LICITACION PÚBLICA NACIONAL (SBE) N° 05/2015

"ADQUISICIÓN DE EQUIPOS INFORMÁTICOS, LICENCIAS Y APARATOS TELEFÓNICOS"

ID: 292310

Asunción, 18 de setiembre de 2015

ADENDA N° 5

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:

MODIFICACIONES

1) Modifíquese la **SECCIÓN I. CALENDARIO DE EVENTOS Y DATOS DE LA SUBASTA,** del Pliego de Bases y Condiciones, a fin de extender las fechas del presente proceso de contratación, conforme al siguiente detalle:

SECCIÓN I.
CALENDARIO DE EVENTOS Y DATOS DE LA SUBASTA

(IAO. SBE)

	B - PLAZOS DE LA SUBASTA	
10.1	Referencia de tiempo	Horario del Servidor del Sistema de Subasta a la Baja Electrónica del Paraguay.
10.3	Inicio y fin de Recepción de propuestas de precios	Fecha: **01/10/2015** desde las ***08:00 a.m.*** hasta las ***08:00 a.m.*** del día **02/10/2015.**
10.13	Inicio de la etapa competitiva	**LOTE N° 1 LICENCIAS WINDOWS: 08:10 horas del día 02 de octubre de 2015;** **LOTE N° 2 EQUIPO CORTAFUEGOS; después del cierre del Lote N° 1;** **LOTE N° 3 EQUIPO FILTRADO DE CONTENIDO; después del cierre del Lote N° 2; y así sucesivamente con los demás Lotes**
13.2; 13.3: 13.4 y 13.5	Plazo de presentación de los documentos de la oferta	Una vez finalizada la Subasta a la Baja Electrónica y levantada el acta de sesión pública virtual en el portal, los 3 (tres) oferentes con el precio más bajo; deberán presentar sus respectivas documentaciones (1 (un) ORIGINAL y 2 (dos) COPIAS) en sobre cerrado con indicación del nombre del/la Oferente participante, a fin de realizar las evaluaciones pertinentes. El sobre deberá estar dirigido a la institución Convocante y/o Unidad Operativa de Contrataciones. La Convocante llevará a cabo el Acto de apertura de las ofertas en público conforme a lo establecido en el Art. 24 de la ley 2051/03 y del Art. 36 – Dto. 1107/14 estableciendo lugar, fecha y hora de presentación de los documentos sustanciales que deberán ser

		presentados. **La fecha de presentación de las documentaciones es el día 05 de octubre de 2015 hasta las 09:00 a.m., en la oficina de la Dirección de UOC, sito en Chile y Manduvira 2° Piso – Ministerio del Interior, Asunción – Paraguay.** **La fecha de apertura de los sobres es el día 05 de octubre de 2015 a las 09:30 a.m., en la oficina de la Dirección de UOC, sito en Chile y Manduvira 2° Piso – Ministerio del Interior, Asunción – Paraguay.** **En caso de la no presentación de las ofertas se aplicará lo establecido en el Art. 37 del Decreto 1107/14.** **Nota: La fecha de la oferta física deberá coincidir con la fecha de Presentación y Apertura Física, sin perjuicio de la validez establecida en la IAO.SBE 10.6.**

2) Modifíquense las **Especificaciones Técnicas** de la Sección III. REQUISITOS DE LOS BIENES Y/O SERVICIOS REQUERIDOS, en lo que respecta al **LOTE N° 3**, el cual queda establecido de la siguiente manera:

SECCION III

REQUISITOS DE LOS BIENES Y/O SERVICIOS REQUERIDOS

1. ESPECIFICACIONES TÉCNICAS

LOTE 3 - EQUIPO DE FILTRADO DE CONTENIDO

PROVISIÓN E IMPLEMENTACIÓN DE SOLUCIÓN DE FILTRADO DE CONTENIDO, SEGURIDAD DE PUBLICACION WEB Y ACCESO A INTERNET

Se deberá proporcionar una solución de filtrado de contenido, seguridad de publicación web y acceso a internet para la navegación de los usuarios.

Solución de Seguridad Web, Filtrado de Contenido.	Caracteristicas	Mínimo Exigido	El bien ofertado cumple con las especificaciones requeridas (SI/NO)
Cantidad	**1**		
Marca	Especificar		
Modelo	Especificar		
Procedencia	Especificar		
Caracteristicas Principales			
Definición:	Sistema de Seguridad informática que sea del tipo Administración Unificada de Amenazas (UTM por sus siglas en inglés)	Exigido	
Funcionalidades y caracteristicas del sistema			
Caracteristicas de Desempeño:	Throughput Firewall: 20 Gbps - 64 byte UDP	Exigido	
	Throughput IPsec VPN: 8 Gbps superior	Exigido	
	Throughput IPS: 6 Gbps o superior	Exigido	
	Throughput SSL-VPN: 1.3 Gbps o superior.	Exigido	
	Sesiones concurrentes: 7 Millones	Exigido	
Caracteristicas de Hardware:	Interfaces GigaEthernet (switcheadas) 10/100/1000: 12	Exigido	

	Interfaz de medios compartidos: 8		
	Interfaces 10 GigaEthernet SFP+: 2	Exigido	
	Interfaces de alta disponibilidad del tipo RJ45 GE:2	Exigido	
	Interfaces de Administración: 1 puerto consola y un puerto de administración RJ45	Exigido	
	Almenos un puerto USB para administracion.		
Caracteristicas del dispositivo:	El dispositivo debe ser una appliance de propósito específico	Exigido	
	Capacidad de reensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware (mediante el uso de un ASIC).	Exigido	
	El equipo deberá poder ser configurado en modo gateway o en modo transparente en la red.	Exigido	
	En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.	Exigido	
Caracteristicas del Sistema operativo incluido:	Por seguridad y facilidad de administración y operación, no se aceptan soluciones sobre sistemas operativos genéricos tales como GNU/Linux, FreeBSD, SUN Solaris, HP-UX de HP, AIX de IBM o Microsoft Windows	Exigido	
Firewall:	Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs	Exigido	
	Las reglas del firewall deberán tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando	Exigido	
	Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.	Exigido	
	Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI como por GUI	Exigido	
	La solución deberá tener la capacidad de balancear carga entre servidores.	Exigido	
	En la solución de balanceo de carga entre servidores, debe soportarse persitencia de sesión al menos mediante HTTP Cookie o SSL Session ID	Exigido	
Conectividad y sistema de ruteo:	Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP	Exigido	
	Soporte a etiquetas de VLAN (802.1q)	Exigido	
	Soporte a ruteo estático	Exigido	
	Soporte a políticas de ruteo (policy routing)	Exigido	
	Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS	Exigido	
	Soporte a ruteo dinámico RIPng, OSPFv3, BGP4+	Exigido	
	Soporte de ECMP (Equal Cost Multi-Path)	Exigido	
	Soporte a ruteo de multicast	Exigido	
	Soporta protocolo sFlow.	Exigido	

VPN Ipsec/L2TP/PPTP:	Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site)	Exigido	
	Soporte para IKEv2 y IKE Configuration Method	Exigido	
	Debe soportar la configuración de túneles L2TP y PPTP	Exigido	
	Soporte de VPNs con algoritmos de cifrado: AES, DES, 3DES.	Exigido	
	Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits	Exigido	
	Posibilidad de crear VPN's entre gateways y clientes con IPSec. Esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site.	Exigido	
	La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN)	Exigido	
VPN SSL:	Capacidad de realizar SSL VPNs.	Exigido	
	Soporte de renovación de contraseñas para LDAP y RADIUS.	Exigido	
	Soporte a asignación de aplicaciones permitidas por grupo de usuarios	Exigido	
	Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.	Exigido	
	Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL.	Exigido	
	La VPN SSL integrada deberá soportar a través de algun plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS	Exigido	
Traffic Shapping / QoS:	Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall	Exigido	
	Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente	Exigido	
	Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo	Exigido	
	Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia	Exigido	
Autenticación y Certficación Digital:	Capacidad de integrarse con Servidores de Autenticación RADIUS.	Exigido	
	Capacidad nativa de integrarse con directorios LDAP	Exigido	
	Capacidad incluida, al integrarse con Microsoft Windows Active Directory	Exigido	
Antivirus:	Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.	Exigido	
	El Antivirus deberá poder configurarse en modo Proxy como en modo de Flujo. En el primer caso, los archivos serán totalmente reconstruídos por el motor antes de hacer la inspección. En el segundo caso, la inspección de antivirus se hará por cada paquete de forma independiente.	Exigido	
	El Antivirus integrado debe soportar la	Exigido	

	capacidad de inspeccionar y detectar virus en tráfico IPv6.		
Antispam:	La capacidad antispam incluída deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje.	Exigido	
	La capacidad AntiSpam incluída deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear).	Exigido	
Filtraje de URLs (URL Filtering):	Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 54 millones de sitios web en la base de datos.	Exigido	
IPS:	El Detector y preventor de intrusos deben poder implementarse tanto en línea como fuera de linea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror	Exigido	
	Capacidad de detección de más de 4000 ataques.	Exigido	
	El Detector y preventor de intrusos deberá de estar orientado para la protección de redes.	Exigido	
Filtraje de tráfico VoIP, Peer-to-Peer y Mensajería instantánea	Soporte a aplicaciones multimedia tales como (incluyendo) : SCCP (Skinny), H.323, SIP, Real Time Streaming Protocol (RTSP).	Exigido	
	El dispositivo deberá técnicas de detección de P2P y programas de archivos compartidos (peer-to-peer), soportando al menos Yahoo! Messenger, MSN Messenger, ICQ y AOL Messenger para Messenger, y BitTorrent, eDonkey, GNUTella, KaZaa, Skype y WinNY para Peer-to-peer.	Exigido	
Generalidades	Sistema de Almacenamiento de Logs y Reportes.	Exigido	
	Dispositivo tipo appliance de propósito específico.	Exigido	
	Sistema operativo propietario	Exigido	
	Interface de administración gráfica (GUI) vía Web (HTTPS)	Exigido	
	Interface de administración vía CLI (Línea de comando), vía ssh y consola serial	Exigido	
	Permite la definición de dominios administrativos independientes para dividir o segmentar el control de la información recibida y almacenada por dispositivo.	Exigido	
	Tiene la posibilidad de definir administradores para la solución, de modo que pueda segmentarse la responsabilidad de los administradores por tareas operativas	Exigido	
	Permite la posibilidad de utilizar repositorio de datos externos (bases de datos)	Exigido	

	Permite integrar dispositivos para que reporten, y establezcan comunicaciones seguras con dichos dispositivos	Exigido	
	Permite asignar cuotas de espacio en disco por dispositivo, de modo que un solo dispositivo no consuma la totalidad del disco de la solución	Exigido	
	Todas las funciones están consolidadas en el dispositivo y/o debe además ofrecer la posibilidad de ser una solución de arquitectura escalable, mediante la asignación de roles específicos o modos de operación a los componentes de la solución (recolector y/o analizador), para optimizar así el manejo y el procesamiento de los logs.	Exigido	
Generación de reportes:	Permite generar reportes personalizados, permite al administrador de la solución el determinar el contenido de los reportes.	Exigido	
	El contenido de los reportes incluye los datos en formato tabular (tablas) y/o gráficas (pie-chart, graph-chart)	Exigido	
	Genera reportes de: Utilización de la red (ancho de banda o conexiones), usuarios, direcciones IP y/o servicios con mayor consumo de recursos.	Exigido	
	Genera reportes de los ataques detectados/detenidos con mayor frecuencia en la red, por fuente y/o por destino.	Exigido	
	Genera reportes de las páginas y/o categorías de URL visitadas con mayor frecuencia, por fuente y/o por destino.	Exigido	
	Permite de generar la incidencia de virus detectados/removidos a nivel red por fuente y/o por destino.	Exigido	
	Permite generar un reporte de las actividades administrativas (entradas de administradores, cambios de configuración) realizadas.	Exigido	
	Permite personalizar los criterios bajo los cuales será obtenido el reporte, tales como fuentes, destinos, servicios, fechas y/o día de la semana.	Exigido	
	Permite especificar el período de tiempo específico para el cual el reporte va a ser obtenido, por períodos relativos (hoy, ayer, esta semana, semana pasada, este mes, mes pasado) o bien por períodos absolutos (de la fecha día/mes/año a la fecha día/mes/año).	Exigido	
	Permite la calendarización de reportes.	Exigido	
	Permite generar reportes en formato PDF y DOC.	Exigido	
	Tiene la opción de generar reportes en idioma inglés y en idioma español	Exigido	
	Permite enviar el reporte vía correo electrónico.	Exigido	
Análisis forense y correlación	Permite hacer búsquedas por username o dirección IP, para que toda la información almacenada de dicho username o dirección IP sea mostrada en un reporte donde pueda darse seguimiento a su actividad.	Exigido	
Análisis de Vulnerabilidades	Permite hacer análisis de vulnerabilidades y	Exigido	

	generar un reporte de cuáles vulnerabilidades fueron encontradas. No deberá tener límite de equipos a analizar.		
Almacenamiento de Contenido:	Permite recibir bitácoras de los protocolos http, SMTP para poder almacenar los mensajes que han fluido en la red a través de dichos protocolos, para su posterior visualización	Exigido	
	Los mensajes pueden ser almacenados completamente, o solo un "resumen" de la conexión. El mensaje completo exhibirá el contenido completo, mientras que el resumen solo mostrará fuente y destino de la comunicación, así como su duración.	Exigido	
	Permite hacer búsquedas sobre los mensajes almacenados	Exigido	
Otras Consideraciones	Almacenamiento incluido como mínimo de 1 TB	Exigido	
	Maneja por lo menos 900 Logs por segundo.	Exigido	
	Tiene un índice de recepción de data de 4 Mbps.	Exigido	
	Conectividad con interfaces Ethernet 10/100/1000.	Exigido	
	El dispositivo deberá ser un hardware dedicado. No se aceptaran virtualizaciones.		
	El Equipo es montable en rack.	Exigido	
Autorización	El oferente deberá contar con una autorización escrita del fabricante o el distribuidor en Paraguay para presentar la oferta. A su vez, el oferente deberá estar debidamente autorizado por el fabricante para prestar servicio técnico y contar con técnicos certificados.	Exigido	
Garantías	El oferente deberá presentar documentación del fabricante donde autorice a la empresa como representante para el Paraguay.	Exigido	
	La oferta deberá incluir soporte on site 24x7x365 del proveedor, por todo el periodo de garantía del equipo.	Exigido	
	El oferente deberá presentar respaldo por escrito del fabricante a la empresa oferente autorizándola a prestar el servicio técnico y el cambio de partes por garantía.	Exigido	
	Los técnicos de la empresa oferente deberán estar certificados por el fabricante. El oferente deberá contar con al menos 2 (dos) técnicos certificados de nivel profesional o equivalente.	Exigido	
	Garantía escrita de un (1) año como mínimo.	Exigido	
Lugar de Entrega	Dirección de Tecnología del Ministerio del Interior	Exigido	
Implementación	La oferta deberá incluir instalación, configuración (Acorde a las política de la Dirección de Tecnología y Comunicaciones) y puesta en funcionamiento de la solución, en un plazo no mayor a 120 días hábiles posterior a la recepción de la orden de compra, además deberá contemplarse la transferencia de conocimiento de la solución al menos a 2 funcionarios técnicos de la Dirección de		

MINISTERIO DEL INTERIOR

	Tecnología, en la modalidad On The Job Trainning.		
Plazo de Entrega	Hasta 120 días hábiles posterior a la recepción de la Orden de Compra correspondiente	Exigido	

Observación: los demás lotes quedan sin modificaciones, cuyas Especificaciones Técnicas se encuentran establecidas en la **Adenda N° 4.**

Sin otras modificaciones que realizar, nos despedimos muy atentamente.

MINISTERIO DEL INTERIOR

Abg. Luis Fernando Basualdo, Director
Dirección de Unidad Operativa de Contrataciones