TÉRMINOS DE REFERENCIA PARA LA CONTRATACIÓN DE SERVICIOS

Servicio de Suscripción Anual a licencias de Software Antivirus del PETACC

1. AREA QUE REALIZA EL REQUERIMIENTO

Unidad de Sistemas y Tecnologías de Información del PETACC.

2. FINALIDAD PÚBLICA

Proporcionar los medios de protección y gestión de la información ante ataques de malware y así realizar correctamente las actividades laborales de manera segura por parte de las Unidades Orgánicas del PETACC.

3. OBJETIVO DE LA CONTRATACIÓN

El objeto del presente servicio es contratar a una persona natural que brinde el SERVICIO SUSCRIPCIÓN ANUAL A LICENCIAS DE SOFTWARE ANTIVIRUS en el PETACC.

El presente servicio se orienta a seleccionar persona natural con negocio o jurídica para que abastezca a la entidad con Licencias Antivirus, para instalación y configuración en los equipos de cómputo, servidores y computadoras personales portátiles de la institución.

Cabe precisar que el requerimiento se encuentra incluido en el Cuadro Multianual de Necesidades (CNM).

4. JUSTIFICACION

El servicio se justifica en la necesidad de garantizar la protección de los equipos de cómputo frente a la posible presencia de malware y virus, los cuales pueden ocasionar daños a la información, al software y al sistema operativo.

5. FUENTE DE FINANCIAMIENTO Y RUBRO

Fuente Financiamiento: Recursos Determinados
Rubro: 18. Canon y Sobrecanon, Regalías, Renta De Aduanas y Participaciones
Meta: (0002) Administración de Proyectos de Inversión

6. ALCANCES Y DESCRIPCIÓN DEL SERVICIO

6.1 DESCRIPCIÓN DEL SERVICIO

Item	Descripción	Medida	Cantidad
01	LICENCIAS DE SOFTWARE ANTIVIRUS	Unidad	82

6.1.1 ACTIVIDADES A REALIZAR: son las siguientes:
SOLUCIÓN DE PROTECCIÓN PARA ESTACIONES DE TRABAJO

- La solución deberá ser compatible con los siguientes sistemas operativos: Microsoft® Windows® 11/10(deben tener compatibilidad con la firma de código de Azure). Ubuntu Desktop 18.04 y superior x64, RedHat para Desktop 8, 9 x64 y superior, Linux Mint 20, 21, 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.
- 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 contenga los siguientes 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.
- 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 cuando se trate de mensajes no deseados o detectados.
- 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.
- 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 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 aplicaciones como los navegadores web, lectores de PDF, clientes por correos electrónicos y Microsoft Office componentes.
- 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.

SOLUCIÓN DE PROTECCIÓN PARA SERVIDORES

- La solución debe ser compatible con los siguientes sistemas operativos: Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022 cuales deben tener compatibilidad con la firma de código de Azure.
- El producto antivirus puede instalarse sobre plataformas de x64 bits RedHat Enterprise Linux (RHEL) 7, 8 y 9; Ubuntu Server 18.04, 20.04 y 22.04 LTS; Debian10,11 y 12; SUSE Linux Enterprise Server (SLES) 15.
- Compatible con versiones del kernel del sistema operativo Linux 3.10.0 y posteriores
- El producto debe contar con un módulo de detección en tiempo real que proteja contra códigos maliciosos en cada acción realizada en el equipo (abrir, crear o ejecutar)
- 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 debe ser capaz de evitar que sus procesos, servicios, archivos o archivos de registro puedan ser detenidos, deshabilitados, eliminados o modificados, para de esta manera garantizar su funcionamiento ante cualquier tipo de ataque de virus.
- El producto para servidores Windows deberá contar con exclusiones automáticas que permitan detectar las aplicaciones críticas del servidor y los archivos críticos del sistema operativo y los agregue automáticamente a la sección de exclusiones al momento de ser instalado.
- El producto debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o carpeta especifica.
- El producto debe pedir una contraseña ante intentos de cambio indebidos en la configuración del producto.
- El producto debe contar con un agente que le permita ser administrado desde una consola centralizada.
- El antivirus deberá permitir generar dentro de la misma solución antivirus repositorios de actualización, los cuales deberán ser distribuidas mediante protocolo http localmente, esto sin depender de aplicaciones externas o de la consola de Administración.
- La protección en tiempo real debe iniciarse con el sistema operativo, así como poder definir qué tipos de medios serán analizados por el módulo.
- 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 debe permitir escanear archivos comprimidos.
- Debe permitir elegir las unidades a escanear para los escaneos bajo demanda.
- En sistemas operativos Windows, el antivirus deberá contar con una herramienta integrada que permita inspeccionar completamente componentes del sistema (Controladores, Aplicaciones Instaladas, Conexiones de Red y entradas importantes del Registro de Windows), esto con la finalidad de determinar la causa de comportamientos sospechosos en el sistema que puede deberse a incompatibilidad de software, hardware o código malicioso.

SANDBOXING

- Uso de Sandboxing en la nube para analizar el comportamiento de archivos, con tiempo máximo de espera para el resultado de análisis de 5 minutos.
- 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.
- 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.

CONSOLA DE ADMINISTRACION CENTRALIZADA

- La consola debe ser con infraestructura en la nube, implementado como un servicio SAAS, adicionalmente debe tener la capacidad de implementarse en forma On-premise.
- La consola de administración debe permitir la configuración y administración remota de la solución antivirus instalada en los puntos finales (Windows, Linux, Mac, Android).
- 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.
- 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: 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 la solución de seguridad con opción a desinstalar 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 contar con una herramienta 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 repositorio instalado en un servidor compatible para que los clientes actualicen desde 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.

6.1.2. REQUISITOS DEL PROVEEDOR.

- Adjuntar DNI en el caso de persona jurídica y/o vigencia de poder en el caso de persona jurídica.
- adjuntar Registro Único de Contribuyentes (RUC), dedicado a la actividad comercial y/o económica.
- adjuntar inscripción vigente en el capítulo servicios del Registro Nacional de Proveedores (RNP).
- Experiencia del postor:
  El postor debe acreditar un monto facturado acumulado equivalente a 3 VECES EL PRECIO OFERTADO, por la contratación de servicios iguales o similares al objeto de la convocatoria, durante los quince (15) años anteriores a la fecha de la presentación de ofertas que se computa desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.

  Se consideran servicios similares a los siguientes: servicio de venta de software antivirus.

  Acreditación:
  La experiencia del postor se acreditará con copia simple de (i) contratos u órdenes de servicios, 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 pago1, correspondientes a un máximo de veinte (20) contrataciones. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados2, para acreditarla

[1] El solo sello de cancelado en el comprobante de pago, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación a que se encuentra cancelado. Es válido el sello colocado por el cliente del postor (sea utilizando el término "cancelado" o "pagado").

[2] Se entiende "privados" como aquellos que no son entidades contratantes.

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 con conformidad o constancia de prestación.

6.2. TIPO DE CONTRATACION:

Tipo de Invitación: Abierta

Tipo de Evaluación: por paquete de ítem

6.3. CRONOGRAMA:

ETAPA	DIAS Y HORA DE INICIO		DIAS Y HORA DE FIN	
Formulación de Consultas (Electrónico)	1 DIA	00:01 Horas	1 DIA	23:59 Horas
Presentación de cotización (Electrónico)	1 DIA	00:01 Horas	1 DIA	23:59 Horas

6.4. LUGAR Y PLAZO DE PRESTACIÓN DEL SERVICIO:

El lugar de prestación del servicio será en las instalaciones del Proyecto Especial tambo Ccaracocha ubicada en la Calle Lambayeque N° 169, Distrito, provincia y departamento de Ica.

El plazo de la prestación del servicio será de cinco (05) días calendarios, que se computará desde el día siguiente de notificada la orden de servicio.

6.5. ENTREGABLES/PRODUCTOS

El servicio por contratar se desarrollará a través de un (01) entregable, indicando el detalle de las actividades desarrolladas, según lo siguiente:

Productos	Descripción	Plazo de presentación y/o fecha de entrega
Único	Deberá presentar un informe con las actividades realizadas, de acuerdo con lo señalado en el numeral 6.1.1 del presente término de referencia	Hasta 05 días calendario después de culminado el plazo del servicio.

6.6. CONFORMIDAD:

La emisión de la conformidad a la prestación del servicio será de responsabilidad de la Unidad de Abastecimiento y Servicios Auxiliares, en un plazo máximo de siete (07) días contabilizados desde el día siguiente de recibido el entregable.

6.7. FORMA DE PAGO

El pago por el servicio se realiza en Único Pago, según el siguiente detalle:

Entregables N°	Descripción	Plazo de presentación	Monto a Pagar (S/)
01	**Primer Informe** de las actividades desempeñadas.	Hasta 05 días calendario después de culminado el plazo del servicio.	100 % del monto contratado

El pago se realizará en un plazo máximo de diez (10) días hábiles luego de otorgada la conformidad por parte de las del Áreas Usuarias (Subjefatura de Obras y Oficina de Administración).

6.8. MODALIDAD DE PAGO

Suma alzada.

6.9. PENALIDADES APLICABLES:

6.9.1. PENALIDADES POR MORA:

En caso de retraso injustificado del contratista 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. La penalidad se aplica automáticamente y se calcula de acuerdo con la siguiente fórmula:

$$\text{Penalidad Diaria} = \frac{0.10 \times \text{Monto}}{F \times \text{Plazo en días}}$$

Dónde: **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 que estos involucraren entregables cuantificables en monto y plazo, al monto y plazo del entregable que fuera materia de retraso, de conformidad con el artículo 120 del Reglamento.

6.9.2. OTRAS PENALIDADES: No aplica

6.10. CONFIDENCIALIDAD:

El proveedor debe indicar mediante declaración jurada la confidencialidad y reserva absoluta en el manejo de la información y documentación a la que se tenga acceso y se encuentre relacionada con la prestación, pudiendo quedar expresamente prohibido revelar dicha información a terceros, en caso corresponda.

6.11. RESPONSABILIDAD POR VICIOS OCULTOS:

La recepción conforme de la entidad no enerva su derecho a reclamar posteriormente por defectos o vicios ocultos. Las discrepancias referidas a defectos o vicios ocultos deben ser sometidas a conciliación y/o arbitraje.

El proveedor es el responsable por la calidad ofrecida y por los vicios ocultos del bien o servicio contratado por un plazo no menor a un (1) año, contado a partir de la conformidad otorgada por el área usuaria.

6.12. DERECHOS Y OBLIGACIONES:

Los derechos y obligaciones del **CONTRATADO** serán exclusivamente los aquí previstos. Por consiguiente, el **CONTRATADO** no tendrá derecho a recibir de la Entidad que corresponda, ni del Gobierno Regional de Ica, ningún beneficio o bonificación.

El **CONTRATADO** será enteramente responsable por demandas y/o denuncias de terceros relacionadas con actos u omisiones imputables al propio **CONTRATADO** en la ejecución del presente Contrato u Orden de Servicio. En ningún caso, se podrá imputar a la Entidad que corresponda, ni al Gobierno Regional de Ica, alguna responsabilidad en relación con dichas demandas y/o denuncias.

6.13. 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 de Contrataciones Públicas. De encontrarse en algunos 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.

Cualquiera de las partes puede resolver, total o parcialmente, el contrato en los siguientes supuestos:

1. Por acumulación del monto máximo de la penalidad por mora o por el monto máximo para otras penalidades, en la ejecución de la prestación a su cargo.

2. Caso fortuito o fuerza mayor que imposibilite la continuación del contrato.
3. Incumplimiento de obligaciones contractuales, por causa atribuible a la parte que incumple.
4. 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.
5. Por incumplimiento de la cláusula anticorrupción.
6. Por la presentación de documentación falsa o inexacta durante la ejecución contractual.
7. 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.

El procedimiento de resolución de contrato será conforme al Reglamento de la Ley N° 32069.

6.14. COMPENSACION POR DAÑOS EN EL SERVICIO:

La Orden de Servicio, no genera derechos de seguros de vida o de incapacidad o de salud para el CONTRATADO.
En caso de incapacidad del CONTRATADO para el cumplimiento del presente contrato, las partes acuerdan que el presente contrato quedará resuelto.
El contratado es responsable por los daños y perjuicios a la Entidad que sus actos, omisiones o demora en la atención y/o ejecución de sus servicios pueda causar. La penalidad no enerva esta responsabilidad para cualquier efecto.

6.15. ANTICORRUPCIÓN Y ANTISOBORNO:

La suscripción de este contrato, o formalización de la orden, EL POSTOR 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 contratante.

Asimismo, EL POSTOR se obliga a mantener una conducta proba e integra 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 POSTOR 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 contratante, 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 POSTOR 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 CONTRATANTE.

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato.

6.16. SOLUCIÓN DE CONTROVERSIAS

Todas las controversias que surjan entre las partes sobre los contratos menores se resuelven mediante conciliación, la cual se regula conforme a lo dispuesto en el numeral 81.3 del artículo 81 de la Ley N° 32069 - Ley General de Contrataciones Públicas.

6.17. 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.

6.18. GARANTÍA:

Conforme al art. 139° del Reglamento de la Ley N° 32069, no se otorga garantía de fiel cumplimiento del contrato ni garantía de fiel cumplimiento por prestaciones accesorias en los siguientes casos: a) En los contratos de bienes y servicios cuyos montos sean menores o iguales a 50 UIT.

6.19. ANEXOS:

No aplica

GOBIERNO REGIONAL DE ICA
PROYECTO ESPECIAL TAMBO CARACOCHA
Ing. Luis Gómez Muro
JEFE DE LA UNIDAD DE SISTEMA Y TECNOLOGÍA DE LA INFORMACIÓN

RESOLUCION JEFATURAL N° 161 -2025-GORE-ICA-PETACC/JP

Ica, 26/09/2025

VISTOS:

La Nota N° 1792-2025-GORE.ICA-PETACC-OA/UASA; Nota N° 075-2025-GORE.ICA-PETACC-OA/USTI; Informe Legal N° 237-2025-GORE.ICA-PETACC-OAJ, y;

CONSIDERANDO:

Que, el numeral 44.6 del artículo 44° del Reglamento de la Ley General de Contrataciones Públicas, refiere, entre otros, que el requerimiento no incluye exigencias desproporcionadas e innecesarias que limiten la concurrencia o favorezcan a determinado proveedor ni hace referencia a procedencia, fabricante, marca, patente, origen o tipos de producción, ni descripción que oriente la contratación hacia ellos, salvo que la autoridad de la gestión administrativa haya aprobado el correspondiente proceso de compatibilización del requerimiento, conforme a las disposiciones que establezca la DGA mediante directiva;

Que, asimismo, en el numeral 12 del Anexo I de Definiciones del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, se define a la Compatibilización del requerimiento como el "proceso de racionalización que realiza la entidad contratante consistente en ajustar a un determinado tipo o modelo los bienes o servicios a contratar, en atención a los equipamientos preexistentes";

Que, la Directiva N°0001-2025-EF/54.01, "Directiva de Compatibilización del Requerimiento", aprobado por Resolución Directoral N°0007-2025-EF/54.01, tiene como objetivo establecer las disposiciones que las entidades contratantes deben observar cuando, de manera excepcional, requieran hacer referencia en el requerimiento para la contratación de bienes o servicios a la procedencia, fabricante, marca, patente, origen o tipos de producción, o la descripción que oriente la contratación hacia ellos;

Que, de acuerdo a lo establecido en los numerales 5.1 y 5.2 de la Directiva, la compatibilización del requerimiento debe responder a criterios técnicos y objetivos que la sustenten, y tiene como finalidad garantizar la funcionalidad, operatividad o valor económico del equipamiento preexistente de la entidad; y para su aprobación debe cumplir con los siguientes presupuestos: a) La entidad contratante posee determinado equipamiento preexistente; b) Los bienes o servicios que se requiere contratar son accesorios o complementarios al equipamiento preexistente, e imprescindibles para garantizar la funcionalidad, operatividad o valor económico de dicho equipamiento;

Que, asimismo el numeral 6.1 de la Directiva establece que el área usuaria o área estratégica elabora un informe técnico sustentando la necesidad de realizar la compatibilización del requerimiento, el cual contiene como mínimo lo siguiente: a) La descripción del equipamiento preexistente de la entidad contratante; b) La descripción del bien o servicio requerido, indicándose la marca o tipo de producto; así como las especificaciones técnicas o términos de referencia, según corresponda; c) El uso o aplicación que se le va a dar al bien o servicio requerido; d) La justificación de la compatibilización del requerimiento, donde se describa objetivamente los aspectos técnicos, la verificación de los presupuestos de la compatibilización señalados y la incidencia económica de la contratación; e) Nombre, cargo y firma de la persona responsable de la evaluación que sustenta la compatibilización del bien o servicio, y del jefe del área usuaria o área técnica estratégica, de ser el caso; f) Periodo de vigencia de la compatibilización del requerimiento, el cual se encuentra sujeto a que se mantengan las condiciones que motivaron la compatibilización; g) La fecha de elaboración del informe técnico;

Que, el numeral 7.1. de la Directiva señala que para iniciar el proceso de contratación de un requerimiento compatibilizado, el área usuaria o el área técnica estratégica, según corresponda, remite a la Dependencia encargada de las contrataciones el informe técnico que sustenta la compatibilización del requerimiento, su documento de aprobación, así como el requerimiento respectivo, a fin de que dicha dependencia realice las actividades necesarias para concretar la contratación del bien o servicio requerido conforme a las disposiciones del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, ya sea mediante un procedimiento de selección competitivo o no competitivo, catálogo electrónico de acuerdos marco, contratos menores u otras modalidades de la contratación pública eficiente, según corresponda;

Que, asimismo señala en el numeral 7.2. del artículo 7° de la Directiva que la Dependencia encargada de las contrataciones, que en este caso la Unidad de Abastecimiento al realizar la estrategia de contratación, es responsable de verificar que, en caso el requerimiento haga referencia a determinada procedencia, fabricante, marca, patente, origen o tipos de producción, o descripción que oriente la contratación hacia ellos, conste en el expediente de contratación;

Que, mediante el Nota N° 075-2025-GORE.ICA-OA/USTI de fecha 16 de septiembre de 2025, el Jefe de la Unidad de Sistemas y Tecnología de la Información sustenta la necesidad de aprobar la "COMPATIBILIZACIÓN DE LA SUSCRIPCION ANUAL DEL SOFTWARE ANTIVIRUS ESET PROTECT ADVANCED EN LA UNIDAD EJECUTORA 1139: PROYECTO ESPECIAL TAMBO CCARACOCHA", por un período de un (01) año;

Que, mediante Nota N° 1792-2025-GORE.ICA-PETACC-OA/UASA de fecha 26 de septiembre de 2025, el Jefe de la Unidad de Abastecimientos y Servicios Auxiliares, señala que luego de verificar aprecia que la Unidad de Sistemas y Tecnologías de la Información ha cumplido con describir los presupuestos que se deben verificar para que proceda la compatibilización conforme a los numerales 5.2 y 6.1 de la Directiva N.° 0001-2025-EF/54.01 – Directiva de Compatibilización del Requerimiento, por lo que considera VIABLE continuar con el trámite de compatibilización; en ese sentido, sugiere la aprobación de la "SUSCRIPCION ANUAL DEL SOFTWARE ANTIVIRUS ESET PROTECT ADVANCED EN LA UNIDAD EJECUTORA 1139: PROYECTO ESPECIAL TAMBO CCARACOCHA", por parte de la Jefatura del PETACC, por un plazo de un (01) año, conforme lo indica la Unidad de Sistemas y Tecnologías de la Información;

Estando a lo expuesto y con el visto de las Oficinas de Administración y de Asesoría Jurídica, y en uso de las facultades conferidas en el Manual de Operaciones del PETACC, aprobado Decreto Regional N° 001-2022-GORE-ICA/GR;

SE RESUELVE:

***Artículo Primero.- APROBAR** el proceso de "COMPATIBILIZACIÓN DE LA SUSCRIPCION ANUAL DEL SOFTWARE ANTIVIRUS ESET PROTECT ADVANCED EN LA UNIDAD EJECUTORA 1139: PROYECTO ESPECIAL TAMBO CCARACOCHA", según Anexo N° 01, por un período de un (01) año, contados a partir del siguiente día de la emisión de la presente resolución;*

***Artículo Segundo.- DISPONER** que la Dependencia Encargada de las Contrataciones del Proyecto Especial Tambo Ccaracocha – PETACC, ejecute las acciones que resulten necesarias en el desarrollo de la siguiente modalidad de adquisición con estricta sujeción a las normas contenidas en la LGCP y su Reglamento.*

***Artículo Tercero.- ENCARGAR** a la Oficina de Tecnologías de la Información, verificar si las condiciones que motivan la presente resolución se mantienen durante el período de vigencia de la compatibilización, quedando sin efecto la presente aprobación de producirse alguna variación a las condiciones que motivaron la presente compatibilización, debiendo informar a la Oficina de Administración.*

***Artículo Cuarto.- DISPONER** que la Unidad de Sistema y Tecnología de la Información, publique la presente Resolución en el Portal Institucional del Proyecto Especial Tambo Ccaracocha – PETACC.*

REGISTRESE Y COMUNIQUESE

GOBIERNO REGIONAL DE ICA
Proyecto Especial Tambo Ccaracocha
ING. LUIS FERNANDO MURGUIA VILCHEZ
JEFE DE PROYECTO