JUNTA MUNICIPAL DE ASUNCION
DIRECCION OPERATIVA DE CONTRATACIONES

ADENDA Nº 1.

LCO N° 01/18 PAC Nº 343.857/18 "ADQUISICIÓN DE EQUIPOS INFORMATICOS Y ACCESORIOS PARA LA JUNTA MUNICIPAL DE ASUNCIÓN, DEFENSORIA MUNICIPAL Y JUZGADO DE FALTAS"

Estimados

Por la presente, la Dirección Operativa de Contrataciones de la Junta Municipal de Asunción cumple en informarles las modificaciones sufridas en el Pliego de Bases y Condiciones del llamado por Licitación por Concurso de Ofertas **PAC N° 343.857/18,** en conformidad a la ley 2051/03 de Contrataciones Públicas, por la que se procede a la Adenda del citado llamado.

Se incluye la siguiente modificación:

Por la presente, la Dirección Operativa de Contrataciones de la Junta Municipal de Asunción cumple en informarles las modificaciones de fechas de Consulta, Entrega y Apertura de Sobres realizadas en el Portal de la Dirección Nacional de Contrataciones Públicas: www.contrataciones.gov.py.

SECCIÓN II. CRITERIOS DE EVALUACIÓN Y REQUISITOS DE CALIFICACIÓN

(B) Experiencia y Capacidad Técnica

El Oferente deberá proporcionar evidencia documentada que demuestre su cumplimiento con los siguientes requisitos de experiencia: *enumerar los requisitos de experiencia*

1. Copias de Contratos y/o de Adquisición de Equipos Informáticos, ejecutados de los últimos 3 años como mínimo (2015, 2016, 2017) y que su volumen de negocio en porcentaje sea igual o mayor al 30 % de la oferta por Cada Lote cotizado.

SECCIÓN III. SUMINISTROS REQUERIDOS

1. Especificaciones Técnicas

No. De Artículo	*Nombre de los Bienes o Servicios*	*Especificaciones Técnicas y Normas*
		LOTE N°1
1	**COMPUTADORA DE ESCRITORIO**	*TIPO 3 Ver Plantilla del SIPC (RESOLUCIÓN 198/16 SENATIC)*
		LOTE N° 2
1	**NOTEBOOK**	*TIPO 1 Ver Plantilla del SIPC (RESOLUCIÓN 198/16 SENATIC)*
		LOTE N° 5
1	**SOFTWARE OFIMÁTICA**	• Licencia Suite Ofimática versión Estándar versión 2016, Office Microsoft • La suite ofimática ofertada deberá constar de un procesador de textos y palabras

Juan Ángel B
Director D.U.O.C
Junta Municipal de A
U.O.C. Nº 2

		• La suite ofimática ofertada deberá debe constar de una hoja de cálculo para formulas, macros y procedimientos matemáticos y numéricos de alto rendimiento • La suite ofimática ofertada deberá debe constar de un procesador y organizador de diapositivas • La suite ofimática ofertada deberá ser la última versión existente en el mercado Además, la suite puede contener un sistema de gestión de bases de datos, herramientas menores de gráficos y comunicaciones, un gestor de información personal (agenda y cliente de correo Electrónico) y un navegador web.
2	**LICENCIA KASPERKY**	• La Solución deberá estar certificada por ICSA Labs "Antivirus Cleaning". ICSA Labs "Desktop/Server Anti-Virus Detection". ICSA Labs "Anti-Spyware Certification".Checkmark AV Level 1. Checkmark AV Level 2. checkmark Anti-Spyware Desktop Certification. Checkmark Anti-Malware Certification Virus Bulletin AV-Comparatives OPSWAT "OESISOK" Av-Test WMWARE Ready CytrixReady TUV • Toda la Solución ofrecida deberá correr sobre un único servidor central y todos los módulos ofrecidos deberán ser del mismo fabricante. • La totalidad de los componentes de la Solución deben requerir de un único agente que se debe instalar en las estaciones de trabajo, la cual deberá realizarse vía protocolo http y https, de forma remota, desatendida y centralizada. • Para las estaciones clientes el agente deberá garantizar que se puede instalar en máquinas con de procesador (Intel Celeron D, 2266 Mhz, Intel Celeron D, 2.53 MHz, Mobile Intel Pentium M 735 (1.7GHz)), 256 megas de RAM o superior, Linux, Windows XP o superior, Macintosh. el Windows Mobile (Smartphones y PocketPC) y Symbiam. • El cliente deberá ser instalado en y el Windows Mobile (Smartphones y PocketPC) y Symbiam. trescientos (300) equipos, debiendo permitir un crecimiento del 20% (veinte), sin necesidad de upgrade de hardware alguno. • Para la protección sobre Servidores deben de ser soportadoras por los sistemas operativos de Microsoft Windows en sus versiones 2000, 2003, 2008, Core 2008; como asi también para el sistema operativo Linux en sus versiones Red Hat/ Mandriva/ SUSE/ Fedora, Debían/ Ubuntu, NetBSD 4.X, BSD 6.X, FreeBSD 7.X, FreeBSD 8.X/ 9X y Sun Solaris, contemplar 5 (cinco) unidades para servidores. • La Solución deberá integrar las distintas herramientas que la conforman de manera nativa. • Deberá permitir cifrar la información a ser remitida desde un dispositivo hacia la consola de la Solución. • Deberá permitir crear repositorios remotos para la distribución del software de antivirus y actualizaciones en sitios remotos. • Soporte para almacenamiento de clientes lo gue a dos en Bases de Datos Oracle, MS Sql Server o base local. • Actualización de la base de firmas de virus al menos una vez por día. • Control de medios extraíbles de almacenamiento. • Soporte para CISCO Network Admission Control. • Soporte para computadoras portátiles. Capacidad de posponer tareas cuando se ejecute con la batería. • El producto ofertado deberá detectar virus en archivos compactados, sin importar el número de niveles de compresión, en los siguientes formatos: .zip, .rar, .arj, .cab, .lzh, .tar, .gz, ace, izh, upx y otros. • El producto ofertado deberá tener un motor heurístico proactivo y preciso de tecnología avanzada.

Lic. Juan Angel Ber
Director DHUOC.
Junta Municipal de Asu
U.O.C. Nº 2

		• El producto ofertado deberá soportar el escaneo y limpieza de paquetes en tráfico HTTP y FTP; tanto en los servidores como en las computadoras personales. • El producto ofertado deberá importar o exportar configuraciones de clientes por medio de archivos XML. • El producto ofertado deberá tener la capacidad de poder enviar a los centros de soporte técnico las muestras de virus o códigos maliciosos, con la finalidad de que puedan ser analizados, y clasificados para su contingencia inmediata. • Características técnicas y funcionalidades respecto a la Consola de Administración. Si la solución cuenta con una consola de administración basada en Windows, la misma • Las herramientas de diagnóstico deben estar incluidas en la consola de administración remota, permitiendo la exploración profunda de los procesos del sistema para encontrar amenazas ocultas. • Debe poder crear unidades de arranque de rescate en CD, DVD o USB para reparar unidades o computadoras infectadas. • Debe poder realizarse la ejecución remota de scripts y paquetes MSI con derechos de administrador a través de la consola de administración. • Reportes vía email y/o SNMP. • Debe poseer herramientas de línea de comando (CLI) para la exploración y limpieza de virus. • Se deberá poder acceder a la consola de administración desde equipos (clientes) con las siguientes características mínimas: Equipos Pentium IV 2.8 Ghz con 1GB de RAM. • Deberá permitir la utilización de una única consola para todas las funcionalidades de administración de la solución. • Deberá ser capaz de asignar permisos de uso a cada usuario de la consola de administración con la capacidad de limitar las funcionalidades de los equipos administrados. • Debe permitir generar log´s de auditoría, de las transacciones que realicen los usuarios que manejan la Solución. • Deberá restringir parcial y totalmente el acceso de los usuarios finales a la configuración local de los productos de protección instalados, limitando a los mismos para que no puedan desinstalar, remover o quitar de memoria la protección antivirus de la solución. • La consola de gestión debe mostrar en tiempo real la lista de servidores y estaciones que tienen el antivirus instalado, conteniendo la siguiente información mínima: nombre de la máquina, Versión de antivirus, versión del motor, fecha de la vacuna, la última fecha de verificación y el estado. • La consola de gestión debe permitir establecer los permisos de manera que sólo el administrador pueda cambiar la configuración, desinstalar o detener el antivirus de las estaciones. • Deberá administrar de manera centralizada y realizar tareas de instalación, actualización y configuración remota de los dispositivos protegidos por la solución. • Posibilidad de rollback de la última versión anterior de vacunas, desde la consola de administración. • Deberá contar con una base de datos en la cual se deberá guardar todos los informes sobre la detección de virus, adware y spyware. • Deberá traer una herramienta para el mantenimiento de la base de datos. • Se deberá visualizar globalmente, de manera resumida y en tiempo real, el estado del equipamiento informático protegido por la solución. • Deberá detectar cualquier equipo nuevo que se conecte a la red, debiendo verificar si la maquina tiene agente o antivirus y permitir tomar una acción, como mínimo, la instalación del agente y su actualización.

Lic. Juan Angel Benin
Director D.U.O.C.
Junta Municipal de Asunci

		• Deberá incluir una herramienta que verifique que parches de microsoft de seguridad tiene o le hacen falta. • Deberá conectarse al sitio de actualizaciones de forma automática cada hora para verificar nuevas actualizaciones de listas de antivirus, malware, anti-spyware y templates de Microsoft. • Deberá obtener las actualizaciones de mejoras y nuevas versiones desde el sitio de Internet del fabricante. • Deberá configurar el modelo de obtención de actualizaciones por Push o Pull o ambas. • Distribuir las actualizaciones de manera incremental, automática y desatendida. • Distribuir actualizaciones sin tener que realizar nuevas validaciones, ni depender de la agrupación de los equipos informáticos en dominios. • Permitir configurar clientes para que se actualicen de diferentes fuentes o equipos según su ubicación y distribución en la estructura de la red. Si la opción fuera por protocolo ftp, deberá incluir la modalidad de descarga "ftp pasivo". • No requerir el reinicio de la estación de trabajo protegidas luego de la actualización de listas de virus y motores de búsqueda. • Deberá mostrar el status de cuando se está bajando las actualizaciones y el porcentaje de Actualizaciones. • Deberá integrarse con una estructura de directorio LDAP, agregando las máquinas de forma automática. • El agente deberá ser flexible en la instalación por medio de login script, ejecutable, via remota • Administrar la configuración de los distintos componentes de la solución permitiendo: • Configurar los distintos programas de la solución en tiempo real. • Aplicar políticas de acciones y procedimientos a seguir ante la detección de virus. • Iniciar rastreos parciales o totales en los nodos protegidos de la red de AFIP. • Planificar rastreos automáticos especificando nodos protegidos de la red de AFIP y día y hora de inicio. • Deberá permitir la configuración de las acciones a tomar ante la detección de un virus y/o malware. • Deberá permitir agrupar los dispositivos protegidos de la red de AFIP en grupos, como mínimo por rango de dirección IP y nombre del equipo, con el objeto de: • Iniciar rastreos. • Planificar rastreos automáticos. • Implementar configuraciones particulares. • Aplicar políticas de acciones y procedimientos a seguir ante la detección de virus. • Efectuar tareas de monitoreo de los nodos protegidos. • Capacidad de aplicar diferentes reglas, a los grupos definidos • Deberá contar con una herramienta para la verificación de la conectividad entre la funcionalidad de administración de la solución y los nodos protegidos de la red de AFIP. • Contar con la funcionalidad de administración de instalación remota de la protección de los nodos de la red de AFIP de la solución que provea lo siguiente: • Selección de los de los nodos de la red de AFIP a instalar. • Selección del producto de software de la solución a instalar y versión. • Comunicación con el nodo a instalar mediante protocolo de red TCP/IP. • Permitir que el reinicio de la estación de trabajo sea opcional.

Lic. Juan Ángel E
Director D.U.O.C
Junta Municipal de As

2. Plan de Entrega (Bienes)

Ítem	Descripción del Bien	Cantidad	Unidad de medida	Lugar de entrega de los Bienes	Plazo de Entrega	Fecha(s) final(es) de entrega de los Bienes
LOTE N° 1						
1	**COMPUTADORA DE ESCRITORIO**	20	UNIDAD	DIRECCION DE ORGANIZACION Y SISTEMA DE LA JMA	20 DIAS, COMPUTADOS A PARTIR DE LA RECEPCIÓN DE LA ORDEN DE COMPRA POR PARTE DEL PROVEEDOR	31/12/2018
LOTE N° 2						
1	**NOTEBOOK**	5	UNIDAD	DIRECCION DE ORGANIZACION Y SISTEMA DE LA JMA	.20 DIAS, COMPUTADOS A PARTIR DE LA RECEPCIÓN DE LA ORDEN DE COMPRA POR PARTE DEL PROVEEDOR	31/12/2018
LOTE N° 3						
1	**SERVIDOR NAS CON 2 DISCOS DE 8 TB**	2	UNIDAD	DIRECCION DE ORGANIZACION Y SISTEMA DE LA JMA	20 DIAS, COMPUTADOS A PARTIR DE LA RECEPCIÓN DE LA ORDEN DE COMPRA POR PARTE DEL PROVEEDOR	31/12/2018
2	**UPS de Servidor**	2	UNIDAD	DIRECCION DE ORGANIZACION Y SISTEMA DE LA JMA	20 DIAS, COMPUTADOS A PARTIR DE LA RECEPCIÓN DE LA ORDEN DE COMPRA POR PARTE DEL PROVEEDOR	31/12/2018
LOTE N°4						
1	**IMPRESORA LASER**	40	UNIDAD	DIRECCION DE ORGANIZACION Y SISTEMA DE LA JMA	20 DIAS, COMPUTADOS A PARTIR DE LA RECEPCIÓN DE LA ORDEN DE COMPRA POR PARTE DEL PROVEEDOR	31/12/2018
2	**UPS**	50	UNIDAD	DIRECCION DE ORGANIZACION Y SISTEMA DE LA JMA	20 DIAS, COMPUTADOS A PARTIR DE LA RECEPCIÓN DE LA ORDEN DE COMPRA POR PARTE DEL PROVEEDOR	31/12/2018
3	**MOUSE**	50	UNIDAD	DIRECCION DE ORGANIZACION Y SISTEMA DE LA JMA	20 DIAS, COMPUTADOS A PARTIR DE LA RECEPCIÓN DE LA ORDEN DE	31/12/2018

JUNTA MUNICIPAL U.O.C. Nº 2

Lic. Juan Ángel
Director D.U
Junta Municipal d

					COMPRA POR PARTE DEL PROVEEDOR	
4	**TECLADO**	50	UNIDAD	DIRECCION DE ORGANIZACION Y SISTEMA DE LA JMA	20 DIAS, COMPUTADOS A PARTIR DE LA RECEPCIÓN DE LA ORDEN DE COMPRA POR PARTE DEL PROVEEDOR	31/12/2018
5	**TECLADO DE PIE**	5	UNIDAD	DIRECCION DE ORGANIZACION Y SISTEMA DE LA JMA	20 DIAS, COMPUTADOS A PARTIR DE LA RECEPCIÓN DE LA ORDEN DE COMPRA POR PARTE DEL PROVEEDOR	31/12/2018
6	**RACK**	5	UNIDAD	DIRECCION DE ORGANIZACION Y SISTEMA DE LA JMA	20 DIAS, COMPUTADOS A PARTIR DE LA RECEPCIÓN DE LA ORDEN DE COMPRA POR PARTE DEL PROVEEDOR	31/12/2018
7	**DISCO**	10	UNIDAD	DIRECCION DE ORGANIZACION Y SISTEMA DE LA JMA	20 DIAS, COMPUTADOS A PARTIR DE LA RECEPCIÓN DE LA ORDEN DE COMPRA POR PARTE DEL PROVEEDOR	31/12/2018
8	**FUENTES 12 V 30 CCTV**	4	UNIDAD	DIRECCION DE ORGANIZACION Y SISTEMA DE LA JMA	20 DIAS, COMPUTADOS A PARTIR DE LA RECEPCIÓN DE LA ORDEN DE COMPRA POR PARTE DEL PROVEEDOR	31/12/2018
9	**FUENTE TIPO ATX**	30	UNIDAD	DIRECCION DE ORGANIZACION Y SISTEMA DE LA JMA	20 DIAS, COMPUTADOS A PARTIR DE LA RECEPCIÓN DE LA ORDEN DE COMPRA POR PARTE DEL PROVEEDOR	31/12/2018
10	**BOBINAS**	05	UNIDAD	DIRECCION DE ORGANIZACION Y SISTEMA DE LA JMA	20 DIAS, COMPUTADOS A PARTIR DE LA RECEPCIÓN DE LA ORDEN DE COMPRA POR PARTE DEL PROVEEDOR	31/12/2018
11	**PACH CORD**	100	UNIDAD	DIRECCION DE ORGANIZACION Y SISTEMA DE LA JMA	20 DIAS, COMPUTADOS A PARTIR DE LA RECEPCIÓN DE LA ORDEN DE COMPRA POR PARTE DEL PROVEEDOR	31/12/2018
LOTE N°5						

U.O.C. N° 2

Lic. Juan Ángel Beni
Director de U.O.C.
Junta Municipal de Asunc

JUNTA MUNICIPAL DE ASUNCION
DIRECCION OPERATIVA DE CONTRATACIONES

1	**SOFTWARE OFIMÁTICA**	25	UNIDAD	DIRECCION DE ORGANIZACION Y SISTEMA DE LA JMA	20 DIAS, COMPUTADOS A PARTIR DE LA RECEPCIÓN DE LA ORDEN DE COMPRA POR PARTE DEL PROVEEDOR	31/12/2018
2	**LICENCIA KASPERKY**	25	UNIDAD	DIRECCION DE ORGANIZACION Y SISTEMA DE LA JMA	20 DIAS, COMPUTADOS A PARTIR DE LA RECEPCIÓN DE LA ORDEN DE COMPRA POR PARTE DEL PROVEEDOR	31/12/2018

JUNTA MUNICIPAL U.O.C. Nº 2

Lic. Juan Ángel Bernni
Director D.U.O.C.
Junta Municipal de Asunción