FORMATO N° 02

TÉRMINOS DE REFERENCIA PARA LA CONTRATACIÓN DE SERVICIO DE SUSCRIPCIÓN DE LICENCIAS DE ANTIVIRUS PARA LA ACADEMIA DE LA MAGISTRATURA

Unidad de Organización	Subdirección de Informática
Meta Presupuestaria	**01**
Actividad del POI	**C0011 - ACCIONES DE LA SUBDIRECCION DE INFORMATICA**
Denominación de la Contratación	Servicio de Suscripción de Licencias de Antivirus para la Academia de la Magistratura.

1. Finalidad Pública

Contribuir a minimizar el riesgo de pérdida, eliminación y daño de los archivos almacenados en los equipos informáticos de la Academia de la Magistratura permitiendo a los funcionarios y trabajadores, el desarrollo normal de sus actividades operativas y administrativos, al reducir el tiempo de indisponibilidad en el uso de sus archivos y herramientas de trabajo.

2. Objetivo de la Contratación

2.1 Objetivo General

Adquirir e implementar un software de protección para los equipos informáticos de la Academia de la Magistratura, con el fin de garantizar la integridad de la información y los sistemas, previniendo ataques cibernéticos y la infiltración de malware o cualquier variante de software malicioso.

2.2 Objetivo Específico

Implementar una solución de seguridad informática que incluya protección en tiempo real, actualizaciones automáticas y capacidad de detección proactiva de amenazas, asegurando la continuidad operativa y la confidencialidad de los datos almacenados en los equipos de la institución.

3. Alcance y Descripción del Servicio

3.1. Descripción del Servicio:

3.1.1. DESCRIPCION DEL SERVICIO

El Postor deberá proveer la suscripción de 220 licencias de antivirus para las computadoras personales y servidores de la Academia de la Magistratura.

a) Este servicio de suscripción deberá garantizar las actualizaciones de protección, a través de la suscripción de licencias de software antivirus y atender oportunamente los incidentes reportados de virus y software malicioso e intrusión, a través del soporte técnico.

3.1.2. SERVIDOR DE ADMINISTRACION Y CONSOLA ADMINISTRATIVA

a) Compatibilidad
   - Microsoft Windows Server 2008
   - Microsoft Windows Server 2012
   - Microsoft Windows Server 2016
   - Microsoft Windows Server 2019
   - Microsoft Windows 10
   - Microsoft Windows 11

b) Características:
   - Se debe acceder a la consola vía WEB (HTTPS) o MMC;
   - Compatibilidad con Windows Failover Clustering u otra solución de alta disponibilidad

Firmado digitalmente por BOHORQUEZ MURGUIA Pablo Fernando FAU 20290898685 soft
Motivo: Soy el autor del documento
Fecha: 27.02.2026 12:36:53 -05:00

- Capacidad de eliminar remotamente cualquier solución antivirus (propia o de terceros) que esté presente en las estaciones y servidores, sin la necesidad de la contraseña de remoción del actual antivirus;
- Capacidad de instalar remotamente la solución de antivirus en las estaciones y servidores Windows, a través de la administración compartida, login script y/o GPO de Active Directory;
- Capacidad de instalar remotamente la solución de seguridad en smartphones y tablets Symbian, Windows Mobile y Android, utilizando estaciones como intermediadoras;
- Capacidad de gestionar estaciones de trabajo y servidores de archivos (tanto Windows como Linux y Mac) protegidos por la solución antivirus;
- La consola de administración debe permitir administración de vulnerabilidades y parches de seguridad de Windows y otros aplicativos.
- Capacidad de gestionar smartphones y tablets (tanto Windows Mobile, Android y iOS) protegidos por la solución antivirus;
- Capacidad de generar paquetes personalizados (autoejecutables) conteniendo la licencia y configuraciones del producto;
- Capacidad de actualizar los paquetes de instalación con las últimas vacunas, para que cuando el paquete sea utilizado en una instalación ya contenga las últimas vacunas lanzadas;
- Capacidad de hacer distribución remota de cualquier software, o sea, debe ser capaz de remotamente enviar cualquier software por la estructura de gerenciamiento de antivirus para que sea instalado en las máquinas clientes;
- Capacidad de desinstalar remotamente cualquier software instalado en las máquinas clientes;
- Capacidad de aplicar actualizaciones de Windows remotamente en las estaciones y servidores;
- Capacidad de importar la estructura de Active Directory para encontrar máquinas;
- Capacidad de monitorear diferentes subnets de red con el objetivo de encontrar máquinas nuevas para que sean agregadas a la protección;
- Capacidad de monitorear grupos de trabajos ya existentes y cualquier grupo de trabajo que sea creado en la red, a fin de encontrar máquinas nuevas para ser agregadas a la protección;
- Capacidad de, al detectar máquinas nuevas en el Active Directory, subnets o grupos de trabajo, automáticamente importar la máquina a la estructura de protección de la consola y verificar si tiene el antivirus instalado. En caso de no tenerlo, debe instalar el antivirus automáticamente;
- Capacidad de agrupamiento de máquinas por características comunes entre ellas, por ejemplo: agrupar todas las máquinas que no tengan el antivirus instalado, agrupar todas las máquinas que no recibieron actualización en los últimos 2 días, etc.;
- Capacidad de definir políticas de configuraciones diferentes por grupos de estaciones, permitiendo que
- sean creados subgrupos y con función de herencia de políticas entre grupos y subgrupos;

c) Debe proporcionar las siguientes informaciones de las computadoras:
- Si el antivirus está instalado
- Si el antivirus ha iniciado
- Si el antivirus está actualizado
- Minutos/horas desde la última conexión de la máquina con el servidor administrativo
- Minutos/horas desde la última actualización de vacunas
- Fecha y horario de la última verificación ejecutada en la máquina
- Versión del antivirus instalado en la máquina
- Si es necesario reiniciar la computadora para aplicar cambios
- Fecha y horario de cuando la máquina fue encendida
- Cantidad de virus encontrados (contador) en la máquina
- Nombre de la computadora
- Dominio o grupo de trabajo de la computadora
- Fecha y horario de la última actualización de vacunas
- Sistema operativo con Service Pack
- Cantidad de procesadores
- Cantidad de memoria RAM

- Usuario(s) conectados en ese momento, con información de contacto (si están disponibles en el Active Directory)
- Dirección IP
- Aplicativos instalados, inclusive aplicativos de terceros, con historial de instalación, conteniendo fecha y hora que el software fue instalado o removido
- Actualizaciones de Windows Updates instaladas
- Información completa de hardware conteniendo: procesadores, memoria, adaptadores de video, discos de almacenamiento, adaptadores de audio, adaptadores de red, monitores, drives de CD/DVD
- Debe permitir bloquear las configuraciones del antivirus instalado en las estaciones y servidores de manera que el usuario no consiga modificarlas
- Capacidad de reconectar máquinas clientes al servidor administrativo más próximo, basado en reglas de conexión como:
  - Cambio de gateway
  - Cambio de subnet DNS
  - Cambio de dominio
  - Cambio de servidor DHCP
  - Cambio de servidor DNS
  - Cambio de servidor WINS
  - Aparición de nueva subnet
- Capacidad de configurar políticas móviles para que cuando una computadora cliente esté fuera de la estructura de protección pueda actualizarse vía internet
- Capacidad de instalar otros servidores administrativos para balancear la carga y optimizar el tráfico de enlaces entre sitios diferentes
- Capacidad de interrelacionar servidores en estructura de jerarquía para obtener informes sobre toda la estructura de antivirus
- Capacidad de herencia de tareas y políticas en la estructura jerárquica de servidores administrativos
- Capacidad de elegir cualquier computadora cliente como repositorio de vacunas y de paquetes de instalación, sin que sea necesario la instalación de un servidor administrativo completo, donde otras máquinas clientes se actualizarán y recibirán paquetes de instalación, con el fin de optimizar el tráfico de red
- Capacidad de hacer de este repositorio de vacunas un gateway para conexión con el servidor de administración, para que otras máquinas que no logran conectarse directamente al servidor puedan usar este gateway para recibir y enviar informaciones al servidor administrativo
- Capacidad de exportar informes para los siguientes tipos de archivos: PDF, HTML y XML
- Capacidad de generar traps SNMP para monitoreo de eventos;
- Capacidad de enviar correos electrónicos para cuentas específicas en caso de algún evento
- Capacidad de habilitar automáticamente una política en caso de que ocurra una epidemia en la red (basado en cantidad de virus encontrados en determinado intervalo de tiempo)
- Capacidad de realizar actualización incremental de vacunas en las computadoras clientes
- Capacidad de realizar inventario de hardware de todas las máquinas clientes
- Capacidad de realizar inventario de aplicativos de todas las máquinas clientes
- Capacidad de diferenciar máquinas virtuales de máquinas físicas

3.1.3. ESTACIONES Y SERVIDORES WINDOWS

a) Compatibilidad:
- Microsoft Windows vista, Windows 7, Windows 8, Windows 10, Windows 11.
- Microsoft Windows Server 2008
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

b) Características:

- Antivirus de archivos residente (antispyware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado
- Antivirus de web (módulo para verificación de sitios y downloads contra virus)
- Antivirus de correo electrónico (módulo para verificación de correos recibidos y enviados, así como sus adjuntos)
- Firewall con IDS
- Autoprotección (contra ataques a los servicios/procesos del antivirus)
- Control de dispositivos externos
- Control de acceso a sitios por categoría
- Control de ejecución de aplicativos
- Capacidad de elegir de qué módulos se instalarán, tanto en instalación local como en la instalación remota
- Las vacunas deben ser actualizadas por el fabricante y estar disponibles a los usuarios, como máximo cada hora, independientemente del nivel de las amenazas encontradas en el período (alto, medio o bajo)
- Capacidad de automáticamente deshabilitar el Firewall de Windows (en caso de que exista) durante la instalación, para evitar incompatibilidad con el Firewall de la solución
- Capacidad de detección de presencia de antivirus de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación
- Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antivirus, (ejemplo: “Win32.Trojan.banker”) para que cualquier objeto detectado con el resultado elegido sea ignorado
- Capacidad de agregar aplicativos a una lista de “aplicativos confiables”, donde las actividades de red, actividades de disco y acceso al registro de Windows no serán monitoreadas
- Posibilidad de deshabilitar automáticamente barridos agendados cuando la computadora esté funcionando mediante baterías (notebooks)
- Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento
- Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo
- Capacidad de verificar solamente archivos nuevos y modificados
- Capacidad de verificar objetos usando heurística
- Capacidad de agendar una pausa en la verificación
- Capacidad de pausar automáticamente la verificación cuando se inicie un aplicativo
- El antivirus de archivos, al encontrar un objeto potencialmente peligroso, debe:
- Preguntar qué hacer, o
- Bloquear el acceso al objeto
- Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador)
- Caso positivo de desinfección, recuperar el objeto para uso
- Caso negativo de desinfección, mover a cuarentena o borrar (de acuerdo con la configuración preestablecida por el administrador)
- Con anterioridad a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto
- Capacidad de verificar correos electrónicos recibidos y enviados en los protocolos POP3, IMAP, NNTP, SMTP y MAPI, así como conexiones cifradas (SSL) para POP3 y IMAP (SSL)
- Capacidad de verificar enlaces introducidos en correos electrónicos contra pishings
- Capacidad de verificar tráfico SSL en los browsers: Internet Explorer, Firefox y Opera
- Capacidad de verificación del cuerpo del correo electrónico y adjuntos usando heurística
- El antivirus de archivos, al encontrar un objeto potencialmente peligroso, debe:
- Preguntar qué hacer, o;

- Bloquear el correo electrónico
- Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador)
- Caso positivo de desinfección, recuperar el correo electrónico al usuario
- Caso negativo de desinfección, mover a cuarentena o borrar el objeto (de acuerdo con la configuración preestablecida por el administrador)
- En caso de que el correo electrónico contenga código que parece ser, pero no es definitivamente malicioso, este debe mantenerse en cuarentena.
- Posibilidad de verificar solamente correos electrónicos recibidos, o recibidos y enviados.
- Capacidad de filtrar adjuntos de correos electrónicos, borrándolos o renombrándolos de acuerdo con la configuración hecha por el administrador
- Capacidad de verificación de tráfico HTTP y cualquier script de Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas
- Debe tener soporte total al protocolo IPv6
- Capacidad de modificar las puertas monitoreadas por los módulos de web y correo electrónico
- En la verificación de tráfico web, en caso de que se encuentre código malicioso el programa debe:
- - Preguntar qué hacer, o;
- - Bloquear el acceso al objeto y mostrar un mensaje sobre el bloqueo o permitir acceso al objeto
- Posibilidad de agregar sitios de la web en una lista de exclusión, donde no serán verificados por el antivirus de web
- Debe contar con módulo que analice las acciones de cada aplicación en ejecución en la computadora, grabando las acciones ejecutadas y comparándolas con secuencias características de actividades peligrosas. Tales registros de secuencias deben ser actualizados juntamente con las vacunas
- Debe contar con módulo que analice cada macro de VBA ejecutado, buscando señales de actividad maliciosa
- Debe contar con módulo que analice cualquier intento de edición, exclusión o grabación del registro, de forma que sea posible elegir claves específicas para ser monitoreadas y/o bloqueadas
- Capacidad de distinguir diferentes subnets y brindar opción de activar o no el firewall para una subnet específica
- Debe tener módulo IDS (Intrusion Detection System) para protección contra port scans y exploración de vulnerabilidades de software. La base de datos de análisis debe actualizarse conjuntamente con las vacunas
- El módulo de Firewall debe contener, como mínimo, dos conjuntos de reglas:
- Filtrado de paquetes: donde el administrador podrá elegir puertas, protocolos o direcciones de conexión que serán bloqueadas/permitidas
- Filtrado por aplicativo: donde el administrador podrá elegir cuál aplicativo, grupo de aplicativo, fabricante de aplicativo, versión de aplicativo o nombre de aplicativo tendrá acceso a la red, con la posibilidad de elegir qué puertas y protocolos podrán ser utilizados
- Debe tener módulo que habilite o no el funcionamiento de los siguientes dispositivos externos, como mínimo:
    - ✓ Discos de almacenamiento locales
    - ✓ Almacenamiento extraíble
    - ✓ Impresoras
    - ✓ CD/DVD
    - ✓ Drives de disquete
    - ✓ Modems
    - ✓ Dispositivos de cinta
    - ✓ Dispositivos multifuncionales
    - ✓ Lectores de smart card
    - ✓ Dispositivos de sincronización vía ActiveSync (Windows CE, Windows Mobile, etc.)
    - ✓ Wi-Fi
    - ✓ Adaptadores de red externos

- ✓ Dispositivos MP3 o smartphones
- ✓ Dispositivos Bluetooth

- Capacidad de liberar acceso a un dispositivo específico y usuarios específicos por un período de tiempo específico, sin la necesidad de deshabilitar la protección, sin deshabilitar el gerenciamiento central o de intervención local del administrador en la máquina del usuario
- Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por usuario.
- Capacidad de limitar la escritura y lectura en dispositivos de almacenamiento externo por agendamiento
- Capacidad de configurar nuevos dispositivos por Class ID/Hardware ID
- Capacidad de limitar el acceso a sitios de internet por categoría, por contenido (video, audio, etc.), con posibilidad de configuración por usuario o grupos de usuarios y agendamiento
- Capacidad de limitar la ejecución de aplicativos por hash MD5, nombre del archivo, versión del archivo, nombre del aplicativo, versión del aplicativo, fabricante/desarrollador, categoría (ej.: navegadores, gerenciador de download, juegos, aplicación de acceso remoto, etc.)
- Capacidad de bloquear la ejecución de un aplicativo que esté en almacenamiento externo
- Capacidad de limitar el acceso de los aplicativos a recursos del sistema, como claves de registro y carpetas/archivos del sistema, por categoría, fabricante o nivel de confianza del aplicativo.
- Capacidad de, en caso de epidemia, activar una política alternativa donde cualquier configuración pueda ser modificada, desde reglas de firewall hasta control de aplicativos, dispositivos y acceso a web.
- Capacidad de, en caso de que la computadora cliente salga de la red corporativa, activar una política alternativa donde cualquier configuración pueda ser modificada, desde reglas de firewall hasta control de aplicativos, dispositivos y acceso a web.

3.1.4. ESTACIONES Y SERVIDORES LINUX

a) Compatibilidad
- ➢ Plataforma 32-64 bits:
- ➢ Red Hat
- ➢ CentOS
- ➢ SUSE Linux
- ➢ Ubuntu
- ➢ Debian

b) Características:
- Antivirus de archivos residente (antispyware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado;
- Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora.
- Capacidad de configurar el permiso de acceso a las funciones del antivirus con, como mínimo, opciones para las siguientes funciones:
- Gerenciamiento de estatus de tareas (iniciar, pausar, parar o reanudar tareas);
- Gerenciamiento de respaldo: Creación de copias de los objetos infectados en un reservorio de respaldo antes del intento de desinfectar o eliminar tal objeto, siendo de esta manera posible la recuperación de objetos que contengan informaciones importantes;
- Gerenciamiento de cuarentena: Cuarentena de objetos sospechosos y corrompidos, guardando tales archivos en una carpeta de cuarentena;
- Verificación por agendamiento: búsqueda de archivos infectados y sospechosos (incluyendo archivos dentro de un rango especificado); análisis de archivos; desinfección o eliminación de objetos infectados.
- En caso de errores, debe tener capacidad de crear logs automáticamente, sin necesidad de otros softwares;
- Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento;
- Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo;

- Capacidad de verificar objetos usando heurística;
- Posibilidad de elegir la carpeta donde los archivos recuperados de respaldo y los archivos se grabarán posibilidad de elegir la carpeta donde se guardarán los respaldos y archivos en cuarentena

3.1.5. DEL SOPORTE TECNICO

a) El contratista deberá proporcionar un número telefónico y/o correo electrónico y/o portal web de soporte para contactar a su mesa de ayuda y los niveles de escalamiento de incidentes.
b) Toda atención de incidentes se realizará de manera presencial o de forma remota.
c) La Academia de la Magistratura notificará las anomalías que se presenten incluyendo la siguiente información:
   - Fecha y hora
   - Descripción del problema y servicios afectados
   - Persona de contacto de la Academia de la Magistratura.
d) Se consideran los siguientes niveles de atención

Atenciones	**Tiempo de Solución**
Incidentes de nivel critico	2 horas como máximo
Incidentes de nivel moderado	24 horas como máximo

   - El tiempo de solución es el tiempo que transcurre desde el envío por correo electrónico del ticket creado en donde se señala el detalle del incidente reportado, hasta la solución del mismo.
   - Incidente de nivel crítico, se considera cuando el servicio se ve interrumpido.
   - Incidente de nivel moderado, se considera cuando el servicio se encuentra operativo, pero uno de los componentes de hardware o software falla y no interrumpe el servicio.
e) Inmediatamente después de solucionado el incidente, el postor ganador deberá realizar y presentar a la Academia de la Magistratura un informe (por correo electrónico) que contendrá por lo menos la siguiente información:
   - Descripción detallada del problema, su causa y solución encontrada.
   - Personal asignado para la resolución de este.
   - Problemas presentados durante resolución.
   - Documentación adjunta de los cambios hechos.
   - Recomendaciones
   - Fecha y hora de resolución.
f) La mesa de ayuda deberá estar disponible las 24 horas, los 7 días de la semana durante el tiempo de prestación del servicio, vía Telefónica, email o chat.

3.1.6. IMPLEMENTACIÓN

La implementación se realizará en 3 fases:

a) Fase de Despliegue de la Consola:
   - Se deberá instalar la consola de administración en la sede principal de la AMAG, en coordinación con la Subdirección de Informática.
   - El contratista se encargará de la instalación, configuración y pruebas de la instalación o actualización de la solución ofertada en la última versión o release disponible, la Academia de la Magistratura proporcionará el servidor físico o virtual para dicha actividad.
   - El contratista deberá incluir todo el software necesario para su implementación, sin incurrir en costo adicional para la AMAG.
   - El contratista deberá designar una persona como coordinador ante la AMAG, quien a su vez designará un responsable con el fin de agilizar las coordinaciones que fueran necesarias para la implementación de la solución ofertada.
b) Fase de Despliegue de los Clientes:
   - El contratista deberá realizar la instalación o actualización de los agentes y/o clientes en las estaciones de trabajo, dispositivos móviles y servidores, sin afectar la seguridad y en normal desarrollo de trabajo.

- El contratista preparara la configuración de una consola o de paquetes de instalación para los equipos de las sedes remotas que no se encuentren en la sede central.

c) Fase de Transferencia de conocimiento:
   - El contratista deberá brindar la transferencia de conocimiento al personal que designe la Subdirección de Informática.
   - La transferencia de conocimiento técnicos será dictada por un periodo de doce(12) horas, en este periodo se incidirá con mayor énfasis los temas de despliegue, configuración y resolución de incidentes de la solución.
   - El contratista deberá entregar al inicio de la transferencia de conocimiento los manuales y/o instructivos de la solución.
   - Al finalizar la transferencia de conocimiento, el contratista deberá entregar un Informe que contenga los temas tratados y los certificados de cada uno de los asistentes.

d) Plazo de Ejecución de la Implementación:
   El contratista deberá completar la totalidad de las fases de implementación en un plazo máximo de veinte (20) días calendario, los cuales deberán culminar inmediatamente antes del 30 de agosto de 2026. La Subdirección de Informática coordinará con el contratista la fecha exacta de inicio de la implementación, asegurando que esta concluya a tiempo para el inicio del período de suscripción.

4. Requisitos del Proveedor y/o Personal

El Postor deberá de presentar documentación que acredite lo siguiente:

a. Perfil
- ✓ Ser persona jurídica.
- ✓ No tener impedimento para contratar con el Estado, conforme al artículo 11° de la Ley de Contrataciones del Estado.
- ✓ No estar inhabilitado para contratar con el Estado.
- ✓ Contar con RUC en estado activo y condición de habido en la SUNAT.
- ✓ Tener Código de Cuenta Interbancario registrado y vinculado con el RUC.
- ✓ Poseer Registro Nacional de Proveedores (RNP) vigente en el OSCE, de ser el caso.
- ✓ Acreditar la condición de Partner Autorizado o Reseller Certificado por el fabricante del software antivirus propuesto. Se demostrará mediante carta de autorización vigente o certificado emitido por el fabricante, con validez en el territorio peruano.
- ✓ Contar con un área de soporte técnico especializado que garantice asistencia remota y presencial, respaldada por personal con certificaciones técnicas vigentes en la solución ofertada.

b. Experiencia
- ✓ El postor deberá acreditar una experiencia mínima de cinco (05) años en la comercialización, renovación y/o soporte técnico de licencias de software de seguridad (Antivirus/EDR/XDR) en el sector público o privado.

c. Acreditación
- ✓ La experiencia se acreditará mediante la presentación de contratos, órdenes de compra u órdenes de servicio con sus respectivas conformidades, o en su defecto, comprobantes de pago cuya cancelación se acredite documental y fehacientemente.
- ✓ Se requiere un mínimo de cinco (05) servicios similares ejecutados dentro de los últimos cuatro (04) años a la fecha de presentación de la oferta.

Servicios similares: Se consideran servicios similares a la comercialización, renovación de suscripciones, implementación, configuración y/o soporte técnico de soluciones de seguridad informática para puntos finales, tales como: Antivirus, Endpoint Detection and Response (EDR), Extended Detection and Response (XDR).

5. Lugar y Plazo de Ejecución

Lugar: El servicio se realizará en la Sede Central de la AMAG ubicada en Jr. Camaná Nº 669, Cercado de Lima.

Plazo: El plazo de ejecución del servicio es de 365 días calendario, contados a partir del día 30 de agosto de 2026.

6. Resultados Esperados-Entregables

La presentación de entregables se realizará por Mesa de Partes de la Academia de la Magistratura, ubicada en Jr. Camaná N° 669 – Cercado de Lima, en el horario de 09:00 am a 16:45 horas en formato físico o en formato digital https://sgd.amag.edu.pe/mpvAmag/inicio.do

a) El contratista deberá presentar la totalidad de los documentos descritos en un plazo máximo de siete (07) días calendario, contados a partir del día siguiente del inicio del servicio (30 de agosto de 2026) el servicio:

- Un documento que certifique el periodo de vigencia de las licencias y el periodo de soporte técnico.
- Informe con el detalle de las acciones de despliegue y las evidencias de que la totalidad de las estaciones de trabajo, dispositivos móviles y servidores, que se encuentran gestionados por la plataforma implementada.
- Procedimiento de apertura de ticket de soporte y datos de los contactos de soporte técnico.
- Bibliografía y/o documentación necesaria para utilizar los elementos que forman parte de la solución ofertada

7. Conformidad

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025. La conformidad es otorgada por la Subdirección de Informática en el plazo máximo de siete (07) días computados desde el día siguiente de recibido el entregable.

De existir observaciones, la Academia de la Magistratura las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar de siete (07) días a partir del día siguiente de recibida la observación. Si pese al plazo otorgado, EL CONTRATISTA no cumpliese a cabalidad con la subsanación, la Academia de la Magistratura puede otorgar al CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar sin considerar los días en los que pudiera incurrir la Academia de la Magistratura para efectuar las revisiones y notificar las observaciones correspondientes.

Este procedimiento no resulta aplicable cuando los servicios manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso la Academia de la Magistratura no efectúa la recepción o no otorga la conformidad, según corresponda, debiendo considerarse como no ejecutada la prestación, aplicándose la penalidad que corresponda por cada día de atraso.

8. Forma y Condiciones de Pago

El pago se realiza de conformidad con lo establecido en el artículo 67 de la Ley.

La Academia de la Magistratura paga las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días hábiles siguientes de otorgada la conformidad por parte del área usuaria y es prorrogable, previa justificación de la demora, por cinco días hábiles.

La Academia de la Magistratura realiza el pago de la contraprestación pactada a favor del contratista en Soles, en un pago único, luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la Academia de la Magistratura debe contar con la siguiente documentación:

- Documento en el que conste la conformidad de la prestación efectuada suscrita por el servidor responsable de la Subdirección de Informática.
- Comprobante de pago.
- Informe del Servicio realizado por el CONTRATISTA.

En caso de retraso en el pago por parte de la Academia de la Magistratura, salvo que se deba a caso fortuito o fuerza mayor, EL CONTRATISTA tiene derecho al pago de intereses legales conforme a lo establecido en el artículo 67 de la Ley N° 32069, Ley General de Contrataciones Públicas.

9. Confidencialidad

Queda totalmente prohibido que los contratistas brinden declaraciones en medios de comunicaciones en representación de la Academia de la Magistratura.

El contratista queda expresamente obligado a mantener absoluta confidencialidad y reserva sobre la información a la que tenga acceso, no pudiendo difundir, aplicar ni comunicar a terceros esta información, y tampoco no puede copiar o utilizar esta información con fin distinto a su objeto.

10. Penalidades

Penalidad por mora en la ejecución de la prestación:

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la Academia de la Magistratura aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable. La penalidad se aplica automáticamente y se calcula de acuerdo con la siguiente fórmula:

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

Donde F tiene los siguientes valores:

Para bienes y servicios: F = 0.40

Tanto el monto como el plazo se refieren, según corresponda, al monto vigente del contrato, componente o ítem que debió ejecutarse o, en caso de que estos involucren entregables cuantificables en monto y plazo, al monto y plazo del entregable que fuera materia de retraso.

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando EL CONTRATISTA acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso la calificación del retraso como justificado por parte de la Academia de la Magistratura no da lugar al pago de gastos generales ni costos directos de ningún tipo, conforme al numeral 120.4 del artículo 120 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

Las penalidades se deducen de los pagos a cuenta, pagos parciales o del pago final, según corresponda.

11. Otras Penalidades

No aplica

12. Resolución del Contrato

Cualquiera de las partes puede resolver el contrato, de conformidad con el numeral 68.1 del artículo 68 de la Ley N° 32069, Ley General de Contrataciones Públicas.

De encontrarse en alguno de los supuestos de resolución del contrato, LAS PARTES procederán de acuerdo con lo establecido en el artículo 122 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025-EF

13. Cláusula Garantías

EL CONTRATISTA entregará (de corresponder) al perfeccionamiento de la Orden de Compra, Servicio la respectiva garantía incondicional, solidaria, irrevocable, y de realización automática en el país al solo requerimiento, a favor de la Academia de la Magistratura, en concordancia con el artículo 61 de la Ley N° 32069, Ley General de Contrataciones Públicas y artículos 138, 139 y 140 del Reglamento de la Ley Nº32069 Ley General de Contrataciones Públicas, manteniéndose vigente hasta la conformidad de la conformidad de la prestación.

14. Cláusula Gestión de Riesgos

Las partes realizan la gestión de riesgos de acuerdo con lo establecido en el presente documento, a fin de tomar decisiones informadas, aprovechando el impacto de riesgos positivos y disminuyendo la probabilidad de los riesgos negativos y su impacto durante la ejecución contractual, considerando la finalidad pública de la contratación.

15. Cláusula Anticorrupción y Antisoborno

A la suscripción de este contrato, EL CONTRATISTA declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de la Academia de la Magistratura.

Asimismo, EL CONTRATISTA se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente.

Aunado a ello, EL CONTRATISTA se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación y/o cualquier servidor de la Academia de la Magistratura, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

Adicionalmente, EL CONTRATISTA se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con la Academia de la Magistratura.

Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a la Academia de la Magistratura el derecho de resolver total o parcialmente el contrato. Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

16. Cláusula Solución de Controversias

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación.

Cualquiera de las partes tiene el derecho a solicitar una conciliación dentro del plazo de caducidad correspondiente, según lo señalado en el artículo 82 de la Ley N° 32069, Ley General de Contrataciones Públicas, sin perjuicio de recurrir al arbitraje, en caso no se llegue a un acuerdo entre ambas partes o se llegue a un acuerdo parcial. Las controversias sobre nulidad del contrato solo pueden ser sometidas a arbitraje.

17. Modalidad de Pago del Servicio

Suma alzada.

18. Cláusula de Cumplimiento

Son causales de resolución de contrato la presentación de información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley de prevención y mitigación del conflicto de intereses en el acceso y salida de personal del servicio público. Asimismo, en caso se incumpla con los impedimentos señalados en el artículo 5 de dicha ley, se aplicará la inhabilitación por cinco años para contratar o prestar servicios al Estado, Bajo cualquier modalidad.

19. Responsabilidad por vicios ocultos

El proveedor es el responsable por la calidad ofrecida y por los vicios ocultos de los bienes o servicios ofertados por

un plazo no menor de un (01) año, contados a partir de la conformidad otorgada por la Entidad.
FIRMA DIGITAL AMAG ACADEMIA DE LA MAGISTRATURA Firmado digitalmente por SABOGAL ROSAS Jose Luis FAU 20290898685 soft Motivo: Soy el autor del documento Fecha: 27.02.2026 12:50:39 -05:00 _____ Firma del Responsable de la Unidad Orgánica