TÉRMINOS DE REFERENCIA PARA LA ADQUISICIÓN DE LICENCIAS SOFTWARE ANTIVIRUS EMPRESARIAL

1. ÁREA QUE REALIZA EL REQUERIMIENTO

Unidad de Soporte Estratégico Institucional.

2. OBJETO DE LA CONTRATACIÓN

Adquirir licencias de software antivirus para las computadoras de escritorio, computadoras portátiles y workstation de la sede central de la Unidad Ejecutora 118.

3. FINALIDAD PÚBLICA

El presente requerimiento tiene por finalidad la adquisición de las licencias software antivirus, dedicadas para la protección y seguridad de la Infraestructura Tecnológica de la sede central de la Unidad Ejecutora 118 contra virus informáticos, troyanos y nuevas variantes de los mismos.

4. DESCRIPCIÓN DEL SERVICIO

El servicio consta de la renovación de las siguientes licencias software antivirus que detallo a continuación:

ITEM	DESCRIPCIÓN
01	Licencias antivirus para computadoras de Escritorio.

4.1. Características del servicio

El software antivirus deberá contar con las siguientes características y consideraciones mínimas:

4.1.1. Protección para computadoras de escritorios

El producto ofertado deberá:

- Poder instalarse en su última versión, sobre plataformas Windows 8, 10 y 11. Contar con Soporte para plataformas de 32 y 64 bits.
- 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.
- Proteger contra malwares del tipo ransomware y realizar el bloqueo de amenazas de día cero.
- Contar con tecnología avanzada con inteligencia artificial que permita detectar y eliminar amenazas de virus, spyware, troyanos, scripts entre otros ataques provenientes de internet.
- Contar con un sistema de detección de intrusos que realice un análisis de contenido del tráfico de red y además permite proteger de ataques haciendo que cualquier tráfico dañino sea bloqueado.

SOPORTE TÉCNICO INFORMÁTICO USE1 V°B° R.S.L.A. PMESUT UE 118 MINISTERIO DE EDUCACIÓN

- Ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o carpeta específica.
- Poder realizar escaneos manuales o programados, indicando las unidades a escanear o las carpetas específicas que requieren ser escaneadas.
- Pedir una contraseña ante intentos de cambio indebidos en la configuración del producto.
- 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.
- Permitir generar dentro de la misma solución antivirus repositorios de actualización, los cuales deberán ser distribuidos mediante protocolo http localmente.
- Poseer un firewall personal que posea modos de filtrado, además que pueda tener la capacidad de bloquear conexiones entrantes y salientes.
- Tener un módulo de protección en tiempo real para el acceso a la web.
- Ser capaz de 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.
- Debe tener un mecanismo contra la desinstalación del endpoint por el usuario y cada dispositivo deberá tener una contraseña única, no siendo autorizadas soluciones con una contraseña que funcione en todos los dispositivos.
- Permitir la utilización de contraseña de protección para posibilitar la reconfiguración local en el cliente o desinstalación de los componentes de protección.
- Debe contar con prevención de intrusión en el host (HIPS), que monitoree el código y bloques de código que pueden comportarse de forma maliciosa antes de ser ejecutados.
- Capacidad de reconocer y bloquear automáticamente las aplicaciones en los clientes basándose en la huella digital (hash) del archivo.

4.1.2. Protección para servidores

El producto ofertado deberá:

- Poder instalarse en su última versión, sobre plataformas Windows Server 2012, 2016 y 2019. Para versiones antiguas del sistema operativo se puede incluir versiones anteriores del software antivirus.
- Poder instalarse sobre plataformas Linux de 32 y 64 bits.
- Contar con un módulo de detección en tiempo real que proteja contra códigos maliciosos.
- Proteger contra malwares del tipo ransomware y realizar el bloqueo de amenazas de día cero.
- 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.
- Ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión o carpeta específica.

- Pedir una contraseña ante intentos de cambio indebidos en la configuración del producto.
- Contar con un agente que le permita ser administrado desde una consola centralizada.
- Contar con protección en tiempo real el cual debe iniciarse con el sistema operativo, así como poder definir qué tipos de medios serán analizados por el módulo.
- Permitir escanear archivos comprimidos.
- Permitir elegir las unidades a escanear para los escaneos bajo demanda.
- Contar con una herramienta integrada que permita inspeccionar completamente componentes del sistema, con la finalidad de determinar la causa de comportamientos sospechosos en el sistema que puede deberse a incompatibilidad de software, hardware o código malicioso.
- 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.
- La protección deberá contar con la capacidad de monitorear los cambios como creaciones o modificaciones sobre carpetas y archivos críticos del sistema basado en una lista pre-definida y poder personalizar dicha lista para sistemas operativos Windows Server 2012 o superior debido a la criticidad de la información que manejan.
- La protección podrá generar una lista blanca de aplicaciones que se ejecuten en el sistema operativo Windows Server 2012 o superior para que esas aplicaciones sean las únicas que se puedan ejecutar.

4.1.3. Protección contra amenazas avanzadas

- Protección de amenazas de día 0 a través de tecnología de deep learning (signature less).
- Funcionalidad de detección de amenazas desconocidas que están en memoria con tecnología deep learning.
- Capacidad de detección, y bloqueo proactivo de keyloggers y otros malwares no conocidos (ataques de día cero) a través del análisis de comportamiento de procesos en memoria.
- Capacidad de detección y bloqueo de troyanos (Trojans) y gusanos (Worms), entre otros malwares, por comportamiento de los procesos en memoria.
- Debe detectar el malware en un tiempo aproximado de no más de 20 milisegundos.
- No debe requerir descarga de firmas de ningún tipo.
- Capacidad de analizar el comportamiento de nuevos procesos al ser ejecutados, en complemento a la exploración programada.
- Análisis forense de lo sucedido, para entender cuál fue la causa raíz del problema con el detalle de los procesos y sub-procesos ejecutados, la lectura y escritura de archivos y de las claves de registro.
- Bloqueo y protección contra amenazas desconocidas potencialmente sospechosas (PUA).
- La solución debe tener capacidad de protección AMSI contra scripts maliciosos.
- La solución debe poseer un IPS Snort de Host.

SOPORTE TÉCNICO INFORMÁTICO USE/ UE 118 R.S.L.N. PMESUT MINISTERIO DE EDUCACIÓN

4.1.4. Protección contra ransomware

- Disponer de capacidad de protección contra ransomware no basada exclusivamente en la detección por firmas (por ejemplo: basada en comportamiento).
- Disponer de capacidad de remediación de la acción de cifrado malicioso de los ransomware;
- Debe informar a la consola todo el detalle del incidente – análisis de causa raíz sin la necesidad de instalar otro agente o dispositivo en la red.
- En el caso de servidores, debe disponer de la capacidad de prevención contra la acción de cifrado malicioso ejecutada por ransomware, posibilitando aún el bloqueo de las computadoras de donde parte tal acción (detección local y remota).

4.1.5. Protección contra vulnerabilidades y técnicas de explotación

- Debe poseer la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidades conocidas o de día cero.
- Mitigación de inyección de códigos en procesos.
- Protección contra robo de credenciales.
- Protección contra malware escondido en aplicaciones legítimas.
- Evitar la migración de procesos maliciosos, evitando que un proceso malicioso migre a otro.
- Evitar obtener escalamiento de privilegios y acceso elevado a recursos.
- Evitar modificación de las claves de registro para la ejecución de código arbitrario.

4.1.6. Consola de Administración

La consola de administración deberá:

- La administración deberá ser a través de una consola central única, basada en web y en sitio o en nube, que deberá contener todos los componentes para el monitoreo y control de protección de estaciones de trabajo y servidores.
- En caso la consola esté alojada en nube, el proveedor enviará los requisitos mínimos a nivel de red, para garantizar las comunicaciones y seguridad. En caso sea basada en sitio, La Organización proveerá de un servidor para la instalación de la solución.
- La consola deberá presentar un Dashboard con el resumen del estado de protección de los ordenadores y usuarios, así como indicar las alertas de eventos de criticidades alta, media e informativa.
- La consola de administración deberá tener usuarios con distintos roles de niveles de acceso y privilegios, como administradores, operadores de la consola y usuarios de sólo lectura.
- La consola debe permitir la división de los ordenadores dentro de la estructura de administración en grupos.
- Debe permitir la sincronización con Active Directory (AD) para la gestión de usuarios y grupos integrados en las políticas de protección.
- Debe poseer la posibilidad de aplicar reglas diferenciadas por grupos de usuarios, usuarios individuales, grupos de máquinas y equipos individuales.

SOPORTE TECNICO INFORMATICO USEI V.°B° R.S.L.N. PMESUT UE 118 MINISTERIO DE EDUCACIÓN

- La solución debe soportar el despliegue del producto a través de los siguientes métodos:
  - La consola debe permitir la división de los ordenadores dentro de la estructura de administración en grupos.
  - Distribución del cliente a través de GPO de Active Directory (AD) para múltiples estaciones de trabajo.
  - Instalación manual a través de paquete instalador descargado desde la consola central.
- Proporcionar actualizaciones del producto y de las definiciones de virus y protección contra intrusos.
- Debe permitir programar el escaneo de amenazas en las estaciones y servidores.
- Debe permitir exclusiones de escaneo para un determinado sitio Web, archivo o carpeta, aplicación o proceso. Tanto a nivel global, como específico en cada política.
- La consola de administración debe permitir la definición de grupos y subgrupos para la administración de las estaciones, usuarios y políticas.
- Utilizar protocolos seguros estándar HTTPS para la comunicación entre la consola de administración y los clientes administrados.
- Los mensajes generados por el agente deben estar en el idioma español o permitir su edición.
- Permitir la exportación de los informes gerenciales a los formatos CSV y PDF.
- Los recursos del informe y el monitoreo deben ser nativos de la propia consola central de administración.
- Posibilidad de mostrar información como nombre de la máquina, versión del antivirus, sistema operativo, dirección IP, versión del motor, fecha de la actualización, fecha de la última verificación, eventos recientes y estado.
- Capacidad de generación de informes estadísticas o gráficos, tales como:
  - Detalle de usuarios activos, inactivos o desprotegidos, así como detalles de los mismos.
  - Detalle de los ordenadores que están activos, inactivos o desprotegidos, así como detalles de las exploraciones y alertas en los ordenadores.
  - Detalle de los periféricos permitidos o bloqueados, así como detalles de dónde y cuándo se utilizó cada periférico.
  - Detalle de las principales aplicaciones bloqueadas y los servidores/usuarios que intentaron acceder a ellas.
  - Detalle de las aplicaciones permitidas que fueron accedidas con mayor frecuencia y los servidores/usuarios que las acceden.
  - Detalle de los servidores/usuarios que intentaron acceder a aplicaciones bloqueadas con mayor frecuencia y las aplicaciones que ellos intentaron acceder.
  - Detalle de todas las actividades disparadas por reglas de fuga de información.
- La solución debe permitir QoS para controlar el ancho de banda de red utilizado para la actualización de cada endpoint.
- La solución deberá permitir las actualizaciones a los equipos que no se encuentran conectados con la red local o mediante un repositorio en la red.

SOPORTE TÉCNICO INFORMÁTICO USEP V°B° R.S.L.N. PMESUT UE 118 MINISTERIO DE EDUCACIÓN

- La solución deberá permitir la selección de la versión del software de preferencia, permitiendo así la prueba de la actualización sobre un grupo de equipos piloto antes de implementarlo en toda la red.
- Actualización incremental, remota y en tiempo real, de las vacunas de los Antivirus y del mecanismo de verificación de los clientes.
- Actualización automática de las firmas de amenazas (malware) y políticas de prevención desarrolladas por el fabricante en tiempo real o con periodicidad definida por el administrador.
- También debe permitir seleccionar un grupo de equipos para aplicar la actualización para controlar el ancho de red. La actualización de la versión debe ser transparente para los usuarios finales.
- La herramienta de administración centralizada debe administrar todos los componentes de la protección para estaciones de trabajo y servidores y debe diseñarse para administrar, supervisar y elaborar informes de endpoint y servidores.
- Debe realizar envío automático de alertas críticas mediante correo electrónico a los administradores.
- Debe permitir la creación de reglas para excluir rangos específicos de direcciones IP.
- La consola debe poseer una gráfica de amenazas conteniendo toda la secuencia de eventos que ocurrieron durante la ejecución del malware o el ataque de un adversario, siendo posible ampliar los detalles de cada evento a fin de obtener un análisis de causa raíz detallado.
- La solución de endpoints y servidores debe ser administrada desde una misma consola en sitio o en la nube, de acuerdo a lo ofertado por el postor.
- Debe permitir identificar y proteger desde la misma consola instancias de servidores desplegados en AWS.

Control de aplicaciones

- Control de aplicaciones para monitorear e impedir que los usuarios ejecuten o instalen aplicaciones que puedan afectar la productividad o el rendimiento de la red.
- Actualización automática de la lista de aplicaciones que se pueden controlar, permitiendo aplicaciones específicas o las categorías específicas de aplicaciones que pueden ser liberadas o bloqueadas.
- Detectar aplicaciones controladas cuando los usuarios acceden, con las opciones de permitir y alertar o bloquear y alertar.

SOPORTE TÉCNICO INFORMÁTICO USE/ V°B° R.S.C.N. PMESUT UE 118 MINISTERIO DE EDUCACIÓN

Control web

- Control de acceso a sitios web por categoría.
- El Control Web debe controlar el acceso a sitios inapropiados, con al menos 10 categorías de sitios inadecuados. También debe permitir la creación de listas blancas y listas negras.
- La aplicación de políticas de control web, debe contar con capacidad de horarios.

Control de periféricos

- Debe permitir el monitoreo y el control de dispositivos extraíbles en los equipos de los usuarios, como dispositivos USB, periféricos de la

propia estación de trabajo y redes inalámbricas, aplicando estas políticas tanto para usuarios como para dispositivos.

- El control de dispositivos debe estar al nivel de permiso, sólo lectura o bloqueo.
- Los siguientes dispositivos deben ser, como mínimo, administrados: HD (hard disks) externos, pendrives USB, almacenables removibles seguras, CD, DVD, Blu-ray, floppy drives, interfaces de red inalámbrica, módems, bluetooth, infrarrojo, MTP (Media Transfer Protocol) y PTP (Picture Transfer Protocol) como cámaras digitales.

Funcionalidades de detección y respuesta

- Utilización del marco MITRE ATT&CK para identificar el nivel de riesgo (1 a 10) de una actividad inusual o sospechosa. Asimismo, se podrá clasificar, categorizar y consolidar las detecciones desde un único panel.
- Debe poder identificar que atributos de código de un objeto son similares a archivos "known-good" y "known-bad" con esto se puede determinar si se pueden permitir o bloquear.
- Debe tener un sistema de registro por cada ataque o intento de ataque que se haya producido en los endpoint con información detallada del malware en sí y el origen de la infección (explorador de Windows, correo electrónico, navegador, etc)..
- Buscar de forma proactiva (threat hunting) indicadores de compromiso por nombre de archivo, SHA, dirección IP.
- La solución deberá permitir al administrador aislar de forma manual una máquina de la red comprometida mientras se investiga el incidente.
- La solución deberá permitir el aislamiento de manera automática de los equipos en caso de presencia de actividad sospechosa.
- La solución deberá de ser capaz de realizar consultas basadas en lenguaje SQL para poder identificar comportamiento malicioso o hacer caza de amenazas (Threat hunting).
- La solución debe permitir la personalización o creación de nuevas consultas para detectar de forma temprana un posible evento de seguridad informática.

SOPORTE TÉCNICO INFORMÁTICO USEI V°B° P. S. L. N. PMESUTI UE 118 MINISTERIO DE EDUCACIÓN

5. PRESTACIÓN ACCESORIAS A LA PRESTACIÓN PRINCIPAL

5.1. Soporte Técnico

El Proveedor brindará el servicio de soporte técnico de manera remota, vía email o telefónico 24x7. De lunes a domingo por un periodo de 12 meses, sin costo adicional para la Entidad.

El Proveedor deberá indicar el procedimiento de atención, los teléfonos, horarios, correo electrónico, contactos y números preferenciales con el fabricante para la atención sobre cualquier avería, incidencia o requerimiento de la solución.

6. REQUISITOS MÍNIMOS QUE DEBE CUMPLIR EL PROVEEDOR

El perfil mínimo que debe tener el proveedores:

- Persona jurídica con experiencia (*) en venta de Licencias de software antivirus
- Contar con Registro Nacional de Proveedores (RNP) vigente.
- Contar con Registro Único contribuyente (RUC) Activo y Habido.
- No tener impedimento para contratar con el Estado.
- El proveedor debe ser partner de la marca ofertar como mínimo.
- Acreditar cinco (05) servicios iguales o similares al objeto de la contratación durante los últimos tres (03) años.

(*) La experiencia se acreditará con copia simple de: (i) contratos, órdenes de compra u órdenes de servicio y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente con voucher de depósito, 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 mismo comprobante de pago.

7. PLAZO DE SERVICIO

La renovación del servicio se realizará por un periodo de doce (12) meses.

8. PLAZO DE ENTREGA

El plazo para la entrega del bien es de siete (07) días calendario, contabilizados a partir del día siguiente de notificada la orden de servicio.

9. FORMA DE PAGO

El pago se efectuará en una (01) armada previa conformidad del servicio.

10. CONFORMIDAD

La conformidad de la será otorgada por la Unidad Soporte Estratégico Institucional, previo visto bueno de la responsable (e) de Control Patrimonial y Almacén, y del responsable de la Unidad de Logística.

11. RESPONSABILIDAD POR VICIOS OCULTOS

El proveedor es responsable de la calidad ofrecida y por los vicios ocultos se aplicará por un plazo máximo de un año, contado a partir de la conformidad del servicio.

12. CONFIDENCIALIDAD

La empresa se compromete a guardar las más absoluta reserva a fin de garantizar la seguridad de los activos pertenecientes al Unidad Ejecutora 118. Así también a no revelar, comentar.

SOPORTE TÉCNICO INFORMÁTICO USE V°B° R. S. L. N. PMESUT UE 118 MINISTERIO DE EDUCACIÓN