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 doscientas veinte (220) licencias de antivirus para las computadoras personales y servidores de la Academia de la Magistratura.

El servicio deberá incluir como mínimo:

- Suscripción vigente de licencias durante el periodo contratado.
- Actualizaciones del motor de protección, firmas, componentes y mejoras del producto.
- Consola centralizada de administración en modalidad on-premise o híbrida, con componentes implementados en la infraestructura tecnológica de la Academia de la Magistratura y/o en infraestructura del fabricante, según la arquitectura de la solución ofertada.
- Soporte técnico para atención de incidentes relacionados con la solución.
- Implementación, configuración inicial y puesta en funcionamiento.
- Transferencia de conocimiento al personal designado por la Subdirección de Informática.

3.1.2. CONSOLA ADMINISTRATIVA Y COMPONENTES DE GESTIÓN DE LA SOLUCIÓN

a) Compatibilidad

Los componentes locales de la solución, en caso existan, deberán ser compatibles con la infraestructura tecnológica de la Academia de la Magistratura.

Como mínimo, cuando la solución requiera componentes on-premise, estos deberán ser compatibles con:

- Microsoft Windows Server 2016

- Microsoft Windows Server 2019

La consola de administración deberá ser accesible de manera segura vía web mediante HTTPS o mecanismo equivalente.

b) Características:
- Se debe acceder a la consola vía WEB (HTTPS) o MMC;
- Compatibilidad con Windows Failover Clustering u otra solución de alta disponibilidad
- 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 desplegar, actualizar, reconfigurar y desinstalar remotamente los agentes y componentes de la solución ofertada
- Capacidad de gestionar estaciones de trabajo y servidores de archivos (tanto Windows, 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 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 actualizaciones de seguridad, para que cuando el paquete sea utilizado en una instalación ya contenga las últimas actualizaciones de seguridad 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 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 seguridad
- 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 seguridad

- 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 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 herencia de tareas y políticas en la estructura jerárquica de servidores administrativos
- Capacidad de exportar informes para los siguientes tipos de archivos: PDF, XML y CSV
- 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 seguridad 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

La solución deberá ser compatible, como mínimo, con los siguientes sistemas operativos Microsoft Windows utilizados por la Academia de la Magistratura:

- Microsoft Windows 10
- Microsoft Windows 11
- Microsoft Windows Server 2008
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows Server 2019

La compatibilidad deberá estar soportada oficialmente por el fabricante al momento de la presentación de la oferta y se acreditará mediante datasheet, ficha técnica, carta del fabricante o documento equivalente

b) Características mínimas

La solución de protección para estaciones de trabajo y servidores Windows deberá contar, como mínimo, con las siguientes funcionalidades:

- Protección en tiempo real para archivos, procesos, memoria y actividades del sistema frente a malware, spyware, troyanos, ransomware y otras amenazas similares.
- Capacidad de análisis bajo demanda y análisis programado.
- Capacidad de detección mediante firmas, heurística, comportamiento y/o tecnologías equivalentes, según la solución ofertada.

- Protección de navegación web y descargas, cuando la solución lo contemple.
- Protección de correo electrónico y archivos adjuntos, cuando la solución lo contemple.
- Capacidad de cuarentena, desinfección, eliminación, bloqueo, restauración o tratamiento equivalente de archivos u objetos sospechosos o maliciosos, según las funcionalidades del fabricante.
- Capacidad de autoprotección del agente frente a deshabilitación, alteración o manipulación no autorizada.
- Capacidad de definir exclusiones por archivos, carpetas, extensiones, procesos, aplicaciones o criterios equivalentes.
- Capacidad de actualizar automáticamente firmas, motor de detección y componentes de protección, con periodicidad configurable según las capacidades del fabricante.
- Capacidad de desplegar, habilitar o deshabilitar módulos y componentes de la solución, tanto en instalaciones locales como remotas, cuando la solución lo permita.
- Capacidad de identificar incompatibilidades con soluciones de seguridad preexistentes y alertar o bloquear la instalación cuando corresponda.
- Capacidad de administrar la configuración del agente desde la consola central, evitando modificaciones no autorizadas por parte del usuario final.
- Capacidad de registrar eventos, alertas, incidentes y resultados de análisis para fines de monitoreo y auditoría.
- Capacidad de operar en entornos IPv4 e IPv6, cuando corresponda.
- Capacidad de aplicar políticas diferenciadas según grupos de equipos, usuarios, sedes o perfiles definidos por la Entidad.
- Capacidad de control de dispositivos externos, cuando la solución lo contemple.
- Capacidad de control o filtrado web por categorías, contenidos o políticas, cuando la solución lo contemple.
- Capacidad de control de aplicaciones o ejecución de software, cuando la solución lo contemple.
- Capacidad de protección de red mediante firewall administrable y/o funciones equivalentes de protección de red, cuando la solución lo contemple.
- Capacidad de aplicar políticas alternativas o dinámicas ante eventos de riesgo, cambios de conectividad o salida de la red corporativa, cuando la solución lo contemple.
- Capacidad de operar con impacto razonable sobre el rendimiento del equipo y, cuando la solución lo permita, optimizar o diferir tareas programadas ante alta demanda de recursos o uso de batería.

c) Gestión y monitoreo

La solución deberá permitir, desde la consola central o mediante herramientas del producto, visualizar como mínimo la siguiente información de los equipos protegidos, cuando esta se encuentre disponible en la solución ofertada:

- Estado de instalación del agente.
- Estado de protección y actualización.
- Fecha y hora de la última conexión con la consola.
- Fecha y hora de la última actualización.
- Fecha y hora del último análisis ejecutado.
- Versión del agente o componente instalado.
- Necesidad de reinicio, de corresponder.
- Nombre del equipo.
- Sistema operativo.
- Dirección IP.
- Usuario conectado, cuando la solución lo permita.
- Eventos o detecciones registradas.
- Información básica de hardware y software inventariado, cuando la solución lo contemple.

d) Consideraciones adicionales

Cualquier funcionalidad adicional como control avanzado de dispositivos, control de aplicaciones, firewall, IDS/IPS, filtrado web, protección de correo, inspección de tráfico cifrado o políticas dinámicas será aceptada

siempre que forme parte nativa de la solución o se ofrezca como módulo oficialmente soportado por el fabricante, sin desnaturalizar el objeto principal de la contratación.

3.1.4. ESTACIONES Y SERVIDORES LINUX

a) Compatibilidad

La solución deberá ser compatible con los sistemas operativos Linux que formen parte del inventario tecnológico vigente de la Academia de la Magistratura y que se encuentren soportados por el fabricante al momento de la presentación de la oferta.

Como referencia, la solución deberá permitir protección para entornos Linux de 64 bits y, de ser requerido por la Entidad, también para entornos de 32 bits, siempre que ello forme parte del inventario institucional vigente.

Entre las distribuciones Linux de referencia se consideran, según corresponda a la infraestructura de la Entidad:

- Red Hat Enterprise Linux o compatibles
- CentOS, de corresponder
- SUSE Linux Enterprise Server
- Ubuntu Server
- Debian

La acreditación de compatibilidad podrá realizarse mediante datasheet, ficha técnica, carta del fabricante o documento equivalente.

b) Características mínimas

La solución de protección para estaciones y servidores Linux deberá contar, como mínimo, con las siguientes funcionalidades:

- Protección en tiempo real o residente para archivos, orientada a la detección de malware, spyware, troyanos y otras amenazas similares, respecto de archivos creados, accedidos o modificados, cuando la arquitectura del sistema operativo lo permita.
- Capacidad de actualización automática de firmas, motor de detección y componentes de protección, con periodicidad configurable según las capacidades del fabricante.
- Capacidad de análisis bajo demanda y análisis programado.
- Capacidad de detección mediante firmas, heurística y/o mecanismos de análisis por comportamiento, según la tecnología del fabricante.
- Capacidad de administrar cuarentena para archivos sospechosos, infectados o corruptos.
- Capacidad de generar registros o logs automáticamente ante eventos, detecciones, errores y tareas ejecutadas, sin necesidad de software adicional no contemplado en la solución ofertada.
- Capacidad de administrar tareas de análisis, incluyendo como mínimo iniciar, detener, pausar o reprogramar tareas, cuando la solución lo permita.
- Capacidad de establecer exclusiones por archivos, carpetas, extensiones, procesos o criterios equivalentes.
- Capacidad de gestionar, desde la consola central o mediante herramientas del producto, la configuración y el monitoreo de la protección instalada en los equipos Linux.
- Capacidad de respaldar, aislar, desinfectar, eliminar o restaurar archivos afectados, según las funcionalidades propias de la solución ofertada.
- Capacidad de definir la ubicación o ruta de almacenamiento de archivos en cuarentena, respaldos o elementos recuperables, cuando la solución lo permita.
- Capacidad de operar con un impacto razonable sobre los recursos del sistema y, cuando la solución lo contemple, de optimizar o diferir tareas programadas ante alta demanda de procesamiento.

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:
- El contratista deberá implementar, configurar y poner en funcionamiento la consola de administración de la solución ofertada en modalidad on-premise o híbrida, en coordinación con la Subdirección de Informática.
- Cuando la solución requiera componentes locales, la Academia de la Magistratura proporcionará la infraestructura física o virtual necesaria para su instalación.
- Cuando la solución contemple componentes híbridos, el contratista deberá habilitar, configurar e integrar dichos componentes con la infraestructura tecnológica de la Entidad, sin costo adicional.
- El contratista deberá incluir todo el software, módulos, conectores y componentes necesarios 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 31 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

a) Requisitos

- ✓ No tener impedimento para contratar con el 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.
- ✓ 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 experiencia en la comercialización, renovación y/o soporte técnico de licencias de software de seguridad (Antivirus, EDR y/o XDR), en el sector público y/o privado.

c) Acreditación

- ✓ La experiencia del postor se acreditará mediante la presentación de contratos, órdenes de compra y/u órdenes de servicio con sus respectivas conformidades; o, en su defecto, comprobantes de pago cuya cancelación se acredite documental y fehacientemente.
- ✓ El postor deberá acreditar, como mínimo, cinco (05) contrataciones de servicios similares ejecutadas dentro de los últimos cinco (05) años, contados 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 31 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 (31 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: 23.03.2026 16:58:59 -05:00

Firma del Responsable de la Unidad Orgánica