

NÚMERO: 318 / 2020

 Unidad Administrativa
Área de Gestión de la Contratación

Exp.: ECON/000045/2020

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: **“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”**

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 Dirección de Innovación y Transformación Digital de Servicios (DITDS),

RESUELVO

Autorizar el inicio y ordenar la tramitación del expediente de contratación del **servicio** 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”**, cuyo presupuesto máximo de licitación *asciende a 3.453.501,35. - €, IVA incluido.*

Motivación de la necesidad del contrato:

Es competencia de la Agencia la seguridad, confidencialidad, integridad y disponibilidad de toda la información que se trata desde todas las Consejerías de la Comunidad de Madrid, por ello 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



La autenticidad de este documento se puede comprobar en www.madrid.org/csv mediante el siguiente código seguro de verificación: **096352402627419006508**

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.**

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)**.

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 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.

Ante la necesidad de garantizar la cobertura de los requerimientos descritos, y siendo competencia de la Agencia proporcionar la cobertura que se pretende, atendiendo a la especificidad de los servicios y suministros 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.

Madrid, a fecha de firma
La CONSEJERA-DELEGADA

