MINISTERIO DE DEFENSA NACIONAL
AGENCIA LOGÍSTICA DE LAS FUERZAS MILITARES
DIRECCIÓN DE CONTRATACIÓN

Bogotá, D.C. 01 de agosto de 2007

No. **ALDCT**

ASUNTO: **Contratación Directa No.112/2007**

AL: **Señores**
INTERNET SOLUTIONS LTDA
Carrera 111 No. 71-41 oficina 202
Tel: 3 12 09 10 fax: 3 12 05 77
Bogotá D.C.

.

Para efecto de dar cumplimiento con lo establecido en el pliego de condiciones, Decretos 2170/02 y 2434/06 pliego de condiciones con sus respectivos adendos, el oferente dispondrá de tres (03) días hábiles a partir del **Primero (01) hasta el tres (03) de agosto de 2007, de las 08:00 hasta las 17:00 horas**, a fin de presentar las observaciones que estimen pertinentes a los informes de evaluación jurídico, financiero y técnico de la **Contratación Directa No. 112//2007 Objeto: ADQUISICIÓN SOPORTE Y MANTENIMIENTO DE LA SUITE ANTIVIRUS TREND MICRO CON DESTINO A LA AGENCIA LOGÍSTICA DE LAS FUERZAS MILITARES.**

Estas Evaluaciones son publicadas en el portal único de contratación **www.contratos,gov,co** y en la página web de la entidad: **www.agencialogistica.mil.co,** las cuales podrán ser consultadas por los oferentes.

En razón a lo anterior, se informa que las observaciones se deben presentar hasta el día **tres (03) de agosto de 2007,** a las 17:00 horas. De igual manera, se solicita el envío de las mismas en medio magnéticas ó a los correos **publicontratos@agencialogistica.mil.co** **www.agencialogistica.mil.co**

Atentamente,

MY. CARLOS JAVIER SOLER PARRA
Encargado de las funciones de la Dirección de Contratación

Elaboró: Lilia O.	Revisaron: Abg. Lucila Salamanca Arbelaez Coordinadora Grupo Precontractual Abg. Esther Julia Velásquez Grupo Precontractual

VERIFICACIÓN – INFORMES DE EVALUACIÓN

Contratación Directa No. 112/2007, Objeto: ADQUISICIÓN SOPORTE Y MANTENIMIENTO DE LA SUITE ANTIVIRUS TREND MICRO CON DESTINO A LA AGENCIA LOGÍSTICA DE LAS FUERZAS MILITARES

FIRMA QUE PRESENTO OFERTA: INTERNET SOLUTIONS LTDA.

INFORME DE EVALUACIÓN JURÍDICO

Mediante estudio No. 312 de fecha 19 de julio de 2007 el comité concluye:

No.	DOCUMENTACIÓN PRESENTADA POR EL OFERENTE	INTERNET SOLUTIONS LTDA.
1	Carta de presentación - Formulario 01	SI CUMPLE
2	Acreditación de la experiencia especifica – Formulario No. 2	SI ANEXA
3	Acreditación de la capacidad de contratación – Formulario No. 3	SI ANEXA
4	Relación de Contratos vigentes o en ejecución al cierre del proceso.	SI ANEXA
5	Propuesta Económica Formulario No 5.	SOBRE CERRADO
6	Compromiso Anticorrupción Formulario No 6.	SI CUMPLE
7	Origen de los bienes ley 816 de 2003Formulario No 7.	SI ANEXA
8	Informe Misión Diplomática Formulario No 8.	NO ANEXA
9	Garantía de seriedad de la oferta	SI CUMPLE
10	Registro Único Tributario	SI CUMPLE
11	Certificado aportes parafiscales – Ley 789/2002 y ley 828/2003	SI CUMPLE
12	Boletín de Responsabilidades Fiscales de la Contraloría General de la República.	VERIFICADO POR EL COMITÉ CUMPLE
13	Certificado disciplinarios PGN.	SI CUMPLE
14	Plazo de ejecución	SI CUMPLE
15	Lugar de ejecución	SI CUMPLE
16	Datos del Oferente	SI CUMPLE
17	Recibo pago términos de referencia.	SI CUMPLE
18	Certificado de Existencia y Representación Legal	SI CUMPLE
20	Registro Mercantil	SI CUMPLE
21	Registro Único de Proponentes	SI CFUMPLE

CONCLUSIÓN:

Una vez analizada la oferta presentada por la firma: **INTERNET SOLUTIONS LTDA.**

El Comité Jurídico encuentra que en su aspecto legal CUMPLE con lo exigido en los términos de referencia. Por lo tanto, se habilita jurídicamente para continuar en el proceso contractual.

Este concepto es emitido sin perjuicio de los estudios técnicos, financieros y económicos a que haya lugar.

INFORME DE EVALUACIÓN FINANCIERO:

Mediante estudio No. 303 de fecha 17 de julio de 2007 el comité concluye:

DOCUMENTOS DE VERIFICACION								
OFERENTES	**BALANCE GENERAL CERTIFICADO**	**ESTADO DE RESULTADOS CERTIFICADO**	**TARJETA PROFESIONAL CONTADOR Y REVISOR FISCAL**	**NOTAS A LOS ESTADOS FINANCIEROS**	**DICTAMEN REVISOR FISCAL Y/O CONTADOR INDEPENDIENTE**	**CERTIFICADO DE INSCRIPCION**	**DECLARACION DE RENTA**	**MULTAS O SANCIONES**
INTERNET SOLUTIONS LTDA.								
INTERNET SOLUTIONS LTDA.	FALTA CERTIFICACION	FALTA CERTIFICACION	SI	SI	SI	SI	SI	NO

INDICADORES FINANCIEROS								
OFERENTES	**NIVEL ENDEUDAMIENTO <= 70%**	**CAPITAL DE TRABAJO >=20%**	**20% PRESUPUESTO OFICIAL**	**CAPACIDAD PATRIMONIAL ACREDITADA**	**CAPACIDAD PATRIMONIAL REQUERIDA = 50%**	**CAPACIDAD RESIDUAL DE CONTRATACION**	**VALOR PRESUPUESTO**	**VALOR PRESUPUESTO EN SMMLV**
INTERNET SOLUTIONS LTDA.	74%	245.812.127,00	11.600.000,00	417.131.807,00	29.000.000,00	1.147,57	58.000.000,00	133,73

CONCLUSION

EL COMITÉ FINANCIERO RECOMIENDA NO TENER EN CUENTA A LA FIRMA **INTERNET SOLUTIONS LTDA, EN RAZON A QUE SUPERA EL NIVEL DE ENDEUDAMIENTO EXIGIDO EN EL PLIEGO DE CONDICIONES**, POR LO TANTO SE ENCUENTRA INCURSO EN LA CAUSAL DE RECHAZO 18, QUE DICE "CUANDO EL PROPONENTE NO CUMPLA CON TODOS Y CADA UNO DE LOS INDICADORES FINANCIEROS ESTABLECIDOS EN LOS TERMINOS DE REFEENCIA.

INFORME DE EVALUACIÓN TÉCNICO:

Mediante estudio No. 164 de fecha 19 de julio de 2007 el comité concluye:

Características o Especificaciones Técnicas:		
Descripción	**Cumple SI/NO**	**No. De Folio**
DESCRIPCION DE LA SOLUCION		
El oferente debe hacer entrega de la actualización de: 470 licencias de Neat Suite (Office Scan, Server Protect, Scan Mail Exchange Win NT/2000 v 6.x (Of.) Interscan Web Security Suite, Interscan Messaging Security. 470 licencias de Control Manager Enterprise (consola de administración, Reportes y limpieza de daños). 470 licencias de Spam Prevention Solution + Network Antispam Services. El oferente debe contemplar el soporte, mantenimiento y actualizaciones automáticas durante un año, sin costo adicional para la Entidad. Así mismo el oferente debe contemplar y garantizar la instalación de mínimo la cantidad de clientes requeridos en la Oficina Principal, Sede 2 y Regional Bogotá los cuales son aproximadamente 250 clientes, así mismo deberá brindar el soporte necesario para realizar las instalaciones en las Direcciones Regionales teniendo en cuenta que a la fecha no hay conectividad con ellas.	**SI**	**71**
ORGANIZACIÓN PARA EL PROYECTO		
El oferente deberá instalar y poner en funcionamiento la Suite, en un plazo máximo de cuarenta y cinco (45) días, de acuerdo a las especificaciones técnicas requeridas en las instalaciones de la Agencia Logística de las Fuerzas militares, Ubicada en la **Carrera 50 No. 18 – 92** puente Aranda.	**SI**	**71**
EXPERIENCIA		
El oferente deberá acreditar experiencia relacionada con el objeto a contratar en mínimo dos (02) Entidades en los últimos tres (3) años, contados con antelación a la fecha de cierre de la presente Contratación Directa. Para ello deberá diligenciar el formato No. 1 “acreditación de experiencia específica”.	**SI**	**71**
IMPLEMENTACIÓN Y PUESTA EN FUNCIONAMIENTO DEL OBJETO CONTRATADO.		
Al finalizar la instalación definitiva del software deberá garantizar que todos los equipos quedarán funcionando a entera satisfacción, cumpliendo con las especificaciones técnicas solicitadas en este pliego.	**SI**	**71**
GARANTÍA DE FUNCIONAMIENTO		
El proponente ofrecerá como mínimo una garantía de calidad y funcionamiento de doce (12) meses para el software, contados a partir del acta de recibo final a satisfacción.	**SI**	**71**
SOPORTE TÉCNICO Y TIEMPO DE RESPUESTA		
Durante el periodo de garantía, el oferente deberá brindar soporte para la identificación, análisis y solución a los problemas que se presenten en el buen funcionamiento y operatividad de la totalidad del objeto del contrato, mediante esquema de Call Center 7x24.	**SI**	**71**
CAPACITACIÓN Y TRANSFERENCIA DE CONOCIMIENTO		
El proponente deberá ofrecer la capacitación correspondiente al personal designado por la Agencia Logística de las Fuerzas Militares en el manejo del software y todos sus componentes que lo complementen.	**SI**	**71**

El proponente deberá realizar toda la transferencia de conocimiento necesaria al personal técnico designado por la Agencia Logística de las Fuerzas Militares que le garantice la administración, configuración, instalación, mantenimiento y la capacidad de solucionar problemas que se presenten una vez sea instalada la solución ofertada.	**SI**	**72**
PROTECCIÓN ANTIVIRUS PARA ESTACIONES DE TRABAJO Y SERVIDORES		
Nombre del Software de las Estaciones. Especificar marca	**SI**	**72**
Versión corporativa del antivirus de estaciones. Especificar Versión	**SI**	**72**
Nombre del Software de Servidores. Especificar Marca	**SI**	**72**
Versión corporativa del antivirus de servidores. Especificar Versión. El oferente debe entregar la última versión liberada.	**SI**	**72**
El proponente debe ofrecer un esquema de licenciamiento a perpetuidad con mínimo un año de mantenimiento incluido. Especificar el tiempo de la licencia y el tiempo de mantenimiento incluido.	**SI**	**72**
Los laboratorios del fabricante deben ser certificados ISO 9001 en el proceso de generación de vacunas.	**SI**	**72**
El antivirus de las estaciones de trabajo, debe estar en capacidad de detectar cualquier código malicioso, virus y código spyware.	**SI**	**72**
El fabricante, debe ofrecer la posibilidad de adquirir un servicio SLA que garantice un tiempo de respuesta de máximo dos horas a partir de la detección, ante la aparición de un nueva amenaza.	**SI**	**72**
El fabricante después de que un nuevo virus haya sido detectado, deberá generar y proveer pocos minutos después de la detección, políticas de prevención que se implementen automáticamente sin requerir la intervención del usuario o del administrador. Estas plantillas deben cerrar automáticamente todas las posibles puertas de entradas del virus (bloqueo de puertos, descompartir carpetas, asignar permisos de solo lectura a archivos, etc.) y deben notificar al administrador las acciones a tomar.	**SI**	**72**
El fabricante, ante cada nuevo virus detectado, debe ofrecer un servicio de limpieza y reparación de daños que se implemente en forma automática cada vez que sea detectado el virus en la red o se puede ejecutar a demanda desde una consola de administración en caso de exista algún equipo desprotegido que haya sido infectado. Esta política debe restaurar automáticamente los daños ocasionados por el virus evitando desplazamiento a los equipos o realizar brigadas de limpieza.	**SI**	**72**
La última versión del antivirus para estaciones debe estar disponible y soportada para estaciones Windows 9X, o superior y la última versión para servidores deberá soportar plataformas Linux Red Hat, Novell y Windows NT 4.0 o superior. No se aceptarán versiones previas, reducidas o que disminuyan o hagan depender sus funcionalidades de una consola (Ej. Escaneo bajo demanda, implementación de políticas, etc.)	**SI**	**72**
El proponente debe proporcionar todas las actualizaciones de productos, versiones de mantenimiento, patrones y cambios con nuevas funcionalidades y mejoras del producto sin costo adicional mínimo durante el tiempo de oferta.	**SI**	**72**
El software antivirus ofertado debe permitir administración centralizada, reportes, actualización y cambios en la configuración en tiempo real	**SI**	**72**
La protección para estaciones de trabajo debe ofrecer escaneo en tiempo real y en demanda, aunque esté fuera del alcance o la injerencia de la consola de administración.	**SI**	**72**
El producto de protección para estaciones y servidores debe permitir administración centralizada mediante la misma consola de administración.	**SI**	**72**
El producto debe permitir instalación remota en sistemas operativos Windows 95 o superior. Y para equipos Windows 9x debe incluir una herramienta que facilite la generación del script de instalación.	**SI**	**73**

El antivirus para estaciones de trabajo, debe estar en capacidad de desinstalar el antivirus actual en forma automática (si es un producto estándar), ahorrando tiempo de instalación y evitando desplazamiento a los equipos. Sin embargo, la desinstalación debe hacerse sobre los equipos deseados por el administrador y no debe reinstalar automáticamente todos los equipos presentes en la red.	**SI**	**73**
El antivirus para estaciones de trabajo, debe realizar un escaneo durante el proceso de la instalación.	**SI**	**73**
La solución antivirus permite realizar actualizaciones automáticas de patrones o vacunas cada hora y de las políticas de prevención cada cinco minutos, sin congestionar la red y garantizando que la red estará desprotegida menos de cinco minutos ante un nuevo virus.	**SI**	**73**
La comunicación entre las estaciones y la consola de administración debe realizarse en forma bidireccional y por eventos; es decir, las estaciones y los servidores se comunican con la consola ante una novedad y la consola se comunica con los servidores y las estaciones cuando tiene una novedad.	**SI**	**73**
El antivirus debe escanear automáticamente los archivos comprimidos mínimo hasta 20 niveles de compresión, sin requerir que el usuario manualmente descomprima el archivo. Igualmente, el antivirus no debe permitir copiar los archivos comprimidos infectados en el disco duro, el escaneo y la limpieza deben realizarse antes de escribirse en el disco.	**SI**	**73**
El antivirus debe soportar al menos 10 algoritmos de compresión y/o codificación. (PKZip, PKLite, LZH, LZExe, ARJ, y MIME incluidos.)	**SI**	**73**
El antivirus debe ser capaz de realizar escaneos inteligentes y tomar medidas específicas según el tipo de virus detectado.	**SI**	**73**
El antivirus debe permitir configurar más de una opción a elegir si encuentra virus.	**SI**	**73**
El software antivirus permite desde la consola de administración configurar usuarios con diferentes niveles de permisos para administrar o tener acceso a las funcionalidades o a la administración de la plataforma antivirus y permitir que sólo el usuario administrador pueda desinstalar o deshabilitar el antivirus.	**SI**	**73**
Permite revisar manual e incrementalmente las carpetas personales de Outlook *.pst y el mailbox del usuario.	**SI**	**73**
La solución de antivirus para las estaciones de trabajo posee un módulo para realizar escaneo sobre el tráfico POP3, aún cuando el equipo está fuera de la red corporativa (Ej, portátiles con conexión vía módem)	**SI**	**73**
El antivirus para la estación de trabajo, permite bloquear puertos en los equipos desde una consola central, sin requerir hacer modificaciones en el firewall.	**SI**	**73**
El antivirus para la estación de trabajo, permite bloquear carpetas o archivos compartidos como medida de seguridad, en forma centralizada desde la consola de administración	**SI**	**73**
El antivirus para la estación de trabajo, permite denegar o permitir el acceso a escritura de archivos a los equipos desde una consola central.	**SI**	**73**
El antivirus de las estaciones de trabajo, debe soportar Cisco Network Admisión Control (NAC)	**SI**	**73**
El antivirus de las estaciones de trabajo, debe ofrecer protección a dispositivos wireless (PDAs, celulares, etc.).	**SI**	**73**
La herramienta antivirus para las estaciones de trabajo, debe actualizar en forma manual y automática el patrón de virus, motor de escaneo, la versión del programa, las políticas de prevención de epidemias, el motor y la plantilla del servicio de limpieza de daño, el patrón spyware, el motor del firewall personal y el patrón para virus de red.	**SI**	**74**
El antivirus para estaciones de trabajo debe poseer un módulo de personal firewall integrado y su instalación no debe requerir un agente adicional.	**SI**	**74**
El antivirus para estaciones de trabajo debe poseer un módulo de IDS para virus y su instalación no debe requerir un agente adicional.	**SI**	**74**

La herramienta debe soportar rollback de actualizaciones evitando corrupción de los archivos de actualización.	**SI**	**74**
Permite instalar el soporte para Wireless y para clientes de VPN de Checkpoint	**SI**	**74**
El oferente debe ofrecer capacitación que incluye conceptos como instalación, configuración, administración y solución a problemas más comunes en la(s) solución(es) de seguridad antivirus.	**SI**	**74**
PROTECCIÓN ANTIVIRUS PARA SERVIDORES DE CORREO ELECTRÓNICO		**74**
Nombre del Software. Especificar marca.	**SI**	**74**
Versión corporativa. Especificar versión	**SI**	**74**
El proponente debe ofrecer un esquema de licenciamiento a perpetuidad con mínimo un año de mantenimiento incluido. Especificar Tiempo licencia y Tiempo mantenimiento incluido	**SI**	**74**
Los laboratorios del fabricante deben ser certificados ISO 9001:2000 en el proceso de generación de vacunas.	**SI**	**74**
El fabricante, ante un nuevo virus, debe garantizar un tiempo máximo de cuatro horas para la generación de una nueva vacuna.	**SI**	**74**
Antivirus disponible para Microsoft Exchange Versión 5.5, 2000 y 2003	**SI**	**74**
El fabricante debe poseer un esquema de nivel se servicios que garantice que la generación de la vacuna se hará en un tiempo máximo de 4 horas.	**SI**	**74**
El proponente debe proporcionar todas las actualizaciones de productos, versiones de mantenimiento, patrones y cambios con nuevas funcionalidades y mejoras del producto sin costo adicional mínimo durante el tiempo de oferta.	**SI**	**74**
El software antivirus ofertado debe permitir administración centralizada, reportes, actualización y cambios en la configuración en tiempo real	**SI**	**74**
El antivirus debe escanear automáticamente los archivos comprimidos mínimo hasta 20 niveles de compresión, sin requerir que el usuario manualmente descomprima el archivo. Igualmente, el antivirus no debe permitir copiar los archivos comprimidos infectados en el disco duro, el escaneo y la limpieza deben realizarse antes de escribirse en el disco.	**SI**	**74**
Soporte para al menos 10 algoritmos de compresión y/o codificación. (PKZip, PKLite, LZH, LZExe, ARJ, y MIME incluidos.)	**SI**	**74**
La solución antivirus permite realizar actualizaciones de patrones o vacuna cada hora y de las políticas de prevención cada cinco minutos, sin congestionar la red y garantizando que la red estará desprotegida menos de cinco minutos ante un nuevo virus.	**SI**	**74**
El antivirus debe permitir configurar más de una opción a elegir si encuentra virus.	**SI**	**74**
Realiza actualizaciones automáticas e increméntales (solo actualiza los que haya cambiado entre una versión y otra).	**SI**	**74**
El antivirus para los servidores de correo electrónico, permite realizar instalación y desinstalación remota	**SI**	**74**
El antivirus debe estar soportado para plataformas Clúster de Microsoft	**SI**	**74**
El antivirus durante la instalación detecta automáticamente si es plataforma clúster o no	**SI**	**74**
En caso de un ataque de virus o código malicioso, puede notificar al remitente, al receptor y al administrador	**SI**	**75**
El antivirus puede escanear a nivel de information store de MS Exchange, en lugar de a nivel de mailboxes, evitando el escaneo redundante y optimizando los recursos del servidor	**SI**	**75**
El antivirus permite realizar escaneo incremental de los mailboxes	**SI**	**75**
Permite realizar notificaciones vía SNMP, vía e-mail y vía Windows NT Event Log	**SI**	**75**

El oferente debe ofrecer capacitación que incluye conceptos como instalación, configuración, administración y solución a problemas más comunes en la(s) solución(es) de seguridad antivirus.	**SI**	**75**
PROTECCIÓN ANTIVIRUS Y DE CONTENIDO PERIMETRAL	**SI**	**75**
Nombre de la solución de protección perimetral	**SI**	**75**
Versión corporativa	**SI**	**75**
Los laboratorios del fabricante deben ser certificados ISO 9002 en el proceso de generación de vacunas.	**SI**	**75**
El fabricante, debe ofrecer la posibilidad de adquirir un servicio SLA que garantice un tiempo de respuesta de máximo dos horas a partir de la detección, ante la aparición de un nueva amenaza.	**SI**	**75**
Escanea contra virus los protocolos SMTP, POP3, FTP Y HTTP	**SI**	**75**
Permite una fácil implementación, instalando en forma modular la protección de cada protocolo (SMTP, FTP, HTTP, POP3) en el punto dónde sea requerido (Gateway, servidor de correo, servidor Web, etc), evitando cambios mayores en la red y su plataforma	**SI**	**75**
La solución debe estar soportado para ser instalado en plataformas Windows, Linux y Solaris sin necesidad de generar costos adicionales ante un cambio de plataforma	**SI**	**75**
Realiza actualizaciones automáticas e increméntales (solo actualiza los que haya cambiado entre una versión y otra).	**SI**	**75**
El fabricante después de que un nuevo virus haya sido detectado, deberá generar y proveer, pocos minutos después de la detección, políticas de prevención que se implementen automáticamente sin requerir la intervención del usuario o del administrador. Estas políticas deben cerrar automáticamente todas las posibles puertas de entradas del virus (correo electrónico, páginas de Internet peligrosas) y deben notificar automáticamente al administrador las acciones a tomar.	**SI**	**75**
El antivirus debe escanear automáticamente los archivos comprimidos mínimo hasta 20 niveles de compresión, sin requerir la intervención del usuario. Igualmente, el antivirus no debe permitir copiar los archivos comprimidos infectados en el disco duro, el escaneo y la limpieza deben realizarse antes de copiarse el archivo en el disco duro	**SI**	**75**
El antivirus debe permitir configurar más de una opción a elegir si encuentra virus.	**SI**	**75**
La solución debe permitir implementar reglas de filtrado de contenido sobre el correo electrónico tales como permitir o negar el ingreso o la salida de correos por tipos de archivos (Extensiones), tamaño de los archivos, tamaño del correo, cantidad de archivos anexos, correos con palabras o frases prohibidas, etc., aplicando estas normas aún si los archivos son renombrados o comprimidos.	**SI**	**75**
La solución debe evitar la generación de correos masivos en el interior de la organización, implementando filtros contra los correos en cadena	**SI**	**75**
La solución debe estar en capacidad de buscar una palabra o frase prohibida en el interior de un archivo anexo a un correo (Word, Excel, Power Point, Acrobat, etc.) mediante el uso de operadores lógicos inteligentes.	**SI**	**75**
Permite implementar y personalizar un disclaimer para todos los correos salientes y otro para los correo entrantes.	**SI**	**75**
Las políticas de seguridad y de filtrado de contenido pueden aplicarse a un usuario, un grupo de usuarios o globalmente a juicio del administrador de seguridad	**si**	**76**
La solución permite bloquear el ingreso o la salida de archivos con excesivos niveles de compresión	**si**	**76**
la solución permite realizar ruteo de dominios	**si**	**76**
El producto maneja colas de e-mails	**si**	**76**

La solución antivirus para correo electrónico debe detectar virus mass mailing en el cuerpo del mensaje, en el adjunto y de correos insertados en otros correos.	**si**	**76**
La herramienta de protección perimetral de correo electrónico debe detectar spam basado en listas blancas y negras, y mediante procesos heurísticos, con una sensibilidad ajustable en cinco diferentes niveles.	**si**	**76**
La solución ofertada debe ser capaz de detectar spyware en http y ftp	**si**	**76**
La solución debe estar en capacidad de bloquear la descarga de archivos nocivos o que vayan en contra de las políticas de seguridad de la organización.	**si**	**76**
La solución debe integrarse en forma transparente, mediante el protocolo ICAP con sistemas web caché	**si**	**76**
La herramienta debe ser capaz de detectar virus en el upload y el download de http y ftp.	**si**	**76**
La solución de protección antivirus y de filtrado de contenido perimetral debe ser administrable desde la misma consola de administración de la protección antivirus interna, permitiendo un único punto de control y administración.	**si**	**76**
Antispam Heuristico	**si**	**76**
Antispam por medio de bases de datos de Reputación	**si**	**76**
Antispyware y Antiphishing	**si**	**76**
El oferente debe ofrecer capacitación que incluye conceptos como instalación, configuración, administración y solución a problemas más comunes en la(s) solución(es) de seguridad antivirus.	**si**	**76**
HERRAMIENTA DE ADMINISTRACIÓN DE LA PLATAFORMA ANTIVIRUS	**si**	**76**
Nombre del Software	**si**	**76**
Versión corporativa	**si**	**76**
La consola de administración, debe ser el único punto de administración y control de todos los productos de la marca tanto de protección interna como perimetral.	**si**	**76**
La administración de la herramienta antivirus para las estaciones de trabajo, no debe requerir instalar un agente sobre la estación.	**si**	**76**
La consola de administración debe informar ante que virus fue detectado, en qué archivos, en qué computadores y que acción tomo el antivirus.	**si**	**76**
La consola debe descargar actualizaciones de políticas de prevención, de vacunas y de servicios de recuperación de daños, en forma automática e incremental (Descarga sólo la diferencia) y debe distribuirla a las demás consola de administración, en caso de que las haya y a los productos antivirus en estaciones y servidores.	**si**	**76**
Desde la consola, se deben poder realizar escaneos simultáneos, programados o manuales a todos los equipos de la red, por grupos o pen forma individual, cómo sea requerido por el administrador.	**si**	**76**
La consola debe ofrecer reportes en logs y gráficos del estado en tiempo real de toda la plataforma antivirus.	**si**	**76**
La consola para realizar la administración y aplicación de políticas antivirus debe permitir hacerse a través del protocolo TCP/IP, por nombre de máquina o usuario o administración por direcciones IP.	**si**	**76**
Los reportes ofrecidos por la consola deben poder visualizarse en formatos PDF,RTF, ActiveX y Cristal Report	**si**	**76**
Los reportes ofrecen información como virus presentes en la red, acciones tomadas, usuarios atacados, usuarios infectados, reporte de violaciones de seguridad, análisis de puntos de entrada, estadísticas de estado de actualización de los patrones, Top 10; etc.	**si**	**77**
La generación de reportes puede hacerse en forma programada o agenda para que se generen y sean enviados al administrador cada cierto tiempo.	**si**	**77**

Se puede obtener un estado actual de la solución por producto (Protección de estaciones, de servidores, de correo, etc.)	**si**	**77**
Permite implementar políticas de seguridad en forma centralizada, tales como el bloqueo de puertos de las estaciones, el bloqueo de carpetas compartidas, la denegación de permisos de escritura, el bloqueo de correos con contenido prohibido, el bloqueo de correos con archivos prohibidos, etc.	**si**	**77**
La comunicación entre el agente y el servidor de la consola de administración debe ser bidireccional y por eventos; es decir, la comunicación se debe realizar sólo cuando la consola tenga una actualización para entregar o cuando el equipo tenga una novedad que reportar (Encendido, ataque, etc.), con el fin de evitar los broadcast innecesarios en la red.	**si**	**77**
La consola de administración debe notificar al administrador cuando se implementa una nueva política de prevención de infecciones	**si**	**77**
la consola de administración debe permitir la instalación de los productos en forma remota y centralizada	**si**	**77**
La consola puede ser el único punto de actualización y se encarga de actualizar a los demás productos	**si**	**77**
El oferente debe ofrecer capacitación que incluye conceptos como instalación, configuración, administración y solución a problemas más comunes en la(s) solución(es) de seguridad antivirus.	**si**	**77**
ESPECIFICACIONES TÉCNICAS EXCLUYENTES EXIGIBLES PARA LA EJECUCIÓN DEL CONTRATO		
	Cumple	**No. De**
Descripción	**SI/NO**	**Folio**
DOCUMENTACIÓN (MANUALES)		
El oferente adjudicatario deberá entregar los respectivos manuales y documentación de operación del software ofertado.	**SI**	**78**
El oferente adjudicatario deberá instalar y probar el software instalado en las Oficinas de la Agencia Logística de las Fuerzas Militares	**SI**	**78**
El oferente adjudicatario suscribirá un acuerdo de confidencialidad donde se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del objeto del contrato, así como sobre los lugares a los cuales tenga acceso con ocasión de su desarrollo, el cual se suscribirá con ocasión a la firma del acta de iniciación.	**SI**	**78**
IMPLEMENTACIÓN Y PUESTA EN FUNCIONAMIENTO DEL OBJETO CONTRATADO.		
La puesta en funcionamiento del objeto del contrato, será efectuada por el oferente adjudicatario, en las oficinas de la Agencia Logística de las Fuerzas Militares ubicadas en la ciudad de Bogotá en la Cra. 50 No. 18 – 92 Puente Aranda.	**si**	**71**
Todos los costos asociados para el cumplimiento del objeto correrán por parte del oferente. El oferente deberá garantizar el personal suficiente, idóneo y necesario para la completa ejecución del objeto del contrato sin que éste genere costo adicional alguno para la Agencia Logística de las Fuerzas Militares.	**SI**	**78**
Todas las especificaciones de configuración que se hayan utilizado en las diferentes instalaciones del software, deberán quedar debidamente documentadas y entregadas en medio impreso y magnético a la Agencia Logística de las Fuerzas Militares.	**SI**	**78**
INSPECCIONES Y PRUEBAS	**SI**	**78**
Para verificar el funcionamiento a entera satisfacción de las soluciones instaladas y como paso previo a la expedición de los certificados de aceptación de la instalación, se ejecutarán la totalidad de pruebas de recibo.	**SI**	**78**

Si después de inspeccionado y probado el objeto del contrato no se ajusta a las especificaciones requeridas en este pliego, la supervisión del contrato lo rechazará y el oferente adjudicatario, sin costo adicional lo reemplazará para cumplir con las especificaciones.	**SI**	**78**
GARANTÍA DE FUNCIONAMIENTO	**SI**	**78**
El oferente adjudicatario deberá cumplir con el tiempo de	**SI**	**78**
Garantía a partir de la fecha del acta de recibo a satisfacción del objeto a contratar.	**SI**	**78**
El oferente adjudicatario deberá brindar un horario de atención, durante el periodo de garantía, de 08:00 a 18:00 horas los días hábiles.	**SI**	**78**
El oferente adjudicatario deberá brindar durante el periodo de	**SI**	**78**
garantía, atención a las llamadas en un tiempo máximo de dos (2) horas.	**SI**	**78**
El oferente adjudicatario, durante el periodo de garantía ofrecido, detectará y corregirá las fallas de funcionamiento del software, sin costo adicional para la Agencia Logística de las Fuerzas Militares.	**SI**	**78**
El proponente deberá garantizar que el representante en Colombia, cuenta con Centros Autorizados de servicio en la Ciudad donde se realiza la entrega.	**SI**	**78**
El oferente deberá contar con un help desk para la atención de los requerimientos del presente acápite de garantía.	**SI**	**78**
ASPECTOS TÉCNICOS ADICIONALES		
NOTA: La AGENCIA LOGISTICA DE LAS FUERZAS MILITARES se reserva el derecho de efectuar los requerimientos necesarios a los proponentes sobre los ASPECTOS TECNICOS ADICIONALES en aplicación del Decreto 2170 de 2002.		
Descripción	**Cumple SI/NO**	**No. De Folio**
EXPERIENCIA DEL OFERENTE		
El oferente deberá adjuntar certificaciones emitidas por las Entidades Contratantes en el **formato No. 1 "acreditación de experiencia específica"**, donde se corrobore la calidad del servicio recibo relacionado con el objeto del contrato.	**SI**	**77**
Los laboratorios del fabricante deben ser certificados ISO 9001 en el proceso de generación de vacunas.	**si**	**77**
La entrega de la solución se hará en la Cra. 50 # 18-92. en las Oficinas de la Agencia Logística de las Fuerzas Militares.	**si**	**71**
El oferente deberá anexar certificación que lo identifique como representante autorizado por el fabricante del software ofertado, vigente a la fecha de cierre del presente proceso contractual, en donde conste que el proponente es distribuidor autorizado.	**si**	**77**

A1= INTERNET SOLUTIONS LTDA

CONCLUSIONES

Después de revisada la oferta entregada por ustedes, nos permitimos concluir que las firma **A1= INTERNET SOLUTIONS LTDA., SI CUMPLE** con las especificaciones técnicas mínimas requeridas de la solicitud de oferta. Por lo anteriormente expuesto nos permitimos habilitar a la firma **A1= INTERNET SOLUTIONS LTDA**. para continuar con el proceso de contratación.