ANEXO N° 1

ESPECIFICACIONES TÉCNICAS PARA LA CONTRATACIÓN DE BIENES EN GENERAL

N° DE PEDIDO DE COMPRA SIGA: 234

FECHA Chachapoyas 24 de junio de 2025	
Órgano y/o Unidad Orgánica	OFICINA DE ADMINISTRACION
Actividad Operativa	ADMINISTRACION DE LOS RECURSOS MATERIALES, HUMANOS, ECONOCIMOS Y FINANCIEROS DE LA DIRECCION REGIONAL AGRARIA AMAZONAS
Meta Presupuestaria	*12*
CCMM	*188*
Descripción del CCMN	*SOFWARE (INC.LICENCIA) ANTIVIRUS COORPORATIVO*
Denominación de la contratación	*Adquisición de licencias de software antivirus corporativo para la Dirección Regional Agraria y Agencias.*

I. FINALIDAD PÚBLICA

La finalidad es adquirir una herramienta para la protección ante malware, virus y ataques informáticos en la entidad, el cual se ajuste y permita mantener y asegurar la información relevante de la Dirección Regional Agraria Amazonas así mantener la alta disponibilidad de los servicios informáticos a los usuarios internos y externos

II. ANTECEDENTES

La Dirección Regional Agraria Amazonas necesita contar con una solución que garantice la adecuada protección de la información almacenada en los equipos de cómputo y de los sistemas informáticos de la institución, de ser modificada, borrada o afectada por programas no deseados como virus informáticos, troyanos, malware, spyware, ransomware y nuevas variantes de estos. En base a las nuevas amenazas es necesario considerar funcionalidades específicas para mitigar los riesgos con que actúen los softwares de código malicioso-malware. Por lo cual se requiere un software antivirus robusto que brinde la protección requerida. Actualmente la Dirección Regional Agraria cuenta con un software ANTIVIRUS, que incluye licenciamiento activo hasta el 06 de junio de 2025. Por ello, es crucial contar con dicha solución de protección antivirus para los equipos informáticos (End Point) debido al nivel de tráfico de información en la red interna (LAN) y extendida (WAN).

III. OBJETIVO DE LA CONTRATACIÓN

Objetivo General

Adquirir licencias de software antivirus corporativo para la Dirección Regional Agraria Amazonas

Objetivos Específicos:

- *Mitigar el riesgo de incidentes o eventos propiciados por virus informáticos que comprometan la seguridad de información almacenada en los equipos de cómputo de la Dirección Regional Agraria Amazonas.*
- *Realizar una gestión centralizada del software de antivirus para los equipos informáticos.*
- *Detectar rápida y fácilmente riesgos de seguridad o problemas ocasionados por código malicioso*

IV. JUSTIFICACIÓN DE LOS BIENES A CONTRATAR

La presente adquisición busca proteger las constantes amenazas informáticas, como virus, malware, ransomware, y ataques de phishing, es imprescindible contar con herramientas adecuadas para proteger los sistemas informáticos de la organización. La adquisición de licencias de software antivirus responde

a la necesidad de garantizar la seguridad, integridad y confidencialidad de la información institucional. Viene a ser una acción estratégica para resguardar los activos digitales de la organización. Por lo tanto, se considera necesaria y prioritaria la adquisición de estas licencias como parte del plan integral de seguridad de la información.

V. CARACTERÍSTICAS Y CONDICIONES DE LA CONTRATACIÓN

a. Descripción y cantidad de los bienes

Los bienes solicitados son los siguientes:

Ítem	Descripción del bien	Cantidad	Unidad de medida
1	Licencias de antivirus	104	Unidad

b. Características técnicas[1] (obligatorio)

El postor debe ofrecer como mínimo las características técnicas mencionadas o podrá ofrecer características superiores a estas:

SOLUCIÓN DE PROTECCIÓN PARA ESTACIONES DE TRABAJO

- *La solución (en su última versión) deberá ser compatible con los siguientes sistemas operativos: Microsoft® Windows® 11/10/8.1/8/7. Ubuntu Desktop 18.04 y superior x64, RedHat para Desktop 7, 8 x64 y superior, SUSE Linux Enterprise Desktop 15 x64 y superior. Apple macOS 10.12 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 de contenido del tráfico de red y además permita proteger de ataques haciendo que cualquier tráfico dañino sea bloqueado.*
- *El producto ofertado deberá permitir realizar un escaneo del equipo en modo seguro bajo línea de comando donde se podrá especificar las opciones para la limpieza de virus.*
- *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 ofertado debe contar con la funcionalidad de evitar que el malware dañe o deshabilite la protección antivirus, por lo que se puede estar seguro de que el sistema permanece protegido constantemente.*
- *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.*
- *Debe permitir elegir las unidades a escanear para los escaneos bajo demanda.*
- *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.*

GOBIERNO REGIONAL DIRECCIÓN DE INFORMACIÓN ESTADÍSTICA AGRARIA AMAZONAS V°B° OTI

[1] En dicho campo no podrán hacer referencia a marcas, modelos u otros que orienten a un determinado producto o proveedor.

- *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.*
- *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 ofertado debe poseer un firewall bidireccional que posea mínimo 4 modos de filtrado entre ellos, automático, interactivo, aprendizaje y modo basado en políticas, además que pueda tener la capacidad de bloquear conexiones entrantes y salientes.*
- *El producto ofertado debe tener la capacidad de tener un filtro web con un mínimo de 27 categorías entre las cuales se deba permitir o bloquear el acceso a las webs según el administrador lo disponga.*
- *El producto ofertado permitirá crear grupos que contengan varios vínculos URL para crear reglas de permiso y bloqueo a determinados sitios web.*
- *El bloqueo web deberá poder asignarse por un rango de tiempo, por grupo y por equipo.*
- *El producto ofertado debe tener un filtro antispam que permita integrarse con clientes como Microsoft Outlook. Esta funcionalidad debe permitir al usuario crear una lista negra o blanca de direcciones de correo.*
- *El producto ofertado deberá analizar protocolos de e-mail POP3, IMAP, MAPI.*
- *La protección del correo electrónico en el cliente debe permitir definir si se desea escanear sólo correo recibido, correo enviado o correo leído.*
- *El producto ofertado debe tener la capacidad de añadir una nota o etiqueta en los correos electrónicos recibidos o leídos.*
- *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.*
- *El producto ofertado debe tener un módulo de protección en tiempo real para el acceso a la web.*
- *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.*
- *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.*

GOBIERNO REGIONAL DIRECCIÓN DE INFORMACIÓN ESTADÍSTICA AGRARIA V°B° OTI AMAZONAS

- *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 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 solución de antivirus debe ejecutar un escaneo o exploración de cualquiera de los siguientes estados en la computadora (Protector de pantalla o salvapantallas activo, Sesión de usuario bloqueada, Sesión de usuario finalizada)*
- *La solución deberá contar con un módulo de protección contra Botnets, este módulo debe ser capaz de detectar conexiones con servidores maliciosos.*
- *La solución deberá integrar un navegador seguro (Chrome), mostrando el logotipo de la solución presentada para asegurar que el módulo funcione correctamente, dando seguridad para proteger las transacciones bancarias, pagos en línea y sitios web.*
- *La solución presentada incluirá una protección con el teclado, contra registradores de pulsaciones.*
- *Uso de Sandboxing en la nube para analizar el comportamiento de archivos, con SLA de 5 minutos hasta 1 hora de respuesta.*
- *Es posible crear una exclusión por ruta, detección y su hash (SHA-1)*
- *Capacidad de sincronizar su licenciamiento con la nube y la consola de administración en sitio o en la nube.*
- *Detectar un archivo sospechoso ejecutado por primera vez se debe mostrar una advertencia, si el análisis se completa antes de ejecutar el archivo por primera vez, no se muestra el aviso archivo en análisis.*
- *Debe borrar automáticamente las muestras de los archivos/ejecutables en los servidores donde fue analizado el comportamiento.*

GOBIERNO REGIONAL DIRECCIÓN DE INFORMACIÓN ESTADÍSTICA AGRARIA V°B° OTI AMAZONAS

- *Capacidad para enviar correos SPAM para su análisis.*
- *Debe tener únicamente estos umbrales de detección: desconocido, limpio, sospechoso, altamente sospechoso y malicioso.*
- *Debe tener la siguiente información de un archivo enviado al Sanboxing en la nube: nombre del equipo desde donde se ingresó el archivo, el usuario que lo ingresó, la razón, hash en SHA-1, nombre del archivo ingresado, tamaño del archivo, categoría.*
- *Debe tener protección proactiva, es decir, que el archivo/ejecutable sea bloqueado hasta recibir el resultado del Sandbox en la nube.*
- *Se debe tener capacidad para integrarse con la solución de antivirus o protección del punto final, para tener mayores posibilidades de protección y aplicación de políticas.*
- *Enviar un archivo/ejecutable a través de una consola de administración del punto final.*
- *La solución deberá ser capaz de cifrar los Endpoints deseados desde el inicio de sistema.*
- *La solución deberá disponer de diversas posibilidades de recuperación de Passwords para usuarios remotos que se vean bloqueados.*
- *La solución deberá poder programar las tareas de cifrado sobre los Endpoints deseados con la posibilidad de pausar la ejecución para retomar luego desde el último punto.*
- *La solución deberá poder ser administrada desde la misma consola central junto con las otras soluciones descriptas en el TDR.*

CONSOLA DE ADMINISTRACIÓN CENTRALIZADA

- *La consola debe ser con infraestructura en la nube, implementado como un servicio SAAS, no debe ser necesario de un servidor local para su implementación.*
- *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.*

GOBIERNO REGIONAL DIRECCIÓN DE INFORMACIÓN ESTADÍSTICA AGRARIA V°B° OTI AMAZONAS

- *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.*
- *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.*
- *Deberá permitir generar grupos de clientes dinámicos y grupos estáticos.*

OTROS

- *El fabricante deberá tener soporte técnico en español y laboratorio de análisis de malware en Sudamérica para atender incidencias que afecten la región.*
- *El fabricante deberá ocupar una posición de Leader o Challenger en el Cuadrante Mágico de Gartner del último año de publicación.*

GOBIERNO REGIONAL DIRECCIÓN DE INFORMACIÓN ESTADÍSTICA AGRARIA OTI AMAZONAS

a. Garantía comercial

- ***Alcance de la garantía:*** *El contratista deberá garantizar la operatividad y funcionamiento del software al 100%. Incluye las nuevas versiones que publique el fabricante y todas las actualizaciones durante el periodo de suscripción de la licencia, sin que esto implique un costo adicional.*
- ***Período de garantía:*** *La garantía será por doce (12) meses y/o durante dure el periodo de suscripción de la licencia.*
- ***Inicio del cómputo del período de garantía****: La garantía rige a partir del día siguiente de emitida la conformidad de implementación del bien.*

VI. CRONOGRAMA DE ENTREGA: (De corresponder)

NO CORRESPONDE

VII. REQUISITOS Y RECURSOS DEL/DE LA PROVEEDOR/A (Obligatorio)

6.1. Requisitos del/de la proveedor/a

6.1.1 Registro Nacional de Proveedores vigente (Obligatorio)
6.1.2. No contar con impedimento para contratar con el estado, según artículo 30 de la Ley General de Contrataciones Públicas. (Obligatorio)

6.2. Experiencia del postor

El postor debe acreditar un monto facturado acumulado equivalente a S/ 5,400.00 (Cinco mil cuatrocientos con 00/100 Soles), por la venta de bienes iguales o similares al objeto de la convocatoria, durante los diez años anteriores a la fecha de la presentación de ofertas, que se computarán desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran bienes similares a los siguientes ADQUISICION ANTIVIRUS

Acreditación: La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compra, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con constancia de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago , o comprobante de retención electrónico emitido por SUNAT por la retención del IGV, correspondientes a un máximo de veinte contrataciones. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados, para acreditarla debe presentar de forma obligatoria lo indicado en el numeral (ii) del presente párrafo; no es posible que acredite su experiencia únicamente con la presentación de contratos u órdenes de compra con conformidad o constancia de prestación.

VIII. LUGAR Y PLAZO DE LA PRESTACIÓN (obligatorio)

8.1 Lugar de entrega: *Se realizará de manera remota, proporcionando el detalle de las licencias al correo admin@draamazonas.gob.pe (Oficina de Tecnologías de la Información) con copia al correo de la Unidad de Almacén almacen@draamazonas.gob.pe, para conocimiento.*

8.2 Plazo: *El periodo de la entrega del bien es de cuatro (04) días calendarios, contabilizados a partir del día siguiente de la notificación de la orden de comprar.*

8.3 El/La proveedor/a deberá presentar su factura, guía de remisión y otros documentos solicitados para el pago mediante la Mesa Partes Presencial del GOREA, en caso de que dichos documentos sean electrónicos también podrán ser presentados por la Mesa de Partes Virtual de Entidad.

GOBIERNO REGIONAL AMAZONAS DIRECCIÓN REGIONAL AGRARIA DIRECCIÓN DE INFORMACIÓN ESTADÍSTICA V°B° OTI

IX. CONFORMIDAD DEL BIEN (obligatorio)

9.1 Área usuaria que emite la conformidad:

La conformidad de la adquisición será otorgada por el responsable de la Oficina de Tecnologías de la Información de la Dirección Regional Agraria Amazonas

9.2 Área técnica que emite la conformidad: (De corresponder)

La recepción y conformidad de la prestación se regula por lo dispuesto en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas. La recepción será otorgada por la UNIDAD DE ALMACÉN y la conformidad será otorgada por la OFICINA DE

TECNOLOGIAS DE LA INFORMACIÓN en el plazo máximo de siete (07) días computados desde el día siguiente de producida la recepción.

De existir observaciones, LA ENTIDAD las comunica al PROVEEDOR, indicando claramente el sentido de estas, otorgándole un plazo para subsanar el cual no debe ser mayor al 30% del plazo del entregable[2]correspondiente, dependiendo de la complejidad o sofisticación de las subsanaciones a realizar. Si pese al plazo otorgado, EL PROVEEDOR no cumpliese a cabalidad con la subsanación, LA ENTIDAD puede otorgar al PROVEEDOR 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 Entidad para efectuar las revisiones y notificar las observaciones correspondientes.

Este procedimiento no resulta aplicable cuando los bienes manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso LA ENTIDAD 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.

X. FORMA DE PAGO (obligatorio)

El pago se realizará en su totalidad, luego de la recepción formal e instalación y pruebas de funcionamiento según lo detallado en las presentes especificaciones técnicas.

La documentación obligatoria a presentar por el/la proveedor/a para la realización del pago, es su comprobante y guía de remisión.

XI. CONSIDERACIONES PARA LA EJECUCIÓN CONTRACTUAL (obligatorio)

10.1. Confidencialidad (obligatorio)

El/La PROVEEDOR no deberá divulgar, revelar, entregar o poner a disposición de terceros, dentro o fuera de la entidad, salvo autorización expresa de la misma, la información proporcionada por esta, para la prestación del servicio y en general toda la información a la que tenga acceso o la que pudiera producir con ocasión del servicio que presta, durante y después de concluida la vigencia del presente documento. Dicha información puede consistir en fotografías, informes, material video gráfico, documentos y otros similares.

10.2. Garantías

El cumplimiento de las obligaciones de los PROVEEDOR debe ser garantizado a través de los mecanismos establecidos en la presente ley, a fin de cubrir el adelanto de pago, y el fiel cumplimiento del contrato, así como el fiel cumplimiento de las prestaciones accesorias.
Los mecanismos de garantía son los siguientes:

- El fideicomiso, constituido tanto para el adelanto de pago como para el fiel cumplimiento del contrato.
- La carta fianza financiera, otorgada como garantía de adelanto de pago, de fiel cumplimiento del contrato y de fiel cumplimiento de las prestaciones accesorias.
- El contrato de seguro, otorgado como garantía de adelanto de pago, de fiel cumplimiento del contrato y de fiel cumplimiento de las prestaciones accesorias.
- La retención de pago, otorgado como garantía de fiel cumplimiento del contrato y de fiel cumplimiento de las prestaciones accesorias.

10.3. Cláusula anticorrupción y antisoborno.

A la suscripción del contrato, EL PROVEEDOR declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera

GOBIERNO REGIONAL DIRECCIÓN DE INFORMACIÓN ESTADÍSTICA AGRARIA V°B° OTI AMAZONAS

[2] En caso de que el plazo obtenido como resultado de la aplicación del porcentaje sea una cifra decimal, corresponde que la entidad contratante efectúe el redondeo a favor del contratista, computándose como un día completo adicional en dicho supuesto.

directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de la entidad.

Asimismo, EL PROVEEDOR 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 PROVEEDOR 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 entidad, 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 PROVEEDOR 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 ENTIDAD.

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 ENTIDAD el derecho de resolver total o parcialmente el contrato. En ningún caso, dicha medida impide el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

10.4. Solución de controversias

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

Todas las controversias que surjan entre las partes sobre la validez, nulidad, interpretación, ejecución, terminación o eficacia de los contratos menores se resuelven mediante conciliación (articulo. 330.1 Decreto Supremo N° 009-2025-EF).

10.5. Resolución de contrato por incumplimiento

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 proceden de acuerdo con lo establecido en el artículo 122 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF. Por ende, cualquiera de las partes puede resolver, total o parcialmente, el contrato en los siguientes supuestos:

- Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.
- Incumplimiento de obligaciones contractuales, por causa atribuible a la parte que incumple.
- Hecho sobreviniente al perfeccionamiento del contrato, de supuesto distinto al caso fortuito o fuerza mayor, no imputable a ninguna de las partes, que imposibilite la continuación del contrato.
- Por incumplimiento de la cláusula anticorrupción.
- Por la presentación de documentación falsa o inexacta durante la ejecución contractual. Configuración de la condición de terminación anticipada establecida en el contrato, de acuerdo con los supuestos que se establezcan en el reglamento para su aplicación.

10.6. Gestión de riesgos

Durante la vigencia del presente contrato, ambas partes —la Entidad Contratante y el Proveedor—

acuerdan aplicar un enfoque de gestión de riesgos en todas las etapas del proceso de adquisición de bienes. Esta gestión tiene por finalidad identificar de manera oportuna los factores que puedan afectar el cumplimiento eficiente del contrato y, a su vez, generar acciones preventivas y correctivas que aseguren el logro de los objetivos contractuales y la adecuada utilización de los recursos públicos.

En virtud de ello, dentro de los primeros quince días calendario contados desde la suscripción del contrato, ambas partes llevarán a cabo un proceso conjunto de identificación y análisis de los principales riesgos asociados a la adquisición, transporte, entrega y recepción de los bienes. Como resultado de este ejercicio, se elaborará un registro que incluirá los riesgos identificados, su nivel de criticidad y posibles consecuencias.

Con base en dicho registro, el Proveedor presentará un plan de gestión de riesgos que contenga las medidas propuestas para prevenir, mitigar o enfrentar cada uno de los riesgos señalados. Este plan deberá ser revisado y validado por la Entidad Contratante en un plazo no mayor de diez días hábiles. Las medidas allí contenidas serán de aplicación obligatoria y formarán parte integral de la ejecución contractual.

Durante el desarrollo del contrato, el plan de gestión de riesgos será objeto de seguimiento y revisión periódica. La frecuencia de dicha revisión será, como mínimo, trimestral o, en su defecto, cada vez que se produzca un evento que altere significativamente el entorno o condiciones del contrato. Cualquier nuevo riesgo identificado deberá ser reportado de inmediato por el Proveedor, proponiéndose las medidas pertinentes para su tratamiento.

Finalmente, el incumplimiento injustificado de las medidas previstas en el plan de gestión de riesgos por parte del Proveedor será considerado una infracción a las obligaciones contractuales, y podrá dar lugar a la aplicación de las penalidades correspondientes o, de ser el caso, a la resolución del contrato, sin perjuicio de otras acciones legales que resulten aplicables.

10.7. Cláusula de cumplimiento (obligatorio)

Son causales de resolución de contrato la presentación con información inexacta o falsa de la Declaración Jurada de Prohibiciones e Incompatibilidades a que se hace referencia en la Ley N° 31564, 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.

10.8. Propiedad intelectual (obligatorio)

La Entidad tendrá todos los derechos de propiedad intelectual incluidos, sin limitación, así como las patentes, derechos de autor, nombres comerciales y marcas registradas respecto a los productos o documentos y otros materiales que guarden una relación directa con la ejecución del servicio o que se hubiere creado o producido como consecuencia o en el desarrollo de la ejecución del servicio.

10.9. Medidas de control durante la ejecución contractual

[En función a la naturaleza de los servicios y la necesidad, determinar las medidas de control (visitas de supervisión, inspección, entre otros), a ser realizadas durante la ejecución del contrato, es decir, durante el desarrollo del servicio. Las medidas de control están orientadas a verificar el cumplimiento de las condiciones establecidas en el contrato.

Asimismo, indicar si estas serán programadas o inopinadas, cuántas serán como mínimo, quién las realizará (personal de la Entidad y/o a través de terceros), dónde se realizará, cuándo se realizará (en caso de ser programadas) y cuál será el alcance de las mismas (si se utilizará alguna normativa para su realización, entre otros).

Asimismo, considerar aspectos relativos al desarrollo de las medidas de control, para lo cual indicar con claridad:

- Áreas que coordinarán con el PROVEEDOR: Señalar las áreas o unidades orgánicas con

GOBIERNO REGIONAL DIRECCIÓN DE INFORMACIÓN ESTADÍSTICA AGRARIA V°B° OTI AMAZONAS

las que el PROVEEDOR coordinará sus actividades.

- Áreas responsables de las medidas de control: Señalar el área o unidad orgánica responsable de las medidas de control previstas durante el desarrollo del servicio y/o en otro momento durante la ejecución contractual.
- Área que brindará la conformidad: Señalar al área o unidad orgánica responsable de emitir la conformidad (área usuaria)]

10.10. Recursos y facilidades para proveer por la Entidad (de corresponder)

10.11. Responsabilidad por vicios ocultos (obligatorio)

La recepción conforme de la prestación por parte de LA ENTIDAD no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto por los artículos 69 de la Ley N° 32069, Ley General de Contrataciones Públicas y el artículo 144 de su Reglamento.

El/La PROVEEDOR es el responsable por la calidad ofrecida y por los vicios ocultos del servicio ofertado por un plazo no menor de un (01) año, contado a partir de la conformidad otorgada por la Entidad).

10.12. Responsabilidad por la asignación de bienes (de corresponder)

En aquellos casos en los cuales, para el cumplimiento de la prestación, la Entidad asigne al/a la PROVEEDOR algún bien mueble o inmueble, éste/a será responsable del buen uso y conservación de los mismos; de lo contrario, responderá por su deterioro o pérdida, debiendo proceder a su reposición dentro del plazo de cinco (05) días hábiles.

10.13. Declaración Jurada de Intereses (obligatorio)

Son causales de resolución de contrato el incumplimiento del requerimiento de presentar la Declaración Jurada de intereses conforme el numeral 11.5 del artículo 11 del Reglamento del Decreto de Urgencia N° 020-2019, Decreto de Urgencia que establece la obligatoriedad de la presentación de la declaración jurada de intereses en el sector público o la presentación de la declaración Jurada de Intereses con información inexacta o falsa.

10.14. Gastos por desplazamiento (de corresponder)

En caso de que, para el cumplimiento de sus actividades, se requiera el traslado del prestador de servicio, en el ámbito nacional, los gastos inherentes a las mismas (pasajes, movilidad, alimentación y hospedaje), correrán por cuenta del GOREA, de acuerdo Anexo N° 17.

10.15. Otras obligaciones de la Entidad (de corresponder)

10.16. Medidas de control durante la ejecución contractual (de corresponder)

XII. PENALIDADES (obligatorio)

13.1. Penalidad (obligatorio)

Si EL PROVEEDOR incurre en retraso injustificado en la ejecución de las prestaciones objeto del contrato, LA ENTIDAD le aplica automáticamente una penalidad por mora por cada día de atraso, de acuerdo con la siguiente fórmula:

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

Donde:

GOBIERNO REGIONAL AMAZONAS DIRECCIÓN DE INFORMACIÓN ESTADÍSTICA AGRARIA V°B° OTI

F = 0.40

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 PROVEEDOR 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 ENTIDAD 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; o si fuera necesario, se cobra del monto resultante de la ejecución de la garantía de fiel cumplimiento.

Cuando se llegue a cubrir el monto máximo de la aplicación de la penalidad por mora y otras penalidades, de ser el caso, LA ENTIDAD puede resolver el contrato por incumplimiento.

13.2. Otras penalidades (de corresponder)

(De acuerdo al tipo de contratación el área usuaria podrá establecer otras penalidades diferentes a la mora, las cuales deberá ser objetivas, razonables y proporcionales con el objeto de la contratación, por lo que se deberá precisar el listado de las situaciones, condiciones, el procedimiento de verificación de las ocurrencias y los montos o porcentajes a aplicar).

GOBIERNO REGIONAL AMAZONAS
DIRECCIÓN REGIONAL AGRARIA
OFICINA DE ADMINISTRACIÓN
CPC. DAVID MARCIAL ORBEGOSO CASTILLO
DIRECTOR DE ADMINISTRACIÓN

GOBIERNO REGIONAL AMAZONAS
DIRECCIÓN REGIONAL AGRARIA
DIRECCIÓN DE INFORMACIÓN ESTADÍSTICA AGRARIA
V°B°
OTI