMORIA JUSTIFICATIVA DE LA NECESIDAD DEL CONTRATO DE SERVICIOS DENOMINADO: “MANTENIMIENTO, SERVICIOS DE SEGURIDAD AVANZADOS Y ADQUISICIÓN DE SOLUCIONES ANTIMALWARE CYTOMIC EPDR IMPLANTADAS EN LA COMUNIDAD DE MADRID”, A ADJUDICAR MEDIANTE PROCEDIMIENTO NEGOCIADO SIN PUBLICIDAD

ANTECEDENTES

De acuerdo con lo establecido en el *Artículo 10 de la Ley 7/2005, de 23 de diciembre, de Medidas Fiscales y Administrativas* (B.O.C.M. núm. 311, de 30 de diciembre de 2005); modificada parcialmente por la *Ley 9/2015, de 28 de diciembre, de Medidas Fiscales y Administrativas* (B.O.C.M. núm. 311, de 31 de diciembre de 2015); por el *Artículo 26 de la Ley 11/2022, de 21 de diciembre, de Medidas Urgentes para el Impulso de la Actividad Económica y la Modernización de la Administración de la Comunidad de Madrid* (B.O.C.M. núm. 304, de 22 de diciembre de 2022); y por el *Artículo 7 de la Ley 8/2024, de 26 de diciembre, de medidas para la mejora de la gestión pública en el ámbito local y autonómico de la Comunidad de Madrid* (BOCM número 308, de 27 de diciembre de 2024), la **Agencia para la Administración Digital de la Comunidad de Madrid** (en adelante la **Agencia**), se configura como ente público de los previstos en el *Artículo 6 de la Ley 9/1990, de 8 de noviembre, Reguladora de la Hacienda de la Comunidad de Madrid*, con personalidad jurídica propia, plena capacidad jurídica y de obrar para el cumplimiento de sus fines y con plena autonomía orgánica y funcional, que tiene por objeto, de acuerdo con las directrices establecidas por la consejería competente en materia de Digitalización, la planificación y ejecución de proyectos y servicios relacionados con tecnologías de la información, comunicaciones electrónicas y ciberseguridad, garantizando la interoperabilidad, escalabilidad, compatibilidad, suministro e intercambio de información, en el ámbito de actuación definido en el apartado dos de este artículo 10.

Entre las **competencias** que, conforme al *Artículo 10 – Tres, de la Ley 7/2005*, se atribuyen a la Agencia, bajo la dirección y coordinación de la Consejería competente en materia de Digitalización, para el cumplimiento de sus objetivos, se recogen, en concreto, las siguientes:

a) *La planificación, desarrollo y ejecución de planes y proyectos de tecnología, de comunicación electrónica y de seguridad de la información de la administración General e Institucional de la Comunidad de Madrid, garantizando la interoperabilidad, escalabilidad, compatibilidad, suministro e intercambio de información.*

d) *La adquisición, el diseño, desarrollo, implantación, mantenimiento, gestión y evolución de la infraestructura tecnológica, sistemas de información y de comunicaciones electrónicas y seguridad de la información de titularidad de la Agencia, así como la ejecución de las actuaciones para su consolidación y racionalización, incluyéndose en particular el puesto de trabajo, las infraestructuras de almacenamiento, los centros de procesos de datos, incluido el uso de nubes públicas y privadas de la Comunidad de Madrid y el archivo electrónico único de los expedientes y documentos electrónicos.*

j) *La elaboración y aprobación de las políticas de seguridad de los sistemas de información y comunicación electrónicas de titularidad de la Agencia y la gestión de los recursos comunes para la prevención, detección y respuesta a los incidentes y amenazas de ciberseguridad en el ámbito de*

sus funciones, sin perjuicio de las competencias de la Agencia de Ciberseguridad de la Comunidad de Madrid.

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**.

JUSTIFICACIÓN DE LA NECESIDAD

El desarrollo de estas competencias de 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, ciber-vigilancia 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.

En virtud de lo expuesto y, 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.

Los cibercriminales utilizan tácticas cada vez más evasivas para eludir las soluciones de seguridad tradicionales, por lo que es necesario también diseñar y poner en marcha **sistemas de seguridad cada vez más complejos y completos**. Este nuevo escenario exige diseñar nuevos modelos de detección y respuesta, que integren en **una solución de seguridad única**, la herramienta, la explotación y el análisis de los datos que proporciona y la protección proactiva.

Comprar una licencia de software es el derecho legal a usar ese software, pero no implica automáticamente la provisión de servicios de monitoreo o supervisión activa por parte del fabricante o de un tercero. Este es un concepto importante a considerar, sobre todo en el ámbito de la ciberseguridad, donde el EPDR (Endpoint, Protection, Detection and Response) es clave para proteger el parque desplegado mediante prevención, protección y respuesta ante cualquier alerta.

Una licencia, del EPDR, es la herramienta, es decir, permite instalar el agente EPDR en los equipos y utilizar las funcionalidades de detección y respuesta que el software ofrece por sí mismo (como la capacidad de registrar eventos, analizar procesos, etc.). Con ella se tiene acceso a la interfaz de la herramienta y a sus capacidades inherentes.

La monitorización es un servicio adicional, para que el EPDR sea verdaderamente efectivo en la protección contra amenazas avanzadas, **se necesita un equipo de analistas de seguridad** que estén constantemente supervisando las alertas que genera el EPDR, investigando comportamientos

sospechosos, realizando caza de amenazas (Threat Hunting) y respondiendo a incidentes. Este servicio de monitorización 24x7x365, es una capa adicional de valor y no viene incluida con la mera adquisición de la licencia.

Sin este servicio de monitorización, la herramienta EPDR, por muy potente que sea, solo generaría datos y alertas que no se tratarían, llegando a producirse posiblemente incidentes que podrían haberse evitado.

Es decir, la licencia proporciona la capacidad, pero el servicio de monitorización ofrece la acción, el análisis y la protección proactiva.

Por lo expuesto, queda justificada la vinculación material y la relación de complementariedad entre las diversas prestaciones objeto del contrato (servicios y suministro), tal y como exige el apartado 2 del art. 34 de la LCSP, a efectos de su contratación en un único expediente; unidad funcional dirigida a la satisfacción de una necesidad concreta, la de contar con una solución de seguridad única y un servicio integral de detección y respuesta.

PROPUESTA DE SOLUCIÓN

Se propone dar continuidad al servicio de **mantenimiento y actualización** de la actual solución de seguridad antimalware **Cytoomic EPDR**, incluyendo el servicio de **Threat Hunting** disponible actualmente, junto con el **soporte técnico avanzado y especializado**.

Además, se requiere incorporar las nuevas capacidades de protección, prevención, detección y respuesta ofrecidas por la plataforma **Cytoomic ORION**, así como la adquisición de licencias adicionales a lo largo del contrato, si la evolución de la planta instalada así lo requiriera. De esta forma se conseguirá dar cumplimiento a los siguientes objetivos:

1. Garantizar la operatividad y disponibilidad actual y futura del servicio de protección.
2. Responder a las peticiones actuales de nuevos equipos a proteger, en un plazo razonable.
3. Ahorrar todos los costes derivados en el supuesto de migración del servicio de protección a un nuevo sistema.

IMPACTO DEL CAMBIO DE LA SOLUCIÓN

La no renovación del mantenimiento de licencias Cytoomic EPDR, así como del soporte técnico experto necesario, tanto en actualización de información de firmas de detección, análisis online, y soporte técnico especializado para la remediación de incidencias supondría:

1. Asumir la pérdida por un tiempo indeterminado hasta la elección de nueva solución, de la protección de seguridad más importante por constituir la última línea de defensa frente a ataques de malware, la del puesto de usuario, dado que la no actualización de muestras y el no contacto con la inteligencia colectiva sobre malware supone una exposición total a nuevos vectores de ataque y variantes de malware.
2. Iniciar un proyecto de homologación de una nueva solución antimalware, que no afecte negativamente a las aplicaciones, sistemas de información y correo corporativo, por el importante grado de interrelación que tienen los sistemas antimalware con los procesos del sistema operativo, dado que interactúan a bajo nivel con la memoria, sistema operativo y librerías de aplicaciones. La implantación de una nueva solución daría lugar a

incompatibilidades, dificultades técnicas de uso, y un impacto desproporcionado en la actividad de mantenimiento de los puestos de trabajo. Cualquier mal funcionamiento del antimalware puede dejar el puesto de trabajo inoperativo.

3. Iniciar un proyecto de integración del producto en las diferentes maquetas ofimáticas homologadas en la Comunidad de Madrid.
4. Elaborar un proyecto de despliegue de la nueva solución en todos los puestos de usuario, dispositivos móviles, así como en todo el parque de servidores gestionado por Madrid Digital, considerando el impacto en el servicio que supondrá el reinicio de todos ellos para la desinstalación de la solución actual e instalación de la nueva.

JUSTIFICACIÓN DEL PROCEDIMIENTO

Para garantizar la ciberseguridad (disponibilidad, integridad, y confidencialidad) de los más de 100.000 puestos de usuarios y aproximadamente 3.500 servidores a proteger de forma continua 24x7x365 días del año, el único proveedor que puede garantizar la ejecución del contrato con la calidad y niveles de servicio requeridos es Panda.

Esta exclusividad se basa en su capacidad única como fabricante y suministrador de las licencias de las Soluciones de Seguridad denominadas, a fecha actual, Cytomic EPDR (Endpoint Protection, Detection and Response), plataforma Orion y su exclusividad para **garantizar actualizaciones continuas 24x7x365**, asegurando que nuestra protección esté siempre al día frente a las últimas amenazas.

Como se ha expuesto, el sistema EPDR (Endpoint Detection and Response) es una herramienta de ciberseguridad altamente **especializada y crítica** para la defensa de nuestra infraestructura. Su mantenimiento no es comparable al de un software genérico o un equipo estándar.

La complejidad y la naturaleza sensible de un EPDR hacen que su soporte y mantenimiento óptimos solo puedan ser garantizados por el propio **fabricante o desarrollador**. Esto es debido a:

- Derechos exclusivos: Nadie puede modificar el software salvo su propietario, que es la empresa **PANDA SECURITY S.L.U.**
- Conocimiento Profundo del Producto: Nadie conoce el producto tan a fondo como la empresa que lo creó y en caso de necesitar alguna modificación solo ellos pueden realizarla. Su equipo de desarrollo e ingeniería tiene una comprensión completa de su arquitectura interna, algoritmos de detección, bases de datos de firmas y comportamiento, y su integración con los sistemas operativos. Esta es una herramienta que evoluciona constantemente para combatir amenazas emergentes.
- Actualizaciones y Parches de Seguridad: El panorama de amenazas cibernéticas cambia a diario. La empresa desarrolladora del EPDR es la única que puede actualizar de manera inmediata cualquier cambio necesario para combatir **nuevas vulnerabilidades, malware y tácticas de ataque**. Por ello, son los únicos que pueden diseñar y distribuir **actualizaciones y parches de seguridad de forma rápida y precisa** para asegurar que el EPDR se mantenga eficaz. **Un tercero no tendría ni la capacidad ni la autorización para generar estas actualizaciones críticas.**
- Soporte Técnico Especializado: Cuando surge un problema técnico o una detección anómala que requiere un análisis profundo, el equipo de soporte del fabricante está compuesto por **expertos especializados** en su propio producto. Tienen las herramientas

de diagnóstico internas y el conocimiento para resolver incidencias complejas que un tercero simplemente no podría abordar con la misma eficiencia o nivel de detalle.

- Acceso a Inteligencia de Amenazas y Desarrollos Futuros: Los fabricantes de EPDR suelen tener acceso a inteligencia de amenazas global y avanzada, que utilizan para mejorar continuamente sus productos. Contratar el mantenimiento directamente con ellos significa que nuestro EPDR se beneficiará de estas mejoras y funcionalidades futuras, asegurando que siempre estemos utilizando la versión más robusta y actualizada en la lucha contra las ciberamenazas.

En resumen, la gestión de un EPDR es una labor de alta especialización y constante actualización. Por ello **el mantenimiento de dicha herramienta no se puede delegar a un tercero que no sea el desarrollador** ya que puede comprometer la **seguridad, la eficacia y la fiabilidad** de una de nuestras herramientas de defensa más importantes. Es una inversión necesaria para garantizar la máxima protección frente a las amenazas cibernéticas en constante evolución.

Por otro lado, es crucial que la adquisición de las licencias de nuestro sistema EPDR se realice a través del mismo proveedor que proporcione el servicio de mantenimiento y soporte de la solución. Esta práctica no solo es una cuestión de conveniencia, sino una necesidad operativa y estratégica. La justificación por la cual es necesario que el proveedor que dé el servicio también sea el que realice el suministro y la necesidad de comprar licencias del mismo tipo a las ya instaladas:

- Garantía de Compatibilidad: El EPDR es un sistema complejo y en constante evolución y que está íntimamente ligado al Sistema Operativo, procesos y programas que se ejecutan en el endpoint, esto hace que adquirir licencias de un tercero podría introducir problemas de compatibilidad, retrasos en la ejecución o incluso la inhabilitación de funcionalidades críticas que lleven a pérdida de servicio. El EPDR desplegado se ajusten perfectamente a nuestros endpoint garantizando que el sistema opere a su máximo potencial sin interrupciones.
- Soporte Técnico Unificado y Eficiente: Cuando surge una incidencia, es vital tener un **punto único de contacto y responsabilidad** ya que la consola de administración del producto no permite distinguir el proveedor de cada licencia desplegada en el parque instalado lo cual nos puede llevar a que, ante una incidencia, podría generar problemas en la identificación de que proveedor debe intervenir en su resolución. Eso sin contar que si fuera otro producto distinto estaríamos gestionando dos consolas distintas

Con ello se garantiza el respaldo integral y especializado necesario para una herramienta tan crítica.

En consecuencia, **PANDA SECURITY S.L.U.** es la única empresa que, por razones de exclusividad técnica, puede prestar el **servicio integral de detección y respuesta requerido**, que se encuentra en posesión de las autorizaciones, conocimientos y medios técnicos que se precisan para acometer los trabajos objeto del contrato de referencia, y **la única que puede prestar la solución completa que se requiere**.

Ante la necesidad de garantizar la cobertura de las necesidades descritas, y siendo competencia de la Agencia proceder a la contratación de los servicios y suministros requeridos, atendiendo a la especificidad de estos, y la necesidad de abordarlos de manera eficaz y con las garantías requeridas, procede la tramitación del oportuno expediente de contratación.

En base a razones técnicas relacionadas con la protección de derechos exclusivos, tan sólo puede encomendarse el objeto del contrato a un único empresario, por lo que esta Dirección propone la tramitación de un **contrato mixto**, mediante **procedimiento negociado sin publicidad**, en virtud

de lo establecido en los Artículos 131.2 y 168 a) 2º de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público (LCSP), siendo la única empresa para invitar en el presente procedimiento:

NOMBRE/RAZÓN SOCIAL	NIF
PANDA SECURITY S.L.U.	B48435218

OBJETO DEL CONTRATO

El objeto del contrato es la prestación de 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.

Todo ello, dentro del ámbito de competencia de la Agencia, de conformidad con lo establecido en el Pliego de Prescripciones técnicas.

Por otro lado, para asegurar la operatividad, seguridad y eficiencia de nuestra infraestructura tecnológica, es indispensable la inclusión de los siguientes Códigos de Vocabulario Común (CPV) en la contratación de servicios:

1. CPV 72267100-0: Mantenimiento de software de tecnología de la información

Este CPV es fundamental porque cubre el **soporte continuo y las actualizaciones necesarias para el EPDR**. La tecnología no es estática; el EPDR requieren mantenimiento periódico para funcionar correctamente, corregir errores, mejorar el rendimiento y, crucialmente, adaptarse a las nuevas amenazas y vulnerabilidades de seguridad.

Sin un mantenimiento adecuado, el software se vuelve obsoleto, vulnerable a ataques, propenso a fallos y menos eficiente. Este CPV garantiza que podemos contratar los servicios que mantendrán el EPDR actualizado.

2. CPV 72611000-6: Servicios de apoyo informático

Este CPV es esencial para asegurar el **funcionamiento diario y la resolución de incidencias** del EPDR. Abarca desde el soporte técnico a usuarios finales (resolución de problemas con hardware, software, red) hasta la administración del EPDR.

La complejidad de los entornos de TI actuales hace que sea inviable operar sin un servicio de apoyo informático especializado. Los **tiempos de respuesta rápidos y la experiencia técnica** que este tipo de servicio proporciona son vitales para minimizar el impacto de cualquier fallo o problema. Este CPV nos permite asegurar que contamos con la asistencia necesaria para mantener la disponibilidad de nuestros sistemas.

3. CPV 48761000-0: Paquetes de software antivirus

La inclusión de este CPV es primordial al estar contratando un servicio de EPDR que incluye el software de antivirus, por ello este CPV nos asegura el acceso a las licencias y la tecnología necesaria para defendernos contra el panorama de amenazas actual.

En conjunto, estos tres CPV son interdependientes y forman un pilar fundamental para una estrategia que prioriza la **seguridad, la fiabilidad y la eficiencia operativa**. Su inclusión nos permitirá contratar los servicios y adquirir las soluciones esenciales para proteger nuestros activos digitales y asegurar la resiliencia de la organización.

División en lotes: No

Justificación de la no división en lotes:

Dadas las características del servicio y los trabajos que constituyen el objeto del contrato, se justifica el no fraccionamiento del mismo en lotes, teniendo en cuenta lo siguiente:

El contrato requiere los servicios y suministros 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).
- Soporte técnico avanzado y especializado de toda la solución con capacidades 24x7x365.
- Servicio de "Threat Hunting" (caza de amenazas).
- 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,).

Todo ello conforma una solución completa e integrada de protección, detección y respuesta ante amenazas y ciberataques, totalmente centralizada a través de una consola en nube que gobierna y supervisa todo el servicio.

La protección continua de los puestos, servidores y móviles (llamados también con carácter general *Endpoints*) contra actividades maliciosas de todo tipo (antimalware, antivirus, ciberamenazas y ciberataques) requiere de una solución tecnológica eficaz, cuyo software además de proteger debe tener capacidades de prevención, detección y respuesta ante ciberamenazas y ciberataques. Todo ello implica que **la solución debe ser capaz de actualizarse de forma continua 24x7x365, a través de Internet contra la base de datos de conocimientos del fabricante, el único capaz de asegurar que la solución actualiza sus capacidades** de protección frente a nuevas amenazas constantemente, permitiendo prevenirlas y bloquearlas en caso de que se produzca un ciberataque.

Según datos del laboratorio Av-Atlas, referencia en la medición y clasificación de malware, durante el año 2024 se detectaron más de 100 millones de muestras de malware nuevo, y las cifras no paran de crecer, estimándose que en la actualidad hay más de 1,2 billones de malware, virus activos, millones de ellos evolucionando constantemente. Sirva esta referencia como evidencia de la dimensión y complejidad de las amenazas a las que se enfrentan los *endpoints* a proteger y de **la necesidad imperiosa de disponer de una solución completa e integrada** de licencias actualizadas constantemente con servicios especializados de gobierno y supervisión (consola centralizada, soporte especializado y servicio *Threat Hunting*).

De todo ello se desprende que el objeto del presente contrato constituye una única unidad funcional que no puede gestionarse por separado, dadas las sinergias y aprovechamiento de recursos que resultan de tener un único proyecto que contemple prestar un servicio integral y completo.

Por lo tanto, en el caso del presente contrato, sí existe un vínculo operativo entre los elementos del objeto, resultando dependientes entre sí e inseparables para el logro de una única finalidad: garantizar la ciberseguridad (disponibilidad, integridad, y confidencialidad) de los más de 100.000 puestos de usuarios y aproximadamente 3.500 servidores a proteger de forma continua 24x7x365 días del año.

A continuación, y para mayor profundidad en el razonamiento de esta exposición, se citan los motivos más relevantes:

1. **La necesidad de coordinar a diferentes contratos conllevaría de un modo sustancial el riesgo de socavar la ejecución adecuada del servicio**, debido a la dificultad de la gestión por separado de la adquisición de la solución software, la de su mantenimiento y de la de soporte, **dada la necesidad de actualización continua 24x7x365 de la solución por el riesgo externo y exponencial de nuevas amenazas**, virus y malware, y **asegurar a la vez de forma controlada, gobernada y supervisada su buen funcionamiento de cada actualización en el endpoint, todo ello gracias al soporte especializado y a los servicios adicionales de Threat Hunting**.
2. Por el mismo motivo se pone en peligro **la garantía de asegurar la ciberseguridad** de todos los Endpoints ante la complejidad de una gestión continua y supervisada 24x7x365 de una solución software y de sus servicios de soporte y Threat Hunting, inherentes e indisolubles, en aras de asegurar **la eficaz y eficiente prestación del servicio**.
3. Adicionalmente, debe ponderarse también el **principio de eficiencia**, que supone obtener un resultado al menor precio posible. El pliego está diseñado para aprovechar todas las sinergias que supone el mantenimiento de la solución, la adquisición de nuevas licencias y los servicios de soporte y *Threat Hunting*, todos ellos necesarios de forma agregada e integrada para garantizar la ciberseguridad de los *endpoints*.

Por lo tanto, las distintas fracciones del objeto del contrato no gozan de sustantividad propia y no son susceptibles de utilización y aprovechamiento por separado, por lo que no es viable la ejecución independiente de cada una de ellas.

En virtud de lo anteriormente expuesto, y a la vista que el objeto del contrato **ha de ser ejecutado por la misma empresa adjudicataria**, no se puede prever la realización independiente de cada una de las partes mediante su división en lotes

PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será de **TREINTA Y SEIS MESES**. A efectos del cálculo del presupuesto y la distribución del importe por anualidades, se ha estimado como fecha de inicio el **1 de noviembre de 2025**.

IMPORTE DEL CONTRATO

El importe máximo del contrato será de **CUATRO MILLONES OCHOCIENTOS SESENTA Y SIETE MIL NOVECIENTOS CINCUENTA Y SEIS EUROS CON SETENTA Y SIETE CÉNTIMOS (4.867.956,77.-€) IVA incluido**, según el siguiente desglose:

CONCEPTO	DESCRIPCIÓN	AÑO 2025	AÑO 2026	AÑO 2027	AÑO 2028	TOTAL
		2 meses	12 meses	12 meses	10 meses	36 meses
CUOTA FIJA	Mantenimiento y actualización de licencias	104.816,91 €	628.901,45 €	628.901,45 €	524.084,54 €	1.886.704,35 €
	Servicios de Seguridad Avanzados	67.082,44 €	402.494,64 €	402.494,64 €	335.412,20 €	1.207.483,92 €
CUOTA VARIABLE	Adquisición de licencias	657.960,00 €	120.680,50 €	78.485,50 €	71.790,50 €	928.916,50 €
TOTAL (sin IVA)		829.859,35 €	1.152.076,59 €	1.109.881,59 €	931.287,24 €	4.023.104,77 €
21% IVA		174.270,46 €	241.936,08 €	233.075,13 €	195.570,33 €	844.852,00 €
TOTAL (IVA incluido)		1.004.129,81 €	1.394.012,67 €	1.342.956,72 €	1.126.857,57 €	4.867.956,77 €

Por lo anteriormente expuesto, esta Subdirección propone el inicio de los trámites oportunos para proceder a la contratación de los servicios referenciados.

La Subdirectora General de Ciberseguridad, Protección de Datos y Privacidad

Firmado digitalmente por: MUÑOZ FUENTES ESTHER
Fecha: 2025.07.18 11:37

Fdo.: Esther Muñoz Fuentes