Asunción, 16 de julio de 2014.

Señor(es)
PROVEEDORES
Presente

Me dirijo a usted(es), con el objeto de remitirle(s) la Comunicación Suplementaria Nº 05 en la cual se transcribe el Addendum N° 04, en el marco de la Licitación por Concurso de Ofertas N° 08/2014 "Adquisición de Antivirus y Anti-Spam para el Congreso de la Nación" con ID Nº 278524, el mismo pasa a formar parte del Pliego de Bases y Condiciones.

ADDENDUM Nº 04

La Unidad Operativa de Contrataciones, amparada en lo que dispone el artículo 22º de la Ley 2051/03 y el artículo 40 del Decreto Nº 21909 que reglamenta la Ley 2051/03, en el marco de la Licitación por Concurso de Ofertas N° 08/2014 "Adquisición de Antivirus y Anti-Spam para el Congreso de la Nación" con ID Nº 278524, procede a introducir las siguientes modificaciones al Pliego de Bases y Condiciones:

1. **En la Sección III. Suministros Requeridos; punto 1. Especificaciones Técnicas**

- **Se modifica la "Descripción del bien" quedando como sigue:**

Ítem	Código Catalogo	Descripción del Bien	Unidad de Medida	Presentación	Cantidad
1	*43233205-001*	**LICENCIAS ANTIVIRUS** (solución de seguridad basada en la nube) Software Antivirus para estaciones de trabajo y servidores de archivos, antivirus y protección antispam de correo electrónico, también denominado Cliente / Servidor, con consola de administración a través de la web, con las siguientes características. • El oferente deberá garantizar que el producto ofrecido funcionará completa y correctamente en todas las plataformas de software y hardware informadas. • Soporte de instalación y actualización centralizada (desatendida del antivirus de PC) • Programación de actualizaciones hacia todos los clientes y servidores en modo: centralizado y automático. • Poseer certificación ICSA LABS o similar. • Poseer certificación Checkmark WestCoast Labs Level 1 y 2 o similar. • VB100 Virus Bulletin • Contar con los siguientes métodos para la instalación desde la consola de administración hacia las estaciones clientes y/o servidores: conexión a red; intranet/internet forma remota; Vía e-mail; otras. • Detección y eliminación de las siguientes amenazas conocidas y desconocidas en las estaciones cliente y/o servidores según el método de rastreo seleccionado (tiempo real, demanda, programado, etc.): - Adware ó software publicitario - Dialers ó discadores telefónicos - Herramientas de Hacking - Keyloggers ó programas de robo de contraseñas - Jokes ó Bromas - Rootkits - Spyware ó Software Espía - Troyanos ó caballos de troya - Virus de arranque - Virus de archivos - Virus en Macros - Virus de VBScrip y Java Script - Virus en archivos compactados - Virus en archivos compactados de hasta 10 niveles como mínimo. • Chequeo automático de la transferencia de archivos entre	*Unid.*	*Unid.*	*501*

Ítem	Código Catalogo	Descripción del Bien	Unidad de Medida	Presentación	Cantidad
		clientes y servidores. • El servidor deberá soportar instalación, configuración y administración centralizada con opción 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. • Protección contra amenazas y exploits que aprovechan vulnerabilidades desconocidas (zero-day) • Posibilidad de realizar en estaciones cliente y servidores los distintos tipos de rastreo en: tiempo real; por demanda; programado; remoto; discos; directorios; archivos seleccionados; otras. • Ante la detección de un virus por cualquiera de los métodos de rastreo seleccionados en las estaciones cliente y servidores posibilidad de: desinfectar; eliminar; mover a cuarentena; otras. • Soporte de administración remota desde cualquier estación de trabajo o servidor con interfaz Web. • Notificación de detección virus vía: correo electrónico, como mínimo. • Posibilidad de realizar informes que muestren (como mínimo): versiones de definiciones y motor de búsqueda; detección de virus; tareas programadas; otros. • Permitir la creación de distintos perfiles de administrador. El administrador podrá programar la actualización de los equipos cliente seleccionado: todas las estaciones de trabajo; grupo de estaciones de trabajo; otras. • 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. desde interfaz web. • Disponer 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 en la ubicación geográfica que se encuentren. • Instalación flexible, automática y/o remota, mediante el despliegue del instalador, distribuido: mediante e-mail con link a la URL de descarga. Localmente, mediante la descarga del instalador desde la consola. Remotamente, mediante herramientas de distribución estándar como login script, Active Directory, Tivoli, SMS, Lan Desk o similares. • La detección de código malicioso deberá realizarse en forma preventiva, antes de que el mismo se esté ejecutando en el equipo. • Poseer protección proactiva en tiempo real para todas las comunicaciones de la PC, incluyendo mensajería instantánea y correo electrónico. • El producto debe incluir un mecanismo de control de dispositivos USB, que permita como mínimo bloquear llaves USB, dispositivos de almacenamiento externos (cámaras, tarjetas de memoria, etc), unidades ópticas CD/DVD, dispositivos Bluetooth y módems de conectividad 3G. • Debe permitir la creación de paquetes de instalación con configuración personalizada (Ejemplo: Paquetes MSI). • Posibilidad de generar instalaciones remotas para sitios que poseen distintos accesos a internet ó no se encuentren enlazados -punto a punto- con la oficina central. • Posibilidad de instalación local con herramienta de distribución a través de TCP/IP. • Posibilidad de crear diferentes tipos de usuarios de administración de la solución y asignación de privilegios según las necesidades de la empresa. • Permitir si fuese necesario la delegación de la administración de un sitio, sucursal o nodo a un tercero entregándole un usuario y contraseña con acceso a lo que la empresa determine conveniente.			

Ítem	Código Catalogo	Descripción del Bien	Unidad de Medida	Presentación	Cantidad
		• La administración centralizada no debe requerir un servidor dedicado en la/las organización/es y debe encontrarse accesible desde internet. • La comunicación entre los nodos y la consola de administración deberá realizarse de forma encriptada (https por ejemplo). • Poseer mecanismos de auto actualización entre terminales (modalidad tipo P2P inteligente o similar) para equipos que no poseen acceso a internet. • Notificación al administrador de la red ante la detección de virus. • Deberá contar con Firewall en el módulo para estaciones de trabajo. • El Firewall deberá poder ser administrado tanto de forma remota como desde la estación de trabajo por el usuario, pudiendo el administrador decidir esta situación. • Deberá soportar la creación de grupos y políticas para facilitar la administración de los equipos protegidos. • La solución deberá integrarse con herramientas de acceso remoto al PC de terceros (LogMeIn, Teamviewer, VNC, etc.). • Poseer un sistema de informes que permita conocer en tiempo real el estado de las protecciones, productos instalados y fechas de los archivos de firmas y actualizaciones de los mismos. • Los reportes generados por la solución deberán ser en múltiples formatos, como mínimo: XML, CSV, TIFF, PDF, HTML, XLS. • Posibilidad de realizar el envío de informes de forma periódica al/los administrador/es con el estado de los nodos protegidos. • Auditorias de malware y estado de vulnerabilidades del parque informático. • Compatible con Windows 8.1, Windows Server 2012, Mac OS X, Linux y sistemas virtuales VMWare, Microsoft y Citrix, incluidos portátiles y oficinas remotas. • Certificación ISO 27001 y SAS 70 para los servicios de computación y almacenamiento de los centros de datos (computación, almacenamiento, Traffic Manager y Connect de Windows Azure) • Configuración del dominio de correo y habilitación de las cuentas de correo desde una consola de administración web. • Solución de seguridad para email basada en software como servicio (SaaS). • Automático: con tecnología optimizada basada en sistemas OpenSource. • Garantizado: modo 100% libre de spam, debe verificar si el remitente existe en lista blanca, si no existe debe solicitar al remitente validación. • Filtrado de correo por conexión: Lista de reputación de IP`s, RBL, SPF. • Protección contra la falsificación de direcciones en el envío de correo electrónico. • Listas Black/White globales (por dominio) y locales (por usuario). • Filtrado de correo por remitente. • Tráfico cifrado (TLS). • Alta de buzones manual, desde fichero o integración con LDAP (Open LDAP, Active Dircetory y Domino). • Estadísticas e informes de actividad del tráfico de correo electrónico. • Cuarentena opcional de Virus accesible únicamente por el administrador. • Personalización logos por dominio y empresa. • Disclaimers por dominio y empresa. • Disponer de sistema multicapa de filtrado y protección, ya sea por usuario o por dominio de correo. • Disponer de administración web basada en perfiles, y permitir			

Ítem	Código Catalogo	Descripción del Bien	Unidad de Medida	Presentación	Cantidad
		configurar a nivel empresa, dominio y usuario. • No requiere instalación de ninguna aplicación en el servidor de correo, ya que su protección se basa en la nube, evitando problemas de incompatibilidad, y pudiendo dar soluciones a diferentes plataformas de servidores de correo. • Disponer de protección frente a caídas de servidores de correo, mediante backups de correos. • Backup completo de e-mail entrante: 10 días para correo válido / 15 días para spam. • Disponer de configuraciones de envíos de informes programados y por demanda, además de notificadores de correo. • Disponer de consola webmail para acceso remoto de los usuarios de correo. • Disponer de motor de reglas que permita configurar políticas de contenido y configurar criterios de tratamiento automático de spam. • Software ecológico (Green IT) • Se deberá Capacitar como mínimo a 4 (cuatro) técnicos del área de Informática en el uso y/o administración del producto. • Con vigencia para 3 (tres) años como mínimo.			

***El presente documento pasa a formar parte del pliego de bases y condiciones*.**

HONORABLE CAMARA DE SENADORES
DIRECCION ADMINISTRACION FINANCIERA
CONGRESO DEL PARAGUAY
U.O.C.

Justina Casco González
Directora
Unidad Operativa de Contratación.