

ANEXO N° 1

ESPECIFICACIONES TÉCNICAS PARA LA CONTRATACIÓN DE BIENES EN GENERAL

N° DE PEDIDO DE COMPRA SIGA: 234

FECHA Chachapoyas 11 de agosto 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 CCMM	SOFTWARE (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 técnicas¹ (obligatorio)

El postor debe ofrecer como mínimo las características técnicas mencionadas o podrá ofrecer características superiores a estas, las cuales deben de ser demostradas, asimismo debe de presentar ficha técnica de la solución propuesta.

Sistemas Operativos soportados:

El producto ofertado debe poder instalarse en su última versión, sobre plataformas, Windows 8, Windows 8.1, Windows 10 y Windows 11. Contar con Soporte para plataformas de 32 y 64 bits.

Agente:

- Se debe poder desplegar el agente de la solución desde la consola de administración y este debe ser el componente administrativo de todas las funcionalidades solicitadas en este documento.
- La solución debe contar con los mecanismos de protección para no poder ser desinstalada o desactivada por el usuario.
- Se deben poder habilitar o deshabilitar los módulos de protección sin ser desinstalados del sistema.

Software cliente

- Se debe poder restringir completamente o parcialmente el acceso a la consola cliente para configurar parámetros individuales sobre el host.
- La desinstalación de la aplicación puede ser protegida mediante contraseñas desplegadas por políticas configuradas por el administrador.
- La solución debe basarse en una plataforma común sobre la cual se incorporan módulos de protección de amenazas, protección web, y Firewall de escritorio, y que permita el intercambio de información entre cada uno de los módulos.

Protección de Amenazas:

- La solución debe de poder configurarse para realizar escaneos por demanda o programados, desde la consola de administración.
- Se debe poder configurar acciones sobre infecciones identificadas:
 - Denegar y/o bloquear acceso
 - Limpiar y/o desinfectar
 - Eliminar
- La solución debe ofrecer opciones de envío de infecciones a cuarentena y ejecutar acciones sobre ítems enviados allí.



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



- La solución de antivirus debe contar con módulos que proteja contra virus, gusanos, troyanos, keyloggers, dialers, adware, spyware, hacktools, rootkits, bots, spam, herramientas de control remoto y otros programas potencialmente peligrosos.
- Debe ser eficiente contra amenazas de tipo ransomware, identificando comportamientos y actividades sin importar la pieza de código (Se conoce el modo de operar de Ransomware por ende es posible bloquear sus actividades).
- Debe permitir realizar la detección en tiempo real.
- La solución debe tener la capacidad de verificar / ejecutar un análisis en todos los hosts para cualquier nombre de archivo, extensión de archivo, archivo MD5 / SHA1 o IOC provisto.
- La solución debe ser capaz de detectar el ataque localmente, sin depender de un servicio en la nube.
- La solución debe poder habilitar la opción de escaneo de click-derecho sobre carpetas específicas.
- La solución debe poder configurar mediante reglas o políticas de protección de:
 - Entradas y llaves de registro de Windows.
 - Prevención de creación de ejecutables portables(.INI,.PIF).

Control WEB:

- La solución debe poder bloquear de forma automática sitios con clasificación de riesgo alto que puedan afectar los equipos y/o la red.
- La solución debe tener la capacidad de evitar el acceso a sitios de phishing.
- La solución deberá poder evitar descargar malware, ayudando así a tener que la protección sea proactiva.
- La solución debe poder especificar que navegadores sean los únicos autorizados para navegar a internet.
- La solución debe permitir el manejo flexible de la licencia de manera que puedan ser reasignadas en caso de que cambie el equipo dentro de un periodo de tiempo configurable.
- Debe contar con la capacidad de realizar inventario de hardware y software de todas las máquinas clientes.
- Capacidad de etiquetar dispositivos o grupos de dispositivos mediante rotulados personalizables.
- Debe contar con la capacidad de monitorear grupos de trabajos ya existentes y cualquier grupo de trabajo que sea creado en la red, con el objetivo de encontrar máquinas nuevas para ser agregadas a la protección.

Control de aplicaciones:

- La solución debe permitir definir manualmente las aplicaciones que deben bloquearse.
- La solución debe permitir excluir aplicaciones que se identifiquen como desconocidas o peligrosas para poder ser ejecutadas a necesidad.
- No debe permitir que las aplicaciones denegadas se ejecuten desde el disco o desde memoria
- No debe permitir que las aplicaciones denegadas se ejecuten desde el disco o desde memoria

Protección contra amenazas:

- La solución deberá poder tomar acciones o de bloqueo o registro según su configuración
- Debe estar basado en reglas de comportamiento configurables tanto desde la consola cliente como la consola central
- Debe estar basado en reglas de comportamiento configurables tanto desde la consola cliente como la consola central

Consideraciones de instalación y despliegue del software

- Debe permitir la implementación, configuración y administración remota de la solución antivirus instalada en las estaciones de trabajo físicos y virtuales incluyendo servidores.
- Capacitación a los usuarios administradores de la solución (Oficina de Tecnologías de la Información) durante la vigencia del contrato.
- Debe ser capaz de manera opcional de detectar otros antivirus de terceros instalados en las máquinas y proceder con la desinstalación automática de estos, antes de instalar el antivirus.





- De ser necesario, el proveedor debe realizar actualizaciones de la versión del software de la consola de administración, siendo ésta la última versión a la fecha brindada por el fabricante.

Características de la Consola de administración

- Debe desplegarse en la nube del fabricante sin incurrir en costos adicionales, se deberá coordinar previamente con la Oficina de Tecnologías de la Información de la Entidad.
- Debe permitir que las actualizaciones se realicen en forma incremental y automática.
- Debe monitorear las estaciones de trabajo activas e inactivas de la totalidad de la red y además permitir tomar acciones en caso se detecte una estación con virus.
- Debe en caso de encontrar equipos que no cumplan con la política de seguridad establecida, que sean vulnerables o se encuentren infectados, deberá tomar las acciones necesarias para subsanar estas deficiencias de seguridad. Asimismo, se deberá efectuar análisis en demanda de los equipos en busca de virus.
- Debe obtener las actualizaciones directamente de los sitios disponibles por el fabricante o a través del proveedor, cada hora, día o semanalmente, y ser aplicadas a cada uno de los productos. Las actualizaciones deberán ser totalmente constantes y auditables.
- La consola debe recoger en la base de datos otra información sobre los equipos que conforman la plataforma antivirus como CPU (velocidad y tipo), memoria, espacio total, versiones de sistema operativo y niveles de parche, que también podrán ser materia de reporte.
- Debe ser totalmente compatible con sistemas de distribución y administración de software.
- Entre las características de inventario a ser recogidas se sugieren:
 - Sistema Operativo
 - Versión de sistema operativo
 - Número de Service Pack
 - Memoria RAM
 - Discos
 - Espacio total de disco
 - Dirección IP de la PC.

Administración de Licencias

La solución debe permitir el manejo flexible de las licencias, de manera que puedan ser reasignadas en caso se cambie de equipo.

c. 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 periodo de garantía:** La garantía rige a partir del día siguiente de emitida la conformidad de implementación del bien.

VI. REQUISITOS Y RECURSOS DEL/DE LA PROVEEDOR/A

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.

VII. LUGAR Y PLAZO DE LA PRESTACIÓN

- 7.1 **Lugar de entrega:** *Se realizará de manera remota, proporcionando el detalle de las licencias al correo tecnologiasdeinformación@draamazonas.gob.pe (Oficina de Tecnologías de la Información) con copia al correo de la Unidad de Almacén almacen@draamazonas.gob.pe, para conocimiento.*
- 7.2 **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.*
- 7.3 *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.*

VIII. CONFORMIDAD DEL BIEN (obligatorio)

8.1 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

8.2 Área técnica que emite la conformidad:

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 entregable²correspondiente, dependiendo de la complejidad o sofisticación de las subsanaciones a realizar. Si pese al plazo otorgado, EL PROVEEDOR no cumpliera 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.

IX. FORMA DE PAGO

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.

X. CONSIDERACIONES PARA LA EJECUCIÓN CONTRACTUAL

10.1. Confidencialidad

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 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

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.





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 (artículo. 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

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

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 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. Responsabilidad por vicios ocultos

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).

10.11. Declaración Jurada de Intereses

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.

XI. 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:

$$F = 0.40$$

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.

