Corte Suprema de Justicia
REPÚBLICA DEL PARAGUAY

PODER JUDICIAL

CIRCUNSCRIPCIÓN JUDICIAL DE PARAGUARÍ
REPÚBLICA DEL PARAGUAY
SUOC

ADDENDUM Nº 01

"ADQUISICIÓN DE EQUIPOS INFORMÁTICOS" - ID Nº 273344

La Sub Unidad Operativa de Contrataciones de la Circunscripción Judicial de Paraguarí, conforme a lo que dispone el Art. 22 de la Ley N° 2051/03 "De Contrataciones Públicas" y el Art. 40 del Decreto Reglamentario N° 21909/03, procede a Introducir la siguiente modificación a la Carta de Invitación:

DONDE DICE:

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

1. Especificaciones Técnicas

Item	Código de Catálogo	Descripción	Especificaciones Técnicas Mínimas Requeridas	Especificaciones del item ofertado (Debe ser llenado por el oferente)	Cantidad
1	43211508-001	COMPUTADORAS PERSONALES (PC)	Procesador: de 4 núcleos, velocidad de reloj de 3.0 Ghz. o superior. Memoria caché de 8 Mb. con bus de sistema de 1333 Mhz. o superior.		12
4	39121004-024	UNIDADES DE SUMINISTRO DE ENERGÍA (UPS)	Aprobación de regulación: CE, GOST, BSI 1363, TUV, etc.		12
6	43222501-001	FIREWALL	Conectividad 3G WAN1 Express Card slot Modem analógico		1

PODER JUDICIAL
UNIDAD OPERATIVA DE CONTRATACIONES
CIRCUNSCRIPCIÓN JUDICIAL DE PARAGUARÍ

C.P. JOSE A. ORTIZ A.

DEBE DECIR:

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

2. Especificaciones Técnicas

Item	Código de Catálogo	Descripción	Especificaciones Técnicas Mínimas Requeridas	Especificaciones del item ofertado (Debe ser llenado por el oferente)	Cantidad
1	43211508-001	COMPUTADORAS PERSONALES (PC)	**Procesador: de 4 núcleos, velocidad de reloj de 3.0 Ghz. o superior. Memoria caché de 6 Mb. o superior, de nivel 3 (L3), con bus de sistema de 1333 Mhz. o superior.**		12
4	39121004-024	UNIDADES DE SUMINISTRO DE ENERGÍA (UPS)	**Aprobación de regulación: OPCIONAL**		12
6	43222501-001	FIREWALL	Router - FIREWALL		1
			Interfaces:		
			Debe poseer como mínimo 2 puertos WAN 10/100/1000 y 7 puertos LAN 10/100/1000.		
			Firewall Throughput:		
			Performance Firewall Troughput 1,5 Gbps. en paquetes de 512 Bytes.		
			Performance Troughput VPN IPSec; 1 Gbps.		
			Performance Troughput IPS; 200 Mbps.		
			Sesiones Concurrentes soportadas, 400.000.		
			Licencia cantidad de usuarios; ilimitado.		
			Statefull Inspection, Soporte de NAT/PAT, port mapping, load balancind.		
			Virtual Domains – Able to apply different Polices for each VLAN.		
			Provisión de Firewall Cliente (Windows) con VPN, antivirus, IPS, Traficc Shaping.		
			Multicast and dynamic routing – RIP, OSPF, BGP, PIM, Firewall certificado por ICSA.		
			VPN:		
			Cant. Túneles VPN IPSec Soportado, 200.		
			Tipo de túneles soportado IPSEC y SSL y PPTP.		
			Certificado ICSA para VPN, IPSEC y SSL.		
			Soporte de VPN tipo Hub and spoke.		
			Soporte de failover de VPN a través de otro proveedor.		
			Seguridad Integrada para inspeccionar trafico VPN por instrucciones, Virus, Spam, Contenido y posibilidad de aplicarse reglas de firewall.		
			VPN traffic shaping.		
			Route based VPN.		
			Encripcion por hardware 3 DES/AES 256.		
			Filtrado de Contenido con Licencia Activa x periodo de 2 años.		
			IPS:		
			El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios.		

			El detector y preventor de intrusos deberá estar integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos. La interfaz de administración del detector y preventor de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso.		
			• Mecanismos de detección de ataques: § Reconocimiento de patrones, Análisis de protocolos, § Detección de anomalías, § Detección de ataques de RPC (Remote procedure call), § Protección contra ataques de Windows o NetBios, § Protección contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail o POP (Post Office Protocol), § Protección contra ataques DNS (Domain Name System), § Protección contra ataques a FTP, SSH , Telnet y rlogin, § Protección contra ataques de ICMP (Internet Control Message Protocol).		
			Antivirus:		
			(HTTP,FTP,SMTP,POP3,IMAP,NNTP,IM) Firewall/VPN (DES, 3DES, AES, MD5, SHA, DH-Group1, Group2, Group5), Web Content filtering, Actualizaciones automáticas de seguridad (AV).		
			Web Content Filtering:		
			Posibilidad de Filtrar contenido web entre todas las interfaces.		
			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 30 millones de sitios web en la base de datos.		
			• Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida. • Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables. • Capacidad de filtrado de scripts en páginas web (JAVA/Active X). • Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida. • Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables. • Capacidad de filtrado de scripts en páginas web		

			(JAVA/Active X).		
			Filtrado SPAM:		
			Posibilidad de filtrar SPAM entre todas las interfaces.		
			Base de datos actualizada en tiempo real actualizable.		
			Control de Aplicaciones:		
			• La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.		
			• La solución debe tener un listado de al menos 1000 aplicaciones ya definidas por el fabricante.		
			• Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping.		
			• El listado de aplicaciones debe actualizarse periódicamente.		
			• La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.		
			• Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log.		
			Certificaciones:		
			Certificación ICSA para el Firewall.		
			Certificación ICSA IPSEC. (VPN IPSec).		
			Certificación ICSA para SSL-TLS (VPN SSL).		
			Certificación ICSA para el Detector de Intrusos (IPS).		
			Certificación ICSA para el Antivirus.		
			Certificación NSS como UTM.		
			Calificación:		
			La empresa oferente debe proporcionar documentación que acredite al menos 3 técnicos certificados dentro de su staff.		
			Garantía:		
			2 años garantía oficial extendida por el fabricante con actualización de Sist. Operativo.		
			2 años, Cobertura por actualización de firmas de seguridad AntiX, Web Filter, IPS y AntiSpam.		

LA CONVOCANTE, A FIN DE DAR A LOS POTENCIALES OFERENTES UN PLAZO RAZONABLE PARA CONSIDERAR LAS MODIFICACIONES INTRODUCIDAS, PRORROGA LA FECHA PARA LA PRESENTACIÓN Y APERTURA DE SOBRES, SEGÚN EL SIGUIENTE CUADRO:

FECHA TOPE PARA ENTREGA DE SOBRES	FECHA DE APERTURA DE SOBRES
03 de setiembre de 2014 Hasta las 9:45	03 de setiembre de 2014 Hora: 10:00

En atención a las disposiciones que rigen la materia, el presente documento integra las Bases Concursales del llamado de referencia.

PODER JUDICIAL
UNIDAD OPERATIVA DE CONTRATACIONES
JOSE A. ORTIZ A.