PODER JUDICIAL
Circunscripción Judicial de San Pedro
Sub Unidad Operativa de Contratación

San Pedro, 23 mayo del 2014.-

# ADENDA N°: 4

## AL PLIEGO DE BASES Y CONDICIONES DE LA LICITACION NACIONAL POR CONCURSO DE OFERTAS PAC N°: 12/2014 "ADQUISICIÓN DE APARATOS INFORMÁTICOS" ID N°: 271.453

**Sección I. Datos de la Licitación (DDL)**

**DICE:**

| | |
|---|---|
| **IAO 1.1 b** | La descripción y número del llamado a Licitación son: ***CONCURSO DE OFERTAS N° 2/2014 "ADQUISICIÓN DE APARATOS INFORMÁTICOS"*** |

**DEBIENDO DECIR:**

| | |
|---|---|
| **IAO 1.1 b** | La descripción y número del llamado a Licitación son: ***CONCURSO DE OFERTAS N° 1/2014 "ADQUISICIÓN DE APARATOS INFORMÁTICOS"*** |

**Sección III. Suministros Requeridos - 1. Especificaciones Técnicas**

**DICE:**

| ÍTEM N° 1: ESTACIÓN DE TRABAJO | | |
|---|---|---|
| **DESCRIPCIÓN** | **ESPECIFICACIONES TÉCNICAS MÍNIMA EXIGIDAS** | **OFERTADO** |
| **Modelo:** | (Indicar) | |
| **Procedencia:** | (Indicar) | |
| **Factor de Forma** | Mini Torre | |
| **Procesador** | Procesador cuatro núcleos velocidad de reloj de 3.3 GHz o superior | |
| **Memoria RAM** | Memoria RAM Instalada: 4GB DDR3 1333MHz o superior<br>Expandible por lo menos a 16Gb | |
| **Ranuras de expansión** | 3 ranuras PCIe x1 y 1 ranura PCIe x16 (para gráficos) | |
| **Unidad de grabador de DVD** | Grabador de DVD 16x con doble capa o superior | |
| **Unidad de Disco Duro** | Disco duro Sata de 7200rpm, 320GBytes mínimo de capacidad | |
| **Interfaces de Periféricos** | Ocho Puertos USB con acceso externo (4 en el frente, 4 atrás) de los cuales 4 puertos 3.0 (2 frontales y 2 posteriores) y 4 puertos 2.0 (2 frontales y dos posteriores)<br>Audio tres conectores en el panel posterior: entrada de | |

PODER JUDICIAL CIRCUNSCRIPCIÓN SAN PEDRO SECCION CONTRATACIONES

Lic. José David Benegas
Jefe - UOC

PDF created with pdfFactory Pro trial version www.pdffactory.com

| | | |
|---|---|---|
| | micrófono, línea de entrada y línea de salida que soporta una ficha estéreo; dos conectores en el panel delantero para entrada de micrófono y salida de auriculares<br>1 Conector VGA de 15 pines<br>1 Conector HDMI<br>1 RJ45 (10/100/1000) | |
| **Tarjeta de video / Sistema Grafico** | Tipo PCI memoria de video no compartida 1GB o superior | |
| **Tarjeta inalámbrica** | WLAN Tipo PCIe de la misma marca del equipo ofertado | |
| **Lector de tarjetas de memoria** | Lector de tarjetas de memoria 19 en 1 o superior | |
| **Monitor LCD** | Monitor LCD Color de 18.5 pulgadas o superior Widescreen (16:9) Resolución de 1360 x 768 a 60HZ Pixel 0.300mm | |
| **Teclado** | Multimedia en español conexión USB | |
| **Mouse / Ratón** | Mouse Laser de 4 botones con mouse pad. | |
| **Sonido** | Parlantes USB externos de la misma marca de los equipos ofertados | |
| **Fuente de alimentación** | Voltaje de fábrica de 275W ATX 115/230VCA a 50/60Hz como mínimo. | |
| **Seguridad** | Gabinete con sistema de seguridad por medio de candado de material de acero y llaves | |
| **Sistema Operativos / Licencias** | Licencia sistema operativo Windows 7 Professional de 64Bit (OEM)<br>Licencia de Microsoft Office Estándar 2010 OLP Gobierno | |
| **Garantía (escrita):** | Para garantizar a la institución, la garantía así como la asistencia técnica especializada, será un requisito indispensable que la garantía pueda ser ejecutada en cualquiera de los CAS del país. La gestión de la ejecución de la garantía, deberá poder ser hecha, directamente a través del oferente, corriendo en su caso, por cuenta del Oferente que resulte adjudicado, la gestión de dicha ejecución. | |
| **Tipo de Garantía y Servicio:** | Provisión de repuestos y partes sin costo, por el periodo de la garantía.<br>Presentar documentación del Fabricante donde certifique por escrito que los equipos ofertados poseen respaldo por la Garantía de Fábrica como así también, Asistencia Técnica especializada y repuestos legítimos de la marca en Paraguay. Asimismo, deberá certificarse por escrito la disponibilidad de partes en Paraguay, para la inmediata atención de reclamos que pudieran existir. | |

**DEBIENDO DECIR:**

| ÍTEM N° 1: ESTACIÓN DE TRABAJO | | |
|---|---|---|
| **DESCRIPCIÓN** | **ESPECIFICACIONES TÉCNICAS MÍNIMA EXIGIDAS** | **OFERTADO** |
| **Modelo:** | (Indicar) | |
| **Procedencia:** | (Indicar) | |
| **Factor de Forma** | Mini Torre | |
| **Procesador** | Procesador cuatro núcleos velocidad de reloj de 3.3 GHz o superior | |
| **Memoria RAM** | Memoria RAM Instalada: 4GB DDR3 1333MHz o superior<br>Expandible por lo menos a 16Gb | |
| **Ranuras de expansión** | 3 ranuras PCIe x1 y 1 ranura PCIe x16 (para gráficos) | |
| **Unidad de grabador de DVD** | Grabador de DVD 16x con doble capa o superior | |

PODER JUDICIAL
SECCION CONTRATACIONES
CIRCUNSCRIPCION DE SAN PEDRO

Lic. José David Benegas
Jefe - UOC

PDF created with pdfFactory Pro trial version www.pdffactory.com

| | | |
|---|---|---|
| **Unidad de Disco Duro** | Disco duro Sata de 7200rpm, 320GBytes mínimo de capacidad | |
| **Interfaces de Periféricos** | Ocho Puertos USB con acceso externo (4 en el frente, 4 atrás) de los cuales 4 puertos 3.0 (2 frontales y 2 posteriores) y 4 puertos 2.0 (2 frontales y dos posteriores)<br>Audio tres conectores en el panel posterior: entrada de micrófono, línea de entrada y línea de salida que soporta una ficha estéreo; dos conectores en el panel delantero para entrada de micrófono y salida de auriculares<br>1 Conector VGA de 15 pines<br>1 Conector HDMI<br>1 RJ45 (10/100/1000) | |
| **Tarjeta de video / Sistema Grafico** | Tipo PCI memoria de video no compartida 1GB o superior | |
| **Tarjeta inalámbrica** | WLAN Tipo PCIe de la misma marca del equipo ofertado | |
| **Lector de tarjetas de memoria** | Lector de tarjetas de memoria 19 en 1 o superior | |
| **Monitor LCD** | Monitor LCD Color de 18.5 pulgadas o superior Widescreen (16:9) Resolución de 1360 x 768 a 60HZ Pixel 0.300mm | |
| **Teclado** | En español, con conector PS/2 o USB, teclas opcionales de acceso rápido a internet, correo y multimedia. No se aceptan teclados de marcas distintas al resto de la computadora. | |
| **Mouse / Ratón** | Optico de 2 botones, y con rueda de scroll, y conector PS/2 o USB. Mouse Pad incluido. No se aceptan mouse de marcas distintas al resto de la computadora. | |
| **Sonido** | Parlantes USB externos de la misma marca de los equipos ofertados | |
| **Fuente de alimentación** | Voltaje de fábrica de 275W ATX 115/230VCA a 50/60Hz como mínimo | |
| **Seguridad** | Gabinete con sistema de seguridad por medio de candado de material de acero y llaves | |
| **Sistema Operativos / Licencias** | Licencia sistema operativo Windows 7 Professional de 64Bit (OEM)<br>Licencia de Microsoft Office Estándar 2010 OLP Gobierno | |
| **Garantía (escrita):** | Para garantizar a la institución, la garantía así como la asistencia técnica especializada, será un requisito indispensable que la garantía pueda ser ejecutada en cualquiera de los CAS del país. La gestión de la ejecución de la garantía, deberá poder ser hecha, directamente a través del oferente, corriendo en su caso, por cuenta del Oferente que resulte adjudicado, la gestión de dicha ejecución. | |
| **Tipo de Garantía y Servicio:** | Provisión de repuestos y partes sin costo, por el periodo de la garantía.<br>Presentar documentación del Fabricante donde certifique por escrito que los equipos ofertados poseen respaldo por la Garantía de Fábrica como así también, Asistencia Técnica especializada y repuestos legítimos de la marca en Paraguay. Asimismo, deberá certificarse por escrito la disponibilidad de partes en Paraguay, para la inmediata atención de reclamos que pudieran existir. | |

**DICE:**

| ÍTEM Nº 5: ROUTER | | |
|---|---|---|
| **DESCRIPCIÓN** | **ESPECIFICACIONES TÉCNICAS MÍNIMA EXIGIDAS** | **OFERTADO** |
| **Marca:** | (Indicar) | |
| **Modelo** | (Indicar) | |
| **Interface** | 8 puertos RJ4510/100/1000bps | |

PODER JUDICIAL
SECCION CONTRATACIONES
CIRCUNSCRIPCION JUDICIAL DE SAN PEDRO

Lic. José David Benegas
Jefe - UOC

PDF created with pdfFactory Pro trial version www.pdffactory.com

| | | |
|---|---|---|
| | Negociación automática / Auto MDI / MDIX | |
| **Estándares y Protocolos** | IEEE 802.3, IEEE 802.3u, IEEE 802.3x<br>CSMA/CD | |
| **Suministro de Energía Externa** | 100-240VAC, 50/60Hz | |
| **Fan Quantity** | Fanless | |
| **Velocidad de transferencia datos** | 10/100Mbps at Half Duplex ;<br>20/200Mbps at Full Duplex | |
| **Indicador LED** | Power, 1, 2, 3, 4, 5, 6, 7, 8 | |
| **Suministro de Energía Eléctrica** | External Power Adapter(Output: 5.0VDC / 0.6A) | |
| **Método de Transferencia** | almacena y envía | |
| **Funciones de Servicio** | tecnología verde, ahorro de energía hasta a 70%<br>Control de flujo 802.3x, la contrapresión<br>Auto-Uplink cada puerto | |
| **Certificación** | FCC, CE, RoHS | |
| **Contenido del Paquete** | Switch de escritorio de 8 puertos 10/100Mbps<br>Adaptador de corriente<br>Guía del usuario | |
| **Requisitos del Sistema** | Microsoft® Windows®, XP, Vista or Windows 7, Windows 8,<br>Mac® OS, NetWare®, UNIX® or Linux. | |
| **Ambiente** | Temperatura de funcionamiento: 0°C ~ 40°C (32°F ~ 104°F);<br>Temperatura de almacenamiento: -40°C ~ 70°C (-40°F ~ 158°F);<br>Humedad: 10% ~ 90% sin condensación;<br>Humedad de almacenamiento: 5% ~ 90% sin condensación | |

**DEBIENDO DECIR:**

| ÍTEM N° 6: ROUTER | | |
|---|---|---|
| **DESCRIPCIÓN** | **ESPECIFICACIONES TÉCNICAS MÍNIMA EXIGIDAS** | **OFERTADO** |
| **Desempeño:** | INTERFACES:<br>DEBE POSEER COMO MÍNIMO 2 PUERTOS WAN 10/100/1000 Y 7 PUERTOS LAN 10/100/1000<br>FIREWALL THROUGHPUT:<br>PERFORMANCE FIREWALL TROUGHPUT 1.2 GBPS EN PAQUETES DE 64 BYTES<br>PERFORMANCE TROUGHPUT VPN IPSEC; 800 MBPS<br>SECIONES CONCURRENTES SOPORTADAS, 450.000<br>NUEVAS SESIONES POR SEGUNDO, 3.000<br>LICENCIA CANT. DE USUARIOS; INLIMITADO | |

PODER JUDICIAL CIRCUNSCRIPCIÓN DE SAN PEDRO SECCION CONTRATACIONES UOC

Lic. José David Benegas
Jefe - UOC

PDF created with pdfFactory Pro trial version www.pdffactory.com

| | | |
|---|---|---|
| | STATEFULL INSPECTIÓN, SOPORTE DE NAT/PAT, PORT MAPPING,LOAD BALANCIND<br>VIRTUAL DOMAINS –ABLE TO APPLY DIFFERENT POLICES FOR EACH VLAN<br>MULTICAST AND DYNAMIC ROUTING – RIP, OSPF, BGP, PIM, FIREWALL CERTIFICADO POR ICSA. | |
| **FIREWALL** | VPN:<br>Cant. Tuneles VPN IPSec Soportado, 180<br>Tipo de tuneles soportado IPSEC y SSL y PPTP<br>Certificado ICSA para VPN, IPSEC y SSL<br>Soporte de VPN tipo Hub and spoke<br>Soporte de failover de VPN a través de otro proveedor<br>Seguridad Integrada para inspeccionar trafico VPN por instrucciones, Virus, Spam, Contenido y posibilidad de aplicarse reglas de firewall<br>VPN traffic shaping<br>Route based VPN<br>Encripcion por hardware 3 DES/AES 256 | |
| **Filtrado de Contenido:** | IPS:<br>Performacne Troughput: 175 Mbps<br>· Capacidad de detección de más de 1400 ataques.<br>· Capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas)<br>· El Detector y preventor de intrusos deberá de estar orientado para la protección de redes.<br>· 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.<br>· El detector y preventor de intrusos deberá soportar captar ataques por Anomalía (Anomaly detection) además de firmas (signature based / misuse detection).<br>· Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo.<br>· Tecnología de detección tipo Stateful basada en Firmas (signatures).<br>· Actualización automática de firmas para el detector de intrusos<br>· El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios.<br>· Mecanismos de detección de ataques:<br>Reconocimiento de patrones, Análisis de protocolos,<br>Detección de anomalías<br>Detección de ataques de RPC (Remote procedure call) | |

PODER JUDICIAL CIRCUNSCRIPCIÓN DE SAN PEDRO SECCION CONTRATACIONES

José David Benegas
Jefe - UOC

PDF created with pdfFactory Pro trial version www.pdffactory.com

| | | |
|---|---|---|
| | Protección contra ataques de Windows o NetBios<br>Protección contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail o POP (Post Office Protocol)<br>Protección contra ataques DNS (Domain Name System)<br>Protección contra ataques a FTP, SSH , Telnet y rlogin<br>Protección contra ataques de ICMP (Internet Control Message Protocol).<br>· Métodos de notificación:<br>Alarmas mostradas en la consola de administración del appliance.<br>Alertas vía correo electrónico.<br>Antivirus<br>Performacne Troughput: 35 Mbps<br>· 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.<br>· Antivirus en tiempo real, 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 categorización del contenido.<br>· La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo appliance, que permita la aplicación de esta protección por política de control de acceso.<br>· Por desempeño y eficiencia, el antivirus deberá funcionar bajo el esquema "Wild list" (Virus en activo solamente) en el cual los virus conocidos que están activos en el Internet son los que se detectan y se detienen.<br>· El appliance deberá de manera opcional poder inspeccionar por todos los virus conocidos (Zoo List)<br>· El Antivirus integrado deberá tener la capacidad de poner en cuarentena archivos encontrados infectados que estén circulando a través de los protocolos http, FTP, IMAP, POP3, SMTP<br>· El Antivirus deberá incluir capacidades de detección y detención de tráfico spyware, adware y otros tipos de malware/grayware que pudieran circular por la red.<br>· El antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging) para al menos MSN Messenger.<br>· El antivirus deberá ser capaz de filtrar archivos por extensión<br>· El antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables por ejemplo) sin importar la extensión que tenga el archivo<br>· Capacidad de actualización automática de firmas Antivirus mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas)<br>AntiSpam:<br>· La capacidad antispam incluida deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, | |

PODER JUDICIAL
CIRCUNSCRIPCIÓN JUDICIAL DE SAN PEDRO
SECCION CONTRATACIONES
UOC

Lic. José David Benegas
Jefe - UOC

PDF created with pdfFactory Pro trial version www.pdffactory.com

| | | |
|---|---|---|
| | decidir rechazar el mensaje.<br>· La capacidad AntiSpam incluida 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). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address)<br>· La capacidad AntiSpam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y checksum del mensaje, como mecanismos para detección de SPAM<br>· En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.<br>Wef Filter:<br>· 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 39 millones de sitios web en la base de datos.<br>· Filtrado de contenido basado en categorías en tiempo real, 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 categorización del contenido.<br>· Configurable directamente desde la interfaz de administración del dispositivo appliance. Con capacidad para permitir esta protección por política de control de acceso.<br>· 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<br>· 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.<br>· Capacidad de filtrado de scripts en páginas web (JAVA/Active X).<br>Filtraje de tráfico VoIP, Peer-to-Peer y Mensajería instantánea<br>· Soporte a aplicaciones multimedia tales como (incluyendo) : SCCP (Skinny), H.323, SIP, Real Time Streaming Protocol (RTSP).<br>· 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.<br>· En el caso de los programas para compartir archivos (peer-to-peer) deberá poder limitar el ancho de banda utilizado por ellos, de manera individual.<br>Alta Disponibilidad:<br>· Posibilidad en FirewallSoporte a Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle.<br>· Alta Disponibilidad en modo Activo-Pasivo<br>· Alta Disponibilidad en modo Activo-Activo<br>· Posibilidad de definir al menos dos interfaces para sincronía | |

PODER JUDICIAL
CIRCUNSCRIPCIÓN DE SAN PEDRO
SECCION CONTRATACIONES
UOC

Lic. José David Benegas
Jefe - UOC

PDF created with pdfFactory Pro trial version www.pdffactory.com

| | | |
|---|---|---|
| | · El Alta Disponibilidad podrá hacerse de forma que el uso de Multicast no sea necesario en la red<br>Virtualización:<br>El dispositivo deberá poder virtualizar los servicios de seguridad mediante "Virtual Systems", "Virtual Firewalls" o "Virtual Domains"<br>La instancia virtual debe soportar por lo menos Firewall, VPN, URL Filtering, IPS y Antivirus<br>Se debe incluir la licencia para al menos 5 (ocho) instancias virtuales dentro de la solución a proveer.<br>Cada instancia virtual debe poder tener un administrador independiente<br>La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales.<br>Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red | |
| **Licenciamiento y actualizaciones** | Tamaño de licencia<br>El licenciamiento de todas las funcionalidades debe ser ILIMITADO en cuanto a usuarios, cajas de correo, conexiones, equipos que pasan a través de él. | |
| **Vigencia de licencia de actualización** | La vigencia de las actualizaciones para los servicios de Antivirus, AntiSpam, IPS y URL Filtering debe proveerse por al menos 3 años. | |
| **Garantía:** | Vigencia de Garantia sobre Hardware, acceso a soporte en el TAC del Fabricante y acceso actualizciones en el Sistema Operativo de por al menos 3 años. | |
| | Antivirus:<br>(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,<br>Web Content Filtering:<br>Posibilidad de Filtrar contenido web entre todas las interfaces.<br>· 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.<br>"• Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al qué pertenezca la conexión siendo establecida<br>• 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.<br>• Capacidad de filtrado de scripts en páginas web (JAVA/Active X).<br>• 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<br>• Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un | |

PODER JUDICIAL
SECCION CONTRATACIONES
CIRCUNSCRIPCION JUDICIAL DE SAN PEDRO

Lic. José David Benegas
Jefe - UOC

PDF created with pdfFactory Pro trial version www.pdffactory.com

| | | |
|---|---|---|
| | sitio correspondiente a una categoría no permitida) deberán ser personalizables.<br>• Capacidad de filtrado de scripts en páginas web (JAVA/Active X).<br>*<br><br>Filtrado SPAM:<br>Posibilidad de filtrar SPAM entre todas las interfaces<br><br>Base de datos actualizada en tiempo real actualizable<br>Características de Administracion:<br>Interfase gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfase debe soportar SSL sobre HTTP (HTTPS)<br>La interfase gráfica de usuario (GUI) vía Web deberá poder estar en español y en inglés, configurable por el usuario.<br>Interfase basada en línea de comando (CLI) para administración de la solución.<br>Puerto serial dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto.<br>Comunicación cifrada y autenticada con username y password, tanto como para la interfase gráfica de usuario como la consola de administración de línea de comandos (SSH o telnet)<br>El administrador del sistema podrá tener las opciones incluidas de autenticarse vía password y vía certificados digitales.<br>Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar.<br>El equipo ofrecerá la flexibilidad para especificar que Los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet,http o HTTPS.<br>El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningun software adicional.<br>Soporte de SNMP versión 2<br>Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos<br>Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.<br>Monitoreo de comportamiento del appliance mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.<br>Certificaciones:<br>Certificación ICSA para el Firewall.<br>Certificación ICSA IPSEC. (VPN IPSec)<br>Certificación ICSA para SSL-TLS (VPN SSL)<br>Certificación ICSA para el Detector de Intrusos (IPS)<br>Certificación ICSA para el Antivirus<br>Certificación NSS como UTM<br>Calificacion :<br>La empresa oferente debe proporcionar documentación que acredite al menos 3 tecnicos certificados dentro de su staff | |

PODER JUDICIAL
SECCION CONTRATACIONES
CIRCUNSCRIPCION JUDICIAL DE SAN PEDRO

Lic. José David Benegas
Jefe - UOC

PDF created with pdfFactory Pro trial version www.pdffactory.com

## Sección IV. Condiciones Especiales del Contrato (CEC)

**DICE:**

| | |
|---|---|
| **CGC 13.1** | La fórmula y el procedimiento para el reajuste serán los siguientes: El precio del contrato estará sujeto a reajustes en el caso que durante el contrato, exista una variación sustancial de precios en la economía nacional (IPC) publicado por el Banco Central del Paraguay, en un valor igual o mayor al 15% (quince por ciento) sobre la inflación oficial y la formula de reajuste será la siguiente: Pr= P x IPC1 IPC0<br>Donde: Pr: Precio Reajustado P: Precio Adjudicado<br>IPC1: Índice de precios al consumidor publicado por el Banco Central del Paraguay, correspondiente al mes de entrega del suministros<br>IPC0: Índice de precios al consumidor publicado por el Banco Central del Paraguay, correspondiente al mes de apertura de ofertas. |

**DEBIENDO DECIR:**

| | |
|---|---|
| **CGC 13.1** | La fórmula y el procedimiento para el reajuste serán los siguientes: El precio del contrato estará sujeto a reajustes en el caso que durante el contrato, exista una variación sustancial de precios en la economía nacional (IPC) publicado por el Banco Central del Paraguay, en un valor igual o mayor al 15% (quince por ciento) sobre la inflación oficial y la formula de reajuste será la siguiente: Pr= P x IPC1 IPC0<br>Donde: Pr: Precio Reajustado P: Precio Adjudicado<br>IPC1: Índice de precios al consumidor publicado por el Banco Central del Paraguay, correspondiente al mes de entrega del suministros<br>IPC0: Índice de precios al consumidor publicado por el Banco Central del Paraguay, correspondiente al mes de apertura de ofertas.<br><br>**PARA PRODUCTOS IMPORTADOS**<br>La fórmula y el procedimiento para el reajuste serán los siguientes: siempre y cuando la variación del Tipo de Cambio del Mercado Libre Fluctuante del Dólar de los Estados Unidos de América, emitido por el Banco Central del Paraguay haya sufrido una variación igual o mayor al cincuenta por ciento (50%) referente a la fecha de apertura de ofertas:<br>Fórmula a Aplicar: P = Po x C.<br>Co<br>Donde<br>P = Precio reajustado de la Oferta<br>Po =Precio Original de la Oferta<br>C = Tipo de Cambio del Mercado Libre Fluctuante (Venta) del dólar emitido por el Banco Central del Paraguay correspondiente al día anterior de la emisión de la factura.<br>Co = Tipo de Cambio del Mercado Libre Fluctuante (Venta) del dólar emitido por el Banco Central del Paraguay correspondiente a la fecha de Apertura de sobre – ofertas.<br>Los reajustes deberán ser solicitados por escrito a la Circunscripción Judicial de San Pedro, por el Proveedor. La solicitud debe realizarse indefectiblemente dentro del mes siguiente al cual se produjeron las variaciones, bajo pena de no poder solicitarlo |

PODER JUDICIAL SECCION CONTRATACIONES CIRCUNSCRIPCION JUDICIAL DE SAN PEDRO

Lic. José David Benegas
Jefe - UOC

PDF created with pdfFactory Pro trial version www.pdffactory.com

| | |
|---|---|
| | posteriormente. No se reconocerán reajuste de precios si los bienes se encuentran atrasados respecto al cronograma de entrega de los bienes. El reajuste tendrá aplicación sobre los bienes entregados posteriores al mes en el cual se produjeron las variaciones, previa resolución de la máxima autoridad de la Convocante |

**Sección VI. Formularios**

**DICE:**

**Formularios N° 1, 2, 3, 5 y 9**
LCO: 03/2014

**DEBIENDO DECIR:**

**Formularios N° 1, 2, 3, 5 y 9**
LCO: 01/2014

PODER JUDICIAL
SECCION CONTRATACIONES
CIRCUNSCRIPCION JUDICIAL DE SAN PEDRO

Lic. José David Benegas
Jefe - UOC

PDF created with pdfFactory Pro trial version www.pdffactory.com