ANEXO TÉCNICO

DESCRIPCIÓN TÉCNICA

Ítem	Contratar la adquisición de 600 nuevas licencias de software antivirus con vigencia de un año para la ANI, Instalación, configuración, soporte.
1.1	**Especificaciones técnicas de hardware y software** • Procesadores soportados: Intel o AMO x86-x64. • Microsoft® Windows® Windows 7.0 - 8.0 - 8.1 Compatible para el nuevo Windows 10 - Soporte para base datos, My SQL, Oracle. • Software antivirus y antispyware debidamente licenciado, referenciado por Gartner **y AVTEST**, y que cuente con actualizaciones automáticas. Este programa deberá contar con respaldo y soporte directo del fabricante. • El licenciamiento debe estar en capacidad de eliminar o bloquear todas las amenazas potenciales causadas por virus, gusanos, rootkits y otras formas de spyware y malware, ya sea que ingresen por dispositivos electrónicos como celulares, tables, USB, Cd, DVD entre otros. • Debe proporcionar protección ante la manipulación indebida y proteger el registro del sistema, los procesos, las aplicaciones y los archivos ante modificaciones no autorizadas y detectar amenazas desconocidas por su conducta sospechosa.
1.2	**Rendimiento** La solución de seguridad antivirus debe garantizar un bajo consumo de recursos de los equipos para que asegure su inicio rápido y un eficiente rendimiento sin interferir en el entorno de trabajo.
1.3	**Módulos** La solución antivirus debe contar con un módulo de herramientas tales como: • Archivos del registro • Estadísticas de protección • Observar la actividad • Procesos activos • Tareas programadas • Cuarentena • EsetSyslnspector • Enviar archivo para su análisis. • Servidor de ESET RemoteAdministrator • ESET SysRescue La solución antivirus debe contar con ESET Live Grid que permita comparar la reputación de archivos con una base de archivos seguros que se encuentra en Internet, la cual vaya creciendo gracias a la utilización de los usuarios, si un archivo fue previamente analizado por un usuario este quedara guardado en la base, lo que reducirá los tiempos de espera de futuros análisis del mismo archivo, ya que comparara los resultados obtenidos por el resto de los usuarios.
1.4	**Consola de Administración** La solución antivirus debe contar con una aplicación que permita administrar los productos ofrecidos, en un entorno de red, estaciones de trabajo y servidores desde una ubicación central. El producto requerido debe soportar los siguientes requisitos del sistema en cuanto a la consola de administración: • La solución de administración debe permitir la instalación impulsada, envió de paquetes de configuración y administración de los productos antivirus instalados en las estaciones y servidores. • La solución de administración debe tener un módulo de generación de reportes que permitan identificar las maquinas desactualizadas, archivos en cuarentena y demás características que permita identificar. También debe contener varias plantillas predefinidas para la creación de estos reportes. • La solución de administración debe permitir administrar los clientes desde la creación y envió de tareas tales como actualizaciones, análisis, tareas de restauración y demás interacción con los equipos clientes donde se instala la solución.

1.5	**Otras especificaciones generales.** • La solución antivirus debe tener un motor ThreatSense® de velocidad y precisión que mantenga los equipos seguros frente ataques, infiltraciones de virus, spyware, troyanos, gusanos, adware, rootkits y otros ataques provenientes de Internet sin entorpecer el rendimiento del sistema de los equipos. • Deberá detectar y eliminar/desinfectar al menos los siguientes tipos de amenazas: Spyware, Adware, Rogues, Ransomware, Keyloggers, Troyanos, Worms, Virus, etc. • La solución requerida debe tener integrado las siguientes funcionalidades para una óptima protección en el equipo, la red, internet y correo electrónico así: • Protección antivirus. • Protección Antispyware. • Filtrado de URL"s. • Protección del sistema de archivos en tiempo real. • Protección de documentos. • HIPS monitoreo de los sucesos dentro del sistema operativo. • Modo de presentación. • Protección Anti-Stealth. • Protección de acceso a la Web. • Protección del cliente de correo electrónico. • La solución antivirus debe permitir explorar y detectar infiltraciones dentro de archivos comprimidos con las siguientes extensiones de archivos: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO, BIN, NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE. • La solución antivirus debe contar con las funcionalidades capaces de estar alerta frente ataques y eventos sospechosos de software malicioso que ponga en peligro los equipos, capaces de eliminar proactivamente infiltraciones de virus, spyware, troyanos, gusanos, Adware, Rootkitsy otro ataques provenientes de interne! sin entorpecer el rendimiento del sistema de los equipos. • La solución antivirus debe contar con un módulo de tareas programadas que permita configurar las diferentes frecuencias de actualización y horarios de análisis diarios, semanales, mensuales y manejo de horarios no laborales. • La solución antivirus debe permitir importar y exportar configuraciones. • La solución antivirus debe permitir, bloquear, o excluir direcciones URL. • La solución antivirus deberá permitir limitar el acceso mediante la selección de categorías de sitios web basada en la clasificación automática en la nube, además de permitir crear reglas detalladas por grupos de usuarios y bloqueos de los sitios que generan un gran volumen de tráfico. • La solución antivirus deberá permitir definir redes de confianza. • La solución antivirus deberá contar con un firewall bidireccional que prevenga el acceso no autorizado a las redes de la entidad. • La solución antivirus deberá tener proteger las comunicaciones de la entidad ante spam y amenazas provenientes del correo electrónico filtrando los protocolos POP3, IMAP, MAPI Y HTTP. • El módulo de protección del cliente de correo electrónico debe ser compatible con los siguientes clientes de correo electrónico Outlook de Office365. • **Políticas y tareas granulares.** • **Antimalware con tecnología de punta (Análisis en tiempo real y análisis heurístico en busca de nuevas amenazas).** • **Cortafuegos Bidireccional (Analiza el trafico entrante y saliente, estableciendo reglas específicas para aplicaciones, puertos y direcciones ip).** • **Control web por palabras.** • **Control de aplicaciones (Permite bloquear cualquier aplicación que se ejecute en el equipo: Navegadores web, aplicaciones office, juegos etc.)**. • **Control por palabras (Permite establecer control de palabras sobre el cliente de correo para evitar que se fugue información delicada para la compañía).** • **Inventario de software instalado en los equipos clientes.** • **Inventario de hardware (Memoria, disco duro, pantalla)** • **Instalación remota de software.** • **Bloqueo de puertos usb y autorun.**

1.6	**Servicio de Instalación** • Servicio de implementación y configuración, servidor principal e instalación en 600 usuarios finales.
1.7	**Capacitación** • Capacitación presencial en la Entidad a dos funcionarios de TI donde explique la configuración y manejo del Antivirus políticas, reglas, objetos, administración general.
1.8	**Soporte** • 5x8 del Antivirus Instalado, escalable según requerimientos del cliente. Para nuevas configuraciones o actualizaciones o el caso que sea critico se debe realizar en sitio o remoto.

CONDICIONES MÍNIMAS GENERALES

El contratista deberá ejecutar el objeto del contrato cumpliendo cada una de las especificaciones técnicas y requerimientos mínimos de los ítems anteriores.

Se debe instalar, configurar y dejar en correcto funcionamiento la solución brindada.

La garantía y soporte del antivirus deberá ser por un periodo mínimo de 12 Meses.

El contratista se compromete con la Entidad, a suministrar una solución de antivirus certificada y garantizada de fábrica, cumpliendo las Normas técnicas vigentes nacionales e internacionales y cumpliendo con todas la exigencias en materia de Antivirus.

El proponente debe comprometerse a entregar un reporte de la instalación y configuración que se haya realizado en la Entidad.

El contratista deberá explicar claramente la metodología que se debe seguir para solicitar y prestar el servicio de soporte.