TÉRMINOS DE REFERENCIA

1. **Denominación de la contratación**
   Servicio de renovación de licencia de antivirus de la Agencia Espacial del Perú - CONIDA.

2. **Finalidad pública**
   Brindar protección ante todo tipo de amenazas tanto conocidas como desconocidas, para evitar los nuevos tipos amenazas que aparecen a nivel mundial, los cuales intentan burlar el mayor número de controles de seguridad, con la finalidad de mitigar los riesgos de infección o secuestro de información que ocasionan tanto en los equipos de computo como en los diferentes tipos de archivos que pueden ser infectados con contenido malicioso.

   Esta renovación permitirá elevar los niveles de seguridad de la Agencia Espacial del Perú – CONIDA, garantizando que estén libre de infección, evitando y reduciendo el riesgo de pérdida e infección de la información.

3. **Actividad del POI:**
   Gestión Administrativo.

4. **Descripción y cantidad del servicio:**
   Contratar el servicio de renovación de Licencia del Antivirus Corporativo para 250 equipos los cuales incluyen estaciones de trabajo, servidores y portátiles.

Descripción del Servicio	Cant.	U.M.	Versión de Licencia	Duración de la licencia	Lugar donde realiza el mantenimiento y actualización
Renovación de Licencia del Antivirus para 250 equipos informáticos	1	Servicio	2024 (incluye actualizaciones)	12 meses	Instalaciones de CONIDA-OFTIN

CARACTERÍSTICAS EN LA PROTECCIÓN PARA ESTACIONES DE TRABAJO Y SERVIDORES:

- La solución para estaciones de trabajo debe brindar soporte a los sistemas operativos:
  - Windows 7, Windows 8, Windows 10 y Windows 11 de 64 bits.
  - Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022 de 64 bits. MAC OS x 10.4.11 o superior.
  - Red Hat Enterprise Linux, CentOS, Ubuntu Server, Debian GNU/Linux, SUSE Linux Enterprise Server y Oracle Linux.

- Debe brindar tecnología de protección capaz de eliminar amenazas de malware tales como virus, troyanos, spyware, adware, rookits, ransomware u otro tipo de software malicioso que comprometa los sistemas de información.

- Debe contar con un módulo de Exploit Prevention que impida que el malware explote vulnerabilidades de los sistemas operativos o aplicaciones que se ejecutan en la red.
- Debe monitorear las aplicaciones mediante detección de comportamiento (Behavior Detection) para proporcionar una capa adicional de vigilancia y protección contra amenazas desconocidas.
- Debe brindar la capacidad de inteligencia contra amenazas asistido en la nube que permita identificar objetos como reputación de archivos, dominios, IP entre otros.
- Debe brindar protección avanzada contra amenazas utilizando un enfoque de aprendizaje automático predictivo conocido como Machine Learning.
- Debe permitir escanear archivos comprimidos.
- Debe permitir remediación mediante el rollback de las acciones realizadas en el equipo por un software malicioso.
- Debe contar con una tecnología que permita mejorar el performance de los escaneos en tiempo real, manuales o programados no realizando escaneos sobre archivos anteriormente revisados o que no hayan sido modificados.
- Debe permitir el cambio de configuración a "modo en la nube" para los componentes de protección ofreciendo un nivel de seguridad óptima con un impacto mínimo en los recursos de los equipos y uso de ancho de banda de Internet.
- Debe permitir detectar vulnerabilidades en los dispositivos que ejecuten el sistema operativo Windows y aplicaciones de terceros y Microsoft.
- Debe permitir detectar las aplicaciones instaladas en los dispositivos que hacen uso de los servicios en la nube.

Protección de correo electrónico:
- Debe poder integrarse con Microsoft Outlook.
- Debe poder escanear a través de los puertos SMTP, POP3, IMAP, NNTP y MAPI.
- Debe permitirnos seleccionar si se deseas escanear solo los correos entrantes o los correos entrantes y salientes.
- Debe tener la opción de no escanear archivos comprimidos adjuntos.
- Debe tener una opción de filtrado de archivos adjuntos, permitiendo especificar qué tipo de archivos serán renombrado o eliminados.

Protección web:
- Debe poder analizar la data transferida mediante los protocolos HTTP, HTTPS y FTP.
- Debe de permitir cambiar la acción que el antivirus realizará al detectar algún archivo infectado.
- Debe de permitir realizar exclusiones de URL para que no sean analizadas por el antivirus.
- Debe tener la capacidad de proteger al usuario de ataques tipo phishing.
- El antivirus debe tener una base de datos de enlaces URL que tienen contenido malicioso y que deben ser bloqueados automáticamente.

Protección de red:
- El producto debe incluir un componente de Firewall y Host Intrusion Prevention.
- El producto debe permitir crear reglas para restringir el tráfico de la red a través de puertos o protocolos específicos.

- El producto debe permitir la creación de reglas que restrinjan la actividad de las aplicaciones.
- Regula el acceso de las aplicaciones a datos confidenciales usando reputación local y en la nube sin afectar su rendimiento.
- El producto debe ser capaz de reconocer las redes (zonas) en la cual se encuentra un equipo en la red.
- Debe ser capaz de detectar ataques de red y bloquear al origen, impidiendo cualquier tipo de comunicación.
- Debe de tener la capacidad de generar una lista de equipos confiables o direcciones IP a los cuales el componente de protección de red módulo no bloqueará.

La solución para estaciones de trabajo debe brindar las siguientes funciones de Control:

Control de aplicaciones:
- El producto debe de permitir crear reglas que autoricen o bloqueen la ejecución de aplicaciones.
- Debe de tener diferentes criterios para especificar las aplicaciones a bloquear, como la ruta de la carpeta que contiene el archivo ejecutable, Metadatos, Hash MD5, etc.
- El producto debe de tener una lista de categorías de aplicaciones provista por el fabricante que permita una selección más organizada.
- Debe permitir tener reglas activas, inactivas o en un estado de supervisión, en donde solo audite el acceso a las aplicaciones especificadas.
- Debe tener la capacidad de descubrir y bloquear aplicaciones que consumen servicios de nube, redes sociales y servicios de mensajería de correo electrónico.

Control de navegación web:
- El producto debe controlar el acceso a sitios web en los protocolos HTTP y HTTPS.
- El componente de control web debe incluir clasificación de URLs en base a categorías que permita una selección más organizada, como por ejemplo Violencia, Chat, Redes Sociales, Pornografía, o cualquier otro contenido especificado en una lista de direcciones individuales.
- Debe permitir especificar los usuarios o grupos a los que se les permite o bloquee el acceso a los recursos web descritos por una regla.
- Debe permitir bloquear o advertir mediante notificaciones el acceso al sitio web que se considere potencialmente riesgoso o que no cumpla con las normas de productividad o buen uso del servicio.
- Debe de tener integración con el Directorio Activo para especificar reglas por usuarios o grupos

Control de dispositivos:
- Debe permitir bloquear por tipo de dispositivo de acuerdo con una lista predefinida que incluya como mínimo: USB, CD-ROM o medios de almacenamiento removibles.
- Debe permitir añadir un nuevo tipo de dispositivo en función al ID de hardware o Cass ID.
- Debe de tener integración con el Directorio Activo para especificar reglas por usuarios o grupos
- Debe permitir manejar una lista de dispositivos de confianza.
- Debe permitir especificar el acceso al dispositivo en modo de lectura o de lectura y escritura por usuarios.

Gestión de vulnerabilidades y parches:

- El producto debe brindar funciones de gestión para Endpoint, esta función debe soportar los sistemas operativos Windows 7, Windows 8, Windows 10 y Windows 11 de 64 bits.
- Windows Server 2012, Windows Server 2016, Windows Server 2019, Windows Server 2022 de 64 bits Debe soportar como mínimo las siguientes características:
- Debe permitir escanear mediante la programación de una tarea a todos los equipos de la red corporativa en busca de vulnerabilidades existentes en los sistemas operativos y aplicaciones para luego permitir distribuir los parches o actualizaciones necesarias con la finalidad de mantener la estabilidad y la seguridad de los Endpoint.
- Debe sincronizarse con los servidores de Microsoft que brindan el servicio de Windows Update para descargar las actualizaciones y revisiones disponibles de los sistemas operativos y aplicaciones Microsoft para luego distribuirlas en la red.
- Debe estar en capacidad de realizar tareas de inventario de software de los equipos de la red de modo que los administradores puedan controlar el uso de software.
- Debe estar en capacidad realizar tareas el inventario de hardware en los Endpoint.
- Debe brindar la capacidad por medio de la Consola de Administración de obtener informes personalizados de activos de hardware y licencias de software.

PROTECCION Y ADMINISTRACION PARA EQUIPOS MOVILES.:

- El producto para dispositivos móviles debe poder instalarse sobre equipos con sistema operativos de Smartphone y Tablets basados en Android 4.2 o superior y iOS 10.0 o superior.
- Debe permite preconfigurar y desplegar aplicaciones de manera sencilla vía Google Play, App Store o su propio Self-Service Portal.
- Debe ofrecer protección antimalware contra las amenazas móviles más recientes, debe incluir análisis heurístico con inteligencia de amenazas asistida en nube para Android.
- Verificación de los objetos en la memoria interna del dispositivo y en las tarjetas de expansión.
- Debe permitir filtro de llamadas y bloquear mensaje de texto non deseado.
- Debe brindar funciones antirrobo como limpiar los datos personales, localizar el dispositivo, recibir el nuevo número en caso se reemplace el SIM Card.
- Debe bloquear el acceso a las aplicaciones y los datos corporativos en dispositivos a los que se aplicado rooting o jailbreaking.
- Permitir navegación segura en los navegadores compatibles con Android y iOS mediante el bloqueo de sitios phishing o maliciosos.
- Configurar listas blancas y listas negras de aplicativos que se podrán ejecutar en el dispositivo Android.

PROTECCION PARA CORREO ELECTRONICO:

- El producto debe brindar protección avanzada contra amenazas para los servicios de comunicación y colaboración de Microsoft Office 365.
- Debe permitir la detección y prevención de amenazas avanzadas como phishing, malware, spam y archivos adjuntos no deseados en los servicios ce nube de Exchange Online, OneDrive, SharePoint Online y Teams.
- Debe estar integrado al servicio de Microsoft Office 365 mediante el uso de API, sin la necesidad de hacer enrutamiento del correo electrónico o cambios de registros DNS hacia otra nube pública.
- Debe brindar soporte para el uso de SPF (marco de políticas del remitente), DKIM (identificación por claves de dominio) y DMARC (autenticación de mensajes basado en dominios) para validar los correos electrónicos y prevenir phishing y spam por correo electrónico.

- Debe contar con un centro de administración vía HTTPS que permita configurar las políticas de protección antiphishing, antimalware, antispam y filtro de archivos adjuntos no deseados en el servicio de nube de Exchange Online.
- Debe permitir aplicar las políticas de protección a todos los usuarios de la organización Office 365 o seleccionar a usuarios específicos.

CONSOLA DE ADMINISTRACIÓN CENTRALIZADA.

- La Consola de Administración debe permitir la configuración centralizada de cada una de las características y funciones provistas por los productos de protección para estaciones de trabajo, servidores físicos o virtuales y dispositivos móviles.
- El licenciamiento debe permitir desplegar la consola de administración íntegramente en Cloud, On Premise y en infraestructura de nube pública como Microsoft Azure o AWS.
- En el caso de ser On Premise debe instalarse sobre Sistemas Operativos Windows Server 2012 o superior y bases de datos SQL, Microsoft Azure SQL y MySQL, incluyendo entornos virtualizados.
- La consola de administración deberá permitir la administración centralizada de equipos basados en Windows, Linux, Mac, Android y iOS.
- El acceso a la Consola de Administración debe ser vía protocolo HTTPS.
- El producto debe ser capaz de crear tareas de desinstalación del propio antivirus y de antivirus de terceros.
- El producto debe ser capaz de mostrar los equipos detectados en la red.
- El producto debe permitir al administrador visualizar características de la PC, tales como:
  a) Sistema Operativo y versión.
  b) Nombre de la PC y dirección IP.
  c) Dominio al que pertenece.
  d) Usuarios que han iniciado sesión el equipo.
  e) Si es máquina virtual, tipo de máquina virtual.
  f) Software instalado en el equipo
  g) Características de hardware del equipo
  h) Procesos que se están ejecutando

- La consola de administración centralizada debe tener la capacidad de mostrar los archivos detectados por la protección en los equipos clientes.
- La consola de administración debe ser capaz de poder tener múltiples políticas de seguridad, pudiendo activar una política específica ante epidemias de virus.
- El producto debe tener la capacidad de crear políticas de protección y control para los dispositivos de usuarios móviles.
- El producto debe ser capaz de detectar la red en la que se encuentra la PC y contactar de manera automática al servidor de políticas y actualizaciones correspondiente.
- El producto debe ser capaz de controlar a través de políticas todos los componentes ofrecidos sin necesidad de usar otras consolas adicionales o productos de terceros.
- La consola deberá permitir una estructura de grupos de dispositivos de manera jerárquica para una mejor administración de los clientes antivirus.
- Las políticas de administración de grupos deben poder heredar las políticas de grupos con mayor jerarquía.
- Debe permitir la creación de políticas en modo de test para recopilar información sobre las aplicaciones que se ejecutan en la red y luego usarlas ajustar la configuración en producción.
- La consola de administración debe permitir visualizar las actualizaciones Windows y de terceros que han sido instaladas y las que aún están pendientes por instalar en los dispositivos.

- El producto debe ser capaz de crear un paquete de instalación consolidado (archivo ejecutable) que puede ser accedido como recurso compartido o desde algún dispositivo extermino (CD, USB, etc.), para la instalación de todos los componentes de software de protección.
- Debe poseer un registro o log de los eventos administrativos o detección de malware de manera detallada.
- Debe permitir la delegación de tareas mediante creación de usuarios basados en MS Active Directory con distintos perfiles de administración.
- El producto debe ser capaz de escanear la red por Directorio Activo, Red IP o Dominios, en busca de nuevos equipos en la red.
- El producto debe permitir la generación de reportes gráficos y personalización de los mismos y deben ser exportables a formatos XML, PDF y HTML
- Los reportes deben ser personalizados y como mínimo deben ser:
  a) Reportes de las maquinas más infectadas
  b) Reportes de virus.
  c) Reportes de Actualizaciones
  d) Reportes de ataques de red
  e) Reporte del estatus de la protección.

- La consola debe ser capaz de permitir realizar un backup de sus configuraciones realizadas y de sus registros almacenados en su base de datos.
- El producto debe ser capaz de generación de alertas ante un evento mediante el envío de un correo, o la ejecución de un archivo de lotes.
- La comunicación debe ser cifrada entre servidores y clientes, usando certificados digitales provistos por el propio fabricante.
- Las actualizaciones deben ser descargadas centralizadamente para que los clientes actualicen desde el servidor de administración sus definiciones de malware y parches del producto.
- El producto debe permitir crear categorías de aplicaciones, para autorizarlas o bloquearlas.
- La consola deberá permitir visualizar todos los archivos que hayan sido desinfectados o eliminados en los equipos clientes, y tener la opción de restaurarlos si fuera necesario.
- Debe de permitir elegir cualquier equipo cliente como un repositorio de actualizaciones y de paquetes de instalación, con el fin de optimizar el tráfico de red especificando el ancho de banda con el sitio remoto.
- Debe contar con un indicador de nivel de protección de dispositivos móviles que permite evaluar el nivel de riesgo del dispositivo como alto, medio o bajo.
- Debe permitir auditar los cambios de configuración se aplicado por los administradores.

ENDPOINT DETECTION AND RESPONSE

- La solución debe permitir visibilidad en tiempo real, detección y respuesta automatizada de todas las actividades ejecutadas en los Endpoint.
- La solución debe ser capaz de recopilar los datos necesarios para la resolución de problemas, sin requerir un acceso físico al punto final.
- El fabricante debe tener experiencia probada en el descubrimiento de vulnerabilidades desconocidas, APTs, campañas de ciber espionaje y malware avanzado. Para ello debe haber publicado no menos de 100 documentos sobre campañas de APT y agentes de amenazas durante el último año.
- La solución EDR debe brindar compatibilidad y soporte a los siguientes sistemas operativos:
- Windows 7, Windows 8, Windows 10 y Windows 11 de 64 bits.

- Windows Server 2012, 2012 R2, Windows Server 2016, Windows Server 2019 y Windows Server 2022 de 64 bits.
- La solución debe admitir una comunicación segura entre la consola de administración y los puntos finales con el agente EDR.
- El agente EDR puede estar integrado o no a la solución de Endpoint Security, y debe ser del mismo fabricante.
- La solución de EDR debe brindar una interface para gestionar las políticas, agentes y reportes desde la misma Consola de administración del Endpoint Security.
- El agente EDR se debe poder configurar por medio de una interfaz de línea de comandos.
- La solución debe admitir la generación automática de indicadores de amenazas y/o compromiso (IoC) después de que se produzca la detección, y luego tener la capacidad de aplicar una acción de respuesta.
- La solución debe tener la capacidad de programar el escaneo en todos los puntos finales donde se ejecute el agente EDR con la información de IoC de acuerdo con una planificación del administrador.
- La solución debe admitir la importación de IoC de terceros en formato Open IoC para su uso en el escaneo de los equipos.
- La solución debe permitir tener visibilidad detallada del incidente relacionado con la amenaza detectada en un Endpoint, el incidente debe incluir como mínimo la siguiente información:
  - Gráfico de la cadena de desarrollo de amenazas (Kill Chain).
  - Información sobre el dispositivo en el que se detecta la amenaza (nombre, dirección IP, dirección MAC, lista de usuarios, sistema operativo).
  - Información general sobre la detección, incluido el modo de detección.
  - Cambios de registro asociados a la detección.
  - Historial de presencia de archivos en el dispositivo.
  - Acciones de respuesta realizadas por la aplicación.

- La información de la cadena de desarrollo de la amenaza (Kill Chain) debe proporcionar información visual sobre los objetos involucrados en el incidente, por ejemplo, sobre los procesos ejecutados en el dispositivo, conexiones de red, bibliotecas, llave de registro entre otras.
- La información de un incidente debe presentar una vista detallada de los artefactos del sistema y los datos relacionados con el incidente para el análisis de la causa raíz como por ejemplo:
  - Proceso de spawning
  - Conexiones de red
  - Cambios en el registro
  - Descarga de archivos
  - Dropped de objetos

- El agente EDR debe tener un mecanismo de autodefensa para evitar que se modifique archivos relacionados con su funcionamiento como las entradas de componentes del sistema.

5. Actividades:

El contratista deberá realizar las siguientes actividades.

a) Remitir al correo electrónico cesar@conida.gob.pe el archivo de licencia y las contraseñas de activación.
b) La atención de las fallas se realizará durante los 365 días del año.
c) Asignar, como mínimo, un personal (que cubra el soporte 8*5) con experiencia, quien tendrá a su cargo la solución a los problemas que presente el software.
d) Brindar asesoría en el servicio de renovación de licencia de antivirus informático para los servidores, estaciones de trabajo y portátiles, sin generar costos adicionales.
e) Garantizar la confidencialidad de los nombres y equipos del personal que labora en la Agencia Espacial del Perú - CONIDA.
f) Contar con la capacidad para atender presencialmente los problemas eventuales que se presenten y brindan la solución sin que este genere costos. En este caso particular, la Entidad comunicará vía correo electrónico al contratista el problema, en horario de oficina, y este deberá acercarse a la Entidad el día hábil siguiente.
g) Realizar a solicitud de la Entidad el traslado de la licencia de un equipo a otro sin que genere costo alguno.
h) Asegurar las actualizaciones del software antivirus hasta el término de plazo contratado, que incluyen nuevas versiones y base de datos.

6. Plan de trabajo

No aplicable para esta contratación.

7. Requisitos según leyes, reglamentos técnicos, normas meteorológicas y/o sanitarias, reglamentos y demás normas

No aplicable para esta contratación.

8. Impacto ambiental

No aplicable para esta contratación.

9. Seguros

No aplicable para esta contratación.

10. Prestaciones accesorias a la prestación principal

No aplicable para esta contratación.

11. Garantía del servicio

El servicio deberá estar garantizado por el periodo contratado.

12. Lugar ejecución de la prestación

El servicio se realizará en las instalaciones de la Agencia Espacial del Perú - CONIDA, calle Luis Felipe Villarán N° 1069 - distrito de San Isidro – Lima.

13. Plazo

El plazo de renovación de licencia de antivirus informático para los servidores, portátiles y estaciones de trabajo de la Agencia Espacial del Perú - CONIDA, será de seis (06) días calendario, para entrega de licencia por correo electrónico, contabilizado a partir del día siguiente de notificada la orden de servicio.

14. Entregables

- El proveedor deberá remitir la constancia firmada por el área usuaria, posterior a la realización del servicio de Mantenimiento y Actualización del Antivirus para "Paquete de 250 estaciones de trabajo".

- Entrega de certificado de licencia del software por correo.

15. Requisitos del proveedor

- Deberá estar inscrito en el Registro Nacional de Proveedores. Capítulo de Servicios. En caso de enmarcarse en una contratación menor a una (1) UIT el contratista se encuentra exceptuado de estar inscrito en el RNP, conforme lo establece el art. 10 del Reglamento de la Ley de Contrataciones del Estado. Sin embargo, no deberá encontrarse impedido o suspendido para contratar con el Estado, conforme el literal l) de la Ley de Contrataciones del Estado. (Valor 1 UIT = S/ 4,600.00).
- Registro Único de Contribuyentes (RUC).

16. Recursos y facilidades a ser previstos por la Entidad

Acceso al servidor de licencias para las configuraciones requeridas, previa coordinación en el área usuaria.

17. Adelantos

No aplicable para esta contratación.

18. Confidencialidad

Toda información del CONIDA a que tenga acceso el contratista, así como su personal, producto de la presente contratación, es estrictamente confidencial. El contratista y su personal se comprometen a mantener las reservas del caso y no transmitirla a ninguna persona (natural o jurídica) sin la autorización expresa de la entidad.

19. Propiedad intelectual

No aplica a la presente contratación.

20. Medidas de control durante la ejecución contractual

El personal de la Oficina de Tecnologías de la Información (OFTIN) supervisara el cumplimiento de los servicios.

21. Conformidad de la prestación

La conformidad del servicio será otorgada por el jefe de la Oficina de Tecnologías de la Información (OFTIN).

22. Forma de pago

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

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

- Informe de conformidad brindada por el área usuaria.
- Comprobante de pago.
- Acta de conformidad.

23. Penalidades aplicables

23.1 Penalidad por mora

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto de la contratación, la Entidad le aplica automáticamente una penalidad por mora por cada día de atraso.

23.2 Calculo de la penalidad diaria:

$$Penalidad\ diaria = \frac{0.10\ x\ monto}{F\ x\ plazo\ de\ vigencia}$$

Dónde:
Monto: monto del servicio.
Plazo de vigencia: en días, desde la recepción de la orden de servicio por parte del contratista hasta el último día del periodo de ejecución del servicio.
F = 0.40, para plazos menores o iguales a 60 días calendarios.
F = 0.25, para plazos superiores a 60 días calendarios.

Cálculo de la penalidad a aplicar:
Penalidad a aplicar = Penalidad diaria x días de retraso.

23.3 Consideraciones generales

- El monto máximo de la penalidad por mora no superará el diez por ciento (10%) del monto de la orden de servicios.
- Esta penalidad se deduce de los pagos a cuenta o del pago final.
- Superado el monto máximo de la penalidad, la Entidad puede resolver la contratación.

24. Responsabilidad por vicios ocultos

La responsabilidad por vicios ocultos es de un (1) año, contado a partir de la recepción conforme del servicio.

San Isidro, 17 de julio de 2024

Firmado Digitalmente

Firmado digitalmente por OTERO CORDOVA Miguel Eduardo FAU 20131371889 hard
Motivo: Soy el autor del documento
Fecha: 18.07.2024 11:26:07 -05:00

Coronel FAP
MIGUEL OTERO CORDOVA
Jefe de Tecnologías de la Información
AGENCIA ESPACIAL DEL PERÚ - CONIDA