MINISTERIO DE EDUCACIÓN Y CULTURA

GOBIERNO NACIONAL
Construyendo Juntos Un Nuevo Rumbo

MINISTERIO DE EDUCACIÓN Y CULTURA

PROYECTO DE MEJORAMIENTO DE LA EDUCACION ESCOLAR BASICA- ESCUELA VIVA II

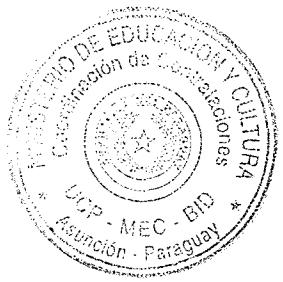
CONVENIO DE PRESTAMO MEC/BID N° 1.880/BL-PR

CONTRATACIÓN DIRECTA N° 02/15

"ADQUISICIÓN DE SOFTWARE INFORMÁTICO"
ID N° 293.347

ADENDA N° 1

Asunción - Paraguay



Unidad Coordinadora de Programas –UCP MEC/BID
Humaitá Nº 145 - Edificio Planeta I
Asunción – Paraguay

Tel: (595 21) 452 380 /2
escuelaviva@escuelaviva-mec.edu.py
www.escuelaviva-mec.edu.py

7. **Fecha y hora límites para realizar consultas:** viernes, 08 de mayo de 2015, hasta las 08:00 horas.

17. **Para propósitos de la presentación de las ofertas, la dirección de la Convocante es:** Humaitá Nº 145 e/ Ntra. Sra. De la Asunción – 6to piso – Edificio Planeta I.

Atención: Lic. Jorge Pineda, Gerente Administrativo Financiero - Programa Escuela Viva II.

La fecha límite para presentar las ofertas es:
Fecha: miércoles, 13 de mayo de 2015
Hora: 09:30

De no contar con un mínimo de 3 (tres) ofertas al vencimiento del plazo de entrega, la Autoridad competente de la Entidad, bajo su exclusiva responsabilidad, podrá disponer la evaluación de las que se hubieren presentado, sin necesidad de realizar una prórroga, debiendo en todos los casos asegurar al Estado Paraguayo las mejores condiciones de contratación, o prorrogar la fecha de entrega y apertura de ofertas, según lo estipulado en las Resoluciones DNCP N° 3416/2014, 805/09 y el artículo 34 de la Ley Nº 2051/03 "De Contrataciones Públicas".

18. **La apertura de las ofertas tendrá lugar en: Dirección:** Humaitá Nº 145 e/ Ntra. Sra. De la Asunción – 6to piso, Edificio Planeta I – Asunción, Paraguay.

Fecha: miércoles, 13 de mayo de 2015
Hora: 10:00

Anexo C
Especificaciones técnicas de los bienes o servicios a ser adquiridos

ITEM	Código de Catalogo	Item Name	Cantidad
1	43232311-001	SQLCAL Lic.SAPk OLP NL Gov UsrCAL - Con Sw Assurance x 2 años (359-01386)	7
2	43231507-001	Prjct 2013 OLP NL Gov	6
3	43231512-9992	Kaspersky Endpoint Security for Business Select	40

ITEM 1

- El oferente brindará capacitación sobre el uso del Sitio VLSC (*VolumeLicensingServiceCenter*) para la descarga del Software y las claves de activación.
- Independientemente deberá entregar copia del medio de instalación en mediosmagnéticos (CD/DVD).
- Los productos detallados en la Planilla de precios deberán contar con dos años de segurode software para posibilitar el acceso a nuevas versiones de los productos durante lavigencia del Seguro de Software (SA)
- Se adjuntara la Autorización del Fabricante al momento de presentación de las ofertas.

Beneficios adicionales:

- Capacitación en el uso de la herramienta por 10 horas. La persona que dará la capacitacióndebe contar con una certificación en base de datos.
- El oferente debe presentar plan de capacitación y carga horaria de 10 horas.

ITEM 2:

- Los Kit's del Software serán entregados con los respectivos manuales en formato digital oimpreso, CD-ROM / DVD (con la última versión disponible en el mercado del productoofertado): Instalación y Usuario.

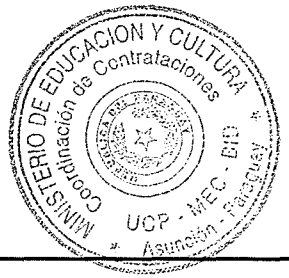
ITEM 3:

La vigencia es de 1 (un) año y no se requiere de instalación.

Software Antimalware con protección para Endpoints y Servidores con consolade Administración Centralizada.
Debe proporcionar las siguientes protecciones:
• Antivirus de archivos residente (antispyware, antitroyano,antimalware, etc.) que verifique cualquier archivo creado,accedido o modificado;
• Antivirus de web (módulo para verificación de sitios ydownloads contra virus)
• Antivirus de correo electrónico (módulo para verificación decorreos recibidos y enviados, así como sus adjuntos)
• Antivirus de mensajes instantáneos (módulo paraverificación de mensajes instantáneos, como ICQ, MSN, IRC,etc.)
• Firewall con IDS
• Autoprotección (contra ataques a los servicios/procesos delantivirus)
• Control de dispositivos externos
• Control de acceso a sitios por categoría
• Control de ejecución de aplicativos
• Control de vulnerabilidades de Windows y de los aplicativosinstalados
• Capacidad de detección de presencia de antivirus de otrofabricante que pueda causar incompatibilidad, bloqueandola instalación
• Capacidad de agregar carpetas/archivos para una zona deexclusión, con el fin de excluirlos de la verificación.Capacidad, también, de agregar objetos a la lista deexclusión de acuerdo con el resultado del antivirus, (ej.:"Win32.Trojan.banker")
• Capacidad de verificar correos electrónicos recibidos yenviados en los protocolos POP3, IMAP, NNTP, SMTP yMAPI, así como conexiones cifradas (SSL) para POP3 y IMAP(SSL);
• Capacidad de filtrar adjuntos de correos electrónicos,borrándolos o renombrándolos de acuerdo con laconfiguración hecha por el administrador.
• Capacidad de verificación de tráfico HTTP y cualquier scriptde Windows Script Host (JavaScript, Visual Basic Script,etc.), usando heurísticas;
• Debe tener soporte total al protocolo IPv6;
• Debe tener módulo de bloqueo de Phishing, conactualizaciones incluidas en las vacunas, obtenidas por Anti-PhishingWorkingGroup (http://www.antiphishing.org/).
• Capacidad de distinguir diferentes subnets y brindar opciónde activar o no el firewall para una subnet específica;
• Debe tener módulo IDS (IntrusionDetectionSystem) paraprotección contra portscans y explotación devulnerabilidades de software. La base de datos de análisisdebe actualizarse conjuntamente con las vacunas.
• El módulo de Firewall debe contener, como mínimo, dosconjuntos de reglas:
• Filtrado de paquetes: donde el administrador podrá elegirpuertas, protocolos o direcciones de conexión que seránbloqueadas/permitidas;
• Filtrado por aplicativo: donde el administrador podrá elegircuál aplicativo, grupo de aplicativo, fabricante de aplicativo,versión de aplicativo o nombre de aplicativo tendrá accesoa la red, con la posibilidad de elegir qué puertas yprotocolos podrán ser utilizados.

• Debe tener módulo que habilite o no el funcionamiento delos 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

El Servidor de Administración y Consola Administrativa y agentes para Endpoints deben poseer compatibilidad con lo siguiente:
• 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
Debe poseer compatibilidad con las principales distribuciones de Linux en 32 y64 bits, entre ellas:
• 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

La solución debe contar con las siguientes características:

- Se debe acceder a la consola vía WEB (HTTPS) o MMC;
- Compatibilidad con Windows FailoverClustering u otrasolución de alta disponibilidad
- Capacidad de eliminar remotamente cualquier solución deantivirus (propia o de terceros) que esté presente en lasestaciones y servidores, sin la necesidad de la contraseña deremoción del actual antivirus;
- Capacidad de instalar remotamente la solución de antivirusen las estaciones y servidores Windows, a través de laadministración compartida, login script y/o GPO de ActiveDirectory;
- Capacidad de instalar remotamente la solución deseguridad en smartphones y tabletsSymbian, WindowsMobile, BlackBerry y Android, utilizando estaciones comointermediadoras;
- Capacidad de gestionar smartphones y tablets (tantoSymbian como Windows Mobile, BlackBerry, Android y iOS)protegidos por la solución antivirus;
- Capacidad de generar paquetes personalizados(autoejecutables) conteniendo la licencia y configuracionesdel producto;
- Capacidad de actualizar los paquetes de instalación con lasúltimas vacunas, para que cuando el paquete sea utilizadoen una instalación ya contenga las últimas vacunaslanzadas;
- Capacidad de hacer distribución remota de cualquiersoftware, o sea, debe ser capaz de enviar remotamentecualquier software por la estructura de gerenciamiento deantivirus para que sea instalado en las máquinas clientes;
- Capacidad de desinstalar remotamente cualquier softwareinstalado en las máquinas clientes;
- Capacidad de aplicar actualizaciones de Windowsremotamente en las estaciones y servidores;
- Capacidad de importar la estructura de Active Directorypara encontrar máquinas;
- Capacidad de que cuando se detecten máquinas nuevas enel Active Directory, subnets o grupos de trabajo,automáticamente se importe la máquina para la estructurade protección de la consola y se verifique si tiene elantivirus instalado. En caso de no tenerlo, debe instalar elantivirus automáticamente;
- Capacidad de agrupamiento de máquinas por característicascomunes entre ellas, por ejemplo: agrupar todas lasmáquinas que no tengan el antivirus instalado, agrupartodas las máquinas que no recibieron actualización en losúltimos 2 días, etc.;
- Capacidad de definir políticas de configuraciones diferentespor grupos de estaciones, permitiendo que sean creadossubgrupos y con función de herencia de políticas entre grupos y subgrupos;

• Capacidad de instalar otros servidores administrativos parabalancear la carga y optimizar el tráfico de enlaces entresitios diferentes;
• Capacidad de interrelacionar servidores en estructura dejerarquía para obtener informes sobre toda la estructura deantivirus;
• Capacidad de herencia de tareas y políticas en la estructurajerárquica de servidores administrativos;
• Capacidad de elegir cualquier computadora cliente comorepositorio de vacunas y de paquetes de instalación, sin quesea necesario la instalación de un servidor administrativocompleto, donde otras máquinas clientes se actualizarán yrecibirán paquetes de instalación, con el fin de optimizar eltráfico de red;
• Capacidad de hacer de este repositorio de vacunas ungateway para conexión con el servidor de administación,para que otras máquinas que no logran conectarsedirectamente al servidor puedan usar este gateway pararecibir y enviar información al servidor administrativo.
• Capacidad de exportar informes para los siguientes tipos dearchivos: PDF, HTML y XML.
• Capacidad de generar traps SNMP para monitoreo deeventos;
• Debe tener compatibilidad con Microsoft NAP, cuando seinstale en un Windows 2008 Server;
• Debe tener compatibilidad con Cisco Network AdmissionControl (NAC);
• Debe tener documentación de la estructura del banco dedatos para generar informes a partir de herramientasespecíficas de consulta (CrystalReports, por ejemplo).
• Capacidad de conectar máquinas vía Wake onLan pararealizar tareas (barrido, actualización, instalación, etc.),inclusive de máquinas que estén en subnets diferentes delservidor);
• Capacidad de habilitar automáticamente una política encaso de que ocurra una epidemia en la red (basado encantidad de virus encontrados en determinado intervalo detiempo);
• Capacidad de realizar actualización incremental de vacunasen las computadoras clientes;
La solución debe poseer la capacidad de brindar la siguiente información de lascomputadoras:
• Si el antivirus está instalado;
• Si el antivirus ha iniciado;
• Si el antivirus está actualizado;
• Minutos/horas desde la última conexión de la máquina conel servidor administrativo;
• Minutos/horas desde la última actualización de vacunas
• Fecha y horario de la última verificación ejecutada en lamáquina;
• Versión del antivirus instalado en la máquina;
• Si es necesario reiniciar la computadora para aplicarcambios;
• Fecha y horario de cuando la máquina fue encendida;
• Cantidad de virus encontrados (contador) en la máquina;
• Nombre de la computadora;
• Dominio o grupo de trabajo de la computadora;
• Fecha y horario de la última actualización de vacunas;
• Sistema operativo con Service Pack;
• Cantidad de procesadores;
• Cantidad de memoria RAM;
• Usuario(s) conectados en ese momento, con información decontacto (si están disponibles en el Active Directory)

• Actuallizaciones de Windows Updates instaladas
• Información completa de hardware conteniendo:procesadores, memoria, adaptadores de video, discos dealmacenamiento, adaptadores de audio, adaptadores dered, monitores, drives de CD/DVD
• Vulnerabilidades de aplicativos instalados en la máquina
• Debe permitir bloquear las configuracioens del antivirusinstalado en las estaciones y servidores de manera que elusuario no logre modificarlas;
• Capacidad de reconectar máquinas clientes al servidoradministrativo más cercano, basado en reglas de conexióncomo:
• Cambio de gateway;
• Cambio de subnet DNS;
• Cambio de dominio;
• Cambio de servidor DHCP;
• Cambio de servidor DNS;
• Cambio de servidor WINS;
• Aparición de nueva subnet;

El sistema debe proveer de Administración Centralizada para DispositivosMóviles (MDM)
El equipo y la marca de la solución ofertada deben tener representación ysoporte técnico de forma local del mayorista autorizado.
El mayorista autorizado debe documentar mediante una nota del fabricante, sucapacidad de distribución y comercialización del producto. La empresa ofertante debe presentar a su vez, una nota del mayoristaautorizado, donde se expresa su habilitación para comercializar productos de la marca ofertada. Además debe contar con personal técnico capacitado parainstalación y soporte de la misma

TODAS LAS DEMAS CONDICIONES PERMANECERAN INVARIABLES E INALTERABLES.-

LIC. DAVID DUARTE
TÉCNICO UOC
UCP MEC/BID

MINISTERIO DE EDUCACIÓN Y CULTURA
Coordinación de Contrataciones
UCP - MEC - BID
Asunción - Paraguay