

Memoria justificativa de la necesidad

**“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”**



La autenticidad de este documento se puede comprobar en www.madrid.org/csv
mediante el siguiente código seguro de verificación: **0981587481916688382764**



MEMORIA JUSTIFICATIVA DE LA NECESIDAD DEL 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” A ADJUDICAR MEDIANTE PROCEDIMIENTO NEGOCIADO SIN PUBLICIDAD

ANTECEDENTES Y JUSTIFICACIÓN DE LA NECESIDAD

La **Agencia para la Administración Digital de la Comunidad de Madrid**, (en adelante la **Agencia**), según se establece en la Ley 7/2005, de 23 de diciembre, de Medidas Fiscales y Administrativas (B.O.C.M. núm. 311, de 31 de diciembre de 2015) tiene asignada, entre otras funciones, la prestación de los servicios informáticos y de comunicaciones a la Comunidad de Madrid (Artículo 10. Tres c).

En concreto, es competencia de esta Agencia la prestación de los siguientes servicios:

1. La administración, mantenimiento y soporte de los equipos físicos y lógicos de tratamiento de la información y de las comunicaciones de cualquier especie que se encuentren instalados en la misma.
2. El desarrollo y adquisición de aplicaciones informáticas y sistemas de información para la Comunidad de Madrid y su mantenimiento y soporte posteriores, de acuerdo con las especificaciones funcionales y necesidades de los distintos centros directivos.
3. La adquisición y dotación de infraestructuras físicas y lógicas de soporte de los sistemas de información.

Asimismo, le corresponde la seguridad, confidencialidad, integridad y disponibilidad de toda la información que se trata desde todas las Consejerías de la Comunidad de Madrid.

En virtud de lo expuesto y en el ejercicio de las precitadas funciones, en la actualidad, se dispone de una solución de seguridad de protección antimalware desplegada en los distintos componentes soporte de los servicios TIC suministrados a la Comunidad de Madrid por la Agencia, como son puestos de usuario o endpoints, servidores Windows y servidores de correo corporativo.

Esta solución de protección, considerada crítica para la organización dado el constante incremento de las amenazas externas relacionadas con malware, facilita capacidades de análisis, detección y bloqueo de malware en los endpoint, ficheros de sistema operativo de servidores Windows y ficheros de servidores de correo corporativo de dos formas, mediante el uso de firmas digitales actualizadas diariamente con las muestras de malware más activas en cada momento, y funcionalidades de análisis on-line de muestras sospechosas no identificadas mediante técnicas de inteligencia colectiva en la nube, así como una monitorización continua de eventos en los endpoint y servidores para detección temprana de infecciones.

La solución homologada que facilita el servicio de protección **se encuentra adaptada e integrada en todas las maquetas ofimáticas desplegadas en los endpoint**, ya sean fijos en modalidad sobremesa o móviles en modalidad portátil, tablet o Smartphone, **y en todos los servidores Windows y servidores de correo Exchange**.

Los procesos de **integración y homologación previa** aseguran la completa compatibilidad del servicio antimalware, tanto en su despliegue mediante el desarrollo de scripts de instalación en cada tipo de componente hardware y sistema de distribución de software utilizado, como en su operación, actualización de motor de búsquedas y ficheros de firma y mantenimiento operativo posterior, asegurando la mínima interferencia en los servicios en Producción y su completa compatibilidad con las aplicaciones, sistemas de información y servicios TIC corporativos administrados y mantenidos por la Agencia.

El servicio facilita una **gestión centralizada** de los procesos de explotación y mantenimiento, mediante consolas de supervisión de toda la planta instalada y medios técnicos expertos dedicados por la Agencia a tal fin, que constituyen un soporte de seguridad de alta cualificación en la identificación,

aislamiento, desinfección y recuperación de servicios afectados por incidentes de seguridad relacionados con malware. Además, permite una gestión delegada del servicio por equipos operativos propios de los distintos centros directivos de la Comunidad de Madrid que así lo demanden, para la atención de primer nivel de incidencias. Este segundo caso es la opción preferida por los centros sanitarios, que combinan los procesos de homologación, integración técnica y soporte técnico experto ofrecidos de forma global por la Agencia con una supervisión, monitorización y atención temprana de eventos de seguridad por equipos informáticos propios.

En la actualidad, el **servicio de protección antimalware se encuentra desplegado en 87.751 componentes hardware**, entre endpoints, servidores Windows y servidores de correo, se basa en la tecnología Panda Endpoint Protection Plus para la totalidad de los centros y en Panda Adaptive Defense para aquellos puestos con requerimientos muy elevados de seguridad.

Debido a la proliferación de ataques a empresas españolas, hospitales y administración española, y que dichos ataques han evolucionado mucho en sus técnicas, es necesario elevar la protección de los puestos y servidores de la CM. Por ello, además de proteger, es preciso disponer de herramientas que permitan detectar las nuevas amenazas en todos los puestos de la Comunidad de Madrid, algo que hace la solución de EDR (Endpoint Detection and Response) de Panda, Adaptive Defense. Esta es una tecnología que monitoriza y responde continuamente para mitigar las amenazas.

Complementario a esta solución, existe un nuevo servicio llamado **Threat Hunting (“caza de amenazas”)**, servicio de búsqueda proactiva de nuevas amenazas avanzadas y ataques, a través del análisis de la información generada por los puestos y servidores que tienen Adaptive Defense. Este servicio permitirá detectar y aislar amenazas avanzadas capaces de evadir las soluciones de seguridad existentes. Todas estas medidas implican una investigación después de que se haya producido una alerta.

La característica más importante de Threat Hunting es su enfoque proactivo frente a las amenazas. Esto quiere decir que no es una respuesta ante incidentes, aunque sí están conectados, ya que a partir de los resultados de la investigación y las conclusiones es posible establecer nuevos indicadores de ataque o de compromiso. **Las medidas de Threat Hunting tratan de suplir lo que las herramientas más tradicionales no pueden ver.**

La empresa **PANDA SECURITY, S.L.** es la única empresa con carácter exclusivo, como fabricante y distribuidora en el territorio de España que puede dar las Soluciones de Seguridad referidas, soluciones que constituyen el objeto del contrato y, en consecuencia, es la única que se encuentra en posesión de los medios técnicos y conocimientos que se precisan para acometer los trabajos objeto del contrato.

Por ello, la única empresa a invitar en el presente procedimiento será:

NIF

B-48435218

Nombre / Razón Social

PANDA SECURITY, S.L.

La empresa Panda ha unificado los productos de antimalware Panda Endpoint Protección Plus y Panda Adaptive Defense y pasan a denominarse **Cytomic EPDR (Endpoint Protection Detection Response)**. El nombre de **Cytomic** se debe a la nueva unidad de negocio dentro de la compañía, Panda, enfocada a grandes empresas.

Por tanto, a fin de dar continuidad al servicio descrito **es necesaria la contratación del mantenimiento y soporte técnico de la solución de seguridad de protección antimalware Panda**, que permita garantizar la correcta protección de todos los activos descritos.

Por otro lado, y con el fin de simplificar los procesos administrativos de adquisición de 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 propone articular una partida variable para la **adquisición de licencias adicionales**, que se abonará sólo si se



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **0981587481916688382764**

materializa la necesidad dentro del periodo de ejecución del contrato, para los siguientes proyectos ya en ejecución:

- Proyecto de Movilización de servicios en el entorno sanitario, con 3.200 tabletas Wifi a proteger.
- Incorporación del Hospital Fundación Alcorcón al servicio de protección antimalware, con 1.500 puestos a proteger.
- Protección de dispositivos móviles con sistema operativo Android y crecimiento de planta instalada, con una estimación de 14.000 dispositivos a proteger.

IMPACTO DEL CAMBIO DE LA SOLUCIÓN

La no renovación del mantenimiento de licencias Panda Endpoint Protection Plus, así como el soporte técnico experto necesario, tanto en actualización de información de firmas de detección, análisis on-line, y soporte técnico on site para la remediación de incidencias supondría:

1. Adquirir otros productos antimalware diferentes, puede dar lugar a incompatibilidades o a dificultades técnicas de uso y mantenimiento desproporcionado de los puestos de trabajo, ya que el proceso de integración técnica con el hardware y software del puesto es muy complejo por la propia naturaleza y funcionamiento de la solución antimalware, ya que requiere interactuar a bajo nivel con la memoria, sistema operativo y librerías de aplicaciones. Cualquier mal funcionamiento deja el puesto de trabajo inoperativo.
2. Asumir la pérdida por un tiempo indeterminado hasta 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.

La empresa Check Point expone, en sus previsiones en materia de ciberseguridad para el 2020, que las amenazas principales estarán en el malware móvil, más ataques de phishing y el ransomware dirigido. Además, según predicción del Centro Criptológico Nacional, para el 2020 se espera un incremento de los ciberataques a la Administración y a empresas de interés estratégico, continuando con la tendencia de extorsión de objetivos mediante ataques de denegación del servicio distribuidos (DDoS) o de Ransomware/Cryptoware.

3. 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 antivirus con los procesos del sistema operativo.
4. Iniciar un proyecto de integración del producto en las diferentes maquetas ofimáticas homologadas en la Comunidad de Madrid.
5. Elaborar un proyecto de despliegue de la nueva solución en todos los endpoint instalados, fijos y específicamente en los móviles, así como en todo el parque de servidores 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.

PROPUESTA DE SOLUCIÓN

Se propone dar continuidad al servicio de mantenimiento y soporte técnico actual de la solución de seguridad antivirus Panda, instalado en puestos y servidores de centros de la Comunidad de Madrid, incorporando a este servicio la posibilidad de adquisición de licencias del producto desplegado.

De esta forma se consigue:

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.

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 los mismos, 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 su tramitación 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).

OBJETO

La prestación de **los servicios de mantenimiento y actualización de licencias, soporte técnico avanzado y especializado**, servicio de "Threat Hunting", "caza de amenazas" de las soluciones de seguridad (**Antimalware Panda**), instaladas en puestos y servidores Windows en centros dependientes de la Comunidad de Madrid, y la adquisición de nuevas licencias del producto durante la vigencia del contrato.

PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será de **TREINTA Y SEIS MESES** comprendidos entre el **1 de septiembre de 2020 y el 31 de agosto de 2023**.

IMPORTE

El importe del contrato no podrá superar el presupuesto máximo de licitación, que asciende a **TRES MILLONES CUATROCIENTOS CINCUENTA Y TRES MIL QUINIENTOS UN EUROS CON TREINTA Y UN CENTIMOS (3.453.501,31 €)**, IVA incluido, según el siguiente desglose de cuantías y anualidades:

	Año 2020	Año 2021	Año 2022	Año 2023	TOTAL
	4 Meses	12 Meses	12 Meses	8 Meses	36 Meses
Mantenimiento de licencias	175.502,00 €	526.506,00 €	526.506,00 €	351.004,00 €	1.579.518,00 €
Servicios	94.070,12 €	282.210,36 €	282.210,36 €	188.140,24 €	846.631,08 €
Adquisición Licencias (Variable)	310.894,23 €	63.370,00 €	49.350,00 €	4.370,00 €	427.984,23 €
TOTAL base imponible	580.466,35 €	872.086,36 €	858.066,36 €	543.514,24 €	2.854.133,31 €
IVA 21%	121.897,93 €	183.138,14 €	180.193,94 €	114.137,99 €	599.368,00 €
TOTAL	702.364,28 €	1.055.224,50 €	1.038.260,30 €	657.652,23 €	3.453.501,31 €

La Directora de Ciberseguridad

Fdo.: Esther Muñoz Fuentes