"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año de la recuperación y consolidación de la economía peruana"

TÉRMINOS DE REFERENCIA

Área Técnica Estratégica	**Oficina General de Tecnología de la información**	
Cuadro Multianual de Necesidades	Código	Denominación
	524500030002	Contratar el servicio de suscripción de licencias de software de protección de antivirus.
Actividad del POI/Acción Estratégica PEI	AOI00015504607: Gestión de Infraestructura Tecnológica y de Comunicaciones del MIDAGRI.	
Denominación de la Contratación	Contratar el servicio de suscripción de licencias de software de protección de antivirus.	

1. FINALIDAD PÚBLICA

La presente contratación tiene por finalidad asegurar la continuidad y fortalecimiento de las actividades del Ministerio de Desarrollo Agrario y Riego (MIDAGRI), mediante la provisión del servicio de suscripción de **licencias de software antivirus**, que garanticen la protección integral de la infraestructura informática institucional.

La implementación de estas licencias permitirá mitigar riesgos asociados a incidentes de seguridad informática, tales como la pérdida, alteración o divulgación indebida de información, que podrían afectar el cumplimiento de los fines y funciones encomendados al MIDAGRI como ente rector del sector agrario. Asimismo, contribuirá a la continuidad operativa de los sistemas de información y a la prestación eficiente de los servicios públicos orientados al desarrollo agrario, la seguridad alimentaria y el bienestar de los productores a nivel nacional, en concordancia con lo establecido en la normativa vigente sobre gobierno digital y seguridad de la información en la administración pública.

2. OBJETIVO DE LA CONTRATACIÓN

Contratar el servicio de suscripción de licencias de software de protección antivirus para el Ministerio de Desarrollo Agrario y Riego – MIDAGRI.

3. ANTECEDENTES

El Ministerio de Desarrollo Agrario y Riego - MIDAGRI necesita contar con una solución que garantice la adecuada protección de la información almacenada en los equipos de cómputo y de los sistemas informáticos de la institución, de ser modificada, borrada o afectada por programas no deseados como virus informáticos, troyanos, spyware y nuevas variantes de estos.

En base a las nuevas amenazas es necesario considerar funcionalidades específicas para mitigar los riesgos con que actúen los softwares de código malicioso-malware. Por lo cual se requiere un software antivirus robustos por ser una institución de impacto nacional.

Actualmente el MIDAGRI cuenta con un software ANTIVIRUS, que incluye licenciamiento activo hasta el 09 de octubre del 2025. Por ello, es crucial contar con una nueva solución de protección antivirus para los equipos informáticos (End Point) debido al nivel de tráfico de información en la red interna (LAN) y extendida (WAN).

La Oficina General de Tecnología de la Información – OGTI realizo el Informe Técnico previo de evaluación de software Nro. 16-2025- MIDAGRI-SG-OGTI para la adquisición de servicio de suscripción licencia de software de protección antivirus con fecha 11 de setiembre de 2025 en el Portal Web del MIDAGRI.
https://cdn.www.gob.pe/uploads/document/file/8657662/6416328-informe-tecnico-previo-de-evaluacion-de-software-n-16-2025-midagri-sg-ogti.pdf?v=1757955848

4. ALCANCES, CARACTERISTICAS Y CONDICIONES DEL SERVICIO

4.1. ALCANCE

La contratación del servicio de "Suscripción de software de Licencia de software de protección antivirus", debe incluir:

ÍTEM	DESCRIPCIÓN	TIPO	CANTIDAD	UNIDAD DE MEDIDA	PERIODO
01	Suscripción de Licencia de software de protección antivirus	Estaciones de trabajo y Servidores	1450	Unidad	12 meses
		Móviles	300		

4.2. CARACTERISTICAS GENERALES

- Todos los componentes que forman parte de la suscripción de seguridad para servidores, estaciones de trabajo, moviles deben ser suministrados por un solo fabricante. No se aceptarán composiciones de productos de diferentes fabricantes.
- El software debe estar basada en consola OnPremise y/o Cloud.
- Opcionalmente la suscripción deberá posicionarse como líder en el cuadrante de Gartner de Endpoint Protection Platforms (diciembre 2022)
- Opcionalmente debe poseer un mecanismo de comunicación vía API, para su integración con otras soluciones de seguridad, como por ejemplo SIEM, SOAR y sistemas de tickets. Este mecanismo de comunicación vía API deberá obtener los eventos y alertas asociados a la consola en al menos, los siguientes formatos: json, cef, or keyvalue.
- Opcionalmente el software La solución debe poseer un IPS Snort de Host
- Opcionalmente debe debe poseer protección anti-ransomware para el sector de booteo.
- Opcionalmente debe contar con protección contra robo de credenciales
- Opcionalmente debe buscar de forma proactiva (Threat Hunting) indicadores de compromiso por nombre de archivo, SHA, direcciones IP.
- Opcionalmente debe poder generar un Snapshot forense durante una investigación de una amenaza.
- Opcionalmente debe poder realizar queries de estandares de cumplimiento de seguridad.
- Opcionalmente debe poder realizar queries de conexiones de Red y transferencias de archivos.
- Opcionalmente debe poder realizar queries de actividad de usuario y autenticación.
- Opcionalmente la protección deberá tener listas de CCL preconfiguradas con al menos los siguientes identificadores, y soportar agregar reglas propias de contenido.
- Opcionalmente debe prevenir el ataque de vulnerabilidades de navegador a través de web exploits.
- Opcionalmente debe contar con protección de amenazas de día 0 a través de tecnología de deep learning (signature less).

4.2.1. CARACTERÍSTICAS 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 20.04 y superior x64, RedHat para Desktop 8, 9 x64 y superior, Linux Mint 20, 21,22 Apple macOS 13 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.

- 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 de protección contra ransomware.
- La solución debe contar con una funcionalidad de corrección de ransomware que realice copias de seguridad y restaure archivos dañados, dicho proceso se activa cuando la detección del ransomware se ha realizado previamente.
- 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.
- 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.
- El producto ofertado debe poseer un firewall bidireccional que contenga los siguientes modos de filtrado entre ellos, automático, interactivo, inteligente, 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 generar una lista de direcciones de correos permitidas o bloqueadas.
- 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.
- 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 para el acceso a la web para la detección y bloqueo de sitios web con contenido malicioso.
- 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, opcionalmente para control de redes inalámbricas.
- 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 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 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 de comando y control.
- 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 de la información ingresada con el teclado, contra registradores de pulsaciones al usar el navegador seguro.

4.2.2. CARACTERISTICAS PARA SERVIDORES

A. GENERALES

- La solución debe ser compatible con los siguientes sistemas operativos: Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022, Windows Server 2025 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) 8 y 9; Ubuntu Server 22.04 y 24.04 LTS; Debian11 y 12; SUSE Linux Enterprise Server (SLES) 15.
- Compatible con versiones del kernel del sistema operativo Linux 4.14 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 específica.
- 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.
- 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.

4.2.3. CARACTERISTICAS PARA MOVILES

- Deberá ser compatible con sistemas operativos Android 9 o superior.
- Deberá proteger en tiempo real contra malware, escaneando automáticamente la carpeta descargas, los archivos de instalación APK y todos los archivos en la tarjeta SD una vez montada, opcionalmente protección contra ransomware.
- Deberá poder explorar de manera automática cuando el dispositivo está en estado inactivo (completamente cargado y conectado a un cargador).
- Deberá contar con una exploración bajo demanda para la desinfección confiable de la memoria integrada y de los medios intercambiables.
- Deberá contar con protección ante la desinstalación con una contraseña administrador.
- Deberá tener una configuración de la seguridad de dispositivo con lo siguiente:
  - Definir los requisitos sobre la complejidad de las contraseñas.
  - Establecer una cantidad máxima de intentos de desbloqueo tras la cual el dispositivo entrará automáticamente en la configuración de fábrica.
  - Establecer un vencimiento para el código de bloqueo de pantalla.
  - Establecer un temporizador para el bloqueo de pantalla.
  - Indicar a los usuarios que cifren el contenido de sus dispositivos móviles.
  - Que notifique cuando se permita instalar de fuentes desconocidas.
  - Que notifique cuando se haya desactivado el GPS.
- Deberá permitir al administrador accionar los comandos remotos desde la consola mediante ejecución de tareas.
- Deberá bloquear en forma remota los dispositivos perdidos o robados.
- Deberá encontrar remotamente el teléfono y rastrear sus coordenadas de GPS.
- Deberá eliminar en forma segura todos los contactos, los mensajes y los datos almacenados en la memoria interna del dispositivo, así como en las tarjetas de memoria SD.

- Deberá poder activarse una alarma en el dispositivo que suene, incluso aunque el volumen esté en silencio.
- Deberá poder hacer un restablecimiento remoto de la configuración predeterminada de fábrica.
- Deberá poder monitorear las aplicaciones instaladas, bloquear el acceso a aplicaciones definidas y reducir el riesgo de exposición instando a los usuarios a desinstalar determinadas aplicaciones.
- Deberá poder bloquear páginas web, aplicado mediante política de la consola administrativa.
- Deberá poder recibir un mensaje personalizado por parte del administrador.

4.2.4. CARACTERISTICAS DE LA CONSOLA DE ADMINISTRACIÓN

- La consola debe ser con infraestructura en la nube, implementado como un servicio SAAS o 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 Edge, 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.

4.2.5. CARACTERISTICAS DE 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 antimalware 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.

4.2.6. CARACTERISTICAS PARA CIFRADO DE DISCO

- La solución deberá compatible con sistemas Windows 10 y 11(64bits).
- La solución es compatible en discos con esquema de particiones GPT.
- La solución es compatible con UEFI.
- La solución deberá ser capaz de cifrar los Endpoints deseados desde el inicio de sistema.
- La solución deberá disponer de diversas posibilidades de recuperación de Passwords para usuarios remotos que se vean bloqueados.
- La solución deberá poder programar las tareas de cifrado sobre los Endpoints deseados con la posibilidad de pausar la ejecución para retomar luego desde el último punto.
- La solución deberá poder ser administrada desde la misma consola central junto con las otras soluciones descriptas en el TDR.

4.2.7. INSTALACION Y CONFIGURACIÓN

- El proveedor deberá trabajar de manera conjunta con el personal técnico de la entidad que supervisaran la implementación correspondiente
- La Configuración de las tareas y políticas en la consola de administración para los equipos del ministerio.
- El proveedor deberá realizar la instalación y configuración solución ofertada se realizará sin afectar las labores normales de la institución y sin interrumpir la normal provisión de los servicios.

4.2.8. SOPORTE TECNICO

- El soporte técnico se realizará durante el periodo de la suscripción (12 meses)
- El proveedor brindara el soporte técnico requerido mediante asistencia técnica en remoto, en línea, por teléfono o de manera presencial, ante fallas o averías (incidencias).
- El soporte técnico incluye la atención y solución de incidentes por parte del postor y del fabricante por fallas en software, y será realizado cuantas veces sea necesario durante la vigencia de la garantía sin costos adicionales para la Entidad.
- Se entenderá por avería a una interrupción parcial o total del servicio, así como a una pérdida de la calidad de este.
- El Contratista debe de considerar estos parámetros para el soporte:
  - Atención de incidentes y requerimientos ilimitados.
  - Escalamiento de problemas a fábrica.
  - Atención 24x5.
  - Actualización de versiones de equipo durante todo el periodo de vigencia del soporte, siempre que sea compatible con el equipo.
- El servicio deberá garantizar el soporte técnico de 24 horas x 5 días, incluidos sábados, domingos y feriados durante el plazo de vigencia del servicio.
- La Entidad comunicara al proveedor los requerimientos o incidencias a través de los medios de comunicación como correo electrónico o enlace telefónico, para la generación del respectivo ticket de atención, debiendo indicar el número telefónico y correo electrónico de contacto en su oferta para el servicio de seguridad gestionada.
- El tiempo de respuesta máxima para la atención de cada requerimiento reportado será de cuatro (04) horas, entendiéndose como tiempo de respuesta el tiempo que transcurre desde que el requerimiento es reportado hasta que el contacto de la ENTIDAD recibe el nro. de ticket de registro del requerimiento.
- El tiempo de respuesta máxima para la atención de cada incidente reportado será de dos (02) hora, entendiéndose como tiempo de respuesta el tiempo que transcurre desde que el incidente es reportado hasta que el contacto de la ENTIDAD recibe el número de ticket de registro de la incidencia.
- La atención deberá ser realizada única y exclusivamente por personal calificado de la empresa proveedora o fabricante, la cual incluirá el registro de la atención mediante la generación de un numero de ticket o número de caso.
- Lugar donde se brindará el soporte: La asistencia o soporte técnico será en remoto, en línea o por teléfono y de forma presencial, de acuerdo con la criticidad de la atención solicitada.
- El contratista debe contar con un procedimiento para el reporte de problemas, el cual debe contemplar la asignación de un número de atención (Ticket) que facilite el seguimiento de la falla reportada.

5. REQUISITOS DEL PROVEEDOR Y/O PERSONAL

5.1. REQUISITOS DEL PROVEEDOR

- Contar con inscripción vigente en el Registro Nacional de Proveedores – RNP, Capítulo de Servicios.
- Habilitada para contratar con el estado peruano.

Experiencia del proveedor
El proveedor debe acreditar un monto facturado acumulado equivalente a S/ 35,000.00 (treinta y cinco mil con 00/100 Soles), 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 cotización que se computa desde la fecha de la conformidad o emisión

del comprobante de pago, según corresponda[1].

Se considera servicios similares a: suscripción de software de antivirus, suscripción de licencias de antivirus, suscripción de licencias software de antivirus, suscripción de licencias de EDR, suscripción de licencias de XDR, licencia de solución de seguridad antivirus.

Acreditación:
La experiencia 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, correspondientes a un máximo de veinte (20) contrataciones. En caso el proveedor sustente su experiencia mediante contrataciones realizadas con privados, para acreditarla debe presentar de forma obligatoria lo indicado en el numeral (ii) del presente párrafo; no es posible que acredite su experiencia únicamente con la presentación de contratos u órdenes de servicio con conformidad o constancia de prestación.

6. REGLAMENTOS TÉCNICOS, NORMAS METROLÓGICAS Y/O SANITARIAS

No Aplica

7. SEGURIDAD

No Aplica

8. PRESTACIONES ACCESORIAS

No Aplica

9. LUGAR Y PLAZO DE LA EJECUCIÓN

9.1. LUGAR

Sede central del MIDAGRI, en horario de lunes a viernes de 08:30 a 16:00 horas, sito en Jr. Cahuide N° 805 – Jesús María.

9.2. PLAZO DE EJECUCIÓN

9.2.1. PLAZO DEL SERVICIO:

El plazo de prestación del servicio es por un periodo de doce (12) meses, contabilizados a partir del momento de la activación de la suscripción del servicio, el mismo que debe ser en un plazo máximo de diez (10) días calendarios, contados a partir del día siguiente de la notificación la orden de servicio.

9.2.2. PLAZO DEL INSTALACIÓN: El plazo de instalación será de diez (10) días calendarios, contados a partir del día siguiente de la notificación la orden de servicio.

[1] Cabe precisar que, de acuerdo con la **Resolución N° 0065-2018-TCE-S1 del Tribunal de Contrataciones del Estado**:

> *"… el solo sello de cancelado en el comprobante, cuando ha sido colocado por el propio postor, no puede ser considerado como una acreditación que produzca fehaciencia en relación con que se encuentra cancelado. Admitir ello equivaldría a considerar como válida la sola declaración del postor afirmando que el comprobante de pago ha sido cancelado"*
> *(…)*
> *"Situación diferente se suscita ante el sello colocado por el cliente del postor [sea utilizando el término "cancelado" o "pagado"] supuesto en el cual sí se contaría con la declaración de un tercero que brinde certeza, ante la cual debiera reconocerse la validez de la experiencia".*

10. ENTREGABLES

EL PROVEEDOR deberá entregar un informe en el cual indicará como mínimo lo siguiente:

- Código de licencias
- Fecha de activación del servicio
- Duración
- Contactos de soporte

El entregable debe ser presentado en un plazo máximo de cinco (05) días calendarios, contado a partir del día siguiente de firmada el acta de culminación del servicio.

Salvo los documentos que emite la entidad contratante, es decir, de recepción y verificación, así como de conformidad, el contratista debe presentar la documentación restante, en la mesa de partes sito en la Jr. Cahuide N° 805, Jesús María en el horario de 08:30 hasta las 16:30 horas o a través de la Plataforma Digital de la Mesa de Partes Virtual (https://mesadepartesdigital.midagri.gob.pe/).

La documentación, se presenta mediante una carta dirigida a la Oficina General de Tecnología de la Información.

11. CONFORMIDAD

La conformidad del servicio será otorgada por la Oficina General de Tecnología de la Información - OGTI del MIDAGRI.

La conformidad se emite en un plazo máximo de (07) siete días computados desde el día siguiente de recibido el entregable, salvo que se requiera efectuar pruebas que permitan verificar el cumplimiento de la obligación.

De existir observaciones, la DEC las comunica al contratista, indicando claramente el sentido de estas, otorgándole un plazo para subsanar dependiendo de la complejidad o sofisticación de las subsanaciones a realizar. El plazo de subsanación no debe ser mayor del 30% del plazo del entregable correspondiente. Subsanadas las observaciones dentro del plazo otorgado, no corresponde la aplicación de penalidades.

El mismo plazo establecido para la subsanación de observaciones resulta aplicable para que la entidad contratante se pronuncie sobre el levantamiento de observaciones.

Si pese al plazo otorgado, el contratista no cumpliese a cabalidad con la subsanación, la entidad contratante puede otorgar al contratista periodos adicionales, conforme a lo señalado en el numeral 144.4 del Reglamento[2], u optar por resolver el contrato, de acuerdo con los supuestos de resolución establecidos en el literal b) del numeral 68.1 del artículo 68 de la Ley[3]. En caso otorgue periodos adicionales corresponde aplicar la penalidad por mora desde el vencimiento del plazo inicial para subsanar, sin considerar los días en los que pudiera incurrir la entidad contratante para efectuar las revisiones y notificar las observaciones correspondientes.

12. FORMA Y CONDICIONES DE PAGO (Artículo 67 Ley / Artículo 229.4 Reglamento)

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

[2] De existir observaciones, la DEC las comunica al contratista, indicando claramente el sentido de estas, otorgándole un plazo para subsanar dependiendo de la complejidad o sofisticación de las subsanaciones a realizar. El plazo de subsanación no debe ser mayor del 30% del plazo del entregable correspondiente. Subsanadas las observaciones dentro del plazo otorgado, no corresponde la aplicación de penalidades.

[3] b) Incumplimiento de obligaciones contractuales, por causa atribuible a la parte que incumple.

único pago.

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

- Conformidad por parte de la Oficina General de Tecnología de la Información - OGTI.
- Comprobante de pago.
- Entregable detallado en el numeral 10 del presente documento.

Salvo los documentos que emite la entidad contratante, es decir, de recepción y verificación, así como de conformidad, el contratista debe presentar la documentación restante, en la mesa de partes sito en la Jr. Cahuide N° 805, Jesús María en el horario de 08:30 hasta las 16:30 horas o a través de la Plataforma Digital de la Mesa de Partes Virtual (https://mesadepartesdigital.midagri.gob.pe/).

La documentación, se presenta mediante una carta dirigida a la Oficina General de Tecnología de la Información.

El pago se realiza en un plazo máximo de diez días hábiles luego de otorgada la conformidad por parte del área usuaria y es prorrogable, previa justificación de la demora, por cinco días hábiles.

13. CONFIDENCIABILIDAD

La confidencialidad y reserva absoluta en el manejo de información y documentación a la que se tenga acceso relacionada con la prestación, pudiendo quedar expresamente prohibido revelar dicha información a terceros. El contratado, debe dar cumplimiento a todas las políticas y estándares definidos por la Entidad, en materia de seguridad de la información.

Esta obligación comprende la información que se entrega, como también la que se genera durante la realización de las actividades y la información producida una vez que se haya concluido el servicio. Dicha información puede consistir en mapas, dibujos, fotografías, mosaicos, planos, informes, recomendaciones, cálculos, diagnósticos, documentos, cuadros comparativos y demás datos compilados o recibidos por el proveedor.

14. GASTOS POR DESPLAZAMIENTO

No Aplica

15. PENALIDADES POR MORA

15.1 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:

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

Donde F tiene los siguientes valores:

Para bienes y servicios: F = 0.40

Tanto el monto como el plazo se refieren, según corresponda, al monto vigente del contrato, componente o ítem que debió ejecutarse o, en caso de que estos involucren entregables

cuantificables en monto y plazo, al monto y plazo del entregable que fuera materia de retraso.
En el caso de sistemas de entrega de obra y consultoría de obra que contenga más de un componente el monto y plazo corresponde al componente que se ejecuta.

El retraso se justifica a través de la solicitud de ampliación de plazo debidamente aprobada. 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 la entidad contratante no da lugar al pago de gastos generales ni costos directos de ningún tipo.

15.2 Otras Penalidades
Se considera para la presente contratación las siguientes Otras Penalidades:

N°	SUPUESTOS DE APLICACIÓN DE PENALIDAD	FORMA DE CÁLCULO	PROCEDIMIENTO
1	No cumplir con el plazo de activación de la suscripción del servicio establecido en el numeral 9.2.1. de los términos de referencia.	*1% de la UIT vigente por cada día de atraso*	*La Oficina General de Tecnología de la Información comunicará a través de un informe técnico a la Oficina de Abastecimiento*
2	No presentar el Informe luego de culminado el servicio dentro del plazo establecido en el numeral 10 de los términos de referencia.	*0.1% de la UIT vigente por cada día de atraso*	

La suma de la aplicación de las penalidades por mora y otras penalidades no debe exceder el 10% del monto vigente del contrato o, de ser el caso, del ítem correspondiente.

El contratista tendrá un plazo máximo de cinco (05) días calendarios, a partir del día siguiente de notificado mediante carta a través de la Oficina de Abastecimiento del MIDAGRI sobre la penalidad incurrida, penalidad que es informada por el área usuaria, para remitir sus descargos en el supuesto, de corresponder.

En un plazo de cinco (05) días calendario contados al día siguiente de recibido el descargo la entidad emitirá la decisión.

16. CLAUSULA 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 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[4] 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[5]. 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[6]. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar[7].

17. RESOLUCIÓN DE CONTRATOS MENORES (Artículo 68 Ley / Artículo 229.3 Reglamento)

Cualquiera de las partes puede resolver total o parcialmente el contrato menor, según corresponda, en los siguientes casos:

a. Incumplimiento de obligaciones contractuales, por causa atribuible a la parte que incumple.
b. Caso fortuito o fuerza mayor, que imposibilite la continuación del contrato menor.
c. Hecho sobreviniente al perfeccionamiento del contrato, que imposibilite la continuación del contrato.
d. Por la presentación de documentación falsa y/o inexacta durante la indagación de mercado, la selección del proveedor o la ejecución contractual.
e. Por incumplimiento de la Cláusula Anticorrupción.
f. Acumulación del monto máximo de penalidad por mora.

18. SOLUCIÓN DE CONTROVERSIAS

Todas las controversias que surjan entre las partes sobre la validez, nulidad, interpretación, ejecución, terminación o eficacia de los contratos menores se resuelven mediante conciliación, la cual se regula conforme lo dispuesto en el artículo 360 del Reglamento de la Ley de Contrataciones del Estado.

a. Son controversias materias de conciliación las siguientes: Resolución de contrato.
b. Ampliación de plazo contractual.
c. Recepción y conformidad de la prestación.
d. Valorizaciones o metrados.
e. Liquidación de contrato.
f. Los que versen respecto de las obligaciones de las partes durante la ejecución del

[4] Artículo 9 de la Ley N°32069, Ley General de Contrataciones Públicas
[5] Literal d) del Numeral 68.1 del Artículo 68 de la Ley N°32069, Ley General de Contrataciones Públicas.
[6] Literal d) del artículo 274 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas
[7] Numeral 122.6 del artículo 122 del Reglamento de la Ley N°32069, Ley General de Contrataciones Públicas

contrato.
g. Controversias sobre sobre indemnización por daños y perjuicios.
h. Prestaciones accesorias
i. Vicios ocultos
j. otras obligaciones que se deben cumplir con posterioridad a la culminación de la ejecución de la prestación principal del contrato

19. RESPONSABILIDAD POR VICIOS OCULTOS (Literal c) del Artículo 69.2 de la Ley)

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

20. GARANTIAS (Artículo 113 Reglamento - Artículo 139 Reglamento)

No aplica.

21. GESTION DE RIEGOS (Artículo 60 de la Ley)

Es un proceso dinámico y abarca todas las etapas de la contratación pública, el cual comprende las actividades y las acciones proactivas, preventivas y transversales adoptadas por una entidad contratante para identificar los riesgos que esta enfrenta en la contratación de bienes, servicios y obras. Dichas actividades y acciones se realizan sobre la base de la identificación, análisis, valoración, gestión, control y monitoreo de riesgos, que permiten tomar decisiones informadas y aprovechar las oportunidades potenciales derivadas de estos. Las entidades contratantes realizan la gestión de riesgos a fin de aumentar la probabilidad y el impacto de riesgos positivos y disminuir la probabilidad y el impacto de riesgos negativos, que puedan afectar el cumplimiento de la finalidad pública buscada. En todo momento, la gestión de riesgos debe considerar una mejora en la administración y en el uso de los recursos públicos.

22. OTROS

Las partes pueden acordar modificaciones al contrato menor (Orden de Servicio o de Compra) siempre que las mismas permitan alcanzar su finalidad de manera oportuna y eficiente y no cambien el monto, el plazo ni desnaturalicen el requerimiento.
La modificación se perfecciona mediante un acta suscrita por ambas partes que se registra en la Pladicop.

23. DECLARACION DE JURADA DE INTERESES

No Aplica