Sistema Integrado de Gestión Administrativa
Módulo de Logística
Versión 25.02.01.U1

Fecha : 12/03/2026
Hora : 10:20
Página : 1 de 1

10.10
14 MAR 2026

PEDIDO DE COMPRA Nº 000054

UNIDAD EJECUTORA : 005 AUTORIDAD AUTONOMA DE MAJES
NRO. IDENTIFICACIÓN : 001137

Tipo Uso : Consumo

Dirección Solicitante : UNIDAD DE LOGISTICA Y SERVICIOS
Entregar a Sr(a) : SALCEDO HUAMANI ROBERT
Fecha : 12/03/2026
Actividad Operativa : C0044 GESTIÓN ADMINISTRATIVA PARA LA ADQUISICIÓN DE BIENES Y SERVICIOS
Motivo : ADQUISICION DE ANTIVIRUS PARA EQUIPOS DE COMPUTO DEL PEMS

FF/Rb	META / MNEMONICO	Función	División Func.	Grupo Func.	Programa	Prod/Pry	Act/Ai/Obr
2-09	0007	10	006	0008	9002	2000270	6000016

Código	Descripción / Especificaciones Técnicas	Clasificador	Cantidad	Unidad Medida
140400030076	SOFTWARE ANTIVIRUS	2.6.6 1.3 2	200.00	UNIDAD

GOBIERNO REGIONAL DE AREQUIPA
PROYECTO ESPECIAL MAJES-SIGUAS
AUTODEMA

Abog. ROBERT SALCEDO HUAMANI
Jefe de la Unidad de Logística y Servicios
Firma del Solicitante

GOBIERNO REGIONAL DE AREQUIPA
PROYECTO ESPECIAL INTEGRAL MAJES-SIGUAS

CPC. Walter Alfredo Hilari Quispe
JEFE DE LA OFICINA DE ADMINISTRACIÓN
Firma Autorizada

Autoridad Autónoma de Majes – Unidad de Logística y Servicios Generales – SERVICIOS INFORMÁTICOS

Autoridad Autónoma de Majes – Jefe Oficina de Administración – V°B°

PEMS - AUTODEMA – V°B° – Gerente Ejecutivo

Autoridad Autónoma de Majes – OPP – V° B° – Área Seguim. y Evaluación

Req. 003

DOC	9355655
EXP	5661244

ESPECIFICACIONES TÉCNICAS
ADQUISICIÓN DE SOFTWARE ANTIVIRUS PARA LA PROTECCIÓN DE EQUIPOS INFORMÁTICOS DEL PROYECTO ESPECIAL MAJES SIGUAS - AUTODEMA

1. **AREA USUARIA:**
PROYECTO ESPECIAL MAJES SIGUAS – AUTORIDAD AUTÓNOMA DE MAJES (PEMS – AUTODEMA) a través de la Unidad de Logística y Servicios – Oficina de Servicios Informáticos.

2. **BASE LEGAL:**
   - Ley N° 32185, Ley de Presupuesto del Sector Publico para el año fiscal 2026.
   - Ley N° 32186, Ley de Equilibrio Financiero del Presupuesto del Sector Publico para el año fiscal 2025.
   - Ley N° 32187, Ley de endeudamiento del sector público para el año fiscal 2026.
   - Ley 32069 Ley Contrataciones del Estado y su Reglamento.
   - Directivas del OSCE
   - Ley N° 27444 – Ley del Procedimiento Administrativo General
   - Código Civil.
   - Ley de Presupuesto del Sector Publico.
   - Directiva N° 002-2023-GRA/OPDI

   Las referencias incluyen los respectivos y modificaciones, de ser el caso.

3. **FINALIDAD PÚBLICA:**
Se requiere la contratación de una persona natural o jurídica con el objetivo de Incorporar un Aplicativo de software Antivirus para la Visualización de Información Relevante de la Propiedad de AUTODEMA en el Ámbito del PEMS I-Etapa.

4. **OBJETIVOS DE LA CONTRATACION**
Adquirir Software de antivirus para la protección de equipos informáticos del Proyecto Especial Majes Siguas - AUTODEMA.

5. **ESPECIFICACIONES TÉCNICAS:**

5.1. Consola de administración:

El servicio principal de administración deberá cumplir con lo siguiente:

- La consola debe ser con infraestructura en la nube, implementado como un servicio SAAS, adicionalmente debe tener la capacidad de implementarse en forma On-premise.
- La consola de administración debe permitir la configuración y administración remota de la solución antivirus instalada en las estaciones de trabajo y servidores (Windows, Linux, Mac). Soporte para dispositivos móviles.
- Debe permitir la delegación de tareas mediante creación de usuarios con distintos perfiles de administración, de tal manera que se puedan agregar usuarios con diferentes niveles de acceso o permisos.
- Por medidas de seguridad la consola de administración debe contar con un doble factor de autenticación para ingresar a la consola, que consiste en una contraseña permanente y una contraseña adicional o token de un solo uso.
- La consola debe tener medidas de protección de acceso frente a ataques de fuerza bruta, como bloquear el acceso luego de varios intentos fallidos de inicio de sesión.
- La consola de acceso al servidor deberá ser 100% web, siendo compatible con los siguientes navegadores: Mozilla Firefox, Microsoft SCCM, Google Chrome, Safari, Opera.
- El servidor se deberá comunicar con los endpoints a través de un agente que sea capaz de almacenar las políticas y ejecutar tareas de manera offline.
- El acceso a la consola a través del interfaz web se bloqueará de forma temporal (aproximadamente 10 minutos), luego de 10 intentos de inicio de sesión no satisfactorios, desde una misma dirección IP.
- El producto debe ser capaz de mostrar los equipos detectados en la red.
- La consola de administración centralizada debe tener la capacidad de mostrar los intentos de infección de virus en los equipos clientes.
- El producto debe ser capaz de controlar a través de políticas todos los componentes mencionados anteriormente (para Workstation y servers) sin necesidad de consolas adicionales para la creación de políticas.
- El producto debe poseer una interfaz web que permita monitorear el estado de los equipos en la red, así como también, mostrar como mínimo reportes sobre: el estado de carga del servidor, clientes con mayor registro de amenazas, principales amenazas, clientes con más amenazas, clientes actualizados /no actualizados y sistemas operativos administrados.
- El producto debe permitir la instalación y desinstalación remota de los servidores y clientes antivirus.
- El producto debe ser capaz de crear tareas de desinstalación del propio antivirus y de antivirus de terceros.
- El producto debe permitir la generación de reportes gráficos y personalización de estos.

Autoridad Autónoma de Majes - V°B° - Jefe Unidad de Logística y Servicios

Autoridad Autónoma de Majes - SERVICIOS INFORMÁTICOS - Unidad de Logística y Servicios Generales

- Los reportes deben ser fácilmente exportables en formatos CSV, PDF.
- El producto debe ser capaz de escanear la red por Directorio Activo, Red IP o Dominios, o una tecnología propia de detección de equipos; en busca de nuevos equipos agregados a la red.
- El producto debe ser capaz de generación de alertas ante un evento específico mediante el envío de un correo.
- Las actualizaciones deben ser descargadas directamente desde los servidores del fabricante y con la opción de usar para que los clientes actualicen desde el servidor de administración sus definiciones de virus, phishing, spam, bases de datos de URLs maliciosas, actualización de parches del producto entre otras.
- Debe permitir gestionar licencias, ya sea como propietario de estas o como administrador de seguridad. Puede llevar un seguimiento de las licencias y los equipos activados con esta, además de observar sucesos relacionados con las licencias como son la caducidad, el uso y las autorizaciones. Esto sin necesidad de consultar la consola de administración.
- La solución debe permitir el manejo flexible de las licencias, de manera que puedan ser reasignadas en caso se restaure el sistema o se cambie de equipo.
- Deberá permitir la ejecución remota de scripts, batch files y paquetes personalizados de terceros a través de la consola.

5.2. Protección para servidores de datos:

- La solución debe ser compatible con los siguientes sistemas operativos: Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows Server 2025 cuales deben tener compatibilidad con la firma de código de Azure.
- El producto antivirus puede instalarse sobre plataformas de x64 bits RedHat Enterprise Linux (RHEL) 8 y 9; Ubuntu Server 22.04 y 24.04 LTS; Debian11 y 12; SUSE Linux Enterprise Server (SLES) 15.
- Compatible con versiones del kernel del sistema operativo Linux 4.14 y posteriores
- La solución es capaz de detectar todo tipo de amenazas, entre los más comunes: virus, gusanos, troyanos, spyware, adware, rootkits, bots, ransomware, etc.
- La solución deberá contar con una funcionalidad antiransomware.
- El producto debe ser capaz de evitar que sus procesos, servicios, archivos o archivos de registro puedan ser detenidos, deshabilitados, eliminados o modificados, para de esta manera garantizar su funcionamiento ante cualquier tipo de ataque de virus.
- El producto para servidores Windows deberá contar con exclusiones automáticas que permitan detectar las aplicaciones críticas del servidor y los archivos críticos del sistema operativo y los agregue automáticamente a la sección de exclusiones al momento de ser instalado.
- El producto debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o carpeta específica.
- El producto debe pedir una contraseña ante intentos de cambio indebidos en la configuración del producto.
- El producto debe contar con un agente que le permita ser administrado desde una consola centralizada.
- El antivirus deberá permitir generar dentro de la misma solución antivirus repositorios de actualización, los cuales deberán ser distribuidas mediante protocolo http localmente, esto sin depender de aplicaciones externas o de la consola de Administración.
- La protección en tiempo real debe iniciarse con el sistema operativo, así como poder definir qué tipos de medios serán analizados por el módulo.
- La solución debe tener sistema de prevención de intrusiones basado en el host, (HIPS).
- El sistema HIPS debe tener los siguientes modos de configuración: automático, inteligente, interactivo, basado en políticas y aprendizaje.
- El producto debe permitir escanear archivos comprimidos.
- Debe permitir elegir las unidades a escanear para los escaneos bajo demanda.
- En sistemas operativos Windows, el antivirus deberá contar con una herramienta integrada que permita inspeccionar completamente componentes del sistema (Controladores, Aplicaciones Instaladas, Conexiones de Red y entradas importantes del Registro de Windows), esto con la finalidad de determinar la causa de comportamientos sospechosos en el sistema que puede deberse a incompatibilidad de software, hardware o código malicioso.
- Debe tener un caché local para aumentar el rendimiento de los entornos virtuales, garantizando que el archivo sólo se explora una vez.
- El fabricante deberá tener soporte técnico en español y laboratorio de análisis de malware en Sudamérica para atender incidencias que afecten la región.
- Que tenga oficinas de la marca en Latinoamérica y presencia local en el país.
- La solución ofrecida debe estar posicionada en el cuadrante mágico de gartner para soluciones EPP en la categoría de lideres o challenger.

Autoridad Autónoma de Majes - V°B° - Jefe Unidad de Logística y Servicios

Autoridad Autónoma de Majes - SERVICIOS INFORMATICOS - Unidad de Logística y Servicios Generales

5.3. Protección para estaciones de trabajo

- La solución deberá ser compatible con los siguientes sistemas operativos: Microsoft® Windows® 11/10(deben tener compatibilidad con la firma de código de Azure). Ubuntu Desktop 20.04 y superior x64, RedHat para Desktop 8, 9 x64 y superior, Linux Mint 20, 21,22 Apple macOS 13 y superior.
- El producto ofertado debe contar con un módulo de detección en tiempo real que proteja contra códigos maliciosos en cada ejecución, uso o creación de archivos en el equipo.
- El producto ofertado debe contar con un sistema de detección de intrusos que realice un análisis del contenido del tráfico de la red y además permita proteger de ataques haciendo que cualquier dañino sea bloqueado.
- Debe contar con un módulo de detección en tiempo real que protega contra virus, gusanos, troyanos, malware, keyloggers,dialers, spyware, adware, hacktools, rootkits, bots, ransomwar y herramientas de control remoto, asi como otros programas potenciamente peligrosos.
- La solución deberá contar con una funcionalidad de protección contra ransomware.
- Debe ser capaz de revisar llaves específicas del registro del sistema operativo e impedir intentos de modificación de escritura y lectura.
- El programa antivirus debe contar con la opción de crear análisis bajo demanda. Estos análisis se podrán configurar para realizarse inmediatamente o a una fecha y hora futura, y también se podrán configurar para realizarse una vez o repetirse a diferentes intervalos, días, semanas, meses, etc.
- El producto ofertado debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o carpeta específica.
- El producto ofertado debe pedir una contraseña ante intentos de cambio indebidos en la configuración del producto.
- El cliente antivirus debe tener un agente que le permita ser administrado desde una consola centralizada. Este agente debe reportar el estado de todas las soluciones antivirus instaladas en la dependencia.
- El producto ofertado deberá permitir generar dentro de la misma solución antivirus repositorios de actualización, los cuales deberán ser distribuidas mediante protocolo http localmente, sin depender de aplicaciones externas o de tareas desde la consola de Administración.
- El producto ofertado debe tener una funcionalidad en donde todas las ventanas emergentes se deshabiliten y la protección del sistema seguirá ejecutándose en segundo plano, pero no requerirá ninguna interacción por parte del usuario.
- El producto ofertado deberá tener una funcionalidad de catalogar a los procesos de los equipos de acuerdo con la reputación basada en la nube. Esta permitirá recopilar información anónima del ordenador afectada con las amenazas detectadas recientemente.
- El producto ofertado debe poseer un firewall que permita filtrar, además que pueda tener la capacidad de bloquear conexiones entrantes y salientes. (Red local e Internet)
- Debe tener la capacidad de realizar un rolback de las firmas de virus en caso no se completa la actualización.
- El producto ofertado debe permitir definir tiempos/horarios de uso para las reglas de control web.
- El producto debe tener la capacidad de establecerse en modo silenciosos, deshabilitando todas las notificaciones del mismo.
- El producto debe tener un control Web para limitar el acceso a sitios web por categoría o bien un sitio web, además de poner mostrar al usuario una notificación de bloqueo
- El producto ofertado deberá analizar protocolos de e-mail POP3, OP3s IMAP, IMAPS, y IMPAP4.
- Debe permitir recopilar información anónima del equipo de computo afectado con las amenazas detectadas recientemente. Esta información en ningún caso podría ser el archivo completo.
- La solución deberá contar con un módulo de protección Anti-Phishing que detecte sitios fraudulentos y bloquee el acceso total, evitando que los usuarios ingresen cualquier tipo de información.
- La solución de antivirus debe ejecutar un escaneo o exploración de cualquiera de lo siguientes estados en la computadora, protector de pantalla o salvapantalla activo, sesión de usuario bloqueado, sesión de usuario finalizado.
- La solución debe ser capaz de definir un listado especifico de usuarios quienes pueden quienes pueden ser uso de los dispositivos. Por dispositivos de almacenamiento, la solución debe permitir configurar los siguientes permisos, Lectura/escritura, bloquear, solo de lectura, advertir.
- Firewall personal, la solución de antivirus debe contar con un firewall personal y debe tener los siguientes modos de configuración: • Modo automático • Modo interactivo • Modo basado en políticas • Modo aprendizaje, cuando se trabaje en entornos virtualizados la solución deberá permitir la creación de una lista blanca de archivos seguros que se comparten dentro de la red virtual.
- El producto ofertado debe ser capaz de escanear a través del protocolo SSL (HTTPS), de manera que se pueda impedir la descarga de archivos infectados.
- El producto ofertado debe de permitir realizar exclusiones de URL para que no sean analizadas por el antivirus tanto en el protocolo HTTP, y HTTPS.

Autoridad Autónoma de Majes - Jefe Unidad de Logística y Servicios - V°B°

Autoridad Autónoma de Majes - Unidad de Logística y Servicios Generales - SERVICIOS INFORMÁTICOS

- La solución deberá contar con un modo transparente de uso, en el cual no muestre ninguna alerta cuando se esté ejecutando una aplicación en pantalla completa.
- La solución deberá contar con módulo de exploración avanzada de memoria que permita detectar las amenazas más sofisticadas que están diseñadas para evadir la detección a través de mecanismos tradicionales.
- La protección de archivos en tiempo real contra malware debe tener las siguientes características; contar con niveles predefinidos de protección e igualmente permitir al usuario personalizar el nivel de protección de acuerdo con sus requerimientos, permitir escanear archivos comprimidos, y definir el nivel de compresión analizar. Permitir exclusiones de unidades, carpetas o archivos, a escanear para la protección en tiempo real, contar con un motor heurístico para detección de posibles nuevo virus.
- Debe contar con un módulo de protección de correo electrónico en tiempo real con las siguientes características, integrarse con clientes de correo electrónico como Microsoft Outlook, Outlook Express, Windows mail y Mozila Thunderbild, escanear a través de los puertos POP3, POP3S, IMAP, IMAPS, SMTP. Tener niveles predefinidos de protección y permitirle al usuario personalizar el nivel de protección de acuerdo con sus requerimientos. Permitir escaneos de correo entrante, saliente o ambos. Contar con la capacidad que después de analizar un mensaje de correo electrónico se pueda adjuntar al mensaje una notificación del análisis. contar con un motor heurístico para detección de posibles nuevo virus. Permitir escanear archivos comprimidos y también definir el nivel de compresión a analizar.
- Debe tener un módulo de protección para la navegación web en tiempo real, con las siguientes características; poder escanear el protocolo http, tener niveles predefinidos de protección e igualmente debe permitir al usuario personalizar el nivel de protección de acuerdo a sus requerimientos. escanear a través del protocolo SSL (HTTPS), de manera que se pueda impedir la descarga de archivos infectados. permitir realizar exclusiones de URL para que no sean analizadas por el antivirus tanto en el protocolo HTTP, y HTTPS. E proteger contra phishing, tener un motor heurístico para detección de posibles nuevo virus
- El producto ofertado debe tener un Módulo de control de dispositivos que permita acceso de solo lectura, lectura/escritura o bloquear dispositivos de acuerdo con una lista predefinida que incluya como mínimo: dispositivos USB, CD-ROM y dispositivos Bluetooth o módems.
- El producto ofertado debe tener un módulo de control de dispositivos que permita crear varios grupos de dispositivos donde se podrán aplicar reglas distintas y además permitirá detectar los dispositivos conectados a la PC y agregarlos al listado de grupo de dispositivos. Además, incluye la funcionalidad de aplicar esta regla por un período de tiempo determinado (hora y días).
- El producto ofertado debe ser capaz de crear CD's, ISO's o USB de rescate, que permitan escanear los equipos Microsoft.
- El producto debe contar con una primera exploración automática después de la instalación del programa, lo que permite asegurar que el equipo se encuentra protegido desde el comienzo.
- El producto debe permitir realizar exploraciones completas mientras el equipo no está en uso, es decir que realice el escaneo cuando el equipo se encuentre bloqueado o suspendido. Esto con la finalidad de obtener un mejor rendimiento y limpieza del sistema.
- El producto ofertado debe contar con una herramienta que permita examinar a fondo el ordenador, y con esta información poder ayudar a determinar la causa de un comportamiento sospechoso en el equipo que pueda deberse a una infección de malware o incompatibilidad de software o hardware. La información para recopilar deberá ser detallada sobre los componentes del sistema (como los controladores, aplicaciones instaladas, conexiones de red o entradas importantes del registro).
- La solución deberá poder realizar exploraciones en estado inactivo para poder brindar de esa forma, una protección proactiva mientras el equipo no está en uso.
- La solución deberá contar con la funcionalidad de bloqueo de exploits, que evite la explotación de vulnerabilidades en las aplicaciones.
- La solución debe contar con un sistema de alerta temprana, que evalué la reputación de los archivos, acelerando las exploraciones del sistema, minimizando la detección de falsos positivos, este sistema deberá estar basando en actualizaciones a través de la nube.
- La solución debe contar con un módulo de exploración avanzada de memoria que permita detectar las amenazas más sofisticadas que están diseñadas para evadir la detección a través de mecanismo tradicionales.
- La solución deberá contar con un módulo de protección contra Botnets, este módulo debe ser capaz de detectar conexiones con servidores maliciosos.

6. PLAZO DE ENTREGA:

Plazo o periodo de entrega, 7 días calendarios a partir del día siguiente de la notificación de la orden de compra.

7. LUGAR DE ENTREGA:

La entrega de los bienes se realizará en el almacén de la AUTORIDAD AUTÓNOMA DE MAJES, sito en la Urbanización La Marina E-8, distrito de Cayma, provincia y departamento de Arequipa; y/o de manera virtual mediante correo electrónico dirigido al área usuaria, previa coordinación con la Entidad.

8. FORMA Y CONDICIONES DE PAGO:

El pago por la prestación de la Adquisición se realizará en una armada, luego de la conformidad del bien, previa recepción de la factura.

El pago se efectuará en soles, después de la entrega de la documentación obligatoria y mediante el abono directo en la cuenta bancaria del sistema financiero nacional, para lo cual deberá comunicar su código de cuenta interbancario (CCI).

9. CONFORMIDAD DE COMPRA

La conformidad de la compra será otorgada por el encargado de Servicios Informáticos y la Unidad de Logística y Servicios.

10. PENALIDADES APLICABLES:

En caso de retraso injustificado del proveedor y/o el contratista en la ejecución de las prestaciones objeto del contrato, la entidad le aplica automáticamente una penalidad por mora por cada día de retraso, según el Artículo 162. Penalidad por mora en la ejecución de la prestación, la penalidad se aplica automáticamente y se calcula de acuerdo a la siguiente formula:

$$\text{Penalidad diaria} = \frac{0.10 \times \text{monto vigente}}{F \times \text{plazo vigente en días}}$$

Donde F tiene los siguientes valores:

a) Para plazos menores o iguales a sesenta (60) días.
Para bienes, servicios en general, consultorías y ejecución
De obra: F 0.40.

b) Para plazo mayores a sesenta (60) días:

b.1) para bienes, servicios en general y consultorías:
F = 0.25

b.2) para obras: F=0.15

162.2. Tanto el monto como el plazo se refiere, según corresponda, al monto vigente del contrato o ítem que debió ejecutarse o en caso que estos involucraran obligaciones de ejecución periódica o entregas parciales, a la prestación individual que fuera materia de retraso.

162.3. En caso no sea posible cuantificar el monto de la prestación materia de retraso. La entidad puede establecer.

11. CONDICIONES MINIMAS DEL PROVEEDOR

El proveedor deberá garantizar los requisitos mínimos, para que de esta manera garantice la ejecución de la compra

- GARANTIA (Solo de ser necesario)
- Contar con RNP – y no estar inhabilitado a contratar con el estado.
- RUC activo y habido, encontrarse dentro del rubro de contratación.
- El postor deberá presentar un documento emitido por el fabricante de la solución ofertada, en el cual acredite que es partner autorizado y/o que se encuentra autorizado para la distribución y/o comercialización del producto ofertado.

Autoridad Autónoma de Majes – Unidad de Logística y Servicios Generales – SERVICIOS INFORMÁTICOS

12. CONFIDENCIALIDAD

El PROVEEDOR deberá guardar confidencialidad y reserva absoluta en el manejo de información a la que tenga acceso y se encuentre relacionada con la prestación, quedando prohibida revelar información a terceros.

13. RESPONSABILIDAD DE VICIOS OCULTOS

La recepción conforme de la entidad no enerva su derecho a reclamar posteriormente por de efectos o vicios ocultos. Las discrepancias referidas a defectos o vicios deben ser sometidas a conciliación y/o arbitraje. En dicho caso el plazo de caducidad se computa a partir de la conformidad otorgada por la entidad hasta treinta (30) días hábiles posteriores al vencimiento del plazo de responsabilidad del contratista previsto en el contrato, según lo dispuesto en el artículo 48° del reglamento de la ley de contrataciones con el estado.

14. AFECTACION PRESUPUESTAL

FUENTE DE FINANCIAMIENTO	: Recursos Ordinarios
META PRESUPUESTAL	: Dirección técnica, supervisión y administración
ACTIVIDAD	: Gestión administrativa para la adquisición de bienes y servicios
ESPECIFICA DE GASTO	: 2.6.6.1.3.2

GOBIERNO REGIONAL DE AREQUIPA
PROYECTO ESPECIAL MAJES-SIGUAS
AUTODEMA

Arequipa, 12 de Marzo del 2026

Abog. ROBERT SALCEDO HUAMANI
Jefe de la Unidad de Logistica y Servicios