ANEXO N° 2

TÉRMINOS DE REFERENCIA PARA LA CONTRATACIÓN DE SERVICIOS

Unidad Orgánica	Unidad de Tecnologías de la Información
Meta Presupuestaria	0020
Actividad del POA	RO.PRO.TI.1 Implementación de Controles, Normas, Procedimientos en el Marco del Sistema de Gestión de Seguridad de Información.
Denominación de la Contratación	**Servicio de soporte sistema de seguridad protección anti-malware**

Unidad de Organización	Unidad de Tecnologías de la Información
Meta Presupuestaria	0026 – Fuente ROOC
Actividad del POA	4.4.3. Contratación de bienes y servicios
Denominación de la Contratación	**Servicio de soporte sistema de seguridad protección anti-malware del proyecto "Mejoramiento y Ampliación de los Servicios de CTI para fortalecer el Sistema Nacional de Ciencia, Tecnología e Innovación"**

1. Finalidad Pública

Coadyuvar a fortalecer la capacidad institucional y organizacional de PROCIENCIA garantizando el desarrollo de las actividades del personal y de los consultores del proyecto "Mejoramiento y ampliación de los servicios de CTI para fortalecer el Sistema Nacional de Ciencia, Tecnología e Innovación" en el uso de los equipos de cómputo y servicios de comunicaciones informáticas como son el internet, correos electrónicos, sistemas de información entre otros.

2. Antecedentes

El Texto Único Ordenado de la Ley N° 28303, Ley Marco de Ciencia, Tecnología e Innovación Tecnológica, aprobado por Decreto Supremo N° 032-2007-ED, y la Ley N° 28613, Ley del Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica - CONCYTEC, establecen que el CONCYTEC es el organismo rector del Sistema Nacional de Ciencia, Tecnología e Innovación Tecnológica – SINACYT, encargado de normar, dirigir, orientar, fomentar, coordinar, supervisar y evaluar las acciones del Estado en el ámbito de la ciencia, tecnología e innovación tecnológica y promover e impulsar su desarrollo mediante la acción concertada y la complementariedad entre los programas y proyectos de las instituciones públicas, académicas, empresariales, organizaciones sociales y personas integrante del SINACYT.

Que, mediante Ley N° 30806, Ley que Modifica Diversos Artículos de la Ley N° 28303, Ley Marco de Ciencia, Tecnología e Innovación Tecnológica, y de la Ley N° 28613, Ley del CONCYTEC, se modifica, entre otros, el artículo 16 de la Ley N° 28303, señalándose que el Fondo Nacional de Desarrollo Científico, Tecnológico y de Innovación Tecnológica – FONDECYT, es una unidad de ejecución presupuestal del CONCYTEC, con patrimonio propio, encargado de captar, gestionar, administrar y canalizar recursos de fuente nacional y extranjera destinados a las actividades del SINACTI, en el país.

Que, mediante Decreto Supremo N° 051-2021-PCM publicado en el diario oficial El Peruano el 25 de marzo de 2021, se crea el Programa Nacional de Investigación Científica y Estudios Avanzados, sobre la base del Fondo Nacional de Desarrollo Científico, Tecnológico y de Innovación Tecnológica, al cual PROCIENCIA absorbe por fusión en calidad de entidad absorbente. PROCIENCIA se encuentra bajo la dependencia de EL CONCYTEC, ente rector del SINACTI.

El Estado peruano, con el Decreto Supremo N°054-2022-EF del 30 de marzo de 2022, aprueba la operación de endeudamiento externo hasta por la suma de US$ 100,0 millones, con el Banco Internacional de Reconstrucción y Fomento (en adelante BM) para financiar parcialmente el "Proyecto de Mejoramiento y Ampliación de los Servicios de CTI para fortalecer el Sistema Nacional de Ciencia, Tecnología e Innovación" (en adelante Proyecto), suscribiéndose el Contrato de Préstamo N°9334-PE el 18 de mayo de 2022, con el objetivo de mejorar los servicios de ciencia, tecnología e innovación en áreas estratégicas y regiones del país priorizadas, con el fin de mejorar la competitividad del Perú. El proyecto tiene una duración global de sesenta y cuatro (64) meses.

El Proyecto consta de los siguientes componentes:

Componente 1: Fortalecimiento de las Instituciones y la Gobernanza del Sistema Nacional de Ciencia, Tecnología e Innovación (SINACTI) para Impulsar la Innovación en Perú.

Este componente fortalecerá la gobernanza del SINACTI al mejorar la capacidad de sus instituciones para apoyar el desarrollo de las capacidades de ciencia, tecnología e innovación y mejorar sus contribuciones al desarrollo sostenible y al

cambio climático. Las actividades del componente 1 permitirán las actividades planificadas en los componentes 2 y 3 mejorando la capacidad para gestionar los instrumentos de apoyo a la investigación, desarrollo e innovación (en adelante "I+D+i").

Componente 2: Desarrollo de capacidades para la generación de conocimiento en Área Estratégicas.
Este componente tiene como objetivo el desarrollo de capacidades para la generación de conocimiento en sectores priorizados, cuyo objetivo es impulsar y fortalecer las capacidades del Sistema Nacional de Ciencia, Tecnología e Innovación, a través del financiamiento de alianzas institucionales, equipamiento científico y el desarrollo de proyectos de I+D+i.
Este componente incluye el financiamiento de becas para que ciudadanos peruanos realicen formación doctoral en los programas de doctorado y cofinanciará subvenciones para apoyar la investigación, el desarrollo tecnológico y la innovación con orientación a la demanda y de alta relevancia apoyados en las Áreas Estratégicas.

Componente 3: Fortalecimiento de los vínculos entre la industria y el mundo académico para acelerar la transferencia de tecnología y la innovación empresarial basada en la Ciencia.
Este componente tiene como objetivo mejorar la relevancia de los productos de I + D para la demanda del mercado principalmente en las Áreas Estratégicas, con al menos el 50 por ciento del financiamiento total del componente destinado al Área Estratégica de Clima.

Componente 4: Gestión de proyectos y seguimiento y evaluación.
Este componente tiene como objetivo apoyar a la gestión del proyecto, el cual será conducido por un equipo de especialistas, técnicos, adquisiciones, ambientales y sociales financieros y de monitoreo y evaluación. El componente también cubrirá consultorías y asistencia técnica que refuercen las medidas de mitigación y adaptación climática durante la implementación y apoyen el monitoreo y evaluación rigurosos de los indicadores relacionados con el clima.

3. Objetivos de la Contratación

El objetivo de implementar el servicio de soporte sistema de seguridad protección Anti-malware para detectar, proteger y eliminar software malicioso que puedan dañar la información que es almacenada en las estaciones de trabajo de PROCIENCIA incluyendo al proyecto "Mejoramiento y ampliación de los servicios de CTI para fortalecer el Sistema Nacional de Ciencia, Tecnología e Innovación".

3.1 Objetivo General

Implementar un servicio de soporte de sistema de seguridad y protección Anti-malware que permita detectar, prevenir y eliminar software malicioso, con la finalidad de proteger la información almacenada en las estaciones de trabajo de PROCIENCIA, incluyendo la información vinculada al proyecto *"Mejoramiento y ampliación de los servicios de CTI para fortalecer el Sistema Nacional de Ciencia, Tecnología e Innovación"*, garantizando la confidencialidad, integridad y disponibilidad de la información.

3.2 Objetivo Específico

- Detectar oportunamente amenazas de malware (virus, ransomware, spyware, troyanos y otros) en las estaciones de trabajo de PROCIENCIA mediante herramientas especializadas de seguridad.
- Prevenir infecciones y propagación de software malicioso, asegurando la protección continua de los equipos y de la información institucional.
- Eliminar y mitigar incidentes de seguridad ocasionados por malware, reduciendo riesgos de pérdida, alteración o fuga de información.
- Fortalecer la seguridad de la información relacionada con el proyecto CTI, asegurando la continuidad operativa y el cumplimiento de buenas prácticas de seguridad informática.
- Brindar soporte técnico especializado para la administración, monitoreo y actualización del sistema Anti-malware implementado.
- Reducir vulnerabilidades en las estaciones de trabajo, contribuyendo a un entorno informático seguro para los usuarios de PROCIENCIA.

4. Descripción del servicio

El costo del servicio de soporte sistema de seguridad protección anti-malware será asumido de acuerdo con lo establecido en el Cuadro 01, siendo financiado tanto por PROCIENCIA como por el Proyecto "Mejoramiento y Ampliación de los Servicios de Ciencia, Tecnología e Innovación (CTI) para Fortalecer el Sistema Nacional de Ciencia, Tecnología e Innovación".

Cuadro 01

Ítem	Descripción	Entidad Solicitante	Cantidad
01	Servicio de soporte sistema de seguridad protección anti-malware	PROCIENCIA	149 equipos de cómputo representan el (70.95%)
02	Servicio de soporte sistema de seguridad protección anti-malware	Proyecto de "Mejoramiento y ampliación de los servicios de CTI para fortalecer el Sistema Nacional de Ciencia, Tecnología e Innovación"	61 equipos de cómputo representan el (29.05%)

El servicio consistirá en una solución anti-malware que permita bloquear el software malicioso y protección de ataques maliciosos y se detalla de la siguiente manera:

4.1. Alcance

Ítem	Descripción	Cantidad	U/M
1	Servicio de soporte sistema de seguridad protección anti-malware	200 Endpoint y 10 servidores	Licencias

4.2. Características Generales

- Solución de "Protección de Próxima Generación con capacidades de Detección y Respuesta Gestionado para la cacería de amenazas sobre estaciones de trabajo y servidores" con funcionalidades de antivirus, antimalware, anti-exploits y anti-ransomware licenciado.
- La solución deberá cubrir a 200 equipos finales (endpoints) y 10 servidores.
- La solución propuesta debe ser un 'líder' en el Cuadrante Mágico de Gartner para plataformas de protección de endpoints (EPP) para el año 2024.
- El proveedor debe ser "líder" en el informe del Cuadrante Mágico de Gartner para plataformas de protección de endpoints (EPP) durante 14 veces consecutivas.
- El proveedor debe ser nombrado líder en el IDC MarketScape 2024 para seguridad de terminales modernas a nivel mundial para medianas empresas.
- La solución propuesta deberá haber participado en la Evaluación ATT&CK de MITRE Engenuity 2023.
- La solución de protección de terminales debe haber sobresalido en la quinta ronda de las evaluaciones MITRE Engenuity ATT&CK® de 2023 con una detección del 99 % de comportamientos adversarios.
- El proveedor debe haber obtenido una puntuación perfecta en el informe de protección de endpoints del segundo trimestre de SE Labs (abril a junio) de 2023.
- Debe haber recibido la certificación de "Producto superior" en las pruebas de AV-TEST de octubre de 2021 para dispositivos Windows.
- 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.
- La solución deberá cubrir a 200 equipos finales (endpoints) y 10 servidores.

4.2.1. Consola de Administración

- Todos los componentes que forman parte de la solución, de seguridad para servidores, estaciones de trabajo deben ser suministrados por un solo fabricante. No se aceptarán composiciones de productos de diferentes fabricantes.
- La consola de monitoreo y configuración deberá ser a través de una central única, basada en web y en nube, que deberá contener todas las componentes para el monitoreo y control de la protección de los dispositivos.
- La consola deberá presentar un Dashboard con el resumen del estado de protección de los ordenadores y usuarios, así como indicar las alertas de eventos de criticidades alta, media e informacional.
- Debe tener la capacidad de extraer información de eventos y alertas del Cloud Dashboard a un SIEM local.

- Debe tener API ofrecidas como puntos finales HTTP RESTful a través de la Internet pública.
- Las API deben tener la capacidad de consultar inquilinos, enumerar y administrar puntos finales y servidores, y consultar alertas y administrarlas mediante programación.
- Debe tener una API que pueda ejecutar osquery en puntos finales conectados a la consola de administración.
- Debe tener una API que pueda ejecutar consultas XDR en Data Lake.
- Debe tener la capacidad de permitir la separación de la gestión patrimonial en el inicio de sesión de diferentes administradores.
- Debe proporcionar a los administradores la capacidad de asignar funciones administrativas predefinidas a los usuarios que necesitan acceso a la Consola de administración.
- Debe poder crear roles personalizados y asignar los productos y el acceso necesarios.
- Debe tener la capacidad de permitir únicamente la sincronización saliente de usuarios/grupos desde los servidores locales de Active Directory al Cloud Dashboard para la gestión de políticas.
- Debe poder comparar dispositivos que tienen instalados los agentes de protección de terminales del proveedor con dispositivos sincronizados desde Active Directory y enumerar los dispositivos no administrados para que pueda instalar protección en ellos.
- La consola de administración debe tener una sección de Verificación del estado de la cuenta donde pueda ver si está utilizando todas las funciones de protección incluidas en su licencia.
- 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.
- 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.
- Debe tener la capacidad de evitar que los usuarios administrativos locales o los procesos maliciosos deshabiliten la protección del endpoint.
- Debe identificar un rootkit al revisar un elemento sin sobrecargar el sistema de endpoint. Los rootkits deben detectarse de forma proactiva.
- Debe tener la capacidad de evitar las siguientes acciones en la solución de protección de endpoints:
    - Detener servicios desde la interfaz de usuario de Servicios
    - Eliminar servicios desde la interfaz de usuario del Administrador de tareas
    - Cambiar la configuración del servicio desde la interfaz de usuario de servicios
    - Detener servicios/editar la configuración del servicio desde la línea de comando
    - Desinstalar
    - Reinstalar
    - Eliminar procesos desde la interfaz de usuario del Administrador de tareas (deseable)
    - Eliminar o modificar archivos o carpetas protegidas
    - Eliminar o modificar claves de registro protegidas
- Debe poder exportar contraseñas de protección contra manipulaciones en formatos CSV o PDF.

4.2.2. Características básicas del agente de protección contra malware:

- Debe proteger contra múltiples amenazas, tanto conocidas como desconocidas, y proporcionar un enfoque confiable e integrado para la gestión de amenazas en el endpoint.
- Debe proteger los sistemas endpoint contra virus, spyware, troyanos, rootkits y gusanos en estaciones de trabajo y portátiles, independientemente de su naturaleza o de los mecanismos de ocultación utilizados.

- Debe proteger contra amenazas relacionadas con archivos ejecutables, así como archivos de documentos que contienen elementos activos como macros o scripts. Debe proteger contra ataques resultantes del descubrimiento (ya sea publicado o no) de fallas de seguridad en sistemas o software.
- Debe tener la capacidad de "buscar" archivos en tiempo real para verificar si son maliciosos. Esta función compara los archivos sospechosos con el malware más reciente en la base de datos Threat Intelligence del proveedor en la nube.
- Debe tener la capacidad de realizar escaneos en tiempo real de archivos locales y recursos compartidos de red en el momento en que el usuario intenta acceder a ellos. Se debe denegar el acceso a menos que el archivo esté en buen estado.
- Debe tener la capacidad de realizar escaneos en tiempo real del acceso a Internet de los usuarios finales. Debe monitorear y clasificar los sitios web de Internet según su nivel de riesgo y poner esta tecnología a disposición de los sistemas endpoint. La solución debe bloquear proactivamente un sitio conocido por albergar códigos maliciosos o sitios de phishing para evitar cualquier riesgo de infección o ataque contra una falla del navegador utilizado. La solución debe realizar comprobaciones en una base de datos de sitios web comprometidos que se actualiza constantemente con nuevos sitios identificados cada día.
- Debe proteger los sistemas administrados de sitios web maliciosos en tiempo real, ya sea que los usuarios finales trabajen dentro de la empresa o fuera de la red segura de la empresa, en casa o mediante Wi-Fi público. Deben ser compatibles todos los navegadores del mercado (Internet Explorer, Firefox, Safari, Opera, Chrome, etc.).
- Debe poder proteger contra virus no identificados y comportamientos sospechosos.
- Debe tener análisis de comportamiento previo a la ejecución y análisis de comportamiento en tiempo de ejecución.
- Debe poder identificar y bloquear programas maliciosos antes de su ejecución.
- Debe poder analizar dinámicamente el comportamiento de los programas que se ejecutan en el sistema y detectar y luego bloquear la actividad que parezca maliciosa. Esto puede incluir cambios en el registro que podrían permitir que un virus se ejecute automáticamente cuando se reinicia la computadora.
- Debe proporcionar protección contra ataques de desbordamiento de buffer.

4.2.3. Funcionalidad de detección proactiva de reconocimiento de nuevas amenazas:

- Debe proporcionar un escáner programado para ejecutarse dependiendo de la frecuencia seleccionada o activando manualmente a través del Explorador de Windows para escanear los directorios especificados (local, remoto o extraíble), con parámetros de análisis utilizados, que pueden ser diferentes de los seleccionados para la protección en tiempo real.
- Debe tener la capacidad de escanear archivos como zip, cab, etc., que se pueden habilitar a través de la configuración de políticas.
- El sistema debe tener escaneo a la velocidad de la luz; En 20 milisegundos, el modelo podrá extraer millones de características de un archivo, realizar análisis profundos y determinar si un archivo es benigno o malicioso. Todo este proceso ocurre antes de que se ejecute el archivo.
- Debe poder prevenir tanto el malware conocido como el nunca antes visto, y también debe poder bloquear el malware antes de que se ejecute.
- Debe proteger el sistema incluso cuando esté fuera de línea y no dependerá de firmas.
- Debe clasificar los archivos como aplicaciones maliciosas, potencialmente no deseadas (PUA) o benignas. El aprendizaje profundo también debe centrarse en los ejecutables portátiles de Windows.
- Capaz de realizar nuevos análisis de amenazas de días cero sin conexión (sin Internet).
- Debe ser más inteligente: debe poder procesar datos a través de múltiples capas de análisis, cada capa haciendo que el modelo sea considerablemente más poderoso.
- Debe ser escalable: debe poder procesar una cantidad significativamente mayor de entradas, puede predecir con precisión las amenazas y al mismo tiempo mantenerse actualizado.
- Debe ser más liviano: el tamaño del modelo será increíblemente pequeño, menos de 20 MB en el punto final, con un impacto casi nulo en el rendimiento.
- El modelo de aprendizaje profundo consistirá en rastrear y evaluar modelos de un extremo a otro utilizando paquetes desarrollados avanzados como Keras, Tensorflow y Scikit-learn.

- Debe poder detectar las comunicaciones entre las computadoras finales y los servidores de comando y control involucrados en una botnet u otros ataques de malware.
- Debe poder prevenir el tráfico de red malicioso con inspección de paquetes (IPS).
- Debe poder escanear el tráfico en el nivel más bajo y bloquear amenazas antes de dañar el sistema operativo o las aplicaciones.

.

4.2.4. Funcionalidad de protección contra ransomware:

- Debe tener la capacidad de revertir los archivos cifrados a un estado previamente cifrado.
- Tanto la protección antiexploits como la protección contra ransomware no necesitan tener una búsqueda en la nube para realizar la detección.
- Cuando la función Anti-cripto sospecha que cierto comportamiento no está de acuerdo con el proceso previsto, el Grabador de datos comienza a almacenar datos en caché mientras dicho comportamiento se revisa de cerca para identificar si la aplicación es legítima o si la actividad está justificada.
- La función anti-criptomoneda revisará todas las modificaciones de archivos maliciosos realizadas por ese proceso y las restaurará a su ubicación original.
- Si una infección de ransomware logra ingresar, se informará un seguimiento histórico detallado de dónde se originó la infección y cómo se propagó (RCA).
- Debe poder protegerse contra ransomware que cifra el registro de arranque maestro y contra ataques que borran el disco duro.

4.2.5. Funcionalidades de control en el agente:

- Debe tener capacidad para controlar y restringir dispositivos de almacenamiento masivo extraíbles (memorias USB, CD Rom, discos duros externos USB, iPods, reproductores MP3, etc.), así como dispositivos de conexión (Wi-Fi, Bluetooth, Infrarrojos, Módems, etc.).).
- Debe tener la capacidad de agregar exenciones de dispositivos ya sea por ID de modelo o ID de instancia.
- Debe tener la capacidad de limitar las aplicaciones necesarias para grupos de usuarios específicos.
- Debe poder detectar y bloquear categorías de aplicaciones que pueden no ser adecuadas para su uso en un entorno empresarial.
- Debe tener categorías de aplicación para aplicaciones de uso común.
- Debe poder bloquear descargas riesgosas, proteger contra la pérdida de datos, evitar que los usuarios accedan a sitios web que no sean apropiados para el trabajo y generar registros de los sitios visitados bloqueados.
- Debe tener opciones de seguridad para configurar el acceso a anuncios, sitios sin categoría o descargas peligrosas.
- Debe brindar al administrador la capacidad de definir configuraciones de "uso web aceptable" (definidas por categorías) para controlar los sitios que los usuarios pueden visitar. El administrador debe tener control de acceso a los sitios web que han sido identificados y clasificados en sus propias categorías.
- Debe tener una opción de protección contra pérdida de datos que permita al administrador controlar el acceso al correo electrónico y las descargas de archivos basados en la web, con opciones para bloquear los datos, permitir el intercambio de datos o personalizar esta opción.

4.2.6. Capacidades de XDR

- El Analista debe poder identificar que atributos de código de un objeto son similares a archivos “known-good” y “known bad” con esto se puede determinar si se pueden permitir o bloquear.
- De tener un Sistema de registro por cada ataque o intento de ataque que se haya producido en los endpoints con información detallada del malware en sí y el origen de la infección (explorador de windows, correo electrónico, navegador, etc.)
- Debe permitir una investigación guiada entregando visibilidad de la dimensión del ataque cómo inicia, cómo impacta, cómo se responde.
- Detectar ataques que pueden haber pasado desapercibidos
- Buscar de forma proactiva (Threat Hunting) indicadores de compromiso por nombre de archivo, SHA, direcciones IP.

- Priorizar eventos para investigación.
- Poder aislar una maquina comprometida de la red de forma automática mientras la investigación del incidente
- Poder generar un Snapshot forense durante una investigación de una amenaza.
- Poder realizar queries de estándares de cumplimiento de seguridad.
- Poder realizar queries de técnicas y tácticas de ataque mapeadas en MITRE ATT&CK.
- Poder realizar queries de conexiones de Red y transferencias de archivos.
- Poder realizar queries sobre información del SO, servicios, parches y más.
- Poder realizar queries de actividad de usuario y autenticación.
- Poder realizar queries de anomalías, actividad o conexiones de red inesperadas.
- Poder realizar queries de eventos en los logs del sistema.
- Poder realizar queries de actividad de procesos y reputación.
- Poder realizar queries de detalles de archivos y acceso a archivos
- Poder realizar queries de accesos y cambios a llaves de registro

4.2.7. Despliegue Agente

- Soportar máquinas con arquitectura de 32 bits y 64 bits;
- El cliente para instalación en estaciones de trabajo debe ser compatible con los sistemas operativos Mac OS X 10.13 en adelante
- El cliente para instalación en estaciones de trabajo debe ser compatible con los sistemas operativos Windows 7 en adelante
- El cliente para instalación en estaciones de trabajo debe ser compatible con los sistemas operativos Windows Server 2008 R2 en adelante.

4.2.8. Soporte Técnico

- Durante el período de garantía comercial, debe contar con un Centro de Operaciones de Seguridad para el servicio de Soporte Técnico 24x7x365 con línea de comunicación gratuita 0800 para la atención de todos los tickets de cambios de configuraciones de políticas en el dispositivo de seguridad.
- El postor deberá contar con un Centro de Operaciones de Seguridad (SOC certificado con ISO 27001) para el servicio de Soporte Técnico, con la finalidad de garantizar que se cuente con procesos de atención óptimos que asegure el cumplimiento de los tiempos de respuesta, la calidad de su atención, así como el aseguramiento de la confidencialidad e integridad del manejo de los datos y de la información de la entidad.
- El servicio de soporte técnico comprenderá la solución de cualquier tipo de evento (incidente y/o problema) que cause una interrupción parcial o total del servicio, así como a la pérdida de la calidad o degradación de este. A todo ello se le denominará “falla”.
- El servicio de soporte técnico comprenderá consultas, solicitudes de reportes, y solicitudes de análisis de auditoría. A todo ello se le denominará “requerimiento”.
- El servicio de soporte técnico debe incluir el análisis, actualización, corrección y documentación de fallas en la solución implementada.
- Deberá brindar soporte técnico In Situ a cargo de expertos profesionales en análisis de seguridad informática, quien asistirá a la ENTIDAD en forma personal. Se precisa que el soporte técnico in situ se dará en caso de fallas que no puedan ser solucionados de manera remota.
- El postor deberá garantizar que la solución completa quede operativa y en óptimas condiciones de seguridad y performance, y de activar un plan de contingencia cuando una falla se produzca.
- El servicio de soporte técnico se efectuará a través de línea telefónica, correo electrónico u otros medios disponibles. Una vez recibida tal notificación, la mesa de ayuda del postor, registrará el requerimiento y/o falla del servicio y proporcionará un número de ticket.

5. Requisitos mínimos del proveedor

5.1 El proveedor del servicio deberá cumplir con los siguientes requisitos:

- No estar impedido de contratar con el Estado.
- Persona Natural o Jurídica.

5.2 Experiencia mínima de la empresa.

- Como mínimo haber realizado cinco (05) servicios de soluciones de anti-malware. Esto se deberá acreditar mediante copias simples de contratos u órdenes de servicios con su respectiva conformidad, y/o comprobantes de pagos y/o actas de conformidad que acrediten los servicios ejecutados.

6. Reglamentos técnicos, normas metrológicas y/o sanitarias

De realizar trabajo presencial (a solicitud del usuario), el ingreso a la Entidad será previas coordinaciones necesarias y autorización.

7. Seguros (De Corresponder)

No corresponde

8. Lugar y Plazo de Ejecución

8.1. Lugar: El servicio se realizará en las instalaciones de PROCIENCIA, sito en Jirón Doménico Morelli 150 Torre II Piso 9, San Borja, Lima Perú.

8.2. La suscripción vigente del servicio de soporte sistema de seguridad protección anti-malware se encuentra activa hasta el 31 de marzo de 2026; en tal sentido, la activación del nuevo servicio se realizará a partir del 31 de marzo de 2026, previa notificación de la correspondiente orden de servicio. Asimismo, el proveedor contará con un plazo máximo de cinco (05) días calendario posteriores a la activación para la implementación integral del servicio.

8.3. El plazo de ejecución del servicio será de hasta doce (12) meses, contabilizado a partir del día siguiente de la activación del servicio.

9. Entregables

El contratista adjudicado deberá presentar por mesa de partes digital a la siguiente dirección https://servicios.concytec.gob.pe/mesaPartesDigital/ (recepción las 24 horas al día los 7 días de la semana) o de manera presencial en la siguiente dirección Av. Del Aire 485, San Borja de lunes a viernes de 08:00 a 16:15 horas previa coordinación con el área usuaria.

Documentos a presentar:

- Documento que acredite la activación del servicio, el cual deberá ser presentado dentro de un plazo máximo de siete (07) días calendario, contados a partir del día siguiente de la activación del servicio.
- Acta de inicio del servicio, debidamente suscrita por las partes correspondientes.
- Memoria descriptiva del servicio de implementación anti-malware hacer uso de imágenes, conclusiones, recomendaciones en formato PDF).
- Plan de implementación detallará los objetivos, alcance, metodología y calendario de la implementación.
- Documentación técnica proporcionará información sobre la instalación, configuración y funcionamiento de la solución de anti-malware.

10. Conformidad

La conformidad de la prestación del servicio se regula por lo dispuesto en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante Decreto Supremo N° 009-2025.
La conformidad será otorgada por la Unidad de Tecnologías de la Información de PROCIENCIA, luego de ejecutada la activación del servicio, en el plazo máximo de siete (7) días computados desde el día siguiente de recibido el entregable.

De existir observaciones, el PROCIENCIA las comunica al CONTRATISTA, indicando claramente el sentido de estas, otorgándole un plazo para subsanar no mayo al 30% del plazo del entregable correspondiente, dependiendo de la complejidad o sofisticación de las subsanaciones a realizar. Si pese al plazo otorgado, EL CONTRATISTA no cumpliese a cabalidad con la subsanación, el PROCIENCIA puede otorgar al CONTRATISTA periodos adicionales para las correcciones pertinentes. En este supuesto corresponde aplicar la penalidad por mora desde el vencimiento del plazo para subsanar sin considerar los días en los que pudiera incurrir el PROCIENCIA para efectuar las revisiones y notificar las observaciones correspondientes.

Este procedimiento no resulta aplicable cuando los servicios manifiestamente no cumplan con las características y condiciones ofrecidas, en cuyo caso el PROCIENCIA no efectúa la recepción o no otorga la conformidad, según corresponda, debiendo considerarse como no ejecutada la prestación, aplicándose la penalidad que corresponda por cada día de atraso.

Para la conformidad, el proveedor presentará su factura y/u otros documentos que sustenten la prestación del servicio, a través del https://servicios.concytec.gob.pe/mesaPartesDigital/ (recepción las 24 horas al día los 7 días de la semana) o de manera presencial en la siguiente dirección Av. Del Aire 485, San Borja de lunes a viernes de 08:00 a 16:15 horas, acompañado de una carta dirigida al Programa Nacional de Investigación Científica y Estudios Avanzados – PROCIENCIA.

11. Forma y Condiciones de Pago

El pago se realiza de conformidad con lo establecido en el artículo 67 de la Ley.

El PROCIENCIA paga las contraprestaciones pactadas a favor del contratista dentro de los diez (10) días hábiles siguientes de otorgada la conformidad por parte del área usuaria y es prorrogable, previa justificación de la demora, por cinco días hábiles

El PROCIENCIA realiza el pago de la contraprestación pactada a favor del contratista en soles, en una armada, luego de la recepción formal y completa de la documentación correspondiente, según lo establecido en el artículo 144 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.

Para efectos del pago de las contraprestaciones ejecutadas por el contratista, el PROCIENCIA debe contar con la siguiente documentación:

Documento en el que conste la conformidad de la prestación efectuada suscrita por la Unidad de Tecnologías de la Información, luego de ejecutado el servicio.

Comprobante de pago.

En caso de retraso en el pago por parte de PROCIENCIA, salvo que se deba a caso fortuito o fuerza mayor, EL CONTRATISTA tiene derecho al pago de intereses legales conforme a lo establecido en el artículo 67 de la Ley N° 32069, Ley General de Contrataciones Públicas.

12. Confidencialidad (De corresponder)

"EL CONTRATISTA no podrá divulgar, revelar, entregar o poner a disposición de terceros dentro o fuera del Pliego CONCYTEC, salvo autorización expresa de las Unidades Ejecutoras CONCYTEC o PROCIENCIA, la información proporcionada por ésta para la prestación del servicio y, en general toda información a la que tenga acceso o la que pudiera producir con ocasión del servicio que presta, durante y después de concluida la vigencia de la presente Orden de Servicio".

13. Penalidades

Penalidad por Mora en la ejecución de la prestación:

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, el PROCIENCIA 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:

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

Donde F tiene los siguientes valores:
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.

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobado. Adicionalmente, se considera justificado el retraso y en consecuencia no se aplica penalidad, cuando EL CONTRATISTA acredite, de modo objetivamente sustentado, que el mayor tiempo transcurrido no le resulta imputable. En este último caso la calificación del retraso como justificado por parte de PROCIENCIA no da lugar al pago de gastos generales ni costos directos de ningún tipo, conforme al numeral 120.4 del artículo 120 del Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado por Decreto Supremo N° 009-2025-EF.
Las penalidades se deducen de los pagos a cuenta, pagos parciales o del pago final, según corresponda.

14. Otras Penalidades (De Corresponder)

No corresponde

15. Responsabilidad por vicios ocultos

El contratista es responsable por la calidad ofrecida y por los vicios ocultos del (los) servicio (s) ofertado (s) por un plazo no menor de un (01) año contado a partir de la conformidad otorgada.

16. Cláusula Anticorrupción y Antisoborno

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 PROCIENCIA.

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 PROCIENCIA, 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 el PROCIENCIA.

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 PROCIENCIA el derecho de resolver total o parcialmente el contrato. Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

17. Cláusula Patrimonial

Por medio de la presente cláusula, el contratista cede los derechos patrimoniales de los cuales sea titular sobre las obras, datos procesados y estadísticas de monitoreo producidos en virtud a este contrato, para su explotación no exclusiva, ilimitada, perpetua y con alcance mundial, a favor de (la Entidad Pública).

Esta cesión de derechos comprende, mas no se limita, a los derechos de reproducción, comunicación al público, distribución, traducción, adaptación, arreglo, edición, modificación, cambio de formato u otra transformación, importación al territorio nacional de copias por cualquier medio incluyendo la transmisión, así como cualquier otra forma de utilización de las obras, datos procesados y estadísticas de monitoreo que no estén contempladas en la ley de la materia como excepción al derecho patrimonial y, en general, para cualquier tipo de utilización y explotación, que la entidad estime pertinentes, en cualquier forma o procedimiento, conocido o por conocerse, pudiendo poner a disposición las obras, datos procesados y estadísticas de monitoreo por medio de autorizaciones o licencias a favor del público en general.

18. Cláusula Solución de Controversias

Las controversias que surjan entre las partes durante la ejecución del contrato se resuelven mediante conciliación.
Cualquiera de las partes tiene el derecho a solicitar una conciliación dentro del plazo de caducidad correspondiente, según lo señalado en el artículo 82 de la Ley N° 32069, Ley General de Contrataciones Públicas, sin perjuicio de recurrir al arbitraje, en caso no se llegue a un acuerdo entre ambas partes o se llegue a un acuerdo parcial. Las controversias sobre nulidad del contrato solo pueden ser sometidas a arbitraje.

19. Cláusula de Cumplimiento

"Son causales de resolución de contrato la presentación con información inexacta o falsa de 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"

Firmado digitalmente por TIRADO BAZAN Miguel Luis FAU 20135727394 soft
Motivo: Soy el autor del documento
Fecha: 03.03.2026 16:23:41 -05:00

_____

Firma y sello del responsable del Área Usuaria

Firmado digitalmente por ALVAREZ SALAZAR Jubalt Rafael FAU 20135727394 soft
Motivo: Doy V° B°
Fecha: 04.03.2026 14:36:09 -05:00