Pliego de especificaciones técnicas para la adquisición de sistema de antivirus para ANLIS.

I.- OBJETO DEL SUMINISTRO:

Adquisición de un sistema antivirus para ANLIS.

II.- CARACTERISTICAS TECNICAS:

<table>
<tr><th>Renglon</th><th>Cantidad</th><th>Detalle</th></tr>
<tr><td>1</td><td>500</td><td>
Renovación de licencias de antivirus de red para computadoras

<u>Antivirus de red</u>
LICENCIAMIENTO:
• La entrega del producto se hará efectiva mediante alguna de las siguientes opciones:
✓ La descarga del producto desde Internet a través de un código.
✓ La entrega de sus originales en CD-ROM con sus respectivas licencias y toda la documentación de los mismos.
• Tipo de Licenciamiento y actualización de bases, definiciones y firmas de virus:
✓ El servicio comenzará a regir a partir de la recepción definitiva de los mismos.
✓ Licenciamiento de uso por el término de 2 (dos) años, con servicio de actualización de bases, definiciones y firmas de virus y upgrade de producto.

CARACTERÍSTICAS TECNICAS
• Usuarios del producto (discriminados por servidores y estaciones cliente):
<table>
<tr><td colspan="2">Servidor/es</td><td colspan="2">Estaciones Cliente</td></tr>
<tr><td>Sistema Operativo</td><td>Cantidad</td><td>Sistema Operativo</td><td>Cantidad</td></tr>
<tr><td>MS Windows 2003 / 2008 / 2012 /2016 Server</td><td>20</td><td>Windows XP Pro /Windows 7/Windows 8.1/Windows 10</td><td>480</td></tr>
</table>
✓ Características técnicas que posee el equipamiento.
</td></tr>
</table>

Servidor/es			Estaciones Cliente		
Procesador	Memoria	Espacio en Disco	Procesador	Memoria	Espacio en Disco
Intel Xeon 2 GHz	2 GB	146 GB	AMD AThon X2 64 2,7 Ghz	1 Gb	80 Gb
Intel Xeon 2.5 GHz	32 -65 Gb	1 Tb	Intel Pentium Dual Core 1.8 Ghz	1 Gb	80 Gb

✓ Se deberá garantizar el correcto funcionamiento del software en base a las características técnicas mencionadas.

Instalación y actualización de licencias

- Soporte de instalación centralizada (desatendida por parte del usuario de la PC).
- El administrador podrá programar la actualización de los equipos cliente seleccionando:
  - ✓ Todas las estaciones de trabajo.
  - ✓ Un grupo de estaciones de trabajo.

Actualización de Información de virus

- Soporte de actualización "en-línea" y manual.
- Soporte de programación de actualizaciones hacia todos los clientes y servidores en modo:
  - ✓ Centralizado y automático
- Actualizaciones, en forma automática, programada o bajo demanda, en forma incremental, con mínimo impacto en el tráfico. Posibilidad de utilizar servidores cascada en el proceso de actualización.
- Deberá poseer certificación ICSA Labs (www.icsalabs.com), o AVTest (www.av-test.org) para "Empresas Windows Client" que supere calificaciones de 5.0/6.0 para "Protección", "Carga del sistema" y "Utilidad". La calificación indicada debe incluir la fecha de emisión, la que no debe ser mayor a 1 año, y debe corresponder con la versión de software antivirus que se está ofertando.

Instalación

✓ Deberá contar con los siguientes métodos para la instalación y/o actualización de versiones del producto desde la consola de administración hacia las estaciones clientes y/o servidores:
  - ✓ Conexión a red
  - ✓ Intranet /Internet
  - ✓ Forma remota
  - ✓ CD

Generales

		• Brindar protección contra virus de todo tipo, troyanos, spyware, key-loggers, cookies, y otros códigos malignos.- • Certificación ICSA y/o Checkmark (West Coast Labs) que acredite cumplimentar el punto anterior. Si el mismo motor de antivirus es utilizado en todas las versiones, es suficiente presentar el certificado de una sola versión.- • Acreditar que el producto ha sido sometido todas las auditorias realizadas por Virus Bulletin en los últimos 12 meses, con independencia de la plataforma (sistema operativo) de la revisión, y que en todas ellas haya detectado el 100 % de los Virus "In the Wild", sin haber emitido ningún falso positivo. • Detección y eliminación de virus conocidos y desconocidos en las estaciones cliente y/o servidores según el método de rastreo seleccionado (tiempo real, demanda, programado, etc.): ✓ Virus de arranque ✓ Virus de archivos ✓ Virus Macros ✓ Virus de VB scrip y Java Script ✓ Virus en archivos compactados ✓ Virus en archivos compactados en distintos niveles ✓ Reconocimiento de "firmas de virus" ✓ Reconocimiento Heurístico • La detección debe realizarse en forma preventiva, antes que el código malicioso se esté ejecutando en el equipo. • Protección contra nuevos virus en forma heurística, adjuntando informes de entidades independientes que permitan comprobar esta capacidad. • Chequeo automático de la transferencia de archivos entre clientes y servidores. • Rastreo de infecciones en un registro de actividad. • Soporte de antispyware. • El servidor deberá soportar instalación, configuración y administración centralizada para múltiples dominios • Generación automática de mensajes de alerta ante la detección de virus. • Notificación al administrador de la red ante la detección de virus. • Posibilidad de realizar en estaciones cliente y servidores los distintos tipos de rastreo en: ✓ Tiempo Real ✓ Por demanda ✓ Programado ✓ Remoto ✓ Unidad de almacenamiento ✓ Directorios ✓ Archivos Seleccionados • Ante la detección de un virus por cualquiera de los métodos de rastreo seleccionados en las estaciones cliente y servidores,

		tendrá la posibilidad de: ✓ Limpiar ✓ Eliminar ✓ Mover a una carpeta • Protección por contraseña de equipos cliente • Notificación de detección virus vía: ✓ Correo Electrónico como mínimo • Realizar notificaciones de detección de virus a: ✓ Distintos niveles de Administrador ✓ Utilizando mensajes pre-configurables • Posibilidad de realizar informes que muestren como mínimo: ✓ Versiones de definiciones y motor de búsqueda ✓ Detección de Virus ✓ Tareas Programadas • Permitir la creación de distintos perfiles de administrador. • Instalación, configuración, actualización y administración centralizada, remota y desatendida, con emisión de alertas en caso de detección de virus, equipos con antivirus no instalado o desactualizado, etc. • Dispondrá de una o más consolas de administración centralizada que permitan visualizar globalmente, de una manera resumida y en tiempo real, el estado de los nodos protegidos por la solución. • Posibilidad de realizar rastreos de equipos individuales, de manera centralizada, manual o programada. • Poder desinstalar los clientes desde la consola de administración remota. • Impedir a los usuarios que puedan desinstalar ni bajar de memoria la protección antivirus. • La administración centralizada no debe requerir un servidor dedicado. • Representación y soporte técnico oficial radicado en el país, el que deberá ofrecer incluido el soporte al cliente 24 hs. (telefónico, por mail, y página web donde se pueda abrir una incidencia). • Deberá incluir un curso de capacitación de instalación y operación para tres (3) personas in situ. **SERVICIOS DE IMPLEMENTACIÓN:** El oferente deberá prestar las siguientes tareas: • Diseño e implementación de políticas de seguridad a aplicar en conjunto con el personal del TI de la ANLIS. • Instalación y configuración de servidor de actualizaciones, habilitación de puertos y permisos de carpetas.

		• Instalación y administración sobre una consola de administración remota en cualquier plataforma. • Armado y configuración de un paquete de instalación para instalaciones remotas push, on sites, y/o script de logon y desinstalación del antivirus viejo, en las computadoras que lo posean. • Instalación remota de todos los nodos que se encuentren online. • Armado y configuración de reportes, alarmas, logs, estadísticas en consola de administración. • Knowledge-transfer durante todo el proceso de instalación para capacitar al personal del TI de la ANLIS, encargados del a administración de la solución. • Testeo de actualizaciones, reportes y alarmas. • Soporte post implementación en forma telefónica o via e-mail. Se deja claramente expresado que en caso que el software tenga contratados los servicios de mantenimiento, corresponde al oferente proveer nuevas versiones del producto en caso de migración de sistema operativo en las estaciones de trabajo sin costo. ***Nota:*** En la actualidad la ANLIS cuenta con el producto ESET Endpioint Antivirus como antivirus de red. Las empresas que ofrecieren otras soluciones antivirus deberán desinstalar los antivirus operativos en las pc y servidores de la ANLIS además de la consola de administración sin que esto genere un costo adicional ni interrumpa el normal funcionamiento de los sistemas de los clientes y cumplimentar con los ítems del apartado “Servicios de implementación” para todos los equipos de la ANLIS. La consola de administración centralizada deberá estar instalada en un Servidor local del Organismo. ***Requisito***: La propuesta técnica de los oferentes no solo deberá ser la simple entrega de los folletos y hojas de datos de los equipos sino que se deberá describir lo que se ofrece para cada ítem solicitado. Asimismo, se deberá indicar la hoja de la propuesta donde se hace referencia a cada una de las especificaciones solicitadas en el pliego. Serán desestimadas todas las propuestas técnicas que no cumplan con lo anteriormente solicitado. **Plazo de entrega:** 20 días hábiles de recibida la orden de compra.

<table>
<tr>
<td>2</td>
<td>100</td>
<td>
Adquisición de 100 (cien) licencias de antivirus de red para computadoras

<u>Antivirus de red</u>
LICENCIAMIENTO:
• La entrega del producto se hará efectiva mediante alguna de las siguientes opciones:
✓ La descarga del producto desde Internet a través de un código.
✓ La entrega de sus originales en CD-ROM con sus respectivas licencias y toda la documentación de los mismos.
• Tipo de Licenciamiento y actualización de bases, definiciones y firmas de virus:
✓ El servicio comenzará a regir a partir de la recepción definitiva de los mismos.
✓ Licenciamiento de uso por el término de 2 (dos) años, con servicio de actualización de bases, definiciones y firmas de virus y upgrade de producto.

CARACTERÍSTICAS TECNICAS
• Usuarios del producto (discriminados por servidores y estaciones cliente):

<table>
<tr><td colspan="2">Estaciones Cliente</td></tr>
<tr><td>Sistema Operativo</td><td>Cantidad</td></tr>
<tr><td>Windows XP Pro /Windows 7/Windows 8.1/Windows 10</td><td>100</td></tr>
</table>

✓ Características técnicas que posee el equipamiento.

<table>
<tr><td colspan="3">Estaciones Cliente</td></tr>
<tr><td>Procesador</td><td>Memoria</td><td>Espacio en Disco</td></tr>
<tr><td>AMD AThon X2 64 2,7 Ghz</td><td>1 Gb</td><td>80 Gb</td></tr>
<tr><td>Intel Pentium Dual Core 1.8 Ghz</td><td>1 Gb</td><td>80 Gb</td></tr>
</table>

✓ Se deberá garantizar el correcto funcionamiento del software en base a las características técnicas mencionadas.
</td>
</tr>
</table>

		Instalación y actualización de licencias • Soporte de instalación centralizada (desatendida por parte del usuario de la PC). • El administrador podrá programar la actualización de los equipos cliente seleccionando: ✓ Todas las estaciones de trabajo. ✓ Un grupo de estaciones de trabajo. **Actualización de Información de virus** • Soporte de actualización "en-línea" y manual. • Soporte de programación de actualizaciones hacia todos los clientes y servidores en modo: ✓ Centralizado y automático • Actualizaciones, en forma automática, programada o bajo demanda, en forma incremental, con mínimo impacto en el tráfico. Posibilidad de utilizar servidores cascada en el proceso de actualización. • Deberá poseer certificación ICSA Labs (www.icsalabs.com), o AVTest (www.av-test.org) para "Empresas Windows Client" que supere calificaciones de 5.0/6.0 para "Protección", "Carga del sistema" y "Utilidad". La calificación indicada debe incluir la fecha de emisión, la que no debe ser mayor a 1 año, y debe corresponder con la versión de software antivirus que se está ofertando. **Instalación** ✓ Deberá contar con los siguientes métodos para la instalación y/o actualización de versiones del producto desde la consola de administración hacia las estaciones clientes y/o servidores: ✓ Conexión a red ✓ Intranet /Internet ✓ Forma remota ✓ CD **Generales** • Brindar protección contra virus de todo tipo, troyanos, spyware, key-loggers, cookies, y otros códigos malignos.- • Certificación ICSA y/o Checkmark (West Coast Labs) que acredite cumplimentar el punto anterior. Si el mismo motor de antivirus es utilizado en todas las versiones, es suficiente presentar el certificado de una sola versión.- • Acreditar que el producto ha sido sometido todas las auditorias realizadas por Virus Bulletin en los últimos 12 meses, con independencia de la plataforma (sistema operativo) de la revisión, y que en todas ellas haya detectado el 100 % de los Virus "In the Wild", sin haber emitido ningún falso positivo. • Detección y eliminación de virus conocidos y desconocidos en las estaciones cliente y/o servidores según el método de rastreo seleccionado (tiempo real, demanda, programado, etc.):

		✓ Virus de arranque ✓ Virus de archivos ✓ Virus Macros ✓ Virus de VB scrip y Java Script ✓ Virus en archivos compactados ✓ Virus en archivos compactados en distintos niveles ✓ Reconocimiento de “firmas de virus” ✓ Reconocimiento Heurístico • La detección debe realizarse en forma preventiva, antes que el código malicioso se esté ejecutando en el equipo. • Protección contra nuevos virus en forma heurística, adjuntando informes de entidades independientes que permitan comprobar esta capacidad. • Chequeo automático de la transferencia de archivos entre clientes y servidores. • Rastreo de infecciones en un registro de actividad. • Soporte de antispyware. • El servidor deberá soportar instalación, configuración y administración centralizada para múltiples dominios • Generación automática de mensajes de alerta ante la detección de virus. • Notificación al administrador de la red ante la detección de virus. • Posibilidad de realizar en estaciones cliente y servidores los distintos tipos de rastreo en: ✓ Tiempo Real ✓ Por demanda ✓ Programado ✓ Remoto ✓ Unidad de almacenamiento ✓ Directorios ✓ Archivos Seleccionados • Ante la detección de un virus por cualquiera de los métodos de rastreo seleccionados en las estaciones cliente y servidores, tendrá la posibilidad de: ✓ Limpiar ✓ Eliminar ✓ Mover a una carpeta • Protección por contraseña de equipos cliente • Notificación de detección virus vía: ✓ Correo Electrónico como mínimo • Realizar notificaciones de detección de virus a: ✓ Distintos niveles de Administrador ✓ Utilizando mensajes pre-configurables • Posibilidad de realizar informes que muestren como mínimo: ✓ Versiones de definiciones y motor de búsqueda

		✓ Detección de Virus ✓ Tareas Programadas • Permitir la creación de distintos perfiles de administrador. • Instalación, configuración, actualización y administración centralizada, remota y desatendida, con emisión de alertas en caso de detección de virus, equipos con antivirus no instalado o desactualizado, etc. • Dispondrá de una o más consolas de administración centralizada que permitan visualizar globalmente, de una manera resumida y en tiempo real, el estado de los nodos protegidos por la solución. • Posibilidad de realizar rastreos de equipos individuales, de manera centralizada, manual o programada. • Poder desinstalar los clientes desde la consola de administración remota. • Impedir a los usuarios que puedan desinstalar ni bajar de memoria la protección antivirus. • La administración centralizada no debe requerir un servidor dedicado. • Representación y soporte técnico oficial radicado en el país, el que deberá ofrecer incluido el soporte al cliente 24 hs. (telefónico, por mail, y página web donde se pueda abrir una incidencia). • Deberá incluir un curso de capacitación de instalación y operación para tres (3) personas in situ. **SERVICIOS DE IMPLEMENTACIÓN:** El oferente deberá prestar las siguientes tareas: • Diseño e implementación de políticas de seguridad a aplicar en conjunto con el personal del TI de la ANLIS. • Instalación y configuración de servidor de actualizaciones, habilitación de puertos y permisos de carpetas. • Instalación y administración sobre una consola de administración remota en cualquier plataforma. • Armado y configuración de un paquete de instalación para instalaciones remotas push, on sites, y/o script de logon y desinstalación del antivirus viejo, en las computadoras que lo posean. • Instalación remota de todos los nodos que se encuentren online. • Armado y configuración de reportes, alarmas, logs, estadísticas en consola de administración. • Knowledge-transfer durante todo el proceso de instalación para capacitar al personal del TI de la ANLIS, encargados del a administración de la solución. • Testeo de actualizaciones, reportes y alarmas. • Soporte post implementación en forma telefónica o via e-mail.

		Se deja claramente expresado que en caso que el software tenga contratados los servicios de mantenimiento, corresponde al oferente proveer nuevas versiones del producto en caso de migración de sistema operativo en las estaciones de trabajo sin costo. ***Nota:*** En la actualidad la ANLIS cuenta con el producto ESET Endpioint Antivirus como antivirus de red. La consola de administración centralizada deberá estar instalada en un Servidor local del Organismo. ***Requisito***: La propuesta técnica de los oferentes no solo deberá ser la simple entrega de los folletos y hojas de datos de los equipos sino que se deberá describir lo que se ofrece para cada ítem solicitado. Asimismo, se deberá indicar la hoja de la propuesta donde se hace referencia a cada una de las especificaciones solicitadas en el pliego. Serán desestimadas todas las propuestas técnicas que no cumplan con lo anteriormente solicitado. **Plazo de entrega:** 20 días hábiles de recibida la orden de compra.