Sede Central: Av. Fernando de la Mora esq. Tte. Alcorta Asunción
Teléfonos (59521) 569000 Casilla de Correo 384
Planta Industrial de Villeta: (595) 2595512
Planta Industrial de Vallemi: (595) 0351230303/14/48

PARAGUAY TODOS Y TODAS

¡Construyendo futuro con cemento Paraguayo!

Licitación Pública Nacional SBE Nº 27/16 "Suministro de Infraestructura de Cómputo y Comunicaciones para Centro de Datos" ID Nº 312.543

ADENDA Nº 2

Por la presente comunicamos a todos los oferentes, las modificaciones introducidas en el Pliego de Bases y Condiciones y las nuevas fechas del presente llamado:

1) **EN LA SECCIÓN III – REQUISITOS DE LOS BIENES Y/O SERVICIOS REQUERIDOS**

LOS PUNTOS N° 1 Y 12 QUEDAN REDACTADOS DE LA SIGUIENTE MANERA:

1. SERVIDORES HYPERVISORES PARA EL CENTRO DE DATOS			PROPUESTA DEL OFERENTE	
Especificaciones Técnicas	Características	Mínimo Exigido	El equipo ofertado cumple las especificaciones requeridas SI/NO	Observaciones. Oferta adicional a especificaciones técnicas
Tipo de equipo	Servidor	Exigido		
Cantidad	3 (tres) unidades	Exigido		
Marca	Indicar exactamente, de manera a comprobar en el catálogo on-line del fabricante	Exigido		
Modelo	Indicar exactamente, de manera a comprobar en el catálogo on-line del fabricante	Exigido		
Numero de parte del fabricante del equipo	Indicar exactamente, de manera a comprobar en el catálogo on-line del fabricante	Exigido		
Origen /Procedencia	Indicar	Exigido		
Gabinete	Rackeable de 2U o superior	Exigido		
Procesador	Cada servidor debe poseer al menos 2 (dos) Procesadores de al menos 10 núcleos y 20 Sub-procesos, 2.2 GHz de Velocidad de reloj y Cache inteligente de 25 MB o superior. El procesador debe ser de la última generación ofrecida por el fabricante.	Exigido		
Memorias RAM	144GB de memoria RAM instalados en 9 módulos de 16GB. El equipo debe poder crecer al menos hasta 3 TB contando con 24 ranuras DIMM como mínimo. Las memorias deberán contar con al menos protección del tipo: Advanced ECC.	Exigido		
Discos Duros	2 unidades de Discos Duros instalados de al menos 600GB 10k SAS.	Exigido		
	Los discos deberán contar con dos indicadores LED, uno para advertir cualquier mal funcionamiento, y otro que indique cual	Opcional		

Abog. Cesar E. Diesel Marin
Gerente U.O.C.
I.N.C.

Ing. Roberto Viveros
Jefe Dpto. T.I.C.
I.N.C.

	es el disco que no debe ser removido en caso de fallas.			
Capacidad de crecimiento	El equipo debe de poder crecer en forma interna en el caso que la institución lo requiera a como mínimo 24 discos duros de forma interna.	Exigido		
Controladora de discos	Controladora con al menos 2GB de Flash BackupWrite Cache, capaz de ralizar RAID 0/1/1+0/5/5+0/6/6+0	Exigido		
Slots de expansión	3 slot PCI-Express 3.0, con capacidad de crecer hasta 6 Slots PCI-Express.	Exigido		
Dispositivo óptico	SATA DVD RW interno.	Opcional		
Gráficos	De al menos 16MB de RAM de video.	Exigido		
Placa de Red	Seis puertos de 1Gb soporte de VMwareNetQueue y Microsoft VMQ.	Exigido		
Puertos	Video: 2 (1 frontal, 1 posterior), Network RJ-45: 4, Administración: 1Gb dedicado, USB 2.0: minimo 2, USB 3.0: mínimo 2, 1 slot interno para tarjetas Micro SD.	Exigido		
Tarjeta HBA FC	Al menos una Tarjeta HBA con dos puertos FC de al menos 8Gb cada uno.	Exigido		
Fuente de Alimentación	2 (dos) Fuentes de poder reemplazables en caliente de mínimo 500Watts con 94% de eficiencia para Redundancia 1+1.	Exigido		
Ventiladores	El equipo debe contar con 6 (seis) ventiladores redundantes de fábrica.	Exigido		
Software para Virtualización	*VMwarevSphere Essentials Plus Kit 6 Processor con 3 años de soporte 24x7 OEM (que no quede atado al HW sino que pueda ser movido en caso de ser necesario), a nombre de la Industria Nacional del Cemento.	Exigido		
Sistema Operativos	* 7 (siete) Licencias de Microsoft Windows 2012 R2 Server STD OLP GOV + 200 CAL de dispositivo a nombre de la Industria Nacional del Cemento	Exigido		
Administración	La herramienta de administración debe ser vía hardware (no se aceptará vía software o sistema operativo). Al menos 2GB de capacidad. Conjunto completo de funcionalidades, los cuales puedan ser utilizados en su instalación, administración y manejo, alerta y soporte remoto. Se deberá poder contar con la habilidad de acceso, despliegue y manejo del servidor en cualquier momento y desde cualquier lugar utilizando una PC, teléfono inteligente o Tablet. El equipo deberá poder ser administrado y monitoreado con solo conectar el cable power y el cable de red al servidor. El equipo deberá contar con la habilidad de configurarse sin necesidad de alguna media como CD-ROM, DVD-ROM, USB, etc. El equipo debe contar con un puerto integrado dedicado para administración, a parte de los puertos de red solicitados anteriormente.	Exigido		
Accesorios	Todos los accesorios requeridos para entregar el producto en perfecto estado de operación (software, utilitarios, cables y otros elementos)	Exigido		
Certificaciones	* De compatibilidad con Microsoft Windows Server, Canonical Ubuntu, VMware, Citrix XenServer, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES).	Exigido		

Ing. Roberto Viveros
Jefe Dpto. T.I.C.
I.N.C.

Abog. César E. Diesel Marin
Gerente U.O.C.
I.N.C.

Servicio Técnico	La marca ofertada deberá poseer al menos un (1) Centro Autorizados de Servicios (CAS) para dar inmediata respuesta ante eventuales fallas de los equipos. Se deberá nombrar la empresa, dirección, número de teléfono de contacto.	Exigido		
Nivel de servicio y tiempo de respuesta ante los reclamos realizados	Como mínimo debe cumplir con los siguientes requisitos: * Atención a las alertas y a los reclamos de la contraparte designada con un tiempo de respuesta no mayor a 2 horas después de recibida la comunicación del inconveniente. En caso de falla total del equipamiento se deberá proveer la respuesta respectiva y el servicio de reinstalación y de buen funcionamiento en 24 hs durante el periodo de garantía. * Disponibilidad del servicio debe ser de 7x24 durante el periodo de extensión del contrato.	Exigido		
Garantía Escrita	Garantía mínima de 3 (tres) años en piezas y mano de obra en sitio del tipo 24x7 con atención dentro de las 4 horas de solicitar el servicio, el mismo debe ser del tipo predictivo o proactivo, el equipo debe ser monitoreado por ingenieros de la marca ofertada y prever cualquier falla posible. El servicio ofertado debe ser del fabricante, es indespensable colocar el Número de Parte del Servicio ofrecido. * Cobertura de la garantía: Provisión de partes y mano de obra certificada, sin costo durante el período de la garantía. * Con el fin de preservar los bienes de la institución se exige que la mano de obra en cualquier asistencia y/o soporte por garantía que sea requerido, la misma debe ser dada por técnicos debidamente calificados, entrenados y certificados por el fabricante de la marca ofertada.	Exigido		
Rack / Bastidor	Un (1) rack de 42"(pulgadas) , puerta frontal y trasera micro perforado, cerradura con llave, profundidad de 1100 mm, 1 bandeja con 4 mini ventiladores, 2 bandejas fijas de 1U, kit de ruedas, 4 canales de tensión de 8 tomas universales c/u, 1 ordenador de cable vertical, panel de metal, 1 ordenador de cable cerrado, metal de 2U.Patchcord necesarios para conectar todos los equipos solicitados en este llamado, como asitambien todos los accesorios necesarios que se necesiten para la correcta implementacion.	Exigido		

12. SOFTWARE ANTIVIRUS PARA SERVIDORES Y ESTACIONES DE TRABAJO			**PROPUESTA DEL OFERENTE**	
ESPECIFICACIONES TÉCNICAS	**Características**	**Mínimo Exigido**	**El equipo ofertado cumple las especificaciones requeridas SI/NO**	**Observaciones. Oferta adicional a especificaciones técnicas**
Marca /Fabricante	Indicar exactamente de manera a comprobar en el catalogo on-line del fabricante	Exigido		
Modelo / Producto	Indicar exactamente de manera a comprobar en el catalogo on-line del fabricante	Exigido		
Origen /	Indicar	Exigido		

Ing. Roberto Viveros
Jefe Dpto. T.I.C.
I.N.C.

Abog. César E. Diesel Marín
Gerente A.I.O.C.
I.N.C.

Procedencia				
Cantidad	200 (doscientas) Unidades por 3 (tres) años de cobertura de soporte técnico y actualizaciones.	Exigido		
Tipo	Software Antimalware con protección para Endpoints y Servidores con consola de Administración Centralizada	Exigido		
Protecciones y funcionalidades	• Antivirus de archivos residente (antispyware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado; • Antivirus de web (módulo para verificación de sitios y downloads contra virus) • Antivirus de correo electrónico (módulo para verificación de correos recibidos y enviados, así como sus adjuntos) • Antivirus de mensajes instantáneos (módulo para verificación de mensajes instantáneos, como ICQ, MSN, IRC, etc.) • Firewall con IDS • Autoprotección (contra ataques a los servicios/procesos del antivirus) • Control de dispositivos externos • Control de acceso a sitios por categoría • Control de ejecución de aplicativos • Control de vulnerabilidades de Windows y de los aplicativos instalados • Capacidad de detección de presencia de antivirus de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación • Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antivirus, (ej.: "Win32.Trojan.banker") • Capacidad de verificar correos electrónicos recibidos y enviados en los protocolos POP3, IMAP, NNTP, SMTP y MAPI, así como conexiones cifradas (SSL) para POP3 y IMAP (SSL); • Capacidad de filtrar adjuntos de correos electrónicos, borrándolos o renombrándolos de acuerdo con la configuración hecha por el administrador. • Capacidad de verificación de tráfico HTTP y cualquier script de Windows Script Host (JavaScript, Visual Basic Script, etc.), usando heurísticas; • Debe tener soporte total al protocolo IPv6; • Debe tener módulo de bloqueo de Phishing, con actualizaciones incluidas en las vacunas, obtenidas por Anti-PhishingWorkingGroup (http://www.antiphishing.org/). • Capacidad de distinguir diferentes subnets y brindar opción de activar o no el firewall para una subnet específica;	Exigido		

Ing. Roberto Viveros
Jefe Dpto. T.I.C.
I.N.C.

Abog. César E. Diesel Marín
Gerente U.O.C.
I.N.C.

	• Debe tener módulo IDS (IntrusionDetectionSystem) para protección contra portscans y explotación de vulnerabilidades de software. La base de datos de análisis debe actualizarse conjuntamente con las vacunas. • El módulo de Firewall debe contener, como mínimo, dos conjuntos de reglas: • Filtrado de paquetes: donde el administrador podrá elegir puertas, protocolos o direcciones de conexión que serán bloqueadas/permitidas; • Filtrado por aplicativo: donde el administrador podrá elegir cuál aplicativo, grupo de aplicativo, fabricante de aplicativo, versión de aplicativo o nombre de aplicativo tendrá acceso a la red, con la posibilidad de elegir qué puertas y protocolos podrán ser utilizados. • Debe tener módulo que habilite o no el funcionamiento de los siguientes dispositivos externos, como mínimo: • Discos de almacenamiento locales • Almacenamiento extraíble • Impresoras • CD/DVD • Drives de disquete • Modems • Dispositivos de cinta • Dispositivos multifuncionales • Lectores de smartcard • Dispositivos de sincronización vía ActiveSync (Windows CE, Windows Mobile, etc.) • Wi-Fi • Adaptadores de red externos • Dispositivos MP3 o smartphones • Dispositivos Bluetooth			
Compatibilidad de los diferentes componentes	• Microsoft Windows Server 2003 o superior • Microsoft Windows Server 2003 x64 o superior • Microsoft Windows Server 2008 • Microsoft Windows Server 2008 Core • Microsoft Windows Server 2008 x64 SP1 • Microsoft Windows Server 2008 R2 • Microsoft Windows Server 2008 R2 Core • Microsoft Windows Server 2012 • Microsoft Windows XP Professional SP2 o superior • Microsoft Windows XP Professional x64 • Microsoft Windows Vista SP1 • Microsoft Windows Vista x64 SP1 • Microsoft Windows 7 • Microsoft Windows 7 x64 • Microsoft Windows 8 • Microsoft Windows 8 x64 Principales distribuciones de Linux en 32 y 64 bits, entre ellas:	Exigido		

Ing. Roberto Viveros
Jefe Dpto. T.I.C.
I.N.C.

Abog. César E. Diesel Marín
Gerente U.O.C.
I.N.C.

	• Canaima 3 • Red Flag Desktop 6.0 SP2 • Red Hat Enterprise Linux 5.8 Desktop • Red Hat Enterprise Linux 6.2 Desktop • Fedora 16 • CentOS-6.2 • SUSE Linux Enterprise Desktop 10 SP4 • SUSE Linux Enterprise Desktop 11 SP2 • openSUSE Linux 12.1 • openSUSE Linux 12.2 • Debian GNU/Linux 6.0.5 • Mandriva Linux 2011 • Ubuntu 10.04 LTS • Ubuntu 12.04 LTS			
Administración y gerenciamiento	1. Se debe acceder a la consola vía WEB (HTTPS) o MMC; 2. Compatibilidad con Windows FailoverClustering u otra solución de alta disponibilidad 3. Capacidad de eliminar remotamente cualquier solución de antivirus (propia o de terceros) que esté presente en las estaciones y servidores, sin la necesidad de la contraseña de remoción del actual antivirus; 4. Capacidad de instalar remotamente la solución de antivirus en las estaciones y servidores Windows, a través de la administración compartida, login script y/o GPO de Active Directory; 5. Capacidad de instalar remotamente la solución de seguridad en smartphones y tabletsSymbian, Windows Mobile, BlackBerry y Android, utilizando estaciones como intermediadoras; 6. Capacidad de gestionar smartphones y tablets (tanto Symbian como Windows Mobile, BlackBerry, Android y iOS) protegidos por la solución antivirus; 7. Capacidad de generar paquetes personalizados (autoejecutables) conteniendo la licencia y configuraciones del producto; 8. Capacidad de actualizar los paquetes de instalación con las últimas vacunas, para que cuando el paquete sea utilizado en una instalación ya contenga las últimas vacunas lanzadas; 9. Capacidad de hacer distribución remota de cualquier software, o sea, debe ser capaz de enviar remotamente cualquier software por la			

Ing. Roberto Viveros
Jefe Dpto. T.I.C.
I.N.C.

Abog. César E. Diesel Marin
Gerente U.O.C.
I.N.C.

	estructura de gerenciamiento de antivirus para que sea instalado en las máquinas clientes; 10. Capacidad de desinstalar remotamente cualquier software instalado en las máquinas clientes; 11. Capacidad de aplicar actualizaciones de Windows remotamente en las estaciones y servidores; 12. Capacidad de importar la estructura de Active Directory para encontrar máquinas; 13. Capacidad de que cuando se detecten máquinas nuevas en el Active Directory, subnets o grupos de trabajo, automáticamente se importe la máquina para la estructura de protección de la consola y se verifique si tiene el antivirus instalado. En caso de no tenerlo, debe instalar el antivirus automáticamente; 14. Capacidad de agrupamiento de máquinas por características comunes entre ellas, por ejemplo: agrupar todas las máquinas que no tengan el antivirus instalado, agrupar todas las máquinas que no recibieron actualización en los últimos 2 días, etc.; 15. Capacidad de definir políticas de configuraciones diferentes por grupos de estaciones, permitiendo que sean creados subgrupos y con función de herencia de políticas entre grupos y subgrupos; 16. Capacidad de instalar otros servidores administrativos para balancear la carga y optimizar el tráfico de enlaces entre sitios diferentes; 17. Capacidad de interrelacionar servidores en estructura de jerarquía para obtener informes sobre toda la estructura de antivirus; 18. Capacidad de herencia de tareas y políticas en la estructura jerárquica de servidores administrativos; 19. Capacidad de elegir cualquier computadora cliente como repositorio de vacunas y de paquetes de instalación, sin que sea necesario la instalación de un servidor administrativo completo, donde otras máquinas clientes se actualizarán y recibirán paquetes de instalación, con el fin de optimizar el tráfico de red; 20. Capacidad de hacer de este repositorio de			

Ing. Roberto Viveros
Jefe Dpto. T.I.C.
I.N.C.

Abog. César E. Diesel Marí
Gerente U.C.C.
I.N.C.

	vacunas un gateway para conexión con el servidor de administación, para que otras máquinas que no logran conectarse directamente al servidor puedan usar este gateway para recibir y enviar información al servidor administrativo. 21. Capacidad de exportar informes para los siguientes tipos de archivos: PDF, HTML y XML. 22. Capacidad de generar traps SNMP para monitoreo de eventos; 23. Debe tener compatibilidad con Microsoft NAP, cuando se instale en un Windows 2008 Server; 24. Debe tener compatibilidad con Cisco Network Admission Control (NAC); 25. Debe tener documentación de la estructura del banco de datos para generar informes a partir de herramientas específicas de consulta (CrystalReports, por ejemplo). 26. Capacidad de conectar máquinas vía Wake onLan para realizar tareas (barrido, actualización, instalación, etc.), inclusive de máquinas que estén en subnets diferentes del servidor); 27. Capacidad de habilitar automáticamente una política en caso de que ocurra una epidemia en la red (basado en cantidad de virus encontrados en determinado intervalo de tiempo); 28. Capacidad de realizar actualización incremental de vacunas en las computadoras clientes.			

LOS PUNTOS N° 2, 3, 4, 5, 6, 7, 8, 9, 10 Y 11 QUEDAN INVARIABLES.

Abog. Cesar E. Diesel Marin
Gerente U.O.C.
I.N.C.

Ing. Roberto Viveros
Jefe Dpto. T.I.C.
I.N.C.

Sede Central: Av. Fernando de la Mora esq. Tte. Alcorta Asunción
Teléfonos (59521) 569000 Casilla de Correo 384
Planta Industrial de Villeta: (595) 2595512
Planta Industrial de Vallemi: (595) 0351230303/14/48

¡Construyendo futuro con cemento Paraguayo!

PARAGUAY TODOS Y TODAS

A continuación se detalla el calendario para el llamado a Licitación:

ACTIVIDAD	FECHA
Fecha tope para respuestas	04/11/2016 10:00 hs.
Fecha inicio de recepción de propuestas	08/11/2016 10:00 hs.
Fecha fin de recepción de propuestas	09/11/2016 10:00 hs.
Etapa de Competencia	09/11/2016 10:10 hs.
Presentación de Sobres	10/11/2016 09:45 hs.
Apertura del Sobre	10/11/2016 10:00 hs.

Abog. César E. Diesel Marín
Gerente U.O.C.
I.N.C.

Abog. César Diesel Marín

Gerente Unidad Operativa de Contratación