Expediente CF050-25-010

Pliego de Prescripciones Técnicas

Renovación de 700 licencias de la Plataforma de Antivirus Corporativa

Es copia auténtica de documento electrónico

Puede verificar la integridad de una copia de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN		
FIRMADO POR	DAVID PELAYO CRUZ	03/04/2025
VERIFICACIÓN	Pk2jmBECBB9EXUGEU5ES87TSUXNLV7	PÁG. 1/6

ÍNDICE

1. INTRODUCCIÓN. 3

2. OBJETO 3

3. JUSTIFICACION DE LA NO DIVISIÓN EN LOTES 3

4. DURACIÓN 3

5. PLAZO DE ENTREGA 3

6. CARACTERÍSTICAS DEL SUMINISTRO 4

7. GARANTÍA 6

8. LUGAR DE ENTREGA DEL SUMINISTRO 6

Es copia auténtica de documento electrónico

Puede verificar la integridad de una copia de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	03/04/2025
VERIFICACIÓN	Pk2jmBECBB9EXUGEU5ES87TSUXNLV7	PÁG. 2/6

1. INTRODUCCIÓN.

VEIASA dispone de una Plataforma Antivirus Corporativa del fabricante Symantec, concretamente Symantec Endpoint Protection, desde la que se gestionan de manera centralizada todos los equipos de la organización. En la actualidad, disponemos de 700 licencias.

2. OBJETO.

Desde la Unidad de Mantenimiento de SSII de VEIASA se precisa la renovación de las 700 licencias Symantec Endpoint Protection actuales y con soporte Essential, a fin de contar con las versiones actualizadas de la solución y parches de seguridad. Para ello es necesario que un ente autorizado gestione el objeto del presente contrato con el fabricante en nombre de VEIASA.

3. JUSTIFICACION DE LA NO DIVISIÓN EN LOTES

El objeto de la presente licitación no es susceptible de la división en lotes debido a que consiste en una única unidad funcional.

4. DURACIÓN

La duración será de 12 meses, a contar desde la fecha de confirmación de la citada renovación, verificada conforme al procedimiento estipulado en el apartado 9 del presente PPT, y que debe ser previa a la caducidad de las licencias actuales, con fecha 24/06/2025.

5. PLAZO DE ENTREGA

El plazo máximo para la renovación y suministro de nuevas licencias será de 15 días hábiles desde la fecha indicada en el pedido, salvo que en la oferta se establezca otro menor, ya que será objeto de valoración la minoración del plazo de entrega, según el apartado 8 del CR.

En el caso de que VEIASA detecte alguna incidencia en las licencias, será responsabilidad del adjudicatario la gestión de la garantía con el fabricante.

Este plazo de entrega se sumará al de duración de las licencias, formando ambos la duración total del contrato.

Es copia auténtica de documento electrónico

Puede verificar la integridad de una copia de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	03/04/2025
VERIFICACIÓN	Pk2jmBECBB9EXUGEU5ES87TSUXNLV7	PÁG. 3/6

6. CARACTERÍSTICAS DEL SUMINISTRO

En la actualidad, se dispone del pedido **76579** que es necesario renovar previo al **24/06/2025**, y que incluye las siguientes líneas:

Line	SKU / Covered Products	Product Description	Qty	User Count
1	R-SW-TIER-3-PRC-CAT-SM/SEP-NEW-AG-500-1K	Renewal Software Maintenance, Tier 3, High Content, Price Category SM/Endpoint Protection, License, ACD-GOV 500-999 Devices	1	550
2	R-SW-TIER-3-PRC-CAT-SM/SEP-NEW-AG-25-50	Renewal Software Maintenance, Tier 3, High Content, Price Category SM/Endpoint Protection, License, ACD-GOV 25-49 Devices	1	30
3	SEP-SUP-AG-100-250/SEP-ADD-AG-100-250	Endpoint Protection, Initial Software Maintenance, ACD-GOV 100-249 Devices 1 YR/Endpoint Protection, Additional Quantity License, ACD-GOV 100-249 Devices	1	120

Cuyo contrato actual dispone de los siguientes datos:

Account Information	
Contract #:	50446501
PO#:	CPA20-55982
End User Name:	JUNTA DE ANDALUCIA

La solución debe proteger múltiples sistemas operativos (Windows, Linux, Mac), incluir mecanismos de despliegue avanzado del agente que se adapten a anchos de banda cambiantes y eliminen automáticamente de forma previa cualquier otra solución antimalware que pueda estar presente en el puesto de trabajo. Los despliegues del agente deberán poder realizarse de forma remota, al menos en las plataformas Windows y Mac.

La herramienta deberá llevar a cabo todas las acciones siguientes de protección y remediación mediante un único agente (que incluya antivirus, antispyware, firewall, IPS, reputación, control de dispositivos y aplicaciones, análisis de comportamiento, comprobación de integridad), que se desplegará sólo una vez. Además, debe tener las siguientes funcionalidades:

- Debe permitir la gestión de la seguridad del puesto de trabajo desde una única plataforma. La solución deberá poder gestionarse desde una única consola que permita la definición de configuraciones de forma simple e intuitiva y que incluya políticas de configuración por defecto para un despliegue inicial más sencillo.

- Incluirá un motor contra Virus, Malware y Spyware. La solución propuesta deberá incluir un motor antivirus y antispyware que permita además de detectar y eliminar

Es copia auténtica de documento electrónico

Puede verificar la integridad de una copia de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	03/04/2025
VERIFICACIÓN	Pk2jmBECBB9EXUGEU5ES87TSUXNLV7	PÁG. 4/6

amenazas conocidas, minimizar al máximo el impacto de escaneos para aumentar el rendimiento, y estar preparado además para ámbitos virtuales (VMWare, Microsoft Hyper-V, Citrix), en los que los análisis deben planificarse adecuadamente.

- Incluirá un cortafuegos de escritorio, que permita el control del tráfico de red entrante y saliente a nivel de puesto, mediante la creación de reglas de configuración desde la consola central.

- Incluirá un motor de prevención de intrusiones, tanto en Windows como en Mac, que analice el tráfico de red entrante y detecte tráfico anómalo, facilitando la detección de código malicioso no conocido.

- Analizar el comportamiento de procesos en tiempo real. La solución propuesta debe examinar los procesos a medida que se ejecutan, para evitar ataques de día cero para los que aún no existen firmas tradicionales.

- Controlar dispositivos y aplicaciones permitiendo definir una lista de dispositivos externos (como discos duros) que puedan usarse dentro de la organización, además de poder restringir el acceso de los usuarios a las aplicaciones previamente aprobadas, todo eso gestionado de forma centralizada.

- Incluir un sistema de reputación que reduzca considerablemente el tiempo e impacto de escaneos, restringiendo estos solo a los ficheros desconocidos y permitiendo llevar a cabo acciones automáticas en aquellos ficheros con una reputación baja o desconocida.

- El sistema de detección/prevención basado en reputación y de creación de firmas incluido, deberá apoyarse en una red de inteligencia con presencia geográfica global, que incorpore información de puestos de trabajo, servidores, usuarios finales, servicios básicos de Internet (correo, navegación...) y tráfico de red.

- Estar optimizado para ámbitos virtuales. La misma plataforma (agente y consola) que protegerá las máquinas físicas debe estar preparada para las virtuales (VMWare, Microsoft Hyper-V, Citrix). En este tipo de ámbitos, la solución debe incluir tecnologías de detección automática de equipos virtuales, sistemas de reputación de ficheros local para un ámbito virtual y definición de equipos base cuyos ficheros se considerarán buenos y, por lo tanto, no serán escaneados.

- Incluir capacidades avanzadas de informes. La solución debe incluir un conjunto amplio de informes predefinidos, además de la capacidad de personalización de estos, y herramientas avanzadas de análisis como dashboards, gráficos y pivot tables para una obtención inmediata de la información deseada.

- La solución deberá estar diseñada para maximizar la efectividad en la protección y remediación, minimizando el número de falsos positivos y el impacto en el rendimiento.

Es copia auténtica de documento electrónico

Puede verificar la integridad de una copia de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	03/04/2025
VERIFICACIÓN	Pk2jmBECBB9EXUGEU5ES87TSUXNLV7	PÁG. 5/6

- Permitir que el agente aplique políticas de protección diferentes en función de la ubicación de red de la máquina protegida o de otros parámetros de configuración del sistema protegido.

- Incluir los servicios de instalación y configuración de la solución propuesta para los servidores y puestos de trabajo.

7. GARANTÍA

La garantía de funcionamiento de la herramienta suministrada debe de mantenerse durante todo el periodo que se establezca con la licencia adquirida, es decir 12 meses. Debiendo de disponer de un servicio de soporte para hacer frente a las nuevas vulnerabilidades que se produzcan durante dicho periodo.
La empresa adjudicataria deberá suministrar los documentos necesarios que justifique dicha garantía.

8. LUGAR DE ENTREGA DEL SUMINISTRO

El material objeto del contrato será prestado por la empresa adjudicataria en la sede de las Oficinas Centrales de VEIASA, sita en Sevilla, en la calle Albert Einstein número 2, C.P. 41902.

David Pelayo Cruz
Jefe de Mantenimiento de Sistemas de Información

Es copia auténtica de documento electrónico

Puede verificar la integridad de una copia de este documento mediante la lectura del código QR adjunto o mediante el acceso a la dirección https://ws050.juntadeandalucia.es/verificarFirma indicando el código de VERIFICACIÓN

FIRMADO POR	DAVID PELAYO CRUZ	03/04/2025
VERIFICACIÓN	Pk2jmBECBB9EXUGEU5ES87TSUXNLV7	PÁG. 6/6