CONTRATACIÓN DIRECTA N° 07/2016
"ACTUALIZACIÓN DE LICENCIAS ANTIVIRUS"
ID: 309.157

ADENDA N° 2

Asunción, 07 de julio de 2016

SEÑORES OFERENTES:

El Ministerio del Interior, de conformidad al Art. 22 inciso "b" de la Ley N° 2051, el Art. 40 del Decreto N° 21.909, que reglamenta la citada Ley y en uso de sus atribuciones, emite la siguiente Adenda a fin de realizar las siguientes modificaciones correspondientes al llamado de referencia:

1) Modifíquese la fecha de presentación y apertura de ofertas del llamado de referencia, las cuales quedarán establecidas de la siguiente manera:

Fecha límite para presentar Ofertas:	**14 de julio de 2016**
Hora Tope:	**09:00 a.m.**
Fecha de Apertura de Ofertas:	**14 de julio de 2016**
Hora:	**09:30 a.m.**

2) Modifíquese el **Anexo C. Especificaciones técnicas de los bienes a ser adquiridos** de la Carta Invitación, el cual quedará establecido de la siguiente manera:

1. Especificaciones Técnicas

ACTUALIZACIÓN DE LICENCIAS KASPERSKY

CANTIDAD: 200 (Doscientos)
Vigencias: 2 años

La institución cuenta actualmente con un parque instalado de licencias kaspersky, por lo cual a fin de unificar la gestión y administración se solicita licencias de la misma marca.

Especificar Marca y Producto	Kaspersky Total Security for Business
Vigencia de	.....
Cantidad	**200 nodos**
Idioma	**Español**
Servicios a ser incluidos	o Instalación completa de la Consola de Administración y Nodos. o Creación y validación de políticas o Transferencia tecnológica y capacitación o El oferente deberá presentar un plan de capacitación de como Mínimo 10 hs., con los ítems a ser incluidos en la misma como anexo a esta planilla, la misma será de carácter sustancial.

Funcionalidades requeridas	o Antimalware y Firewall o Control de Aplicaciones y Dispositivos o Protección para Servidores de Colaboración, Servidores de Archivos, y Servidores de Correo o Administración de Admisión a la Red o Administración de Listas Blancas de Aplicaciones o Control Web o Manejo y Seguridad para dispositivos móviles o Encriptación o Administración de Parches o Escáner de Vulnerabilidades o Configuración y Despliegue de Sistemas
Consola Centralizada de Administración	o Configuración y administración de políticas de seguridad en varias plataformas, como Windows, Linux y Mac. o Configuración de seguridad de grupos de servidores, estaciones de trabajo o dispositivos individuales. o Ejecución de análisis de virus, a pedido o por cronograma. o Proceso de objetos que se han puesto en cuarentena. o Administración de las actualizaciones de bases de datos antivirus. o Administración de la protección con posibilidad de asistencia en la nube. o Definición de políticas de control de aplicaciones para prevenir la ejecución de programas no deseados en la red corporativa. o Administración de privilegios de acceso para cualquier dispositivo que los usuarios conecten a la red corporativa, según el tipo de dispositivo, el bus o el número de serie de cada dispositivo. o Supervisión y control del acceso a la Web, y privilegios relacionados incluida la segmentación de grupos de usuarios.

Administración de Endpoints	o Antimalware basados en firmas, proactivos, comprobados o en la industria y basados en la nube. o Control de dispositivos a través de políticas para Bloquear o regular aplicaciones (o categorías de aplicaciones). o Control de Dispositivos a través de programación y aplicación de políticas de datos con almacenamiento removible y otros controles de dispositivos periféricos conectados por USB o cualquier otro tipo de bus. o Controles de navegación basados en el End-point que sigan al usuario, ya sea en la red corporativa o mientras se encuentra en roaming. o Lista Blanca Dinámica con Informes en tiempo real sobre la reputación de los archivos
Seguridad Móvil	o Antimalware con detección combinada basada en firmas, con posibilidad de asistencia en la nube con protección en tiempo real. o Posibilidad de Soporte para dispositivos de los funcionarios, con inscripción transparente para los usuarios. o Monitoreo de aplicaciones instaladas en los dispositivos móviles en base a políticas pre-definidas. o Pre-configuración y despliegue de aplicaciones de manera centralizada a través de SMS, Correo Electrónico y PC o Supervisión de SIM, Bloqueo remoto, borrado y búsqueda evitando acceso no autorizado a datos corporativos en casos de pérdida o robo del dispositivo móvil
Protección de datos y encriptación	o Encriptación invisible y transparente para los usuarios. o Posibilidad de selección de nivel de disco completo o archivo, con el respaldo del Estándar de Encriptación Avanzado con encriptación de 256 bits o Creación de paquetes encriptados y de auto-extracción o Aplicación de políticas de encriptación de datos en los dispositivos removibles.

Seguridad de Correo y Web	o **Licencia para 200 buzones de correo** o Protección antimalware y Anti-Spam para servidores. o Tecnologías de reconocimiento de spam inteligentes La aplicación debe escanear todos los mensajes en busca de spam basándose en los atributos formales, como correo electrónico y dirección IP del remitente, tamaño del mensaje, encabezado del mensaje, entre otros. Debe analizar el contenido del mensaje y los adjuntos utilizando tecnologías inteligentes que incluyen firmas gráficas que detecten spam en formato de imágenes. o Posibilidad para el acceso a la base de datos basada en la nube de y obtención de información en tiempo real sobre spam nuevo. o Filtrado por reputación Servicio de escaneo Antis-pam adicional para aumentar la precisión de la detección de spam y reducir la probabilidad de falsos positivo Anti-spam. o Escaneo de mensajes adicional: Escaneo utilizando lista de direcciones de spammer y tecnología que detecten las direcciones URL de los spammers en los mensajes. o Clasificación de mensajes. Configurar de reglas de procesamiento de los correos no solicitados para prevenir la pérdida de información.

	o Listas blancas y negras: Posibilidad para Usuarios de creación de listas propias de confianza (blancas) y listas negras según la dirección SMTP o IP del remitente. o Protección contra malware: Escaneo en tiempo real Detección y eliminación de todo tipo de virus, gusanos, troyanos y otros objetos maliciosos del flujo de mensajes entrantes y salientes, incluyendo los formatos de archivos adjuntos. o Detección y eliminación de programas potencialmente peligrosos. o Escaneo en segundo plano a pedido y programado o Los mensajes y carpetas almacenados en el servidor podrán estar sujetos a escaneo en segundo plano o de fondo con impacto mínimo en la carga del servidor. o Copia de respaldo: Antes de eliminar los mensajes la aplicación debe realizar copias de respaldo, para restaurar información importante o Administración flexible. o Configuración personalizada: Configuración de aplicaciones según políticas de seguridad de TI y las capacidades del hardware de la Institución. o Opción de administración remota. o Informes detallados: Informes HTML detallados que deben estar también en el registro de eventos de Windows. Con control sobre la frecuencia de los informes y la información que se incluirá en ellos. Todos los informes se deben poder guardar en el disco duro o enviarse por correo electrónico. o Sistema de notificación: Notificaciones al administrador sobre eventos cruciales en la operación de la aplicación a través del correo electrónico o del registro de eventos de Windows. o Acceso seguro a Internet en toda la organización al retirar Automáticamente los programas maliciosos y potencialmente hostiles en tráfico HTTP(S) / FTP / SMTP y POP3.
Administración de Parches	o Inventario de Hardware, Software y Licencias o Escaneo avanzado de vulnerabilidades, con distribución automatizada de parches. o Creación, almacenamiento y despliegue de imágenes del sistema desde una ubicación central. o Control de Admisión a la Red con Creación de políticas de red para "invitados". o Despliegue centralizado de software a las máquinas de la Institución,

Mejora de la seguridad y ampliación de la gestión de sistemas.	- Eliminación de vulnerabilidades conocidas - Administración de los activos de software y hardware - Optimización de la distribución de aplicaciones - Automatización y optimización de la implementación del sistema operativo - Reducción del tráfico: distribución remota. - Integración con Active Directory: La aplicación debe posibilitar la autenticación de usuarios de Active Directory.
El software ofertado deberá tener representación local	- Requerido.
Carta de Autorización de venta para el país.	- Requerido, del fabricante o representante para comercializar el producto en el país. La certificación debe estar dirigida a la Institución y guardar relación a este llamado.
Requisitos indispensables para la empresa Oferente	- Atendiendo que se deberá trabajar en la integración de servidores de Windows Server y System Center se solicita contar mínimamente con las siguientes certificaciones: Microsoft® Certified Technology Specialist en Administering and Deploying System Center 2012 Configuration Manager o equivalente y en Administración de Directorio Activo.
Palazo de Entrega	• A los 30 días a partir de la recepción de la orden de compra por parte del contratista. El contratista deberá instalar la solución en todos los Equipos a ser disponibilizados por el Ministerio, se deberá realizar un primer escaneo una vez instalado la cual en caso de estar infectado se deberá dar una Solución al problema existente. Además el equipo instalado deberá estar registrado en la consola de administración centralizada y contar con la actualización de las bases de datos de virus activas.

Sin otras modificaciones que realizar, me despido de uds. respetuosamente.

MINISTERIO DEL INTERIOR
Dirección General de Administración y Finanzas

Lic. Javier Sasiain Cano, Director General
Dirección General de
Administración y Finanzas

garl