"ADQUISICIÓN DE LICENCIAS DE SOFTWARE ANTIVIRUS PARA LOS EQUIPOS DE COMPUTO DE LA UNIVERSIDAD NACIONAL AGRARIA DE LA SELVA"

OBJETO.
Adquirir licencias de antivirus para la seguridad y protección de las estaciones de trabajo y servidores de la Universidad Nacional Agraria de la Selva.

FINALIDAD PÚBLICA.
Salvaguardar la seguridad de información brindando protección antivirus de forma eficiente de los equipos de cómputo de la Universidad Nacional Agraria de la Selva.

CARACTERÍSTICAS Y CONDICIONES DE LOS BIENES A CONTRATAR.

- Descripción y cantidad de los bienes a contratar:

N° Ítem	DESCRIPCIÓN DEL SERVICIO	UNIDAD DE MEDIDA	CANTIDAD
1	Licencia de Software Antivirus	UNIDAD	1000

- Descripción de las características técnicas de licencias de Antivirus para las estaciones de trabajo y servidores:

SOLUCIÓN DE PROTECCIÓN PARA ESTACIONES DE TRABAJO	• La solución (en su última versión) deberá ser compatible con los siguientes sistemas operativos: Microsoft® Windows® 11/10/8. (32-64 bits) Ubuntu, RedHat , SUSE, CentOS, Fedora, Mandriva, Open Suse, Mac Os. • 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 del contenido del tráfico de la red y además permita proteger de ataques haciendo que cualquier dañino sea bloqueado. • Debe contar con un módulo de detección en tiempo real que protega contra virus, gusanos, troyanos, malware, keyloggers,dialers, spyware, adware, hacktools, rootkits, bots, ransomwar y herramientas de control remoto, asi como otro programas potenciamente peligrosos. • Debe ser capaz de revisar llaves específicas del registro del sistema operativo e impedir intentos de modificación de escritura y lectura. • 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. • El producto ofertado debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o carpeta específica. • El producto ofertado debe pedir una contraseña ante intentos de cambio indebidos en la configuración del producto. • El cliente antivirus debe tener un agente que le permita ser administrado desde una consola centralizada. Este agente debe reportar el estado de todas las soluciones antivirus instaladas en la dependencia. • El producto ofertado deberá permitir generar dentro de la misma solución antivirus repositorios de actualización, los cuales deberán ser distribuidas mediante protocolo http localmente, sin depender de aplicaciones externas o de tareas desde la consola de Administración. • El producto ofertado debe tener una funcionalidad en donde todas las ventanas emergentes se deshabiliten y la protección del sistema seguirá ejecutándose en segundo plano, pero no requerirá ninguna interacción por parte del usuario. • El producto ofertado deberá tener una funcionalidad de catalogar a los procesos de los equipos de acuerdo con la reputación basada en la nube. Esta permitirá recopilar información anónima del ordenador afectada con las amenazas detectadas recientemente. • La solución debe usar un sandboxing para analizar el comportamiento del malware • Debe tener la capacidad de realizar un rolback de las firmas de virus en caso no se completa la

	actualización. • El producto ofertado debe permitir definir tiempos/horarios de uso para las reglas de control web. • El producto debe tener la capacidad de establecerse en modo silenciosos, deshabilitando todas las notificaciones del mismo. • El producto debe tener un control Web para limitar el acceso a sitios web por categoría o bien un sitio web, además de poner mostrar al usuario una notificación de bloqueo • El producto ofertado deberá analizar protocolos de e-mail POP3, OP3s IMAP, IMAPS, y IMPAP4. • Debe permitir recopilar información anónima del equipo de computo afectado con las amenazas detectadas recientemente. Esta información en ningún caso podría ser el archivo completo. • 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. • La solución de antivirus debe ejecutar un escaneo o exploración de cualquiera de lo siguientes estados en la computadora, protector de pantalla o salvapantalla activo, sesión de usuario bloqueado, sesión de usuario finalizado. • La solución debe ser capaz de definir un listado especifico de usuarios quienes pueden quienes pueden ser uso de los dispositivos. Por dispositivos de almacenamiento, la solución debe permitir configurar los siguientes permisos, Lectura/escritura, bloquear, solo de lectura, advertir. • 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. • 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 protección de archivos en tiempo real contra malware debe tener las siguientes características; contar con niveles predefinidos de protección e igualmente permitir al usuario personalizar el nivel de protección de acuerdo con sus requerimientos, permitir escanear archivos comprimidos, y definir el nivel de compresión analizar. Permitir exclusiones de unidades, carpetas o archivos, a escanear para la protección en tiempo real, contar con un motor heurístico para detección de posibles nuevo virus. • Debe contar con un modulo de protección de correo electrónico en tiempo real con la siguientes características, integrarse con clientes de correo electrónico como Microsoft Outlook, Outlook Express, Windows mail y Mozila Thunderbild, escanear a través de los puertos POP3, POP3S, IMAP, IMAPS, SMTP. Tener niveles predefinidos de protección y permitirle al usuario personalizar el nivel de protección de acuerdo con sus requerimientos. Permitir escaneos de correo entrante, saliente o ambos. Contar con la capacidad que después de analizar un mensaje de correo electrónico se pueda adjuntar al mensaje una notificación del análisis. contar con un motor heurístico para detección de posibles nuevo virus. Permitir escanear archivos comprimidos y también definir el nivel de compresión a analizar. • Debe tener un modulo de protección para la navegación web en tiempo real, con las siguientes características; poder escanear el protocolo http, tener niveles predefinidos de protección e igualmente debe permitir al usuario personalizar el nivel de protección de acuerdo a sus requerimientos. escanear a través del protocolo SSL (HTTPS), de manera que se pueda impedir la descarga de archivos infectados. permitir realizar exclusiones de URL para que no sean analizadas por el antivirus tanto en el protocolo HTTP, y HTTPS. E proteger contra phishing, tener un motor heurístico para detección de posibles nuevo virus • El producto ofertado debe tener un Módulo de control de dispositivos que permita acceso de solo lectura, lectura/escritura o bloquear dispositivos de acuerdo con una lista predefinida que incluya como mínimo: dispositivos USB, CD-ROM y dispositivos Bluetooth o módems. • El producto ofertado debe tener un módulo de control de dispositivos que permita crear varios grupos de dispositivos donde se podrán aplicar reglas distintas y además permitirá detectar los dispositivos conectados a la PC y agregarlos al listado de grupo de dispositivos. Además, incluye la funcionalidad de aplicar esta regla por un período de tiempo determinado (hora y días). • El producto ofertado debe ser capaz de crear CD's, ISO's o USB de rescate, que permitan escanear los equipos Microsoft. • El producto debe contar con una primera exploración automática después de la instalación del programa, lo que permite asegurar que el equipo se encuentra protegido desde el comienzo.

	• El producto debe permitir realizar exploraciones completas mientras el equipo no está en uso, es decir que realice el escaneo cuando el equipo se encuentre bloqueado o suspendido. Esto con la finalidad de obtener un mejor rendimiento y limpieza del sistema. • El producto ofertado debe contar con una herramienta que permita examinar a fondo el ordenador, y con esta información poder ayudar a determinar la causa de un comportamiento sospechoso en el equipo que pueda deberse a una infección de malware o incompatibilidad de software o hardware. La información para recopilar deberá ser detallada sobre los componentes del sistema (como los controladores, aplicaciones instaladas, conexiones de red o entradas importantes del registro). • La solución deberá poder realizar exploraciones en estado inactivo para poder brindar de esa forma, una protección proactiva mientras el equipo no está en uso. • La solución deberá contar con la funcionalidad de bloqueo de exploits, que evite la explotación de vulnerabilidades en las aplicaciones. • La solución debe contar con un sistema de alerta temprana, que evalué la reputación de los archivos, acelerando las exploraciones del sistema, minimizando la detección de falsos positivos, este sistema deberá estar basando en actualizaciones a través e la nube. • La solución debe contar con un modulo de exploración avanzada de memoria que permita detectar las amenazas mas sofisticadas que están diseñadas para evadir la detección a través de mecanismo tradicionales. • La solución deberá contar con un módulo de protección contra Botnets, este módulo debe ser capaz de detectar conexiones con servidores maliciosos. • El fabricante debe brindar servicios de ciberseguridad informática como por ejemplo, penetration testing, vulnerability assessment o análisis de GAP. • El fabricante debe contar con soporte técnico en español. • El fabricante deberá ser un producto reconocido en el mercado, estando presente como minimo en 2 reportes de gartners de los ultimos 3 años (2023-2022-2021) dentro del cuadrante de lideres o challengers para plataformas de proteccion endpoint (Magic Quadrant for Endpoint Protection Platforms) • Magic Quadrant, es una empresa estadounidense dedicada a la consultoría e investigación de las tecnologías de la información. Cuenta con una denotada reputación mundial y ha elaborado un Cuadrante Mágico (Magic Quadrant) muy reconocido, y utilizado como guía empresarial a la hora de elegir proveedores tecnológicos.
SOLUCIÓN DE PROTECCIÓN PARA SERVIDORES.	• El software antivirus debe poder instalarse en su última versión, sobre plataformas Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022. • 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. • La solución debe tener sistema de prevención de intrusiones basado en el host, (HIPS). • El sistema HIPS debe tener los siguientes modos de configuración: automático, inteligente, interactivo, basado en políticas y aprendizaje. • El producto debe permitir escanear archivos comprimidos. • Debe permitir elegir las unidades a escanear para los escaneos bajo demanda. • En sistemas operativos Windows, el antivirus deberá contar con una herramienta integrada que permita inspeccionar completamente componentes del sistema (Controladores, Aplicaciones

	Instaladas, Conexiones de Red y entradas importantes del Registro de Windows), esto con la finalidad de determinar la causa de comportamientos sospechosos en el sistema que puede deberse a incompatibilidad de software, hardware o código malicioso. • Debe tener un caché local para aumentar el rendimiento de los entornos virtuales, garantizando que el archivo sólo se explora una vez.
CONSOLA DE ADMINISTRACIÓN CENTRALIZADA.	• La consola debe ser con infraestructura en la nube, implementado como un servicio SAAS, no debe ser necesario de un servidor local para su implementación. • La consola de administración debe permitir la configuración y administración remota de la solución antivirus instalada en las estaciones de trabajo y servidores (Windows, Linux, Mac). Soporte para dispositivos móviles. • Debe permitir la delegación de tareas mediante creación de usuarios con distintos perfiles de administración, de tal manera que se puedan agregar usuarios con diferentes niveles de acceso o permisos. • Por medidas de seguridad la consola de administración debe contar con un doble factor de autenticación para ingresar a la consola, que consiste en una contraseña permanente y una contraseña adicional o token de un solo uso. • La consola debe tener medidas de protección de acceso frente a ataques de fuerza bruta, como bloquear el acceso luego de varios intentos fallidos de inicio de sesión. • La consola de acceso al servidor deberá ser 100% web, siendo compatible con los siguientes navegadores: Mozilla Firefox, Microsoft SCCM, Google Chrome, Safari, Opera. • El servidor se deberá comunicar con los endpoints a través de un agente que sea capaz de almacenar las políticas y ejecutar tareas de manera offline. • El acceso a la consola a través del interfaz web se bloqueará de forma temporal (aproximadamente 10 minutos), luego de 10 intentos de inicio de sesión no satisfactorios, desde una misma dirección IP. • El producto debe ser capaz de mostrar los equipos detectados en la red. • La consola de administración centralizada debe tener la capacidad de mostrar los intentos de infección de virus en los equipos clientes. • El producto debe ser capaz de controlar a través de políticas todos los componentes mencionados anteriormente (para Workstation y servers) sin necesidad de consolas adicionales para la creación de políticas. • El producto debe poseer una interfaz web que permita monitorear el estado de los equipos en la red, así como también, mostrar como mínimo reportes sobre: el estado de carga del servidor, 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 los servidores y clientes antivirus. • El producto debe ser capaz de crear tareas de desinstalación del propio antivirus y de 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 ser 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 para que los clientes actualicen desde el servidor de administración 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.

PERFIL DEL PROVEEDOR

El proveedor deberá cumplir los siguientes requisitos y acreditarlos, al momento de formalizar el contrato (Orden de Servicio):

- Persona Jurídica.
- Experiencia de 3 años mínimo en brindar servicios iguales o similares.
- Contar con Registro Nacional de Proveedores (RNP), si la propuesta económica es >1UIT.
- Contar con Código de Cuenta Interbancaria (CCI) – cuenta relacionada al número de RUC.
- Contar con registro único de contribuyentes (RUC) vigente
- Declaración jurada simple de no estar impedido y/o inhabilitado para contratar por el estado
- El postor deberá ser partner autorizado de la marca ofertada y como mínimo deberá contar con la categoría Silver.
- Deberá contar con Un (01) Profesional titulado en Ingeniería Electrónica y/o Ingeniería de Sistemas y/o Ingeniería de Software y/o telecomunicaciones y/o redes y comunicaciones y/o electrónica y/o redes y comunicaciones de datos y/o informática y sistemas, con certificados técnicos del fabricante.

GARANTÍA:

Garantía mínima de 12 meses contados a partir de la instalación de las licencias de antivirus en la consola de Administración.

SOPORTE TECNICO:

El contratista brindará la documentación del contacto autorizado (nombre completo, número telefónico, correo electrónico y dirección de ser necesario), al momento de la firma del contrato.

El postor deberá de contar con un Centro de Operaciones de Seguridad (SOC) propia para brindar el soporte 24x7x365, que debe contar con las siguientes características:

- Soporte (24x7), de un técnico especializado hasta llegar a solucionar la emergencia.
- Soporte técnico online, en forma remota, correo electrónico y telefónicamente.
- El proveedor de antivirus deberá contar como mínimo con dos personas de soporte certificados por la marca del producto.
- El proveedor deberá entregar un informe técnico detallado luego de realizar las tareas y pruebas de soporte.

El fabricante deberá contar con un laboratorio antivirus instalado en la región de Sudamérica para garantizar respuestas inmediatas frente a emergencias de infección o ataques de malware.

CAPACITACIÓN:

- La empresa proveedora deberá brindar capacitación sobre el uso de las herramientas administrativas del software y la configuración de cada producto de la solución entregada, según el perfil del usuario (Administradores y soporte técnico).
- La capacitación deberá realizarse dentro de los 30 días calendarios posteriores a la fecha de recepción e instalación del producto.
- El instructor o los instructores designados por el postor deberán estar certificados por el fabricante del producto que presenten, debiendo presentar sus certificaciones y tener como mínimo Bachiller en estudios de Ingeniería Informática.
- La empresa proveedora asumirá todos los costos que impliquen la capacitación.
- El proveedor deberá realizar charlas sobre temas generales de Seguridad de la información y protección frente a malware a solicitud al menos 3 veces durante la vigencia de la licencia.

VIGENCIA TECNOLÓGICA:

- Cuando se presenten versiones nuevas de la solución antivirus durante el periodo de 12 meses de vigencia de la licencia, el proveedor deberá hacer la entrega de todos los componentes del software actualizados sin costo adicional.
- El proveedor deberá realizar la actualización, migración e instalación de los componentes del software antivirus necesarios para contar con la versión actualizada y estable. Estas tareas deberán ser detalladas en un plan de trabajo

LUGAR Y PLAZO DE EJECUCION DE LA PRESTACIÓN:

- **Lugar de entrega licencias:** Las licencias serán configuradas y habilitadas directamente en el servidor de Antivirus de manera digital debiendo de enviar información de la adquisición de licencias al correo: oti.redes@unas.edu.pe, , en el horario de lunes a viernes de 8:00 am a 16:00 pm horas.

- **Plazo de entrega de equipos:** Las licencias deberán ser entregadas y configuradas en el plazo de QUINCE (15) días calendarios, contados a partir del día siguiente de la suscripción del contrato o de recibida la Orden de Compra.

FORMA DE PAGO:

Se realizará según lo dispuesto en el Art. 149º del reglamento de Ley de Contrataciones del Estado, previa entrega del comprobante de pago y conformidad del servicio del área usuaria.

PENALIDADES:

En caso de retraso injustificado del contratista en la ejecución de la prestación objeto de la contratación, la Entidad le aplicará automáticamente una penalidad por cada día de atraso, la cual se calculará de conformidad al artículo 162° del reglamento de la Ley de Contrataciones del Estado.

OBLIGACIONES DE LA UNAS:

La UNAS como entidad contratante se compromete a:

- Proporcionarle al contratista todas las facilidades durante la ejecución del contrato o orden de compra.
- Realizar el pago de los servicios según lo pactado.

OBLIGACIONES DEL PROVEEDOR DEL SERVICIO:

El proveedor se compromete a cumplir con las condiciones ofrecidas en su proforma de acuerdo con los términos de referencia y la orden de servicio.

- El Contratista es el único responsable de cumplir con la entrega de las licencias a contratar, no pudiendo transferir esa responsabilidad a otras entidades ni a terceros.
- El contratista se encargará de realizar la activación de las licencias de antivirus en la consola de administración.

DOCUMENTOS ENTREGABLES Y CONSIDERACIONES OBLIGATORIAS PARA LA PROVISIÓN DEL BIEN

- El Postor en su oferta técnica, debe presentar una descripción de todas las características técnicas de las licencias de antivirus, indicando (marca y versión), acompañado con información complementaria contenida en folletos, instructivos, catálogo, manuales, fichas técnicas, u documentos técnicos del fabricante o representante de la marca.
- El postor deberá adjuntar documentación oficial del fabricante de la solución ofertada o del Distribuidor Autorizado o representante de la marca en el Perú.
- El postor deberá presentar una declaración jurada el cual se comprometerá a brindar los servicios de soporte técnico y Centro de Operaciones de Seguridad SOC, por el periodo del servicio contratado.

CONFORMIDAD DEL SERVICIO A CONTRATAR:

La conformidad del servicio estará a cargo de la dirección de la Oficina de Tecnologías de Información de la Universidad Nacional Agraria de la Selva.

La previa verificación de la calidad, funcionamiento y cumplimiento de los términos de referencia, tal como lo establece el artículo 143º del reglamento de la Ley de Contrataciones del Estado.

CONFIDENCIALIDAD:

Toda información a que tenga acceso el contratista, su personal, es estrictamente confidencial, debiendo mantener las reservas del caso y no transmitirla en ninguna circunstancia.