UNIVERSIDAD NACIONAL AGRARIA DE LA SELVA
OFICINA DE TECNOLOGIA DE LA INFORMACION Y COMUNICACIÓN
www.unas.edu.pe soporte.ctic@unas.edu.pe
Av. Universitaria Km. 1.2 - Telf. (062) 562056

INFORME N.º 006-2022-AREA DE SOPORTE TECNICO-OTIC-UNAS

PARA : **Ing. Carlos Quito López.**
Director de la Oficina de Tecnología de la Información y Comunicación.

DE : **Gonzalo P. Meléndez Guerra.**
Téc. AST - OTIC

REFERENCIA : Oficio: N.º 023-2022-OTIC-UNAS.

FECHA : 08/02/2022

Universidad Nacional Agraria de la Selv
Tingo María
CENTRO DE TECNOLOGIA DE LA INFORMACIÓN Y COMUNICACIÓN
RECIBIDO
09 FEB 2022
Firma: Hora: 10:15

De mi estima consideración;

Por medio de la presente me dirijo a su persona para manifestarle mi afectuoso saludo, y a la vez informarle el requerimiento para la adquisición de Antivirus, para la protección de los equipos de cómputo de la corporación universitaria:

TÉRMINOS DE REFERENCIA

"ADQUISICIÓN DE LICENCIA DE SOFTWARE ANTIVIRUS"

La presente tiene como objetivo contar con un software antivirus que permitirá la seguridad y protección de los servicios y sistemas de usuario de la institución.

REQUERIMIENTO

Nº	DESCRIPCION	CANTIDAD	UNIDAD DE MEDIDA
01	Licencia de Software Antivirus	1000	UND

I. PLAZO DE ENTREGA Y DESPLIEGUE

1. El proveedor deberá entregar la licencia del producto en un plazo máximo de 5 días calendarios.
2. El proveedor deberá instalar, configurar y/o implementar la solución de antivirus en un plazo no mayor de 15 días calendarios contados a partir del día siguiente de la firma de contrato.

II. ESPECIFICACIONES TÉCNICAS

1. **CONTAR CON UNA VERSIÓN DE ANTIVIRUS PARA ESTACIONES DE TRABAJO Y SERVIDORES QUE CUMPLA CON:**

   1.Debe poder instalarse sobre todas las versiones de Windows 8, 8.1 y 10; en las arquitecturas de 32 y 64 bits.
   2. Debe poder instalarse sobre todas las versiones de Windows Server, 2012, 2016, 2019.
   3. Debe poder instalarse como mínimo sobre las siguientes distribuciones de Linux: Red Hat, CentOS, Fedora, Mandriva, OpenSuse y Ubuntu, en las arquitecturas de 32 y 64 bits.

4. Debe poder instalarse sobre Mac OS X 10.6, 10.7, 10.8, 10.9, en las arquitecturas de 32 y 64 bits.
5. El fabricante deberá ocupar una posición de Líder o Challenger en el Cuadrante Mágico de Gartner en las plataformas Antivirus en el último año.
6. El fabricante deberá poseer al menos el 80% de éxito en las participaciones en los premios VB100 de Virus Bulletin hasta el 2020.
7. El fabricante deberá haber recibido el premio Gold o Silver por las pruebas de protección contra malware de AV-Comparatives en el año 2020.
8. El fabricante deberá haber recibido el premio Gold o Silver por las pruebas de falsos positivos de AV-Comparatives en el año 2020.
09.Debe tener la capacidad de funcionar sobre los siguientes requerimientos mínimos de hardware: Memoria RAM de 512 MB. Procesador Intel Core2Duo hacia adelante.
10. Debe contar con un módulo de detección en tiempo real que proteja contra: virus, gusanos, troyanos, malware, keyloggers, dialers, adware, spyware, hacktools, rootkits, bots, ransomware y herramientas de control remoto, así como otros programas potencialmente peligrosos.
11. El producto debe contar con un Firewall de Protección para una Red Local e Internet.
12. Debe ser capaz de monitorear el comportamiento de aplicaciones específicas, para determinar el posible uso o intento de modificación de estas aplicaciones por agentes maliciosos y bloquear estas acciones.
13. Debe ser capaz de revisar llaves específicas del registro del sistema operativo e impedir intentos de modificación, de escritura y de lectura.
14. Debe analizar protocolos de e-mail POP3, POP3s, IMAP, IMAPS y IMAP4.
15. Debe contar con herramientas de exploración bajo línea de comando (CLI) para la exploración y limpieza de virus.
16. 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.
17. Debe contar con un sistema de alerta temprana, que evalúe la reputación de los archivos acelerando las exploraciones del sistema, minimizando la detección de falsos positivos, este sistema deberá estar basado en actualizaciones a través de la nube.
18. Debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o carpeta específica.
19. Debe poder realizar escaneos manuales o programados, indicándose las unidades a escanear o las carpetas específicas que requieren ser escaneadas.
20. Debe pedir una contraseña ante intentos de cambio indebidos en la configuración del producto.
21. Debe permitir ser administrado desde una consola centralizada.
22. Debe permitir la actualización del producto a través de la red local e internet.
23. Debe tener la capacidad de generar dentro del mismo producto, repositorios de actualización, los cuales deberán ser distribuidas mediante protocolo HTTP, sin depender de aplicaciones externas.
24. Debe tener la capacidad de realizar un rollback de las firmas de virus en caso no se completa la actualización.
25. Debe tener la capacidad de establecerse en modo silencioso, deshabilitando todas las notificaciones del mismo.
26. Debe permitirle al usuario y/o administrador de red la creación de reglas con el fin de evitar o permitir las modificaciones y accesos no autorizados en carpetas, registro del sistema, acceso a aplicaciones y archivos.
27. Debe contar con un sistema avanzado de alerta que permita combatir las amenazas emergentes según su reputación.

28. Debe permitir recopilar información anónima del equipo de cómputo afectado con las amenazas detectadas recientemente. Esta información en ningún caso podrá ser el archivo completo.
29. La solución debe tener un módulo Antiransomware.
30. La protección de archivos en tiempo real contra malware debe tener las siguientes características:
a. Contar con niveles predefinidos de protección e igualmente permitir al usuario personalizar el nivel de protección de acuerdo con sus requerimientos.
b. Permitir escanear archivos comprimidos y definir el nivel de compresión a analizar.
c. Permitir la exclusión de unidades, carpetas o archivos a escanear por la protección en tiempo real. d. Contar con un motor heurístico para detección de posibles nuevos virus.
31. Debe contar con un módulo de protección de correo electrónico en tiempo real, con las siguientes características:
a. Integrarse con clientes de correo como Microsoft Outlook, Outlook Express, Windows Mail y Mozilla Thunderbird.
b. Escanear a través de los puertos POP3, POP3S, IMAP, IMAPS, SMTP.
c. Tener niveles predefinidos de protección y permitirle al usuario personalizar el nivel de protección de acuerdo con sus requerimientos.
d. Permitir escaneo de correo entrante, saliente o ambos.
e. Contar con la capacidad que después de analizar un mensaje de correo electrónico se pueda adjuntar al mensaje una notificación del análisis.
f. Tener la capacidad de proteger al usuario de ataques tipo phishing.
g. Tener un motor heurístico para detección de posibles nuevos virus
h. Permitir escanear archivos comprimidos y también definir el nivel de comprensión a analizar.
32. Debe tener un módulo de protección para la navegación web en tiempo real, con las siguientes características:
a. Poder escanear el protocolo http.
b. Tener niveles predefinidos de protección e igualmente debe permitir al usuario personalizar el nivel de protección de acuerdo a sus requerimientos. c. Escanear a través del protocolo SSL (HTTPS), de manera que se pueda impedir la descarga de archivos infectados.
d. Permitir realizar exclusiones de URL para que no sean analizadas por el antivirus tanto en el protocolo HTTP, FTP y HTTPS.
e. Proteger contra phishing.
f. Tener un motor heurístico para la detección de posibles nuevos virus.
33. Debe tener un módulo de control de dispositivos, con las siguientes características: a. Permitir el acceso de solo lectura, lectura/escritura o bloquear dispositivos de acuerdo a una lista predefinida que incluya como mínimo: dispositivos USB, CD-ROM y dispositivos Bluetooth o módems. b. Tener la capacidad de analizar automáticamente el dispositivo al ser conectado al ordenador.
34. Debe tener un sistema de prevención de intrusos, este sistema debe encontrarse disponible para el host y debe proteger el sistema frente a un código malicioso o cualquier actividad no deseada que intente perjudicar la seguridad de la PC.
35. Debe ser capaz de crear CD's, ISO's o USB de rescate, que permitan escanear particiones FAT y NTFS.
36. El fabricante deberá contar con Soporte Técnico en idioma español.
37. El fabricante deberá tener documentación publicada en internet en idioma español.
38. El fabricante deberá brindar servicios de seguridad informática como, por

ejemplo: penetration testing, vulnerability assessment o análisis de GAP.
39. El fabricante deberá contar con un laboratorio de análisis y detección de malware en Latinoamérica.
40. El fabricante deberá tener educación de seguridad en español.
41. Deberá contar con oficinas de la marca en Latinoamérica y presencia local en el país.
42. 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.
43. El producto debe tener un control web para limitar el acceso a los sitios web por categoría o bien una categoría de sitios web, además de poder mostrar al usuario una notificación de bloqueo.
44. Deberá tener la capacidad para instalar los parches del sistema operativo.
45. La solución deberá contener dentro del módulo de firewall la funcionalidad de bloqueo de exploits, que evite la explotación de vulnerabilidades en las aplicaciones.
46. La solución debe usar sandboxing en la nube para analizar el comportamiento del malware.
47. 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.
48. a solución deberá contar con un 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.
49. La solución deberá contar con un módulo de protección Anti-Phishing, que detecte sitios fraudulentos y bloqueo el acceso total, evitando que los usuarios ingresen cualquier tipo de información.
50. 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
51. La solución debe ser capaz de permitir o negar el uso de los dispositivos en base a los siguientes criterios: Fabricante, Modelo, Número de serie
52. La solución debe ser capaz de definir un listado específico de usuarios quienes pueden hacer uso de los dispositivos. Para dispositivos de almacenamiento, la solución debe permitir configurar los siguientes permisos: Lectura/Escritura, Block, Solo de lectura, Advertir
53. Cuando se conecta o usa un dispositivo de almacenamiento, la solución de antivirus debe proporcionar las siguientes opciones: Escanear, No realizar ninguna acción, Recordar esta acción
54. El sistema HIPS debe tener los siguientes modos de configuración: Modo automático o Modo inteligente o Modo interactivo, Modo basado en políticas, Modo aprendizaje
55. Firewall personal, la solución de antivirus debe contar con un firewall personal y debe tener los siguientes modos de configuración: Modo automático, Modo interactivo, Modo basado en políticas, Modo aprendizaje
56. Las reglas de firewall creadas deberán ser capaces de permitir todas las siguientes acciones: Denegar, Permitir, Preguntar
57. Cuando se trabaje en entornos virtualizados, la solución deberá permitir la creación de una lista blanca de archivos seguros que se compartan dentro de la red virtual.
58. Para los dispositivos de almacenamiento, la solución debe permitir definir los siguientes permisos para su uso: Lectura/escritura, Bloquear, Solo Lectura, Advertir
59. La solución deberá contar con un módulo de protección contra Botnets, este

módulo debe ser capaz de detectar conexiones con servidores maliciosos.
60. La solución al conectar un dispositivo de almacenamiento o utilizar un medio de extraíble, deberá brindar las siguientes opciones al usuario: Explorar ahora, Explorar más tarde, Configurar, la exploración automática ó no hacerlo.

2. **CONTAR CON UNA CONSOLA DE ADMINISTRACIÓN CENTRALIZADA QUE CUMPLA CON:**

1. Debe permitir la configuración y administración remota del antivirus instalado en las estaciones de trabajo y/o servidores (Windows, Linux, Mac).
2. Debe contar con manual de ayuda que facilite la configuración del producto.
3. Debe tener una interfaz totalmente gráfica, amigable e intuitiva.
4. Debe tener la capacidad de creación de usuarios y perfiles de acceso a la consola.
5. Debe tener soporte para la administración de dispositivos móviles.
6. Debe poder instalarse sobre Windows Server 2019, 2016, Windows server 2003, Windows server 2008, Microsoft Windows Server 2008 R2 (versiones de 32 y 64 bits), Windows Server 2012, Windows 7, Windows 8.1 windows 10. o en distribuciones server Linux de 32 y/o 64 bits.
7. Debe tener la capacidad de enviar acciones de red como (wake on lan, ping, apagado remote, RDP y mensajes).
8. Debe ser capaz de mostrar en tiempo real los equipos detectados en la red.
9. Debe tener la capacidad de mostrar los intentos de infección de virus en los equipos clientes.
10. Debe permitirle al usuario administrador visualizar las características del equipo de cómputo, tales como: Sistema Operativo y versión del mismo. Nombre del equipo. Dirección IP. Software antivirus instalado en los equipos.
11. Debe ser capaz de controlar a través de políticas todos los componentes mencionados anteriormente (para estaciones de trabajo y servidores) sin necesidad de consolas adicionales para la creación de políticas.
12. Debe poseer una interfaz web que permita monitorear el estado de los equipos en la red mediante una gama de múltiples reportes como el estado de carga del servidor, clientes con mayor registro de amenazas, principales amenazas, clientes con más amenazas, clientes actualizados y no actualizados, etc.
13. Debe permitir una estructura jerárquica para una mejor administración de los clientes antivirus.

14. Debe permitir mostrar el contenido de la cuarentena de los clientes y crear tareas para restaurar o borrar los archivos de cuarentena basados en una variedad de criterios o excluirlos de futuros análisis.
15. Debe tener soporte para Microsoft Network Access Protección (NAP).
16. Debe permitir la instalación y desinstalación remota del antivirus en los equipos clientes.
17. Debe permitirla instalación y administración del antivirus a través de un agente.
18. Debe poseer un log de eventos detallados para auditoría.
19. Debe ser capaz de escanear la red por Directorio Activo, Red IP o Dominios, en busca de nuevos equipos agregados a la red.
20. Debe permitir la generación de reportes gráficos y personalizados, fácilmente exportables en formatos HTML y CSV como mínimo.

21. Como mínimo se deben contar con los siguientes reportes: Reportes de las máquinas más infectadas. Reportes de malware. Clientes no actualizados.
22. Debe ser capaz de permitir backup de las configuraciones realizadas en el sistema.
23. Debe ser capaz de generar alertas ante un evento específico mediante el envío de un correo.
24. Las actualizaciones del producto antivirus de las estaciones cliente debe ser descargada centralizadamente a través del servidor de administración.
25. Debe permitir soporte para múltiples bases de datos, como mínimo: Microsoft SQL Server, MySQL y Oracle.
26. Deberá permitir la ejecución remota de scripts, batch files y paquetes personalizados a través de la consola, de terceros.
27. Debe permitir generar grupos de clientes dinámicos y grupos estáticos.
28. El fabricante debe proporcionar al menos tres diferentes formas de realizar la instalación de la consola de administración. Instalador todo en uno, Instalación por componentes, Aparato virtual
29. El aparato virtual debe soportar al menos las siguientes plataformas de virtualización, VMWare vSphere, Oracle Virtual Box, Microsoft Hyper-V, Azure - ambiente basado en la nube
30. La consola de Administración deberá soportar su instalación sobre Linux.
31. Deberá tener una consola de administración de licencias en la nube, donde se pueda revisar el detalle de los equipos a los que se les ha provisionado licenciamiento.
32. Activar el acceso a la consola de antivirus con doble factor de autenticación, deber estar integrada a la misma consola de antivirus, sin ningún add-on ó software adicional.
33. La solución debe tener el mecanismo para quitar otras soluciones antivirus presentes en el endpoint. Este mecanismo debe ser o estar: Integrado a la solución antivirus, Como una herramienta independiente, Disponible solamente a través de una consola de administración

III. CAPACITACIÓN

1. 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).
2. El instructor o los instructores designados por el postor deberán estar certificados por el fabricante del producto que presenten, se requiere mínimo una experiencia de 5 años implementando soluciones similares y tener como mínimo Titulo en estudios de Ingeniería Informática o afines debiendo presentar sus certificaciones.
3. La empresa proveedora asumirá todos los costos que impliquen lacapacitación.
4. El proveedor deberá realizar charlas sobre temas generales de Seguridad de la información y protección frente a malware a solicitud de la UNAS, al menos 2 veces durante la vigencia de la licencia.

IV. SOPORTE

1. La empresa 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.
2. El proveedor deberá proporcionar soporte técnico a solicitud de la UNAS durante la vigencia de la licencia y contará con las siguientes características:

- Soporte técnico online, en forma remota, correo electrónico y telefónicamente.

3. El proveedor de antivirus deberá contar como mínimo con dos personas de soporte certificados por la marca del producto.
4. El proveedor deberá entregar un informe técnico detallado luego de realizar las tareas y pruebas de soporte.

REQUISITOS DE CALIFICACIÓN

EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD

El postor deberá contar como mínimo con 2 universidades implementando una solución antivirus con una envergadura similar o mayor a la UNAS, es decir 1000 licencias a más.
El postor debe acreditar un monto facturado acumulado equivalente a S/ 200,916.40 (Doscientos Mil novecientos dieciséis Con 40/100, por la venta de bienes iguales o similares al objeto de la convocatoria, durante los cinco (5) años anteriores a la fecha de la presentación de ofertas que se computaran desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda.
Se consideran bienes similares a los siguientes SOLUCIONES DE SOFTWARE ANTIVIRUS PARA LA EMPRESA Y CORPORACIONES

Acreditación:
La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de compra, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con voucher de deposito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por Entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago correspondientes a un máximo de veinte (20) contrataciones.

EXPERIENCIA DEL PERSONAL CLAVE
El personal técnico del proveedor a cargo del servicio debe contar con capacitación o certificación de la marca del software antivirus.

Acreditación:
La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto y mínimo bachiller en Ingeniería Informática se validara en la web de https://enlinea.sunedu.gob.pe

Es todo cuanto puedo informar para los casos que se requiera.

Atentamente,

UNIVERSIDAD NACIONAL AGRARIA DE LA SELVA
TINGO MARIA
GONZALO P. MARTINEZ GUERRA

CC: Archivo.