TÉRMINOS DE REFERENCIA PARA LA CONTRATACIÓN DE SERVICIOS

N° DE PEDIDO DE SERVICIO: 000218-2026

FECHA: Lima, 05 de junio de 2026	
Unidad Orgánica	OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN (UNIDAD DE SISTEMAS E INFORMÁTICA)
Actividad Operativa	AOI00108900136: EJECUCIÓN DEL MANTENIMIENTO AL EQUIPAMIENTO INFORMÁTICO Y RENOVACIÓN DE LICENCIAS.
Meta Presupuestaria	003
Denominación de la contratación	Servicio de renovación de suscripción de licencias de software Antivirus para la APCI

1. MARCO LEGAL

La presente contratación se rige por las disposiciones contempladas en la Ley N° 32069, Ley General de Contrataciones Públicas y su Reglamento, aprobado mediante el Decreto Supremo N° 009-2025-EF.

2. FINALIDAD PÚBLICA

La presente contratación tiene por finalidad garantizar la protección y seguridad de los activos de información de la Agencia Peruana de Cooperación Internacional (APCI), mediante la renovación de la suscripción las licencias del software antivirus institucional, a fin de prevenir y mitigar amenazas informáticas para proteger y prever ataques de virus informáticos, así como spam, troyanos, ransomware que puedan afectar a los usuarios, red de datos, servidores y parque Informático de la APCI, contribuyendo al cumplimiento de la Actividad Operativa Institucional AOI00108900136: "Ejecución del mantenimiento al equipamiento informático y renovación de licencias".

3. OBJETIVOS DE LA CONTRATACION

El presente servicio tiene por objetivo contratar a una persona natural o jurídica que brinde el servicio de renovación de suscripción de licencias de software Antivirus con capacidades de detección y respuestas extendidas (EDR/XDR) para proteger el parque informático y servidores de la Agencia Peruana de Cooperación Internacional – APCI.

4. DESCRIPCIÓN DEL SERVICIO

El servicio comprende la adquisición, provisión y soporte integral de una solución de protección para endpoints y servidores, licenciada durante doce (12) meses, bajo la modalidad a todo costo de acuerdo con el siguiente detalle:

4.1. Cantidad y Distribución de Licencias:

• 180 Licencias de antivirus para dispositivos finales / estaciones de trabajo (compatibles con Windows y macOS).

• 22 Licencias de antivirus para servidores (compatibles con sistemas operativos Windows Server y Linux).

4.2. Características Generales de la Solución

La solución ofertada debe ser un producto de ciberseguridad consolidado de última generación que integre funcionalidades de antivirus, antimalware, anti-exploits y anti-ransomware nativo de IA. Debe cumplir con los siguientes estándares:

- Estar presente dentro del cuadrante de líderes o visionarios en el Magic Quadrant for Endpoint Protection Platforms de Gartner dentro de los últimos tres años, o contar con la máxima distinción (Leader/Top Player) en reportes de analistas de la industria con similar alcance global como Forrester Wave o Radicati Group.
- Contar con una efectividad de seguridad certificada mayor o igual al 95% según reportes especializados (en laboratorios especializados como NSS Labs, SE Labs, o AV-TEST).
- Deberán ser soluciones de propósito específico para cada tipo de dispositivo a proteger (endpoints, servidores). Es decir, un agente para endpoint y otro agente para servidores.
- Todos los componentes de seguridad deben ser suministrados por un solo fabricante (no se aceptarán composiciones de productos fragmentados de diferentes fabricantes).

4.3. Consola de Administración Centralizada

La gestión de la solución se realizará a través de una consola central única basada en entorno Web (en la nube o en sitio):

- Dashboard visual en tiempo real que resuma el estado de protección, alertas de criticidad (alta, media, informativa) y filtros pre-construidos para corregir equipos de manera remota.
- Mecanismo de comunicación e integración nativa vía API que soporte formatos JSON, CEF o KEYVALUE para el envío y correlación de alertas hacia herramientas externas (por ejemplo, SIEM) sin borrar la información de la consola origen.
- Control de acceso basado en roles con distintos niveles de privilegios (Administrador, Operador, Solo Lectura), resguardado por un registro de auditoría seguro y exportable en formatos CSV y PDF.
- Sincronización nativa con Active Directory (AD) para la gestión y asignación automática de políticas, segmentación por grupos/subgrupos y detección de dispositivos desprotegidos.
- Capacidad de despliegue automatizado y flexible mediante GPO de Active Directory, instalación remota desde consola, preinstalación en imágenes de SO, y paquetes manuales silenciosos.
- Programación avanzada de escaneos y configuración de exclusiones globales y específicas de directorios, archivos, procesos o rangos de direcciones IP.
- La consola de administración deberá tener usuarios con distintos roles de niveles de acceso y privilegios, como administradores, operadores de la consola y usuarios de sólo lectura.

- Sólo los usuarios administradores podrán asignar operadores de la consola y usuarios de sólo lectura.
- Las operaciones que se realicen en la consola deberán guardarse en un registro que permita su posterior revisión si fuese necesario.
- La consola debe permitir la división de los ordenadores dentro de la estructura de administración en grupos.
- Debe poseer la posibilidad de aplicar reglas diferenciadas por grupos de usuarios, usuarios individuales, grupos de máquinas y equipos individuales.
- Proporcionar actualizaciones del producto y de las definiciones de virus y protección contra intrusos.
- Debe permitir programar el escaneo de amenazas en las estaciones y servidores.
- Debe permitir exclusiones de escaneo para un determinado sitio Web, archivo o carpeta, aplicación o proceso. Tanto a nivel global, como específico en cada política.
- La consola de administración debe permitir la definición de grupos y sub grupos para la administración de las estaciones, usuarios y políticas.
- Actualizar de forma automática las políticas de seguridad del agente cuando una estación se mueve de un grupo a otro.
- Utilizar protocolos seguros estándar HTTPS para la comunicación entre la consola de administración y los clientes administrados.
- Los mensajes generados por el agente deben estar en el idioma español o permitir su edición.
- Permitir la exportación de los informes gerenciales a los formatos CSV y PDF.
- Los recursos del informe y el monitoreo deben ser nativos de la propia consola central de administración.
- Posibilidad de mostrar información como nombre de la máquina, versión del antivirus, sistema operativo, dirección IP, versión del motor, fecha de la actualización, fecha de la última verificación, eventos recientes y estado.
- Capacidad de generación de informes estadísticas o gráficos, tales como:
    - Detalle de usuarios activos, inactivos o desprotegidos, así como detalles de los mismos.
    - Detalle de los ordenadores que están activos, inactivos o desprotegidos, así como detalles de las exploraciones y alertas en los ordenadores.
    - Detalle de los periféricos permitidos o bloqueados, así como detalles de dónde y cuándo se utilizó cada periférico.
    - Detalle de las principales aplicaciones bloqueadas y los servidores/usuarios que intentaron acceder a ellas.
    - Detalle de las aplicaciones permitidas que fueron accedidas con mayor frecuencia y los servidores/usuarios que las acceden.
    - Detalle de los servidores/usuarios que intentaron acceder a

aplicaciones bloqueadas con mayor frecuencia y las aplicaciones que ellos intentaron acceder.

- Detalle de todas las actividades disparadas por reglas de fuga de información.

- Actualización incremental, remota y en tiempo real, de las vacunas de los Antivirus y del mecanismo de verificación (Engine) de los clientes.
- Actualización automática de las firmas de amenazas (malware) y políticas de prevención desarrolladas por el fabricante en tiempo real o con periodicidad definida por el administrador.
- La herramienta de administración centralizada debe administrar todos los componentes de la protección para estaciones de trabajo y servidores y debe diseñarse para administrar, supervisar y elaborar informes de endpoint y servidores.
- La consola debe soportar los siguientes idiomas; Español e Ingles.
- Control y optimización del ancho de banda mediante Quality of Service (QoS) y uso de servidores caché locales o relés de mensajes (message relay) para endpoints fuera de la red local o sin conexión permanente.
- La consola de administración debe incluir un panel con un resumen visual en tiempo real para comprobar el estado de seguridad.
- Deberá proporcionar filtros pre-construidos que permitan ver y corregir sólo los ordenadores que necesitan atención.
- Deberá mostrar los ordenadores administrados de acuerdo con los criterios de categoría (detalles del estado del equipo, detalles sobre la actualización, detalles de avisos y errores, detalles del antivirus, etc.), y ordenar los equipos en consecuencia.
- Una vez que se identifique un problema, debe permitir corregir los problemas de forma remota, con al menos las siguientes opciones:
- Proteger el dispositivo con la opción de inicio de una exploración.
- Forzar una actualización en ese momento.
- Ver los detalles de los eventos ocurridos.
- Ejecutar la comprobación completa del sistema.
- Forzar el cumplimiento de una nueva política de seguridad.
- Mover el equipo a otro grupo.
- Borrar el equipo de la lista.
- Aislarlo a demanda de la red corporativa.
- Ejecutar una interfaz de línea de comando sobre el dispositivo.
- Actualizar las directivas de seguridad cuando un equipo se mueve de un grupo a otro, manualmente o automáticamente.
- Debe contener varios informes para el análisis y control de los usuarios y endpoints. Los informes se deben dividir, como mínimo, en informes de: eventos, usuarios, control de aplicaciones, periféricos y Web, indicando todas las funciones solicitadas para los endpoints.
- Permitir la ejecución manual de todos estos informes, así como la programación y envío automático por correo electrónico en los formatos CSV y PDF.

- Deberá tener la posibilidad de implementar servidores de caché locales para utilizar de manera eficiente el uso del ancho de banda.
- Deberá tener la posibilidad de instalar un servidor para reenvío de eventos (message relay) en caso de que el agente no pueda comunicarse con la consola en la nube, esto si la administración ofrecida por el postor está basada en la nube.
- Debe realizar envío automático de alertas críticas mediante correo electrónico a los administradores.
- Debe permitir la creación de reglas para excluir rangos específicos de direcciones IP.
- La consola debe poseer una gráfica de amenazas conteniendo toda la secuencia de eventos que ocurrieron durante la ejecución del malware o el ataque de un adversario, siendo posible ampliar los detalles de cada evento a fin de obtener un análisis de causa raíz detallado.
- La solución de endpoints y servidores debe ser administrada desde una misma consola en sitio o en la nube, de acuerdo a lo ofertado por el postor

4.4. Compatibilidad del Agente de Protección

El agente único de protección deberá instalarse de manera transparente y ser compatible nativamente con:

- Estaciones de Trabajo: Microsoft Windows 10, Windows 11; macOS 11, 12, 13 o superiores.
- Servidores: Microsoft Windows Server 2012 R2, 2016, 2019, 2022 o superiores; entornos Linux tales como, Ubuntu 20.04 o superior, Debian 9/10.
- Autoprotección del Agente: Mecanismos protegidos por contraseña única por dispositivo para evitar que usuarios locales o administradores no autorizados detengan los servicios, reconfiguren, deshabiliten o desinstalen la solución.
- Desinstalación competitiva: Capacidad nativa de remover soluciones antivirus previas existentes en el parque informático durante el proceso de despliegue.

4.5. Características de Protección de Malware

El agente integrado debe proveer las siguientes capas críticas de seguridad:

- Protección contra Malware y Amenazas del Día Cero Análisis proactivo en tiempo real (tanto online como offline) mediante motores de Inteligencia Artificial basados en Redes Neuronales Profundas (Deep Learning / Signature-less) capaces de interceptar y dictaminar de manera inmediata comportamientos maliciosos directamente en la memoria del dispositivo antes de la pre-ejecución del código, prescindiendo del uso exclusivo de firmas tradicionales..
- El agente deberá proteger, detectar y prevenir amenazas en tiempo real, independientemente del estado de conexión de la estación de trabajo o servidor, es decir estando online (con conexión a Internet) o en estado offline (sin conexión a Internet).
- El agente también deberá trabajar bajo demanda o programado para detectar, bloquear y limpiar todos los virus, troyanos, gusanos y spyware. En Windows, el agente también debe detectar PUA, adware y comportamiento sospechoso.
- Detección del malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido.

- Debe realizar la verificación de todos los archivos accedidos en tiempo real, incluso durante el proceso de arranque.
- Debe realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente indeseables (PUA).
- Debe proteger las funciones críticas en los navegadores de Internet (Safe Browsing).
- Debe permitir la autorización de detecciones maliciosas y excluir de la exploración de directorios y archivos específicos.
- Se requiere protección integrada, es decir, en un solo agente, contra amenazas de seguridad, incluyendo virus, spyware, troyanos, gusanos, adware y aplicaciones potencialmente no deseadas (PUA).
- Debe poseer la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidad conocida.
- Ser capaz de aplicar un análisis adicional, inspeccionando finamente el comportamiento de los códigos durante la ejecución, para detectar el comportamiento sospechoso de las aplicaciones, tales como desbordamiento de búfer.
- Debe prevenir el ataque de vulnerabilidades de navegador a través de web exploits.
- Posee la funcionalidad de protección contra el cambio de la configuración del agente, impidiendo a los usuarios, incluyendo el administrador local, reconfigurar, deshabilitar o desinstalar componentes de la solución de protección.
- Debe tener un mecanismo contra la desinstalación del endpoint por el usuario y cada dispositivo deberá tener una contraseña única, no siendo autorizadas soluciones con una contraseña que funcione en todos los dispositivos.
- Permitir la utilización de contraseña de protección para posibilitar la reconfiguración local en el cliente o desinstalación de los componentes de protección.
- Debe contar con prevención de intrusión en el host (HIPS), que monitoree el código y bloques de código que pueden comportarse de forma maliciosa antes de ser ejecutados.
- Capacidad de reconocer y bloquear automáticamente las aplicaciones en los clientes basándose en la huella digital (hash) del archivo.
- Además del control de amenazas, el mismo agente (al menos Windows) debe proporcionar control de dispositivos, control de aplicaciones, control web y prevención de fuga de información (DLP)

4.6. Protección contra amenazas Avanzadas

- Protección de amenazas de día 0 a través de tecnología de deep learning (signature less) / Machine learning.
- Funcionalidad de detección de amenazas desconocidas que están en memoria con tecnología deep learning / Machine learning.
- Capacidad de detección, y bloqueo proactivo de keyloggers y otros malwares no conocidos (ataques de día cero) a través del análisis de comportamiento de procesos en memoria.
- Capacidad de detección y bloqueo de troyanos (Trojans) y gusanos (Worms), entre otros malwares, por comportamiento de los procesos en memoria.

- No debe requerir descarga de firmas de ningún tipo.
- Capacidad de analizar el comportamiento de nuevos procesos al ser ejecutados, en complemento a la exploración programada.
- Análisis forense de lo sucedido, para entender cuál fue la causa raíz del problema con el detalle de los procesos y sub-procesos ejecutados, la lectura y escritura de archivos y de las claves de registro.
- Bloqueo y protección contra amenazas desconocidas potencialmente sospechosas (PUA).
- Generación de excepciones ante falsos positivos.
- La solución debe tener capacidad de protección AMSI contra scripts maliciosos.
- La solución debe poseer un IPS Snort de Host

4.7. Protección contra Ransonware

- Capacidad de reconocer y bloquear automáticamente las aplicaciones en los clientes basándose en la huella digital (hash) del archivo.
- Disponer de capacidad de protección contra ransomware no basada exclusivamente en la detección por firmas (por ejemplo: basada en comportamiento).
- Disponer de capacidad de remediación de la acción de cifrado malicioso de los ransomware;
- Debe poseer protección anti-ransomware para el sector de booteo (master boot record).
- Debe restaurar automáticamente los archivos cifrados por un proceso malicioso de ransomware.
- Debe informar a la consola todo el detalle del incidente – análisis de causa raíz sin la necesidad de instalar otro agente o dispositivo en la red.
- En el caso de servidores, debe disponer de la capacidad de prevención contra la acción de cifrado malicioso ejecutada por ransomware, posibilitando aún el bloqueo de las computadoras de donde parte tal acción (detección local y remota).

4.8. Protección contra vulnerabilidades y Técnicas de Explotación

- Debe poseer la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidades conocidas o de día cero.
- Detección y protección de más de 20 técnicas de explotación.
- Mitigación de inyección de códigos en procesos.
- Protección contra robo de credenciales.
- Protección contra malware escondido en aplicaciones legitimas (code cave).
- Evitar la migración de procesos maliciosos, evitando que un proceso malicioso migre a otro.
- Evitar obtener escalamiento de privilegios y acceso elevado a recursos.
- Modificación de las claves de registro para la ejecución de código arbitrario

4.9. Funcionalidad de Control de Aplicaciones

- Control de aplicaciones para monitorear e impedir que los usuarios ejecuten o instalen aplicaciones que puedan afectar la productividad o el rendimiento

de la red.

- Actualización automática de la lista de aplicaciones que se pueden controlar, permitiendo aplicaciones específicas o las categorías específicas de aplicaciones que pueden ser liberadas o bloqueadas.
- Detectar aplicaciones controladas cuando los usuarios acceden, con las opciones de permitir y alertar o bloquear y alertar.

4.10. Funcionalidad de Control Web

- Control de acceso a sitios web por categoría.
- El Control Web debe controlar el acceso a sitios inapropiados, con al menos 14 categorías de sitios inadecuados. También debe permitir la creación de listas blancas y listas negras.
- La aplicación de políticas de control web, debe contar con capacidad de horarios.

4.11. Funcionalidad de control de Periféricos

- Debe permitir el monitoreo y el control de dispositivos extraíbles en los equipos de los usuarios, como dispositivos USB, periféricos de la propia estación de trabajo y redes inalámbricas, aplicando estas políticas tanto para usuarios como para dispositivo.
- El control de dispositivos debe estar al nivel de permiso, sólo lectura o bloqueo.
- Los siguientes dispositivos deben ser, como mínimo, administrados: HD (hard disks) externos, pendrives USB, almacenables removibles seguras, CD, DVD, Blu-ray, floppy drives, interfaces de red inalámbrica, módems, bluetooth, infrarrojo, MTP (Media Transfer Protocol) y PTP (Picture Transfer Protocol) como cámaras digitales.
- Debe permitir adicionar exclusiones

4.12. Funcionalidad de Prevención de fuga de la Información

- Solución de administración de archivos, asegurando que un archivo específico no salga de La Organización, buscando palabras claves o información confidencial. Se debe bloquear la carga o el envío de la información confidencial antes de enviar el archivo.
- Debe poseer protección de fugas o pérdida de datos sensibles en el mismo agente de protección, considerando su contenido, además de la posibilidad de evaluar la extensión del archivo y múltiples destinos.
- Permitir la identificación de información confidencial (como números de pasaporte u otra información personal identificable) utilizando reglas lógicas integradas y plantillas de control de contenido (Content Control Lists) provistas nativamente por el fabricante, ejecutadas en tiempo real directamente por el mismo y único agente de protección, sin requerir el despliegue de módulos de software independientes.
- Capacidad de autorizar, bloquear y confirmar el movimiento de información sensible y en todos los casos, grabar la operación realizada con las principales informaciones de la operación.
- Posibilitar el bloqueo, sólo registrar el evento en la Consola de administración, o preguntar al usuario si él o ella realmente quiere transferir el archivo identificado como sensible.

- Debe tener listas de CCL preconfiguradas con al menos los siguientes identificadores.
- Números de tarjetas de crédito
- Números de cuentas bancarias
- Números de pasaportes
- direcciones
- Números de teléfono
- Lista de correos electrónicos
- Soportar agregar reglas propias de contenido con un asistente proporcionado para este propósito.
- Permitir el control de datos para al menos los siguientes medios:
- Adjunto en el cliente de correo electrónico (al menos Outlook y Outlook Express)
- Adjunto en el navegador (al menos IE, Firefox y Chrome)
- Adjunto en el cliente de mensajería instantánea (al menos Skype)
- Adjunto a dispositivos de almacenamiento (al menos USB, CD / DVD)

4.13. Funcionalidad de Detección y Respuestas Extendida e Investigación (EDR/XDR)

La solución debe dotar a los analistas de TI de la APCI de capacidades robustas de análisis y respuesta ante incidentes avanzados:

- Análisis Predictivo de Atributos: Identificar qué atributos de código de un objeto en ejecución son similares a archivos catalogados históricamente como confiables o maliciosos para determinar acciones preventivas automatizadas.
- Registro de Origen de Infección: Mantener un sistema de registro detallado por cada vector de ataque detectado en los endpoints, identificando la aplicación origen (explorador de archivos, cliente de correo, navegadores web, etc.).
- Investigación Guiada y Análisis Forense: Proveer visibilidad completa de la dimensión de una brecha mediante gráficos interactivos de la secuencia del ataque que detallen visualmente el alcance, procesos e hilos ejecutados, modificaciones en llaves de registro y manipulación de archivos (Análisis de Causa Raíz).
- Threat Hunting basado en Lenguaje Estándar o Interfaz de Consultas Avanzadas: Para la caza proactiva de amenazas, la solución debe permitir interrogar el estado en vivo de los endpoints y servidores mediante consultas basadas en lenguaje estructurado (como SQL estándar) o a través de un motor avanzado de búsqueda e indexación de artefactos. El sistema debe permitir la inspección profunda de elementos del sistema operativo tales como procesos activos, modificaciones de llaves de registro, conexiones de red en tiempo real, telemetría de memoria, logs del sistema y hashes de archivos (SHA-256)
- Catálogo de Búsquedas Predefinidas: La solución debe incorporar de manera nativa en su consola un catálogo o repositorio preestablecido de un mínimo de 100 escenarios de búsqueda o consultas predefinidas listas para su ejecución inmediata por el analista, permitiendo además la personalización, creación y programación automatizada de nuevas directrices de búsqueda

- Aislamiento Remoto y Conducción Segura: Capacidad de aislar dispositivos comprometidos de la red corporativa de manera manual o automatizada inmediatamente ante una sospecha de brecha. Se debe disponer de una interfaz tipo terminal de comando (CMD/Terminal) accesible de forma segura vía web desde la consola central para interactuar directamente sobre los endpoints y servidores aislados con fines de remediación.
- Almacenamiento Histórico en Nube: Retención de la telemetría y los datos de los Indicadores de Compromiso (IoC) detectados en la consola de gestión basada en nube por un periodo mínimo de treinta (30) días, posibilitando auditorías e investigaciones históricas aun cuando los dispositivos estén apagados u offline.
- Enriquecimiento de Inteligencia: Integración nativa con fuentes de reputación externas (tales como VirusTotal, SANS ISC, entre otros) para agilizar las investigaciones y contar con un ecosistema adaptativo impulsado por IA para el resumen y correlación de casos.

5. PRODUCTOS O ENTREGABLES

El contratista deberá presentar su comprobante de pago, carta de garantía emitida por el proveedor, carta de compromiso de soporte técnico por un año y documento, certificado o acta emitida por el proveedor que acredite la activación y vigencia de ciento ochenta (180) licencias para dispositivos finales y veintidós (22) licencias para servidores, indicando la fecha de inicio y término de la vigencia debidamente firmado por el proveedor y el área usuaria; solicitados para el pago mediante la Mesa de Partes de la APCI, sito en Av. José Pardo Nº 261 – Miraflores, en el horario de 8:30 a.m. hasta las 04:00 p.m.; o, en su defecto a través de la Mesas de Partes digital, accediendo al Link: https://d-tramite.apci.gob.pe/mesa-de-partes-virtual/index.php en el horario de 08:30 am hasta las 05:00 pm, de lunes a viernes. Los documentos recibidos fuera de este horario o en feriados serán revisados al siguiente día hábil.

6. REQUISITOS QUE DEBE CUMPLIR EL CONTRATISTA

6.1 Requisitos del proveedor

- Contar con Registro Nacional de Proveedores (RNP) vigente.
- Contar con RUC activo y habido
- Ser partner vigente de la marca de antivirus, lo cual deberá ser acreditado mediante un certificado de la marca de antivirus.
- No contar con impedimento para contratar con el Estado, según el artículo 30 de la Ley N.º 32069.

6.2 Experiencia en la especialidad

Contar como mínimo cinco (5) servicios de servicios iguales o similares al objeto de la contratación, durante los siete (7) años anteriores a la fecha de la presentación de cotizaciones que se computa desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

Se consideran servicios similares a los siguientes: venta y/o adquisición y/o renovación de licencias de antivirus

Acreditación:
La experiencia se acreditará con copia simple de (i) contratos u órdenes de

servicio, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente o con voucher de depósito o nota de abono o 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 correspondientes u otra documentación que acredite fehacientemente lo requerido.

7. OTRAS CONSIDERACIONES PARA LA EJECUCIÓN DE LA PRESTACIÓN

7.1 Garantía

La garantía del servicio deberá ser por un periodo no menor de doce (12) meses desde el día en que se realizó el servicio, tiempo en el cual se deberá contar con el soporte integral por parte del contratista. Asimismo, Todo daño producido durante la ejecución de la garantía a los bienes o infraestructura de la institución, será asumido en su totalidad por el contratista.

El contratista deberá presentar una carta la garantía por el servicio junto con su entregable.

7.2 Confidencialidad

El contratista 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 videográfico, documentos y otros similares.

7.3 Clausulas Anticorrupción Y Antisoborno

El proveedor o contratista declara y garantiza no haber, directa o indirectamente, o tratándose de una persona jurídica a través de sus socios, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o personas vinculadas, en concordancia a lo establecido en la Ley N° 32069, Ley General de Contrataciones Públicas, y su Reglamento aprobado mediante Decreto Supremo N° 009-2025-EF.

Asimismo, el proveedor o contratista se obliga a conducirse en todo momento, durante la ejecución del contrato, con honestidad, probidad, veracidad e integridad y de no cometer actos ilegales o de corrupción, directa o indirectamente o a través de sus socios, accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores y personas vinculadas, en virtud a lo establecido en la Ley N° 32069, Ley General de Contrataciones Públicas, y su Reglamento aprobado mediante Decreto Supremo N° 009-2025-EF.

Además, el proveedor o contratista se compromete a comunicar a las

autoridades competentes, de manera directa y oportuna, cualquier acto o conducta ilícita o corrupta de la que tuviera conocimiento, y adoptar medidas técnicas, organizativas y/o de personal apropiados para evitar los referidos actos o prácticas.

7.4 Prevención y Mitigación del Conflicto de Intereses (Ley N°31564)

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.

7.5 Responsabilidad por Vicios Ocultos

La recepción conforme de la prestación por parte de la APCI no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos, conforme a lo dispuesto en el artículo 69 de la Ley N° 32069, Ley General de Contrataciones Públicas y 144 de su Reglamento aprobado por Decreto Supremo N° 009-2025-EF.

El contratista 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

7.6 Responsabilidad por la Asignación de Bienes

En aquellos casos en los cuales, para el cumplimiento de la prestación, la Entidad asigne al contratista 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.

7.7 Otras Obligaciones de la Entidad

No aplica

8. LUGAR Y PLAZO DE LA PRESTACIÓN

8.1. LUGAR

En las instalaciones de la Agencia Peruana de Cooperación Internacional APCI, Sito: Av. José Pardo N° 261- Miraflores.

8.2. PLAZO

8.2.1 Plazo de ejecución del servicio

El contratista deberá realizar la instalación o implementación de las ciento ochenta (180) licencias para dispositivos finales y veintidós (22) licencias para servidores el 27 de junio de 2026.

8.2.2 Vigencia de las licencias

La vigencia de las licencias será de doce (12) meses, contados a partir de la fecha de activación del servicio.

9 CONFORMIDAD DE EJECUCIÓN DEL SERVICIO

Será otorgada por la Oficina de Tecnologías de la Información (Unidad de Sistemas e Informática); en el plazo de siete (07) días calendario, contabilizados desde el día siguiente de recibido el entregable (documentos para emisión de conformidad).

Asimismo, son aplicables las disposiciones correspondientes a la conformidad establecidas en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025-EF.

10 FORMA DE PAGO

Se realizará un único pago previa conformidad del servicio, otorgado por la Oficina de Tecnologías de la Información (Unidad de Sistemas e Informática).
El pago se realiza en un plazo máximo de diez (10) días hábiles luego de otorgada la conformidad por parte del área usuaria, y es prorrogable, previa justificación de la demora, por cinco días hábiles;
El pago incluirá los impuestos de Ley y todo costo o retención que recaiga en el servicio, no debiendo proceder pagos a cuenta por servicios no efectuados, ni adelanto alguno.

11 RESOLUCIÓN CONTRACTUAL

La APCI puede resolver el contrato, en los siguientes casos:

a) Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.
b) Incumplimiento de obligaciones contractuales, por causa atribuible a la parte que incumple.
c) 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.
d) Por incumplimiento de la cláusula anticorrupción y antisoborno debidamente acreditada
e) Por la presentación de documentación falsa o inexacta durante la ejecución contractual.

Asimismo, puede resolverse de forma total o parcial la Orden de servicio y/o contrato por mutuo acuerdo entre las partes, previa opinión del área usuaria.

12 SOLUCIÓN DE CONTROVERSIAS

Todas las controversias que surjan entre las partes sobre la validez, nulidad, interpretación, ejecución, terminación o eficacia, se resuelven mediante conciliación, conforme lo dispuesto en el numeral 81.3 del artículo 81 de la Ley. El procedimiento conciliatorio será regulado mediante el numeral 330.2 del artículo 330 del Reglamento de la Ley N° 32069.

13 GESTIÓN DE RIESGOS

LAS PARTES realizan la gestión de riesgos de acuerdo con lo establecido en el presente contrato y los documentos que lo conforman, 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.

14 PENALIDADES

14.1. PENALIDAD POR MORA

En caso de retraso injustificado del PROVEEDOR en la ejecución de las prestaciones objeto del contrato, la Entidad contratante le aplica automáticamente una penalidad por mora por cada día de atraso que le sea imputable, esto de conformidad con el artículo 120 del reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, de acuerdo con la siguiente fórmula:

$$\textbf{Penalidad diaria} = \frac{\mathbf{0.10} \times \textbf{monto}}{\boldsymbol{F} \times \textbf{plazo}}$$

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.

La Entidad tiene derecho para exigir, además de la penalidad, el cumplimiento de la obligación.

14.2. OTRAS PENALIDADES

Todo daño producido por el contratista a los bienes o infraestructura de la institución en la ejecución del servicio, previo informe que acredite el daño por parte del área usuaria, se aplicará 2% de la UIT

La suma de la aplicación de las penalidades por mora y de otras penalidades no puede exceder el 10% del monto del entregable correspondiente.

REPÚBLICA DEL PERÚ Firma Digital
Firmado digitalmente por: GOICOCHEA GANVINI Alan Enrique FAU 20504915523 soft
Motivo: En señal de conformidad
Fecha: 05/06/2026 17:30:34-0500

REPÚBLICA DEL PERÚ Firma Digital
Firmado digitalmente por: ZAVALETA IBAÑEZ Giancarlo FAU 20504915523 soft
Motivo: En señal de conformidad
Fecha: 05/06/2026 17:24:59-0500

Ejecutivo de Sistemas e Informática