Firmado Digitalmente por: LAURA CASTILLO Jan Jorge FAU 20100188828 soft. Razón: SOY AUTOR DEL DOCUMENTO. Ubicación: Arequipa. Fecha: 11/06/2026 08:10:12

Firmado Digitalmente por: RIZZO REYES Aldo Gonzalo FAU 20100188828 hard. Razón: SOY AUTOR DEL DOCUMENTO. Ubicación: Arequipa. Fecha: 12/06/2026 10:02:34

Firmado Digitalmente por: DE TABOADA QUENAYA Mahgodi Francois FAU 20100188828 hard. Razón: SOY AUTOR DEL DOCUMENTO. Ubicación: Arequipa. Fecha: 15/06/2026 10:40:07

RECIBIDO
15 JUN 2026
UNIDAD DE LOGISTICA
seal

REQUERIMIENTO DE ÁREA USUARIA

Servicio de Renovación de Licencias de una herramienta para Monitoreo y Protección de los endpoints de SEAL

Nº PLD/TIC-0012-2026

1. **Área Usuaria:** Unidad de Tecnologías de la Información y Comunicaciones

2. **Objeto de la contratación:** Se requiere contratar a una persona natural o jurídica que se encargue de la Actualización de Licencias de una herramienta para Monitoreo y Protección de endpoints de SEAL.

3. **Justificación de la necesidad**: SEAL requiere adquirir una solución que permita detectar, contener, dar respuesta a amenazas, teniendo visibilidad de ataques de día cero en forma automatizada con detección local en el dispositivo sin firmas y sin la necesidad de crear o actualizar reglas de detección de forma manual, sin enviar información a la nube, incrementando así el nivel de seguridad de la información y equipamiento informático de SEAL.

4. **Finalidad Pública**
   Incrementar la seguridad en los endpoints de SEAL, asegurando la disponibilidad y seguridad de la información.

5. **Actividad del POI**
   El objetivo estratégico operativo asociado del Plan Operativo Institucional es el OEI 2. Mejorar la Satisfacción del cliente.

6. **Programación de la Necesidad en el CDNM**

   El presente requerimiento de Servicio de Renovación de Licencias de una herramienta para Monitoreo y Protección de endpoints de SEAL tiene la necesidad programada por la Unidad de Tecnologías de la Información y Comunicaciones entre sus requerimientos de contrataciones para el ejercicio del 2026, dentro del CDNM.

7. **Descripción y/o alcance de especificaciones técnicas y/o términos de referencia:**

7.1 Características mínimas requeridas (bien) o actividades a desarrollar (servicio).

Se requiere contratar la renovación de suscripción de 265 Licencias para el Servicio de Adquisición de una herramienta para Monitoreo y Protección de endpoints de SEAL

Se requiere que el Software de Monitoreo y Protección debe cumplir con lo siguiente:

1. **Sistema de administración central**
   1.1. La solución debe proporcionar la consola de administración 100 % en la nube.

1.2. La solución debe tener una plataforma avanzada que centralice datos de tu entorno y de seguridad, facilitando la detección temprana y la respuesta rápida a amenazas al consolidar datos EDR.
1.3. La solución debe permitir la administración de todas las capacidades ofertadas a través de una única consola web.
  1.3.1. La consola debe presentar el título de licencia a nombre del **"Nombre de la empresa"** que puede ser acreditado con el fabricante, a través de la gestión y documentación adicional, que indique como mínimo:
  1.3.2. Plazo de la licencia.
  1.3.3. Total de agentes adquiridos/instalados.
  1.3.4. Políticas aplicadas.

1.4. La consola web debe permitir a los administradores acceder a la interfaz de administración desde cualquier equipo, sin instalar software adicional.
1.5. La solución debe considerar una política centralizada y una arquitectura administrativa que permita el escalamiento de cientos de miles de puntos finales en una sola consola.
1.6. Debe ser una consola multisitio, multiusuario, y multigrupo, sin limitar el número de sitios, ubicaciones, departamentos y entornos geográficamente separados.
1.7. La aplicación de políticas debe de tener la capacidad de heredar en cualquier nivel, y puede ser incluso segmentado por diferentes sitios o ubicaciones.
1.8. La consola debe presentar una base de conocimientos y documentación, sin necesidad de utilizar otras credenciales del sistema.
1.9. La consola debe ser intuitiva y fácil de navegar con flujos de trabajo que permitan responder a incidentes.
1.10. La consola de administración debe permitir el acceso granular, basado en roles y por usuario a nivel de sitios y cuentas globales.
1.11. La solución debe permitir el acceso completo a la API, a todos los recursos de gestión y acceso a datos.
1.12. La API debe estar bien documentada y disponible sin necesidad de configuración especial.
1.13. La solución debe tener fácil acceso a capacidades de ejecutar rápidamente la API en el conjunto de datos de la consola.
1.14. La solución debe admitir 2FA y SSO (SAML 2.0) para acceder a la consola de administración.
1.15. La consola debe mantener y enviar a fuentes externas registros relacionados con la auditoría de actividades realizadas a través de la solución.
1.16. La consola debe mantener todos los datos almacenados cifrados durante el almacenamiento de dispositivos gestionados, incluida la etapa de transmisión de datos.
1.17. La solución ofertada debe estar posicionada en el cuadrante de líderes de Gartner en los últimos seis años.
1.18. La solución ofertada debe participar en el análisis anual de las pruebas de MITRE ATT&CK, demostrando una tasa de detecciones de técnicas de ataque del 100%.

2. Sistemas operativos compatibles

2.1. La solución debe admitir como mínimo, entre otras, las siguientes versiones de sistemas operativos:

2.1.1. Windows Server Core 2012, 2016 e 2019
2.1.2. Windows Server 2019, 2016, 2012 R2, 2012, 2008 R2 SP1
2.1.3. Windows Storage Server 2016, 2012 R2, 2012
2.1.4. Windows 7 Sp1, 8, 8.1, 10
2.1.5. Windows XP SP3
2.1.6. Windows Server 2003 SP2 ou posterior, ou R2 SP2 ou posterior
2.1.7. Windows 2008 (pré-R2)
2.1.8. Microsoft Hyper-V
2.1.9. Oracle VirtualBox
2.1.10. VMware Fusion
2.1.11. VMware Horizon
2.1.12. VMware vSphere
2.1.13. Estaciones de Trabajo VMware
2.1.14. CENTOS
2.1.15. Debian
2.1.16. Red Hat Enterprise Linux (RHEL)
2.1.17. Servidor empresarial SUSE Linux
2.1.18. Ubuntu

2.2. Debe admitir implementaciones en la nube de forma nativa, como mínimo para las nubes de AWS, AZURE y GOOGLE CLOUD.

2.3. El periodo de validez de los agentes y consola de administración debe ser el mismo, siendo considerado desde la activación de la consola de administración central y finalizando según vigencia del contrato.

2.4. Todo soporte de solución debe considerar el período de licencia activada.

3. Agente

3.1. La solución debe proporcionar capacidades de respuesta de detección de puntos finales de protección de terminales (EPP/EDR) disponible en un solo agente sin necesidad u obligación de instalar varios paquetes de software.

3.2. Debe ser una solución de agente único, sin módulos adicionales, que se instalará en equipos, portátiles, servidores o máquinas virtuales, en sistemas operativos Windows, Linux y MacOS.

3.3. El agente debe asegurarse de que un usuario final (incluso con credenciales de administrador local) no puede eliminar, desactivar o modificar el producto de ninguna manera (anti-tamper).

3.4. El agente debe tener la capacidad de iniciar la tarea de buscar malware o garantizar que se ha solucionado una amenaza (desde la consola y/o el endpoint).

3.5. Los agentes deben poder recibir programaciones de la consola de administración, individualmente o por grupos.

3.6. La solución debe permitir limitar el número de agentes que pueden descargar una actualización en un momento dado.

3.7. La actualización de los agentes no debe afectar al usuario final.

3.8. Si el número de instalaciones de agentes alcanza un número superior al contratado por este proceso, la solución debe mantener su funcionamiento normal.
3.9. La solución debe tener una función para la cancelación automática de los agentes que no se comunican con la consola administrativa después de un cierto período de tiempo.
3.10. La solución debe permitir desactivar temporalmente el agente a través de la consola administración para solucionar problemas o ejecutar pruebas temporales
3.11. El agente no debe solicitar un reinicio del sistema cuando se realiza una actualización de versión.
3.12. El agente de Windows debe ejecutarse en el espacio del kernel para garantizar el máximo nivel de protección contra manipulación (anti-tamper).
3.13. La solución debe exportar inventarios de dispositivos/agentes, o como mínimo, CSV.
3.14. La solución debe permitir la aplicación de políticas de forma dinámica a los agentes según la información de metadatos de los proveedores de la nube.
3.15. La solución debe proporcionar la capacidad de enviar mensajes de notificación a la computadora del usuario final

4. Prevención de amenazas

4.1. La solución debe proporcionar prevención en todos los principales sistemas operativos, siendo al menos Windows, Linux y MacOS.
4.2. La solución debe brindar protección contra malware conocido y desconocido.
4.3. La solución debe examinar los archivos a medida que el disco duro los lee o escribe.
4.4. La solución debe brindar protección contra ataques de día cero, a través del análisis de comportamiento en el punto final, sin depender de firmas.
4.5. La solución debe proteger el endpoint contra malware, incluso cuando el sistema no esté conectado a la red.
4.6. El agente no debe depender de la consola de administración, la nube o cualquier otro recurso externo para detectar y responder correctamente a amenazas sofisticadas (día cero, sin archivos, basados en RAM, cero exploits diarios, ransomware, mineros, movimiento lateral, APT) en tiempo real, a medida que se detectan amenazas.
4.7. El agente debe ser autónomo, debe realizar detección y mitigación y respuesta en tiempo real ante ataques en el endpoint, sin dependencia de otros controles de seguridad e intervención de un Centro de Operaciones de Seguridad (SOC).
4.8. El agente debe revisar la información del proceso en el dispositivo antes de enviar información de alerta a la consola de administración y remediación automática, reduciendo el tiempo de detección y remediación de un ataque.

4.9. El agente debe utilizar inteligencia artificial o recursos de aprendizaje automático para analizar archivos antes de su ejecución y comportamiento mientras se ejecuta un archivo.
4.10. La solución debe brindar protección contra documentos y scripts maliciosos.
4.11. La solución debe monitorear y proteger los movimientos laterales.
4.12. La solución debe buscar programas potencialmente no deseados.
4.13. La solución debe monitorear y proteger contra amenazas internas.
4.14. La solución debe tener la opción de garantizar la descarga segura de un archivo o archivo malicioso enviado a cuarentena.
4.15. Los datos de alerta de incidentes deben estar disponibles durante al menos 365 días.
4.16. La solución debe presentar visualmente un árbol de procesos para eventos maliciosos y no maliciosos.
4.17. La solución debe tener la capacidad de etiquetar un grupo completo de eventos, o eventos aislados, como una amenaza y tomar medidas de respuesta, mitigación y/o remediación

5. Capacidades de respuesta y remediación

5.1. Debe soportar la gestión a través de un shell remoto completo.
5.2. No se aceptará un conjunto limitado o restringido de comandos a través del acceso al Shell.
5.3. El acceso remoto a través de shell debe ser rastreado y registrado, para garantizar la veracidad y seguridad de cada acceso.
5.4. Debe poder alertar sobre comportamientos de amenazas sospechosos y maliciosos.
5.5. La solución debe poder actuar sobre un proceso malicioso, archivos que están en cuarentena y también puede eliminar la cuarentena de un archivo a través de la consola de administración de forma centralizada o mediante API.
5.6. La solución debe poder deshacer cualquier cambio del sistema relacionado con un ataque, como ediciones del registro, cambios de configuración, etc.
5.7. Debe tener la capacidad de revertir cambios a archivos afectados durante un incidente en máquinas Windows (rollback) sin tener la necesidad de utilizar secuencia de comandos y debe ejecutarse manera automatizada, y/o con un solo con 1 solo clic desde la consola en caso de ataques de ransomware. No debe de tener límite de numero de archivos o tamaño de archivos. Se debe de soportar archivos de 100 megas o más.
5.8. La acción de reversión debe poder recuperar archivos eliminados o cifrados en caso de un ataque de ransomware, y restaurar archivos a su estado previo al ataque
5.9. Debe poder poner en cuarentena un dispositivo en la red.
5.10. Debe poder configurar la política de cuarentena para dispositivos de red.
5.11. Debe poder automatizar respuestas.
5.12. Se podrán tomar acciones correctivas en múltiples sistemas o eventos al mismo tiempo.

5.13. Debe poder agregar notas/comentarios a un evento.
5.14. Debe ser capaz de establecer el estado de un problema o evento (por ejemplo: resuelto, en curso, no resuelto).

6. Política de instalación

6.1. Debe ser capaz de aplicar políticas a una cuenta, sitio o grupo de dispositivos.
6.2. Debe ser capaz de soportar la asignación de políticas dinámicas de acuerdo con los atributos del dispositivo.
6.3. Los agentes podrán ser instalados y asignados directamente a un grupo específico de dispositivos en el momento de la instalación.
6.4. El contexto de la política debe proporcionar la opción de activar o desactivar tipos específicos o por motores (mecanismos de ejecución previos y en tiempo de ejecución).
6.5. Debe ser capaz de aplicar las políticas de forma rápida, considerando el tiempo real.

7. Exclusiones

7.1. La solución debe contar con una lista predefinida de exclusiones conocidas o recomendadas.
7.2. Debe ser capaz de excluir fácilmente falsos positivos.
7.3. Debe permitir a los administradores de consola ejecutar exclusiones de políticas en varios niveles (cuenta, sitio, grupo).
7.4. Debe ser capaz de sincronizar acciones entre el nivel de cuenta y administración para que las exclusiones establecidas no necesiten ser recreadas.
7.5. Debe permitir a los administradores configurar exclusiones para suprimir independientemente alertas relacionadas con el aprendizaje automático basadas en archivos y/o mecanismos de comportamiento.
7.6. Debe permitir a los administradores configurar las exclusiones para manejar problemas de interoperabilidad en rutas ejecutables específicas o exclusivas, reduciendo el monitoreo de los procesos principales y/o junto con todos sus procesos secundarios generados.
7.7. Debe permitir a los administradores configurar las exclusiones para abordar problemas de rendimiento en rutas individuales o ejecutables específicas que interrumpen la supervisión de los procesos principales y/o procesos junto con todos sus procesos secundarios generados.
7.8. Debe permitir a los administradores de consola realizar exclusiones mediante un hash, path, certificado, browser o tipo de archivo.

8. Control de dispositivos y visibilidad de aplicaciones

8.1. La solución debe ofrecer bloqueo de medios USB externos, función de solo lectura y función de escritura o lectura para estos dispositivos.
8.2. La solución debe ofrecer bloqueo de dispositivos Bluetooth externos.
8.3. El control de dispositivos USB debe ser lo suficientemente granular como para aplicarse a un número de serie o tipo de dispositivo específico.

8.4. La solución debe identificar aplicaciones de software de terceros sin parches que puedan tener vulnerabilidades.
8.5. La solución debe proporcionar un inventario de todas las aplicaciones instaladas en todos los equipos de la empresa.
8.6. La solución debe contar con las funcionalidades de control de dispositivos (Bluetooth y thunderbolt)

9. Funcionalidad - Control de Firewall

9.1. La solución debe ser capaz de habilitar funciones de firewall en los agentes instalados en los dispositivos.
9.2. La activación de reglas de firewall en los agentes debe tener prioridad sobre el firewall nativo de los dispositivos Windows y/o Linux.
9.3. La solución podrá crear una única regla de firewall para aplicarse en grupos y en distintos sistemas operativos.
9.4. Las reglas de firewall podrán ser creadas para aplicarse a un grupo específico de dispositivos (utilizando grupos de etiquetado o políticas).

10. Integraciones

10.1. La solución debe ser compatible con Active Directory, soportar la lectura de grupos, múltiples dominios y bosques.
10.2. La solución debe tener integraciones con VirusTotal.
10.3. La solución podrá transmitir datos de EDR en tiempo real al Data Lake interno.
10.4. La solución podrá enviar registros de eventos a través de syslog.

11. Soporte y servicios

11.1. La solución debe proporcionar respuesta y detección gestionada con todas las funciones.
11.2. La solución debe ofrecer la opción de contar con un administrador de cuenta técnica o un nivel de soporte más alto.
11.3. El fabricante de la solución ofrecida debe estar disponible 24x7x365.

12. Paneles e informes

12.1. Debe presentar todas las vulnerabilidades conocidas en los programas instalados.
12.2. Debe permitir la exportación de la información.
12.3. Los datos podrán ser exportados a informes de terceros como Tableau o PowerBi.

7.2 Cantidad del Requerimiento

01 Servicio de adquisición de Licencias de una herramienta para Monitoreo y Protección de endpoints de SEAL.

7.3 Código del material (EN CASO DE COMPRAS)

No Aplica.

7.4 Garantía del Bien/Servicio

La licencia del producto ofrecido deberá contar con una garantía de un (01) año.

El tiempo de vigencia de las licencias y servicios de actualización será de 365 días calendario (12 meses)

7.5 Características del proveedor

- El contratista deberá presentar el documento emitido por el fabricante o representante de la marca en PERÚ, que acredite ser partner autorizado de la marca.
- Declaración jurada que Acredite contar con un Centro de Atención al Usuario local.
- Declaración jurada que acredite contar con un NOC/SOC local y una mesa de servicio.
- El postor debe acreditar una experiencia mínima de S/. 80,000.00 (ochenta Mil con 00/100 soles), por la contratación de servicios iguales o similares al objeto del presente requerimiento. Se consideran servicios similares a los siguientes: Venta y/o Licenciamiento y/o Renovación de software y/o software de seguridad y/o protección informática.

Acreditación:
La experiencia del postor en la especialidad se acreditará con copia simple de: copias simples (i) contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia en servicios iguales o similares a los solicitados

7.6 Características del personal requerido

No Aplica.

7.7 Infraestructura, equipo / herramientas (OPCIONAL)

No Aplica.

7.8 Medidas de Seguridad a Adoptarse

La Contratista debe cumplir con:

a) Ley N° 29783, Ley de Seguridad y Salud en el Trabajo y sus modificatorias vigentes.
b) Reglamento de la Ley de Seguridad y Salud en el Trabajo, D.S. 005-2012-TR y sus modificatorias vigentes.
c) Reglamento de Seguridad y Salud en el Trabajo con Eléctricas, Resolución Ministerial N° 111-2013/MEM/DM y sus modificatorias vigentes.
d) Código Nacional de Electricidad: suministro, Resolución Ministerial N° 214-2011-MEM DM. Parte 4 "Reglas generales para los trabajadores".
e) Normas Técnicas de Seguro Complementario de Trabajo de Riesgos, D. S. N° 003-98 SA.

f) R.M. N° 050-2013-TR Formatos Referenciales con la información mínima que deben contener los registros obligatorios del sistema de gestión de seguridad y salud en el trabajo
g) D.S N° 009-2020-TR Aprueba Normas reglamentaria D.U. N° 044-2016 Seguro Vida Ley
h) R.M. 312 -2011 – MINSA Documento técnico protocolos de exámenes medico ocupacionales y guías de diagnóstico de los exámenes médicos obligatorios por actividad y sus modificatorias vigentes.
i) RM-004-2014-MINSA Modificatoria del Documento Técnico Protocolos De Exámenes Médicos Ocupacionales y Guias de Diagnóstico de los Exámenes Médicos Obligatorios por actividad.
j) Código Nacional de Electricidad – Utilización 2006 (en caso corresponda)
k) Reglamento Nacional de Tránsito.
l) Otros dispositivos legales y otros requisitos solicitados por el área de seguridad y salud en el trabajo.

La Ley de Seguridad y Salud en el Trabajo (LSST) establece que la empresa principal es responsable de coordinar y vigilar que sus contratistas cumplan la normativa en sus instalaciones, asumiendo el incumplimiento si no lo hace. La empresa debe exigir a sus proveedores el cumplimiento de las normas de Seguridad y Salud en el Trabajo (SST), considerando que es una obligación legal de la empresa principal para garantizar un entorno seguro en su centro de trabajo, respondiendo solidariamente por incumplimientos de contratistas. Esto implica coordinar, verificar su documentación (IPER, política SST) y exigir procedimientos claros, pues la falta de control conlleva sanciones y responsabilidad solidaria por daños.

- ✓ **Documentación:** La matriz IPER (Identificación de Peligros, Evaluación de Riesgos y Medidas de Control), políticas de SST, Reglamento Interno de SST, y otros documentos obligatorios.
- ✓ **Procedimientos**: Presentación de procedimientos específicos para tareas de alto riesgo (trabajos en altura, espacios confinados, bloqueos, etc.) según corresponda.
- ✓ **Capacitación:** Prueba de que sus trabajadores están capacitados en SST.
- ✓ Verificación: Realizar inspecciones periódicas y usar listas de chequeo (checklists) para confirmar el cumplimiento del proveedor.

7.9 Medidas para Protección de Medio Ambiente a Adoptarse

La Contratista debe cumplir con:
a) Ley N° 28611: Ley General del Ambiente.
b) Decreto Supremo N° 014-2019-EM: Reglamento para la Protección Ambiental en las Actividades Eléctricas del Ministerio de Energía y Minas.
c) Decreto Legislativo N° 1278: Ley de Gestión Integral de Residuos Sólidos.
d) Resolución Ministerial N°0021-2021-MINEM/DM, Aprueban la "Guía Metodológica para la elaboración del Plan de Gestión Ambiental de Bifenilos Policlorados (PGAPCB) aplicable a la actividad eléctrica" y la "Guía Metodológica para el Inventario de Existencias y Residuos para la identificación de Bifenilos Policlorados (PCB)" (en caso corresponda).
e) Decreto Supremo N°018-2025-SA que aprueba el Reglamento Técnico para la Gestión Sanitaria y Ambiental para los Bifenilos Policlorados (en caso

corresponda).

f) Resolución Ministerial N°0200-2025-MINAM, Guía para la Descripción de Proyectos de Inversión en el Marco del Sistema Nacional de Evaluación del Impacto Ambiental" (en caso corresponda)
g) Resolución Ministerial N°392-2025-MINEM/DM, Aprueban Lineamientos de Gestión Ambiental de Proyectos Calificados como Sistemas Eléctricos Rurales (SER) (en caso corresponda).
h) Otros dispositivos legales – normatividad que esté relacionada a la gestión ambiental aplicables al sector.

NOTA: La Contratista deberá revisar, implementar y cumplir, según corresponda, lo establecido en los siguientes documentos, los cuales se encuentran publicados en la página web de SEAL, debiendo considerarse su última versión vigente:

- RE-05-02 "Reglamento de Seguridad, Salud en el Trabajo y Medio Ambiente para Empresas Contratistas de SEAL".

- MT-05-29 "Profesiograma para empresas contratistas y visitantes".

Link:
https://www.seal.com.pe/seguridad%20y%20medio%20ambiente/Seguridad/Forms/AllItems.aspx

Asimismo, los exámenes médicos ocupacionales deberán realizarse en un Servicio de Atención Médica Ocupacional (SAMO) debidamente acreditado por DIGESA o GERESA, según corresponda.

De igual manera, los Certificados de Aptitud Médica Ocupacional (CAMO) deberán ser claros y legibles, y contar con la firma del médico ocupacional, quien debe estar registrado con Registro Nacional de Especialidad (RNE) y/o Registro Nacional de Maestría (RNM).

La información solicitada constituye un requerimiento mínimo y se encuentra alineada al marco normativo vigente; sin embargo, ello no limita la facultad de SEAL de solicitar requisitos adicionales que considere necesarios para asegurar el cumplimiento legal y la adecuada gestión de SSTMA.

7.10 Prestaciones complementarias (OPCIONAL)

No Aplica.

7.11 Penalidades

a) 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:

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

Donde F tiene los siguientes valores:

- Para bienes y servicios: F = 0.40

- Para obras:
  a) Para plazos menores o iguales a sesenta días: F = 0.40.
  b) Para plazos entre sesenta y uno a ciento veinte días: F = 0.25.
  c) Para plazos mayores a ciento veinte días: F = 0.15

- Para consultorías de obras:
  a) Para plazos menores o iguales a sesenta días: F = 0.40.
  b) Para plazos mayores a sesenta días: F = 0.25.

7.12 Resolución y/o nulidad

Resolución

a) En el caso que el contratista incumpla injustificadamente las condiciones de la prestación del servicio o demás condiciones contractuales, se le podrá requerir mediante carta simple o notarial el cumplimiento de sus obligaciones, otorgando para ello un plazo no mayor de diez (10) días calendario para su subsanación.
b) En caso de persistir el incumplimiento se dispondrá a través de otra carta simple o notarial emitida por el Equipo de Contrataciones de la Unidad de Logística, la resolución del pedido de compra. En ese caso, se iniciará una nueva contratación en caso el área usuaria persista con la necesidad.
c) Cuando se llegue a cubrir el monto máximo de la penalidad, la entidad podrá resolver el pedido de compra, parcial o totalmente por incumplimiento, mediante carta simple o notarial suscrita por el área usuaria.

Nulidad

a) Cuando contravengan las normas legales, contengan un imposible jurídico o prescindan de las normas o formas esenciales.
b) Por contravenir a lo establecido en el artículo 11° de la Ley N° 30225, Ley de Contrataciones del Estado o norma que la sustituya o modifique.
c) Cuando se verifique que la trasgresión del principio de presunción de la veracidad durante el procedimiento, previo descargo.

7.13 Obligaciones del Contratista

SEAL requiere contratar a una persona natural o jurídica que provea los servicios solicitados tiene las siguientes obligaciones:

A. Entregar los servicios y licencias en los plazos indicados.
B. Cumplir con los compromisos ofertados en tiempo y calidad

Nota: Para el caso de contratación de servicios "El Contratista está en la obligación de mantener la confidencialidad de la información que le proporcione SEAL y a la que tenga acceso con ocasión de la ejecución del servicio. Dicha obligación se mantendrá vigente durante la ejecución contractual y hasta 180 días calendario de culminada la misma."

7.14 Obligaciones de SEAL

Las principales obligaciones de SEAL durante la vigencia del contrato serán:

A. Cumplir con el pago de los comprobantes validos dentro del tiempo pactado.
B. Dar las facilidades al proveedor para la entrega de los bienes en los almacenes de SEAL

8. Sistema de contratación

La Contratación del Servicio de Renovación de Licencias de una herramienta para Monitoreo y Protección de endpoints de SEAL, se realizará bajo el sistema de Suma alzada.

9. Plazo de ejecución contractual, informes y entregables

El plazo de ejecución para la renovación de Licencias de una herramienta para Monitoreo y Protección de endpoints de SEAL deben ser activados hasta en un plazo no mayor a 7 días calendario contados a partir del envio de la Orden de Compra o firma del contrato.

10. Lugar de ejecución del servicio/adquisición/consultoría:

Los servicios de configuración e instalación serán ejecutados en las oficinas de SEAL en Consuelo 310 cercado Arequipa y en las sedes que el área de TIC se les indique presencial o remotamente

11. Entregables y lugar de presentación.

Certificado de vigencia de las licencias emitido por la marca.

12. Conformidad del servicio/bien

La conformidad del servicio/bien estará a cargo de la Unidad de Tecnologías de la Información y Comunicaciones en un plazo máximo de 7 días calendario desde la presentación del entregable o entrega del bien, que comenzará a computarse a partir de la verificación y **aceptación** del comprobante de pago presentado; de no ser conforme será rechazado y no admitida su presentación.

13. Forma de pago

La Entidad realizará el pago de la contraprestación pactada a favor del contratista en un solo pago.

Documentos para efectos de pago:

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, la entidad debe contar y presentar con la siguiente documentación

Para el caso de Servicios

La necesidad de registrar las operaciones en tiempo real o según los nuevos plazos previstos en la norma como el DL 1669, para no perder el crédito fiscal del IGV, los comprobantes electrónicos deben anotarse en el mes de emisión, así como los emitidos por operaciones sujetas al SPOT, en el periodo en que se hayan anotado el comprobante de pago respectivo en el Registro.

Los comprobantes de pago electrónicos (facturas) deben ser presentados en mesa de partes virtual solo cuando se cuente con el acta de conformidad validada y el informe firmado por el administrador del contrato, de lo contrario será rechazada la presentación del comprobante.

Con el fin de fortalecer los mecanismos de control y modernización de la gestión tributaria, enfocándose en la fehaciencia (veracidad y prueba) de las operaciones exige mayor diligencia y oportunidad en el registro contable, se requiere el siguiente sustento:

a) Comprobante de pago electrónico – (adjuntar el archivo PDF, XML y CDR), el CDR no debe de tener observaciones de recepción por SUNAT, la emisión de los comprobantes de pago electrónicos se debe de considerar los **requerimientos adicionales**, los **requisitos mínimos** y la **condición de emisión**.
b) Informe del proveedor debidamente firmado y visado por el administrador del contrato (de tratarse de informe con carácter confidencial el área usuaria emitirá informe indicando que obra en su poder y bajo custodia) el mismo que debe encontrarse adjunto con el informe del proveedor
c) Copia del pedido de compra o contrato (incluir adendas), debidamente firmados. El pedido de compra debe estar recepcionado por el proveedor con su firma, sello y fecha.
d) En el caso de empresas de intermediación o tercerización, deberán presentar el sustento de boletas de pago de remuneraciones, así como los voucher de transferencia, constancia de pago de los aportes y descuentos, EsSalud, AFP, ONP, SUNAT, y los que les corresponda de acuerdo a las normas sociolaborales vigentes.
e) Certificado de cuentas bancarias emitida por la entidad del sistema financiero de la empresa (tienen que estar activas).

Los mencionados documentos deben ser presentados por mesa partes física o virtual.

La Entidad debe pagar las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días hábiles siguientes de otorgada la conformidad de los bienes, servicios o consultoría servicios, siempre que se verifiquen las condiciones establecidas en el contrato para ello, bajo responsabilidad del servidor competente.

14. Confidencialidad y Propiedad Intelectual

La información y material producido bajo los términos de este servicio/adquisición, tales como escritos, medios magnéticos, digitales, y demás documentación generados por el servicio, pasará a propiedad del SEAL. El proveedor deberá

mantener la confidencialidad y reserva absoluta en el manejo de la información y documentación a la que se tenga acceso relacionada a la prestación.

15. **Responsabilidad por Vicios Ocultos**
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.

16. **Cláusula de cumplimiento (Ley de prevención y mitigación del Conflicto de interés en el acceso y salida de personal del Servicio público, 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 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

17. **Cláusula Anticorrupción y Antisoborno**

- El contratista declara conocer los compromisos antisoborno del OECE, el cual se estable en su Política del Sistema Integrado de Gestión y se encuentra disponible en el portal web del OECE:
https://www.gob.pe/institucion/osce/campa%C3%B1as/1861-politica-del-sistemaintegrado-de-gestion-del-osce
- A la suscripción de este contrato, El Contratista declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a los evaluadores del proceso de contratación o cualquier servidor de la entidad contratante. Asimismo, El Contratista se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo, en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente. Aunado a ello, El Contratista se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, actores del proceso de contratación y/o cualquier servidor de la 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 Contratista se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con La Entidad Contratante.

- 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 Contratante el derecho de resolver total o parcialmente el contrato. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar3
- El proveedor se compromete a denunciar, en base de una creencia razonable o de buena fe cualquier intento de soborno, supuesto o real, que tuviera conocimiento a través del canal de denuncias de soborno ubicado en el portal web del OECE

18. Acuerdo de Confidencialidad

- El contratista se compromete a guardar reserva de la información privilegiada que conociera en el ejercicio de sus funciones, tareas y demás actividades como parte de la ejecución de la prestación, no revelando en forma oral, escrita, ni por cualquier otro medio, hechos, datos, procedimientos, documentación e información de acceso restringido (confidencial), a la que tuviera acceso a partir del inicio de las prestaciones relacionadas con el referido servicio, manteniendo la confidencialidad de la misma, de manera permanente.
- De igual manera se compromete a cumplir con: la Política Integrada de la Gestión de la Calidad ISO 9001, Gestión de Seguridad de la Información ISO 27001 y Gestión Antisoborno ISO 37001 de SEAL, las Políticas de Seguridad de la Información de SEAL, y demás normas y Leyes correspondientes a seguridad de la información, vigentes.
- En caso de que incumpliera con cualquiera de las obligaciones estipuladas en el presente acuerdo, SEAL está autorizado a iniciar todas las acciones judiciales o extrajudiciales necesarias para resarcir del perjuicio, y la obligación de confidencialidad perdurará mientas la información conserve las características para considerarse Confidencial.

19. 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.

20. Solución de Controversias

Todos los conflictos que se deriven de la ejecución e interpretación de la presente contratación son resueltos mediante trato directo o conciliación.

21. Cláusula de Compliance en Contratos de Bienes y Servicios

El CONTRATISTA se compromete a respetar los principios y valores establecidos por SEAL. Como muestra de su responsabilidad, se compromete a mantener una política de tolerancia cero frente al incumplimiento de las obligaciones legales que le resulten aplicables. En caso de que el contratista tenga conocimiento o sospechas de que alguno de sus trabajadores o representantes participe, de forma activa o pasiva, en conductas que puedan constituir una infracción a las obligaciones de compliance que involucren a SEAL, deberá comunicarlo de manera inmediata a través del Canal de Denuncias de SEAL. Asimismo, el CONTRATISTA se compromete a garantizar que ninguno de sus trabajadores y/o representantes realice actos que puedan comprometer el cumplimiento legal relacionado con el servicio prestado a SEAL. El CONTRATISTA declara conocer y se obliga a cumplir la Política de Compliance de SEAL, disponible en la siguiente ruta web: https://www.seal.com.pe/compania/PageWeb/politica_integrada_seal.aspx.

El CONTRATISTA se compromete a capacitar a su personal en las obligaciones legales y compromisos de compliance que correspondan al servicio prestado a nombre de SEAL.

El CONTRATISTA que anula un CPE (Comprobante de Pago Electrónico) ya pagado, la empresa tomará las acciones inmediatas como: requerir su corrección vía **carta notarial**, exigir la emisión de un CPE ratificatorio o nuevo conforme a la Ley, aplicar penalidades por incumplimiento y si es necesario, iniciar la resolución del contrato y gestionar con el área legal de la empresa reclamar daños y perjuicios, dejando constancia de todo por escrito para minimizar contingencias tributarias y evitar futuras infracciones tributarias o legales. Así mismo evaluar la presentación de la denuncia ante SUNAT, por una presunta evasión tributaria.

22. Fecha y Firma del usuario en todos los folios del requerimiento

CEGE (dato presupuestal):	2A20406000
CECO (dato controlling):	2A20406005
Posición Presupuestaria (dato contrable – presupuestal):	6344001000
Cuenta de Destino (dato controlling):	
Código de actividad	

Aprobación de Jefatura	Aprobación de Gerencia	Unidad de Presupuesto	Unidad de Contabilidad
Firmado Digitalmente	Firmado Digitalmente	V°B° (CONFORMIDAD)	V°B° (CONFORMIDAD)

Para el caso de adquisición de bienes, se debe contar con el V°B° del Jefe de Equipo de Almacenes de la Unidad de Logística, el mismo que certificará la necesidad del requerimiento de acuerdo al stock de los bienes que obran en el almacén y su rotación.

Aprobación de Jefe de Equipo de Almacenes V°B° (CONFORMIDAD)

Administrador del contrato: Jan Jorge Laura Castillo

Elaborado por: Jan Jorge Laura Castillo

Nota:

- En el caso de que el elaborador sea un cargo CAP se colocará el Código y en caso sea un personal de Apoyo se colocará el DNI.
- Es indispensable que todos los folios del requerimiento estén debidamente visados por el Usuario responsable, numerados y se consigna el cargo de la fecha de entrega de este a la Unidad de Logística.