UNIVERSIDAD AUTÓNOMA DE YUCATÁN

LICITACIÓN PÚBLICA INTERNACIONAL

LA-931056978-I1-2013

EQUIPO DE CÓMPUTO, AUDIOVISUAL Y DE REFRIGERACIÓN

C O N T R A T O

UADY
UNIVERSIDAD AUTÓNOMA DE YUCATÁN

CONTRATO NÚMERO 006-2013-LPF

CONTRATO DE COMPRAVENTA QUE CELEBRAN, POR UNA PARTE, LA **UNIVERSIDAD AUTÓNOMA DE YUCATÁN**, A LA QUE EN LO SUCESIVO SE LE DENOMINARA **"LA UADY"**, REPRESENTADA POR EL DIRECTOR GENERAL DE FINANZAS, CONTADOR PUBLICO **AURELIANO MARTÍNEZ CASTILLO**, Y POR LA OTRA PARTE, **PROTEKTNET, SOCIEDAD ANONIMA DE CAPITAL VARIABLE,** A QUIEN LO SUCESIVO SE LE DENOMINARA **"EL PROVEEDOR"**, REPRESENTADO POR EL SEÑOR **ENRIQUE ISRAEL GUTIÉRREZ GUTIÉRREZ**, EN SU CARÁCTER DE APODERADO GENERAL, AL TENOR DE LAS SIGUIENTES DECLARACIONES Y CLÁUSULAS:

D E C L A R A C I O N E S

DE "LA UADY":

1. Que es una institución pública, de enseñanza superior, autónoma por Ley, descentralizada del Estado, con plena capacidad, personalidad jurídica y patrimonio propios, que se rige por su Ley Orgánica contenida en el Decreto número 257, publicado en el Diario Oficial del Gobierno del Estado con fecha 31 de agosto de 1984 y que tiene por finalidades, educar, generar el conocimiento y difundir la cultura en beneficio de la sociedad, como establecen los artículos 1 y 3 de su Ley Orgánica;

2. Que el Contador Público Aureliano Martínez Castillo, Director General de Finanzas, en su carácter de apoderado general, cuenta con facultades suficientes para suscribir el presente contrato, lo cual acredita con la escritura pública número quinientos diecinueve de fecha once de septiembre del año dos mil siete, pasada ante la fe del Abogado Gonzalo Enrique Irabien Arcovedo, titular de la Notaría Pública número setenta y siete del Estado de Yucatán;

3. Que señala como domicilio para efectos del presente contrato, el siguiente: predio número 491-A. de la calle 60 con 57, Edificio Central, Código Postal 97000, Mérida, Yucatán, México; y

4. Que su Registro Federal de Contribuyentes es: UAY8409012S1.

DE "EL PROVEEDOR":

1. Que es una Sociedad Anónima de Capital Variable, constituida por escritura pública número Catorce Mil Novecientos Setenta y Siete, de fecha veintiocho de agosto del año dos mil dos, otorgada en la ciudad de Monterrey, Nuevo León, ante la fe del Licenciado Enrique Morales Montemayor, Notario Público número Ochenta y Cinco, en ejercicio en el Primer Distrito Registral de dicho Estado, inscrita bajo el número 11179, volumen 3, Libro Primero del Registro Público de Comercio del Primer Distrito de Monterrey, Nuevo León, con fecha once de noviembre del año dos mil dos;

2. Que su Administrador Único es el señor Héctor Florentino Leal Gutiérrez, y que en este otorgamiento comparece el señor Enrique Israel Gutiérrez Gutiérrez, en su carácter de apoderado general, quien cuenta con facultades suficientes para suscribir el presente contrato, según acredita con la escritura pública número Nueve Mil Ciento Ochenta y Uno, de fecha veintiuno de enero del año dos mil trece, otorgada en la ciudad de Monterrey, Nuevo León, ante la fe del Licenciado César González Cantú, Notario Público número Sesenta y Nueve, en ejercicio en el Primer Distrito Registral de dicho Estado;

3. Que su domicilio fiscal es: Prolongación Aramberri número 2700 entre José L. Garza y Capitán Aguilar, Colonia Lomas de Chepevera, Código Postal 64000, Monterrey, Nuevo León, México; y

4. Que su Registro Federal de Contribuyentes es: PRO020828PX3.

DE ACUERDO CON LO ANTERIOR, LAS PARTES CONVIENEN EN LAS SIGUIENTES:

C L Á U S U L A S

OBJETO DEL CONTRATO

PRIMERA.- "EL PROVEEDOR" vende y, en consecuencia, conviene en entregar a **"LA UADY"**, los siguientes (**7**) equipos adquiridos en la **Licitación Pública Internacional LA-931056978-I1-2013**, relativa a **Equipo de Cómputo, Audiovisual y Refrigeración:**

PARTIDA	EQUIPO O ARTICULO	CANT.	IMPORTE
55	Solución IPS en línea marca **CYBEROAM** modelo **300**. Características: Solución IPS en línea con sistema de Firewall/VPN que deberá estar basado en un dispositivo Appliance, el cual debe incluir las funcionalidades siguientes: Debe ser compatible y totalmente administrable por la consola de administración que se encuentra en la partida 66. Funcionalidades de Firewall/VPN (Stateful inspection firewall.) y QoS, VPN's SSL y IPSec, además de ofrecer Antivirus Perimetral, Filtrado de contenido en Internet, detector de intrusos y de anti-spam. Deberá estar basado en sistema operativo propietario, de tiempo real, instalado como Firmware y deberá contar con un disco duro. Deberá ofrecer una protección basada en la identidad del usuario en tiempo real. Deberá soportar una inspección de antivirus, antispyware, antispam, phising, pharming sistema de prevención de intrusos y filtrado de contenido, soporte a bloqueo de Applets de Java, Cookies y Active X. Deberá ofrecer Prevención de Ataques DoS y DDoS, filtrado de MAC e IP-MAC Spoofing. Deberá tener la capacidad de escanear de virus los protocolos HTTP, FTP, SMTP, POP3, IMAP y además de filtrar los mismos en Túneles de VPN. Deberá contar con un Área de Cuarentena para los archivos. Este dispositivo deberá tener la capacidad de aplicar Escaneos y entregas dependiendo el tamaño del archivo, y también bloquearlos dependiendo el tipo de archivo. Deberá ofrecer la opción de agregar una frase a los correos (Disclaimer Signature). Deberá contar con un escaneo de los mensajes de correo en los encabezados, tamaño, recipiente, destino y además de poder marcar cada correo una etiqueta en el Asunto, además de revisar. los encabezados de tipo MIME y además de filtrarlo por una Lista Negra (RBL). Deberá ofrecer una configuración de Lista Negra y Lista Blanca personalizada. Deberá tener la capacidad de re-direccionar los correos a un Servidor dedicado de Correo, además de usar una tecnología de RPD basada en el filtrado de imágenes. Deberá ofrecer una Protección de Zero Hour Virus Outbreak. Deberá de brindar la funcionalidad de administración de ancho de banda y administración de múltiples links con los métodos de round robbin y por peso de ruta, además de soportar un failover en caso de que uno de los enlaces no esté disponible. Deberá soportar la funcionalidad de Parent Proxy via FQDN y HTTP Proxy. Deberá ofrecer los Servicios de DDNS y Cliente PPPoE. Debe contar	2	$ 338,836.00

	con módulo de reporteo que permita conocer de modo gráfico y detallado las operaciones. El dispositivo debe ofrecer la Funcionalidad de trabajo en un Modo Ruteo (Gateway), o Modo Transparente (Bridge) y en un Modo Hibrido (Gateway – Brigde). Debe contar con 6 Puertos Ethernet 10/100/1000, además de ofrecer una configuración de zonas de seguridad tales como de DMZ/WAN asignadas a una Interfase. Además de contar con 2 puertos que se comporten como un Bypass de Hardware en caso de tener el equipo en L2. Deberá contar con 2 Puertos USB y un puerto Consola de tipo Serial, donde los puertos USB pueden ser utilizados con un modem USB con servicio de 3G para una redundancia en la salida a internet. Deberá soportar un throughput de firewall de 1,800 Mbps en TCP y de 2,600 Mbps en UDP. Deberá ofrecer 15,000 nuevas sesiones por segundo y además de soportar 500,000 sesiones concurrentes. El equipo debe de ofrecer un throughput en IPS de 850 Mbps y de UTM 350 Mbps. Deberá Contar con analizador de tráfico en tiempo real. Deberá incluir la funcionalidad integrada de VPN en SSL (Secure Socket Layer) en el mismo appliance. Deberá soportar los diferentes estándares para túneles de VPN: Encripción - 3DES, DES, AES, Twofish, Blowfish, Serpent. Hash Algorithms - MD5, SHA-1. Autenticación - Preshared key, Digital certificates. IPSec NAT Traversal. Soporte a Dead peer detection y PFS. Diffie Hellman Grupos - 1, 2, 5, 14, 15, 16. Soporte a entidades de una Autoridad Certificadora. Soporte a Exportar configuraciones de Conexiones de tipo Road Warrior. Soporte de Túneles a usuarios finales por Nombre Dominio. Conexión Redundante de VPN. Soporte de Overlapping. Soporte de VPN Hub & Spoke. Importación de Configuración de VPN's. Deberá ofrecer un Procesamiento a 325 Mbps 3DES y de 400 Mbps a AES. Deberá cumplir con las siguientes certificaciones y estándares de: ICSA Firewall – Corporate. VPNC - Basic y AES interoperabilidad. Nivel 5 de Certificación de Checkmark. CIPA. IPv6 Ready Gold Logo. Soporte a los siguientes Protocolos de Ruteo Dinámicos tales como RIP v1 y v2, OSPF, BGP, Multicast Forwarding, soporte a 802.1q VLANS, soporte a H323 NAT Transversal. Deberá ofrecer un servicio de Políticas de Ruteo. Deberá soportar un Voltaje de entrada 100-240 VAC y ofrecer un Consumo 40 W. Deberá brindar la opción de Aplicar políticas por usuario, donde se le asigne de forma granular lo siguiente: Ancho de banda asignado a: Aplicaciones. Servicios. Políticas. Usuarios. Filtrado de Antivirus. Filtrado de Contenido vía http. Prevención de Intrusos. Anti-Spam. MAC Address en el mismo. Zona Destino. IP Fuente. IP Destino. Servicio Calendarizado. Deberá contener al menos un total de 3000 firmas en el Sistema de Prevención de Intrusos y podrá ser personalizable. Deberá ofrecer un filtrado para Prevención de intrusos el cual pueda bloquear lo siguiente: Protocol Anomaly Detection Block. P2P aplicaciones como Skype. Proxies Anonimos como UItra surf. Actividad de tipo "Phone home". Keylogger. Deberá ofrecer un filtrado de contenido HTTP con una base de datos local basada en Categorías, la cual debe de tener al menos 82+ categorias y deberá soportar la generación de categorías personalizadas, soportando en el filtrado HTTP y HTTPS. Deberá soportar mensajes personalizados por categoría y asignación de un horario por categoría para el uso de la misma. Deberá ofrecer un Filtrado de Aplicaciones integrado desde una base de datos local, donde deberá tener al menos 11 Categorías tales como IM, P2P, Proxies, etc. Deberá poder integrarse con un Directorio Activo, Controlador de Dominio, LDAP, Radius o la generación de una base de datos interna para la autenticación de los usuarios, soportando la función de single sign on, además de ofrecer soporte a un Cliente ligero con MS Windows 2003 Server con Terminal Services y Citrix XenApp. Deberá contener los siguientes reportes al menos 40 por default: Historia de registros en Tiempo real. Notificación de estos reportes Vía email, de Virus y ataques. Prevención de Intrusos. Violaciones de Políticas. Filtrado Web por uso de categorías. Información transferida (Por Host, Grupo y Direcciones IP). Incidencias de Virus por usuario y por dirección IP. Deberá contar con la opción de configuración vía Web y además una ayuda por pasos en el mismo equipo, una administración por roles administrativos y de múltiples administradores, ofreciendo un nivel de acceso a usuarios. Deberá contar con un Sistema de Administración vía HTTP, Serial, Telnet, SNMP (v1, v2c, v3), HTTPS, con la capacidad de generar roles de acceso. Deberá ofrecer en el mismo equipo sin software de terceros una Consola que correlacione todo los eventos que están generándose en el mismo equipo, con al menos 100 diferentes tipos de reportes, los cuales puedan cumplir regulaciones de Seguridad como HIPPA, PCI, GLBA, SOX y FISMA. El sistema operativo deberá ofrecer la capacidad de encriptar el contenido mostrado en los todos los registros que genera el mismo equipo para evitar que sean obtenidos o leídos por una persona no autorizada, además de prevenir que una sola persona tengo el control de la administración de esta información. **GARANTIA Y SERVICIOS**: **EL EQUIPO DEBERA CONTAR CON DOS AÑOS (2) DE GARANTIA DE REMPLAZO INMEDIATO A PARTIR DE LA FECHA DE SU ADQUISICION ESTA DEBERA DE CUBRIR LA FALLA EN CUALQUIERA DE SUS COMPONENTES Y PERMITIR QUE DICHA GARANTIA SE PUEDA EXTENDER HASTA POR 3 AÑOS MÁS AL VENCIMIENTO DE LA MISMA.** Los requerimientos planteados no deberán requerir la compra de equipo, programas o cualquier otro dispositivo adicional para realizar lo solicitado, todos los requerimientos planteados deberán ser cubiertos por el Sistema o Solución ofrecida. Entendiendo por Solución la suma de todos los		

	componentes, equipos, licencias y accesorios requeridos para el funcionamiento, operación y administración. La Solución entregada funcionando debe ser la más reciente comercializada por el fabricante. En caso de liberarse alguna nueva versión durante el periodo de garantía, se deberá actualizar el sistema sin cargo extra para la Universidad Autónoma de Yucatán. Deberá tener un centro de atención telefónica especializada 7x24, los 365 días del año. Deberá asignar un ingeniero certificado por el fabricante, que se encuentre disponible para asistencia telefónica las 24 horas del día y en caso necesario, en forma presencial en 4 horas máximo. Se deberá dar acceso vía Web en el sitio de Internet del fabricante a material relacionado con la configuración, actualización, administración, seguridad, descargas de actualizaciones y parches así como prácticas recomendadas. La instalación, configuración y puesta a punto de los equipos, será realizada por el proveedor, y los costos asociados están incluidos en el costo ofertado para el proyecto. El proveedor contará al menos con una persona certificada en las Soluciones ofertadas por el fabricante representado. El proveedor contará con un plan de trabajo preliminar a la consideración de la Universidad Autónoma de Yucatán, para acordar los ajustes de la versión final que se deberá realizar. El Sistema deberá estar funcionando, puesto a punto y optimizado a satisfacción del personal responsable de Tecnologías de la Universidad Autónoma de Yucatán. El proveedor es distribuidor autorizado de la marca ofertada. El fabricante es obligado solidario del proveedor. LA SOLUCIÓN DEBE DE SER COMPATIBLE Y TOTALMENTE ADMINISTRABLE POR LA CONSOLA DE ADMINISTRACIÓN QUE SE SOLICITA EN LA PARTIDA 66.		
56	Plataforma de seguridad IPS para centro de operaciones marca **CYBEROAM** modelo **2500** Características: Plataforma de seguridad IPS con las siguientes especificaciones: Incluya un EQUIPO IPS RACKEABLE DE 2U EL CUAL DEBERÁ SOPORTAR FUNCIONALIDADES DE FIREWALL, VPN´s (STATEFUL INSPECTION FIREWALL) Y QoS, VPN´s IPSEC/SSL. DEBERÁ CONTAR CON 2 DISCOS DUROS EN ARREGLO RAID 1. Deberá contar con las siguientes Interfases: CopperGBEPorts 14. 1GbE SFP (Mini GBIC) Ports 4. 10GbE SFP (Mini GBIC) Ports 2. Configurable Internal/DMZ/WANPorts Si. Console Ports (RJ45) 1. USBPorts 2. Hardware Bypass Segments 2. Deberá contar con los siguientes componentes internos: Procesador DualCore Si. RAID 1 (2 Discos de 500Gb) Si. Memoria RAM 6 Gb. Deberá ofrecer un rendimiento de procesamiento para los siguientes módulos: Firewall throughput (UDP) (Mbps) 36,000. Firewall throughput (TCP) (Mbps) 28,000. New sessions/second 200,000. Concurrent sessions 3,500,000. IPSecVPNthroughput (Mbps) 4,000. Anti-Virus throughput (Mbps) 5,500. IPS throughput (Mbps) 6,000. UTMthroughput (Mbps) 4,000. Deberá operar bajo las siguientes condiciones: Input Voltage 90-260 VAC. Consumption 258 W. Total Heat Dissipation (BTU) 881. Operating Temperature 0 to 40 °C. Storage Temperature -25 to 75 °C. Relative Humidity (Non condensing) 10 to 90%. Deberá ser de 2U con las siguientes dimensiones para montaje en rack: HxWxD (cms) 9 x 44.5 x 59. Weight 19kg, 41.8lbs. Deberá estar basado en procesadores Dual Core para mejorar el rendimiento en el procesamiento de las diferentes tareas que ofrece el equipo. Deberá ofrecer una protección basada en la identidad del usuario en tiempo real. Deberá contar con la funcionalidad de aplicar Políticas de Bloqueo basadas en las IP's o Grupos de IP's de diferentes Países o Grupos de Países. Deberá de brindar la funcionalidad de administración de ancho de banda y administración de múltiples links con los métodos de round robbin y por peso de ruta, además de soportar un failover en caso de que uno de los enlaces no esté disponible, descubrimiento de Aplicaciones y Usuarios para la asignación de prioridades. Deberá cumplir con la capacidad para Identificación por Usuario – Capa 8 (Contar con Patente). Deberá soportar la funcionalidad de Parent Proxy via FQDN y HTTP Proxy. Deberá ofrecer los Servicios de DDNS y Cliente PPPoE. Deberá contar con módulo de reporteo integrado que permita conocer de modo gráfico y detallado las operaciones, sin necesidad de equipos adicionales o software de terceros. Deberá contar con 14 Puertos Ethernet 10/100/1000 GBE, además 4 puertos SFP (Mini GBIC) de 1 GbE, 2 puertos (Mini GBIC) de 10 GbE, deberá ofrecer una configuración de zonas de seguridad tales como de DMZ/WAN asignadas a una o varias Interfaces. Deberá ofrecer la Funcionalidad de trabajo en un Modo Ruteo (Gateway), o Modo Transparente (Bridge) y en un Modo Hibrido (Gateway – Brigde). Deberá ofrecer un Hardware bypass al menos en 2 grupos de 2 Interfaces. Deberá contar 2 Puertos USB, un puerto Consola de tipo Serial y Un puerto Consola RJ45, donde los puertos USB pueden ser utilizados con un modem USB con servicio de 3G/4G/Wimax para una redundancia en la salida a internet. Deberá incluir la funcionalidad integrada de VPN en SSL (Secure Socket Layer) en el mismo dispositivo. Soporte a Protocolos TCP&UDP sobre el Túnel. Autenticación puede ser vía: Directorio Activo, LDAP, RADIUS, RSA Secure ID, Local. Autenticación Multinivel para el cliente a través de Certificados, Usuario y Contraseña. Asignación de Políticas por usuario y/o grupo. Acceso a Red de forma: Total o Parcial. Acceso al cliente basado en Web a través de un Portal. Cliente ligero para acceso a través del Túnel. Acceso granular a los recursos de la Red.Controles y Administración de: Sesión time out, Dead Peer Detección, Personalización del Portal de acceso. Acceso basado en aplicaciones TCP como: HTTP, HTTPS, RDP, TELNET, SSH, FTP, IBM Server Terminal.	2	$ 338,836.00

	Deberá soportar los diferentes estándares para túneles de VPN: Encripción - 3DES, DES, AES, Twofish, Blowfish, Serpent. Hash Algorithms - MD5, SHA-1. Autenticación - Preshared key, Digital certificates. IPSec NAT Traversal. Soporte a Dead peer detection y PFS. Diffie Hellman Grupos - 1, 2, 5, 14, 15, 16. Soporte a entidades de una Autoridad Certificadora. Soporte a Exportar configuraciones de Conexiones de tipo Road Warrior o Cliente IPSec. Soporte a las diferentes Plataformas: Windows 2000, WinXP 32/64- bit, Windows 2003 32-bit, Windows 2008 32/64-bit, Windows Vista 32/64-bit, Windows 7 RC1 32/64-bits, Windows 8 32/64 bits. Soporte de Túneles a usuarios finales por Nombre Dominio. Conexión Redundante de VPN. Soporte de Overlapping. Soporte de VPN Hub & Spoke. Importación de Configuración de VPN's. Deberá soportar 3,000 túneles de VPNs IPSec. Deberá cumplir con las siguientes certificaciones y estándares de: ICSA Firewall – Corporate. VPNC - Basic y AES interoperabilidad. Checkmark UTM Level 5 Certification. CIPA. "IPv6 Ready" Gold Logo. Deberá cumplir con los siguientes Compliances: CE / FCC / UL. El dispositivo deberá ofrecer Alta disponibilidad y redundancia: Activo-Activo. Activo-Pasivo con sincronización. Failover. Alertas en el equipo de cambios de estatus. Deberá ofrecer la opción de configuración vía Web y además una ayuda por pasos en el mismo equipo, una administración por roles administrativos y de múltiples administradores, además de ofrecer un nivel de acceso a usuarios. Debera ofrecer un soporte Multilenguaje: Ingles, Chino, Hindi, Coreano y Francés. Deberá contar con un Sistema de Administración vía HTTP, Serial, Telnet, SNMP (v1, v2c, v3), HTTPS, con la capacidad de generar roles de acceso. Deberá estar basado en procesadores Dual Core para mejorar el rendimiento en elprocesamiento de las diferentes tareas que ofrece el equipo. La solución deberá ofrecer soporte directo del fabricante en horario 24x7 durante la vigencia de la garantía del equipo (**TRES AÑOS**). Deberá incluir gastos de envíos para reemplazo de equipo además de contar con apoyo para la instalación y/o configuración del nuevo dispositivo. Deberá cubrir la falla en cualquiera de sus componentes y permitir que dicha garantía se pueda extender hasta por tres años más al vencimiento de la misma. Los requerimientos planteados no deberán requerir la compra de equipo, programas o cualquier otro dispositivo adicional para realizar lo solicitado, todos los requerimientos planteados deberán ser cubiertos por la solución ofrecida. Entendiendo por solución la suma de todos los componentes, equipos, licencias y accesorios requeridos para el funcionamiento, operación y administración. La solución debe ser entregada funcionando con la más reciente versión comercializada por el fabricante en caso de liberarse alguna nueva versión durante el periodo de garantía, se deberá actualizar el sistema sin cargo alguno para la Universidad Autónoma de Yucatán. El proveedor contará con un centro de atención telefónica especializado 7 x 24, los 365 días del año. Deberá asignar un ingeniero certificado por el fabricante, que se encuentre disponible para la asistencia telefónica las 24 horas del día y en caso de ser necesario, en forma presencial en 4 horas máximo. Se deberá dar acceso vía web en el sitio de internet del fabricante a material relacionado con la configuración, actualización, administración seguridad, descargas de actualizaciones y parches así como practicas recomendadas. La instalación, configuración y puesta a punto de los equipos, deberá ser realizada por el proveedor, y los costos asociados están incluidos en el costo ofertado para el proyecto. El proveedor contará con al menos con una persona certificada en las soluciones ofertadas por el fabricante representado. El proveedor contará con un plan de trabajo preliminar a la consideración de la Universidad Autónoma de Yucatán, para acordar los ajustes de la versión final que se deberá realizar. El sistema se entregará funcionando, puesto a punto y optimizado a satisfacción del personal responsable de tecnologías de la Universidad Autónoma de Yucatán. El proveedor es distribuidor autorizado de la marca ofertada. El fabricante es obligado solidario con el proveedor. El proveedor cuenta con al menos un ingeniero certificado para la Solución ofertada.		
66	Consola de administración de IPS marca **CYBEROAM** modelo **CCC 50** Características: SOLUCIÓN CCC RACKEABLE DE 1U PARA LA ADMINISTRACIÓN CENTRALIZADA DE DISPOSITIVOS IPS, EL CUAL DEBERÁ ADMINISTRAR HASTA 50 DISPOSITIVOS EQUIPOS CYBEROAM DE DIFERENTES MODELOS, con las características siguientes: Interfaces: 10/100/1000 GBE Ports 6. Console Ports (RJ45) 1. SFP (Mini GBIC) Ports - USB Ports 2. El dispositivo deberá ser de 1U con las siguientes dimensiones para montaje en rack: H x W x D (inches) 1.72 x 17.25 x 11.50. Weight (lbs) 12.188. Power: Input Voltage 100-240VAC. Redundant Power Supply 128W. Total Heat Dissipation (BTU) 375 - Environmental: Operating Temperature 5 to 40 C. Storage Temperature 0 to 70 C. Relative Humidity (Non condensing) 10 to 90%. Cooling System (40mm Fan) 3. No de Equipos serie CR soportados 50. La solución deberá ofrecer soporte directo del fabricante en horario 24x7 durante la vigencia de la **GARANTÍA DEL EQUIPO (UN AÑO).** Deberá incluir gastos de envíos para reemplazo de equipo además de contar con apoyo para la instalación y/o configuración del nuevo dispositivo. Deberá cubrir la falla en cualquiera de sus componentes y permitir que dicha garantía se pueda extender hasta por tres años más al vencimiento de la misma. Los requerimientos planteados no deberán requerir la compra de equipo, programas o cualquier otro dispositivo adicional para realizar lo solicitado, todos los requerimientos	1	$ 90,000.00

	planteados deberán ser cubiertos por la solución ofrecida. Entendiendo por solución la suma de todos los componentes, equipos, licencias y accesorios requeridos para el funcionamiento, operación y administración. La solución debe ser entregada Funcionando. La solución debe ser entregada funcionando con la más reciente versión comercializada por el fabricante en caso de liberarse alguna nueva versión durante el periodo de garantía, se deberá actualizar el sistema sin cargo alguno para la Universidad Autónoma de Yucatán. El proveedor contará con un centro de atención telefónica especializado 7 x 24, los 365 días del año. Deberá asignar un ingeniero certificado por el fabricante, que se encuentre disponible para la asistencia telefónica las 24 horas del día y en caso de ser necesario, en forma presencial en 4 horas máximo. Se deberá dar acceso vía web en el sitio de internet del fabricante a material relacionado con la configuración, actualización, administración seguridad, descargas de actualizaciones y parches así como practicas recomendadas. La instalación, configuración y puesta a punto de los equipos, deberá ser realizada por el proveedor, y los costos asociados deberán estar incluidos en el costo ofertado para el proyecto. El proveedor contará con al menos con una persona certificada en las soluciones ofertadas por el fabricante representado. El proveedor contará con un plan de trabajo preliminar a la consideración de la Universidad Autónoma de Yucatán, para acordar los ajustes de la versión final que se deberá realizar. El sistema se entregará funcionando, puesto a punto y optimizado a satisfacción del personal responsable de tecnologías de la Universidad Autónoma de Yucatán**.** El proveedor es distribuidor autorizado de la marca ofertada. El proveedor contará con al menos cuenta con un ingeniero certificado para la solución ofertada. LA CONSOLA DEBE SER COMPATIBLE CON LA SOLUCIÓN DE LA PARTIDA 55.		
67	Administrador de direcciones IP marca **VIA SCOPE** modelo **SAMART IP 2000**. Características: EQUIPO Administrador de direcciones IP RACKEABLE DE 1U QUE SOPORTE LA ADMINISTRACIÓN DE 2,000 IP´s. con las características siguientes: MEDIDA EN RACK 1U. CPU Intel Core 2 Duo 2.8GHz. OS Windows Embedded. RAM DDR3 3GB. HDD 500GB. Interface Ethernet 10/100/1000 Mbps 4Port. Console 1Port (RJ-45). Trunk Protocol IEEE 802.1q Support. Capacity Up to 2000 active IP addresses (Distributable up to 5000 active IP addresses). DHCP Server Yes. DBMS Db2 v9.7. El dispositivo deberá ser de 1U con las siguientes dimensiones para montaje en rack: W x D x H (mm) 438 x 292.1 x 44. Weight (Kg) 5.2. Operating Enviroment: Temperature 5 – 40 °C. Humidity 20% - 90%. Input Voltage AC 100V-240V / 50-60 Hz. Power 200W. La solución deberá ofrecer soporte directo del fabricante en horario 24x7 durante la vigencia de la **GARANTÍA DEL EQUIPO (UN AÑO).** Deberá incluir gastos de envíos para reemplazo de equipo además de contar con apoyo para la instalación y/o configuración del nuevo dispositivo. Deberá cubrir la falla en cualquiera de sus componentes y permitir que dicha garantía se pueda extender hasta por tres años más al vencimiento de la misma. Los requerimientos planteados no deberán requerir la compra de equipo, programas o cualquier otro dispositivo adicional para realizar lo solicitado, todos los requerimientos planteados deberán ser cubiertos por la solución ofrecida. Entendiendo por solución la suma de todos los componentes, equipos, licencias y accesorios requeridos para el funcionamiento, operación y administración. La solución debe ser entregada funcionando con la más reciente versión comercializada por el fabricante en caso de liberarse alguna nueva versión durante el periodo de garantía, se deberá actualizar el sistema sin cargo alguno para la Universidad Autónoma de Yucatán. El licitante contará con un centro de atención telefónica especializado 7 x 24, los 365 días del año. Deberá asignar un ingeniero certificado por el fabricante, que se encuentre disponible para la asistencia telefónica las 24 horas del día y en caso de ser necesario, en forma presencial en 4 horas máximo. Se deberá dar acceso vía web en el sitio de internet del fabricante a material relacionado con la configuración, actualización, administración seguridad, descargas de actualizaciones y parches asi como practicas recomendadas. La instalación, configuración y puesta a punto de los equipos, deberá ser realizada por el proveedor, y los costos asociados están incluidos en el costo ofertado para el proyecto. El proveedor cuenta con al menos con una persona certificada en las soluciones ofertadas por el fabricante representado. El proveedor cuenta con un plan de trabajo preliminar a la consideración de la Universidad Autónoma de Yucatán, para acordar los ajustes de la versión final que se deberá realizar. El sistema se entregará funcionando, puesto a punto y optimizado a satisfacción del personal responsable de tecnologías de la Universidad Autónoma de Yucatán. El proveedor es distribuidor autorizado de la marca ofertada. El proveedor contará al menos con un ingeniero certificado para la solución ofertada. El fabricante es obligado solidario con el ofertante**.**	1	$ 169,766.00
68	Actualización de Cluster de Firewall marca **CYBEROAM** y **VIASCOPE 2500-300 IP 2000**. Características: LICENCIAMIENTO DE SOFTWARE DE CLUSTER DE FIREWALL (SOLUCIÓN UTM) **POR 3 AÑOS COMPATIBLE CON LA PARTIDA 56** que cumpla con las características siguientes: Deberá ofrecer licenciamiento para Firewall, Antivirus Perimetral, Filtrado de contenido en Internet, Detector de Intrusos y Anti-Spam. Firewall throughput (UDP) (Mbps) 36,000. Firewall throughput (TCP) (Mbps) 28,000. New	1	$ 1,299,200.00

	sessions/second 200,000. Concurrent sessions 3,500,000. IPSecVPNthroughput (Mbps) 4,000. Anti-Virus throughput (Mbps) 5,500. IPS throughput (Mbps) 6,000. UTMthroughput (Mbps) 4,000. Deberá ofrecer Soporte para inspección de Antivirus, Antispyware, Antispam, Phising, Pharming Sistema de Prevención de Intrusos y Filtrado de Contenido y Aplicaciones WEB, soporte a bloqueo de Applets de Java, Cookies y Active X. Deberá soportar Escaneo de virus para los protocolos HTTP, FTP, SMTP, POP3, IMAP y además de filtrar los mismos en Túneles de VPN. Deberá ofrecer Prevención de Ataques DoS y DDoS, Filtrado de MAC e IP-MAC Spoofing. Deberá tener la capacidad de aplicar Escaneos y entregas dependiendo el tamaño del archivo y también bloquearlos dependiendo el tipo de archivo. Deberá contar con área de Cuarentena para los archivos detenidos por el antispam. Deberá permitir agregar una frase a los correos (Disclaimer Signature). Deberá ofrecer Escaneo de los mensajes de correo en los encabezados, tamaño, recipiente, destino y además de poder marcar cada correo una etiqueta en el Asunto, al igual que revisar los encabezados de tipo MIME y también filtrarlos por una Lista Negra (RBL). Deberá permitir la Configuración de Lista Negra y Lista Blanca personalizada para filtrado de correos. Deberá tener la capacidad de re-direccionar los correos a un Servidor dedicado de Correo, además de usar una tecnología de Recurrent Pattern Detection (RPD) basada en el filtrado e imágenes. Deberá ofrecer Protección de Zero Hour Virus Outbreak. Deberá ofrecer la funcionalidad potente de Anti-Spam de Entrada / Salida. Deberá contener al menos 4500+ firmas en el Sistema de Prevención de Intrusos y podrá ser personalizable. Deberá contar con Filtrado para Prevención de intrusos el cual pueda bloquear lo siguiente: Protocol Anomaly Detection Block. P2P aplicaciones como Skype. Proxies Anónimos como Ultra surf. Actividad de tipo “Phone home”. Keylogger. Deberá contar con Filtrado de contenido HTTP con una base de datos local en disco duro integrado basada en Categorías, la cual debe de tener al menos 82+ categorías y deberá soportar la generación de categorías personalizadas, soportando en el filtrado HTTP y HTTPS. Deberá ofrecer como característica el Servicio de correlacionador de eventos en el mismo dispositivo de forma embebida, sin incurrir en un costo adicional. Este Servicio deberá contar con: Más de 1000+ reportes. Reportes Historicos. Busqueda de Reportes. Reportes Customizados. Reportes Incluidos de: Seguridad, Spam, Virus, Tráfico, Bloqueos. Más de 45 Reportes que cumplen con alguna norma o estándar de Seguridad. Todos los reportes exportables a archivos de tipo PDF y Excel. Deberá almacenar un Registro de todo lo copiado (upload) a Internet Vía HTTP para evitar el robo de información, el cual en el registro debe aparecer el Usuario, IP Fuente, Directorio de donde se copió, IP Destino. Deberá ofrecer una categorización por clasificación de URL’s según el Nivel de Riesgo, Características de las Aplicaciones o el Modo de Conexión. Deberá incluir la característica que ofrezca un control de Capa 8 en el acceso a YouTube a una categoría específica de material de videos exclusivo para Escuelas. Deberá soportar mensajes personalizados por categoría y asignación de un horario por categoría para el uso de la misma. Deberá poder integrarse con un Directorio Activo, Controlador de Dominio, LDAP, Radius o la generación de una base de datos interna para la autenticación de los usuarios, soportando la función de single sign on (SSO). Deberá contar con Filtrado de Aplicaciones integrado desde una base de datos local, donde deberá tener al menos 11 Categorías tales como IM, P2P, Proxies, etc. Deberá Contar con analizador de tráfico en tiempo real. Registros en Tiempo real. Notificación de estos reportes Vía email, de Virus y ataques. Prevención de Intrusos. Violaciones de Políticas. Filtrado Web por uso de categorías. Palabras buscadas en un search engine o buscador. Información transferida (Por Host, Grupo y Direcciones IP). Incidencias de Virus por usuario y por dirección IP. Deberá brindar la funcionalidad de Aplicar políticas por usuario, donde se le asigne de forma granular lo siguiente (Criterio de Control de Acceso): Ancho de banda asignado. Filtrado de Aplicaciones Web. Filtrado de Contenido vía http. Prevención de Intrusos, Anti-Spam. MAC Address en el mismo. Zona Destino. IP Fuente. IP Destino. Servicio Calendarizado. La licencia deberá permitir las descargas de actualizaciones de firmware de forma ilimitada y sin costo adicional mientras ésta se encuentre vigente. DEBERÁ INCLUIR 4 LICENCIAS DE RENOVACION POR UN AÑO DE SOFTWARE UTM PARA SOLUCION IPS CYBEROAM MODELO CR300i CON EL QUE CUENTA LA UNIVERSIDAD AUTÓNOMA DE YUCATÁN, la cual deberá contemplar las caracteristicas siguientes: Deberá ofrecer licenciamiento para Firewall, Antivirus Perimetral, Filtrado de contenido en Internet, Detector de Intrusos y Anti-Spam para los equipos instalados con los siguientes números de serie: C070000288-EABLZB. C070000305-D3589Y. C070000341-HE6BI1. C070000324-UJF3KK. Deberá soportar un throughput de firewall de 1,800 Mbps en TCP y de 2,600 Mbps en UDP. Deberá ofrecer 15,000 nuevas sesiones por segundo y además de soportar 500,000 sesiones concurrentes. Deberá ofrecer Soporte para inspección de Antivirus, Antispyware, Antispam, Phising, Pharming Sistema de Prevención de Intrusos y Filtrado de Contenido y Aplicaciones WEB, soporte a bloqueo de Applets de Java, Cookies y Active X. Deberá soportar Escaneo de virus para los protocolos HTTP, FTP, SMTP, POP3, IMAP y además de filtrar los mismos en Túneles de VPN. Deberá ofrecer Prevención de Ataques DoS y DDoS, Filtrado de MAC e IP-MAC Spoofing. Deberá tener la capacidad de aplicar Escaneos y entregas dependiendo el		

	tamaño del archivo y también bloquearlos dependiendo el tipo de archivo. Deberá contar con área de Cuarentena para los archivos detenidos por el antispam. Deberá permitir agregar una frase a los correos (Disclaimer Signature). Deberá ofrecer Escaneo de los mensajes de correo en los encabezados, tamaño, recipiente, destino y además de poder marcar cada correo una etiqueta en el Asunto, al igual que revisar los encabezados de tipo MIME y también filtrarlos por una Lista Negra (RBL). Permitirá la Configuración de Lista Negra y Lista Blanca personalizada para filtrado de correos. Deberá tener la capacidad de re-direccionar los correos a un Servidor dedicado de Correo, además de usar una tecnología de Recurrent Pattern Detection (RPD) basada en el filtrado de imágenes. Deberá ofrecer Protección de Zero Hour Virus Outbreak. Deberá ofrecer la funcionalidad potente de Anti-Spam de Entrada / Salida. Deberá contener al menos 4500+ firmas en el Sistema de Prevención de Intrusos y podrá ser personalizable. Deberá contar con Filtrado para Prevención de intrusos el cual pueda bloquear lo siguiente: Protocol Anomaly Detection Block. P2P aplicaciones como Skype. Proxies Anónimos como Ultra surf. Actividad de tipo "Phone home". Keylogger. Deberá contar con Filtrado de contenido HTTP con una base de datos local en disco duro integrado basada en Categorías, la cual debe de tener al menos 82+ categorías y deberá soportar la generación de categorías personalizadas, soportando en el filtrado HTTP y HTTPS. Deberá ofrecer como característica el Servicio de correlacionador de eventos en el mismo dispositivo de forma embebida, sin incurrir en un costo adicional. Este Servicio deberá contar con: Más de 1000+ reportes. Reportes Historicos. Busqueda de Reportes. Reportes Customizados. Reportes Incluidos de: Seguridad, Spam, Virus, Tráfico, Bloqueos. Más de 45 Reportes que cumplen con alguna norma o estándar de Seguridad. Todos los reportes exportables a archivos de tipo PDF y Excel. Deberá almacenar un Registro de todo lo copiado (upload) a Internet Vía HTTP para evitar el robo de información, el cual en el registro debe aparecer el Usuario, IP Fuente, Directorio de donde se copió, IP Destino. Deberá ofrecer una categorización por clasificación de URL's según el Nivel de Riesgo, Características de las Aplicaciones o el Modo de Conexión. Deberá incluir la característica que ofrezca un control de Capa 8 en el acceso a YouTube a una categoría específica de material de videos exclusivo para Escuelas. Deberá soportar mensajes personalizados por categoría y asignación de un horario por categoría para el uso de la misma. Deberá poder integrarse con un Directorio Activo, Controlador de Dominio, LDAP, Radius o la generación de una base de datos interna para la autenticación de los usuarios, soportando la función de single sign on (SSO). Deberá contar con Filtrado de Aplicaciones integrado desde una base de datos local, donde deberá tener al menos 11 Categorías tales como IM, P2P, Proxies, etc. Deberá Contar con analizador de tráfico en tiempo real. Registros en Tiempo real. Notificación de estos reportes Vía email, de Virus y ataques. Prevención de Intrusos. Violaciones de Políticas. Filtrado Web por uso de categorías. Palabras buscadas en un search engine o buscador. Información transferida (Por Host, Grupo y Direcciones IP). Incidencias de Virus por usuario y por dirección IP. Deberá brindar la funcionalidad de Aplicar políticas por usuario, donde se le asigne de forma granular lo siguiente (Criterio de Control de Acceso): Ancho de banda asignado. Filtrado de Aplicaciones Web. Filtrado de Contenido vía http. Prevención de Intrusos, Anti-Spam. MAC Address en el mismo. Zona Destino. IP Fuente. IP Destino. Servicio Calendarizado. La licencia deberá permitir las descargas de actualizaciones de firmware de forma ilimitada y son costo adicional mientras ésta se encuentre vigente. DEBERÁ INCLUIR 1 LICENCIA POR UN AÑO DE SOFTWARE LA CUAL DEBERÁ SER **COMPATIBLE CON LA PARTIDA 67** y contemplar las características siguientes: El Sistema de administración de direcciones IP deberá ser capaz de monitorear y controlar el uso de direcciones IP / MAC de cualquier dispositivo IP en un entorno estático y/o Dinámico (DHCP). Deberá ser un dispositivo tipo appliance con un sistema operativo endurecido para uso específico de la plataforma de seguridad basada en IPS. El Sistema de administración de direcciones IP deberá constar de un servicio donde se alojarán políticas y una consola de administración para el seguimiento y control de direcciones IP / MAC. Deberá contar con una Consola de administración de IP, con las siguientes características: Mostrar el estado actual de todas las IP. Mostrar Dirección MAC incluyendo IP. Mostrar Direcciones IP/ MAC en Línea. Mostrar direcciones IP/MAC Fuera de Línea. Mostrar direcciones IP No Utilizadas. Mostrar Histórico de Cambios de una IP. Mostrar duplicación de IP, Mostrar el uso de nuevas direcciones IP, Mostrar el nuevo uso de las direcciones MAC, etc. La Consola de Administración deberá proporcionar la identificación de múltiples usuarios y contraseñas para un ambiente de administradores múltiples. La Consola de Administración deberá proporcionar el nivel de privilegio sofisticados para los diferentes administradores. El dispositivo deberá ser capaz de monitorear y controlar el uso de las IP's mediante el uso de paquetes de red sin necesidad de instalar ningún programa o agente en la PC's en el mismo segmento de Broadcast. El dispositivo deberá proporcionar la opción de actualización y descarga remota. El dispositivo deberá facilitar el acceso telnet y puerto serie para la configuración inicial. El dispositivo deberá soportar un ambiente de VLAN's con 802.1Q. Debera contar con monitoreo y control de la dirección IP, con las características siguientes: Deberá ofrecer cetección automática,		

	actualización y monitoreo de las Direcciones IP's, Direcciones MAC, nombre de host, nombre de grupo, por tiempo detectado, etc. Deberá contar con una reserva de dirección IP / protección para Direcciones IP's no utilizadas, con las siguientes características: Deberá proporcionar la Pre-Definición de bloqueo de direcciones IP no asignada, cualquier dirección IP libre tendrá el control el administrador de TI para la asignación en el futuro. Deberá contar con una vinculación IP-MAC, con las siguientes características: Cuando se Vincule la Dirección IP y la dirección MAC, el usuario no puede cambiar su dirección IP sin el permiso del administrador. Deberá contar con un inventario en tiempo real IP / MAC, con las siguientes características: La consola muestra el inventario completo de dispositivos IP en tiempo real para toda la red. Deberá contar con una descripción IP/MAC en columna y búsqueda rápida, con las siguientes características: La consola deberá ofrecer una columna adicional de descripción que hace más sencillo encontrar IP adicionales / Direcciones MAC, el administrador de IP puede averiguar IP / MAC de los dispositivos de inmediato. Deberá contar con una detección de eventos y registro, con las siguientes características: Detecta y guarda los eventos relacionados con IP / MAC, tales como (cambio de IP, los conflictos de IP, Nueva MAC, etc) en tiempo real y guarda los registros en MySQL, MS-SQL o en una base de datos Oracle. Deberá contar con una agrupación de IP, con las siguientes características: La consola deberá ofrecer la creación de grupos de usuarios y la categorización de IP's en grupos de físicos y lógicos para una administración integral. Deberá contar con una protección de conflictos de administración IP, con las características siguientes: Deberá ofrecer protección de equipos de Misión Crítica de un conflicto de Red. Deberá proteger las direcciones IP de los dispositivos importantes de la red de conflictos de IP vinculándolos por IP y MAC. Deberá ofrecer detección automática de conflicto de IP y la prevención mediante el registro de la dirección MAC de cada dirección IP estática. Deberá contar con el servicio de Network Access Control, Capa 2 nivel de bloqueo, con las características siguientes: Sin tocar los dispositivos en el nivel físico o desactivar los puertos del switch, proporciona en Capa 2 un nivel estricto de comandos de bloqueo. Deberá contar con el servicio de bloqueo de una red basada en IP/MAC, con las características siguientes: Permitirá a los administradores bloquear cualquier IP y / o MAC que deba permanecer fuera de la red sin necesidad de instalar ningún programa o agente en los clientes de las PC. Deberá respetar las configuraciones sin la necesidad de cambiar la infraestructura de red existente o de configuración. El sistema deberá identificar de forma automática los dispositivos no administrables por el sistema de control de acceso que hay en la red y que forman parte de la red de telecomunicaciones de la Institución, como por ejemplo: Teléfonos IP. Cámaras IP. Impresoras. Plotters, Etc. Deberá contar con el servicio de autenticación MAC, con las características siguientes: Detectar y guardar la dirección MAC de forma automática. Sin registrar la dirección MAC se bloquea al instante o temporal dependiendo de la política. El proceso de autenticación de MAC es simple y sin complicaciones. Deberá contar con el servicio de acceso a visitantes con un control de tiempo, con las características siguientes: Deberá ofrecer un Direccionamiento IP/MAC de control basados en políticas, donde se Pueden pre-definir los períodos de acceso a la red para los visitantes. Deberá contar con el servicio de control por el nombre de host, con las características siguientes: Registro de nombres de host y cualquier bloqueo, en caso de violar la regla definida. Deberá contar con el servicio de control de IP/ MAC por tiempo de expiración, con las características siguientes: Administrará de forma proactiva las IP/MAC cuando los usuarios ya no están activos en la red en un número determinado de días. Deberá contar con el servicio de control de seguridad para los puntos de acceso inalámbrico, con las características siguientes: Ser independiente del entorno de red (cable y/o inalámbrica), controlar todas las IP/MAC de los puntos de acceso, y será controlado por los administradores de TI. Deberá permitir la administración de usuarios inalámbricos. Deberá soportar la administración simultánea de 2,000 IP´s. Deberá contar con el servicio de seguridad para el servidor DHCP, con las características siguientes: Funciones mejoradas de servidor DHCP con una mayor seguridad. Proporcionar dos tipos de pool DHCP: una para los clientes DHCP autorizados y otro para los clientes DHCP no autorizados. Pool autorizado. Pool de Direcciones MAC registradas en el Servidor de DHCP. Direcciones IP en los pools autorizados para conceder acceso permanente a la red en base a direcciones MAC registradas. Pool no autorizada: Pool de Direcciones no autorizadas de direcciones MAC. MAC no autorizadas recibirán una dirección IP temporal de inicio al acceso a la red por un tiempo limitado, pero el acceso se dará por terminado si no es autorizado por el administrador de TI. Deberá contar condDetección y prevención automática en el Servidor de DHCP para denegar el uso de la direcciones IP estática. Detección automática de otro servidor DHCP existente en la misma red. Deberá contar con el servicio de bloqueo de dispositivos no autorizados por direcciones MAC, con las características siguientes: Aplicar inmediatamente el bloqueo de direcciones MAC no autorizadas o permitir el uso de la red temporalmente. 1 LICENCIA POR UN AÑO DE SOFTWARE LA CUAL DEBERÁ SER **COMPATIBLE CON LA PARTIDA 66** Y CONTEMPLAR LAS CARACTERISTICAS SIGUIENTES: El software deberá cubrir el licenciamiento para Centralización de Información, Alertas y Administrador de Equipos IPS´s. El software de administración remota y centralizada deberá		

	permitir la configuración y administración de los dispositivos de manera individual o por grupos. El software deberá contemplar la aplicación de políticas generales para: Sistema de Administración. Interface del Usuario deberá ser Segura vía WEB. 2 Interfaces de línea de Comando (CLI). Interface línea de Comando vía Segura (SSH). Basado en Roles de Administrador. Interface de configuración Básica. Interface para regresar a la configuración de Fábrica. Opción de respaldar y recuperar toda la información. Información de registros Auditable. Capacidad de agregar y Borrar dispositivos. Capacidad de generar grupos de Dispositivos. Sistemas de Mensajes y Alertas. Correos de Alertas Agendados. Mensajes de dispositivos o grupos de Dispositivos. Mensajes de Contraseñas de fábrica no cambiadas. Dispositivos no Registrados. Alerta de cuando se necesite un Cambio de actualización. Alerta de actualización exitosa. Alertas en caso de cambios de estatus de Conectividad. Alertas de cambio en el estatus de Conexiones de VPN. Disponibilidad de Procesamiento del Equipo. Alertas de amenazas en Virus. Alertas de tráfico no común en la red. Ataques en el IPS. Ataques de Spam. Actualización de Firmas requeridas en Antivirus e IPS. Actualización requerida en el Filtrado de Contenido. Centralización y Administración Remota. Configuración y Administración de Dispositivos Individuales y por Grupo en: Configuración y Sincronización. Actualización Centralizada de AV, IPS y Categorías de Filtrado Web. Aplicación de Políticas y de umbrales. Mejoramiento reforzamiento de políticas en: Host y Grupos de Hosts. Servicios. Agenda. Políticas de Acceso a Internet. Administración de Ancho de Banda. Políticas en el IPS y Firmas personalizadas. Políticas en Antivirus y Antispam. Categorías personalizadas en Filtrado de Contenido WWW. Categorías personalizadas en tipos de Archivos. Categorías personalizadas en Aplicaciones. Respaldo y reposición de la configuración original. Actualizaciones de Sistema Operativo. SNMP (V1, V2c, V3). Compatible con un Servidor de Syslog. Sincronización con un Server de NTP. Comunicación encriptado vía SSL RC4 a 128bit. Monitoreo en Tiempo Real. Ofrece un Pizarrón y Monitoreo principal en actividades como: Dispositivos: Grupos de Dispositivos. Grupo de Información en Dispositivos y Grupos de Notificaciones. Sistema de monitoreo de la salud de los equipos. Amenazas identificadas en el IPS. Ataques de Virus en HTTP y Mail. Monitoreo de Spam y seguimiento. Estatus de Conectividad de dispositivos. Disponibilidad de Información de dispositivos. Modo de Instalación. Detalles de configuración de la Red. Información de las llaves de los Dispositivos y Modelo. Versión del Sistema Operativo. Detalles de la Suscripción. Autenticación para el Usuario. Autenticación Local. Integración con un Directorio Activo. Integración con LDAP y Radius. Compliance: CE. FCC. Actualización de la Consola: Firmas de Antivirus e IPS. Categorías de Filtrado de Contenido WWW. Actualización de Dispositivos. El proveedor deberá tener un centro de atención telefónica especializado 7 x 24, los 365 días del año. Deberá asignar un ingeniero certificado por el fabricante, que se encuentre disponible para la asistencia telefónica las 24 horas del día y en caso de ser necesario, en forma presencial en 4 horas máximo. Se deberá dar acceso vía web en el sitio de internet del fabricante a material relacionado con la configuración, actualización, administración seguridad, descargas de actualizaciones y parches asi como practicas recomendadas. La instalación, configuración y puesta a punto del software, será realizada por el proveedor, y los costos asociados estén incluidos en el costo ofertado para el proyecto. El proveedor contará al menos con una persona certificada en las soluciones ofertadas por el fabricante representado. El proveedor cuenta con un plan de trabajo preliminar a la consideración de la Universidad Autónoma de Yucatán, para acordar los ajustes de la versión final que se deberá realizar. El sistema se entregará funcionando, puesto a punto y optimizado a satisfacción del personal responsable de tecnologías de la Universidad Autónoma de Yucatán. El proveedor es distribuidor autorizado de la marca ofertada. El proveedor contará al menos con un ingeniero certificado para la solución ofertada. El fabricante es obligado solidario con el ofertante.		
T O T A L:		**7**	**$ 2,236,638.00**

SEGUNDA.- "EL PROVEEDOR" se compromete a cumplir con todos los términos contemplados en las bases de la **Licitación Pública Internacional LA-931056978-I1-2013**, relativa a **Equipo de Cómputo, Audiovisual y Refrigeración;** así mismo, se obliga a que los equipos relacionados en la cláusula primera, cumplan con la totalidad de las especificaciones descritas en sus proposiciones técnicas y económicas, las cuales se anexan al presente contrato.

TERCERA.- "EL PROVEEDOR", tomando en cuenta que las líneas eléctricas con las que se cuenta en las diferentes Facultades y Escuelas de **"LA UADY"**, son de 110 y 220 Volts, deberá proveer con estas especificaciones los equipos, materia de este contrato.

FORMA DE PAGO

CUARTA.- "EL PROVEEDOR" acepta que el pago por los equipos, materia del presente contrato, el cual es por la cantidad de **$ 2,236,638.00 (SON: DOS MILLONES DOSCIENTOS TREINTA Y SEIS MIL SEISCIENTOS TREINTA Y OCHO PESOS, SIN CENTAVOS, MONEDA NACIONAL),** sea efectuado por **"LA UADY"**, **veinte** días después de que ésta reciba todas las facturas para su pago, siempre y cuando **"EL PROVEEDOR"** haya realizado la **entrega total** de dichos equipos, a entera satisfacción de **"LA UADY"**.

QUINTA.- "EL PROVEEDOR" entregará, juntamente con los equipos materia de este contrato, las facturas correspondientes al monto total de los mismos, las cuales deberán reunir los requisitos fiscales, así como la descripción detallada de los mencionados equipos, la marca, el modelo y el tiempo de garantía.

GARANTÍA

SEXTA.- "EL PROVEEDOR" se compromete a suministrar a **"LA UADY"**, en el momento de la entrega de los equipos materia de este contrato, una póliza de garantía en todas sus partes y mano de obra, sin costo adicional alguno, la cual cubrirá fallas, descomposturas o defectos de fabricación, por el término establecido en los formatos de proposiciones técnicas y económicas, a partir de la fecha de instalación de los mismos, comprometiéndose también a dar la garantía en sitio del cliente. La vigencia mínima de dicha garantía será de **UN AÑO** para los equipos de las partidas **66** y **67**, de **DOS AÑOS** para el equipo de la partida **55** y de **TRES AÑOS** para los equipos de las partidas **56** y **68.**

SÉPTIMA.- "EL PROVEEDOR" se compromete a contar con el personal técnico necesario para la instalación y puesta en operación de los equipos materia de este contrato, así como su oportuna atención en sitio del cliente en caso de fallas o descomposturas de los mismos, en un tiempo de respuesta no mayor de tres días hábiles, comprometiéndose también, a hacer todos los trámites y diligencias necesarios para hacer efectiva la garantía, ya sea directamente con el fabricante, a un número 0800 o ante el Centro de Servicio Autorizado en esta ciudad de Mérida o del lugar donde sea procedente. También se compromete a proporcionar la capacitación para el manejo de dichos equipos si fuere necesario.

OCTAVA.- "EL PROVEEDOR" se compromete a cambiar los equipos materia de este contrato por otros similares, dentro del término de la garantía, cuando a juicio de un experto en la materia, nombrado por la Universidad Autónoma de Yucatán, sea necesaria su sustitución por defectos observados en los mismos, imputables al proveedor, distribuidor y/o fabricante.

PÓLIZA DE FIANZA

NOVENA.- "EL PROVEEDOR" deberá exhibir al momento de la firma de este contrato, **póliza de fianza por el 12% del monto total del mismo, sin incluir el Impuesto al Valor Agregado,** la cual deberá estar vigente durante el lapso de un año (término mínimo de la garantía), contando a partir de aquel en que **"LA UADY"** reciba de conformidad los bienes materia del contrato. **Dicha Póliza deberá tener incluida la leyenda comprendida en el anexo IV de las bases de la convocatoria**.

DÉCIMA.- La póliza de fianza estará denominada en la misma moneda que el contrato y sólo podrá cancelarse por escrito y a solicitud de **"LA UADY"**.

ENTREGA DEL EQUIPO

DÉCIMA PRIMERA.- "EL PROVEEDOR" se obliga y compromete a entregar a **"LA UADY"** los equipos materia de este contrato, descritos en la cláusula primera del mismo, en un término no mayor de **CUARENTA DÍAS NATURALES,** contados a partir de la fecha de firma del presente contrato y en caso contrario, a pagar a **"LA UADY"** una **pena convencional del dos al millar diario**, por cada día de retraso, sobre el monto total del mismo, salvo que las causas de incumplimiento no le sean imputables, lo cual deberá acreditar en forma fehaciente a **"LA UADY"**.

DÉCIMA SEGUNDA.- "EL PROVEEDOR" se obliga y compromete a presentar a **"LA UADY"**, en el momento de la entrega de los equipos materia de este contrato, los datos complementarios tales como número de serie y cualesquiera otro elemento que permita la identificación de los mismos, los cuales también deberán constar en las facturas correspondientes.

DÉCIMA TERCERA.- Todos los equipos deberán transportarse adecuadamente empacados, de manera que se reduzcan los riesgos de transporte.

LUGAR DE ENTREGA DEL EQUIPO

DÉCIMA CUARTA.- Las partes convienen en que la entrega de los equipos, materia de este contrato, será en las Dependencias de **"LA UADY"**, que para tal efecto les comunique por escrito el Comité Institucional de Adquisiciones de **"LA UADY"**, al momento de la firma del mismo.

SEGUROS

DÉCIMA QUINTA.- "EL PROVEEDOR" se compromete a asegurar contra todo riesgo de transporte, todos y cada uno de los equipos materia de este contrato.

INSTALACIÓN

DÉCIMA SEXTA.- "EL PROVEEDOR" se obliga y compromete a efectuar la instalación y puesta en operación de los equipos de referencia, sin cargo alguno para **"LA UADY"**, así como a realizar las pruebas necesarias para el correcto funcionamiento de los mismos, a plena satisfacción de **"LA UADY"**. Esta instalación deberá realizarse en un plazo no mayor de **TRES DÍAS** hábiles, contados a partir de la recepción de los mismos, comprometiéndose **"LA UADY"** a proporcionar las instalaciones necesarias y adecuadas para dichos equipos.

MANTENIMIENTO Y DISPONIBILIDAD DE CENTROS DE SERVICIO

DÉCIMA SÉPTIMA.- "EL PROVEEDOR" se compromete a proporcionar, por separado y sin costo alguno para **"LA UADY"**, una póliza de servicio que contendrá: mantenimiento preventivo (dos veces al año) y correctivo (cuando se requiera) en sitio del cliente. Dicha póliza de servicio deberá tener una vigencia de **UN AÑO**, a partir de la entrega de los equipos. Asimismo, se compromete a señalar las instalaciones con las que cuenta para proporcionar dicho servicio, indicando a **"LA UADY"**, su teléfono, fax y dirección completa.

REFACCIONES

DÉCIMA OCTAVA.- "EL PROVEEDOR" se compromete a notificar por escrito a **"LA UADY"**, tan pronto como tenga conocimiento, si algún equipo será descontinuado, comprometiéndose a surtir las partes y refacciones pertinentes durante cinco años, a partir de la fecha de la entrega del mismo.

MANUALES DE OPERACIÓN

DÉCIMA NOVENA.- "EL PROVEEDOR" deberá entregar un juego de catálogos conteniendo toda la información pertinente para el manejo, instalación y operación de los equipos, materia de este contrato, en idioma español o inglés.

CAPACITACIÓN

VIGÉSIMA.- "EL PROVEEDOR" se compromete a otorgar al personal que **"LA UADY"** designe (tres personas), la capacitación necesaria para el manejo de los equipos si fuere necesario. Dicha capacitación será impartida sin cargo alguno para **"LA UADY"**, durante el tiempo que se requiera, por personal debidamente calificado, en las instalaciones que indique **"LA UADY"** y consistirá en demostraciones, asistencia a cursos y literatura necesaria.

RELACIONES LABORALES

VIGÉSIMA PRIMERA.- El personal que participe en cualquier actividad de capacitación que se derive de este contrato, continuará bajo la dirección y dependencia de **"EL PROVEEDOR"** o de la institución con la que tenga establecida su relación laboral, por tal motivo, en ningún caso se considerará a **"LA UADY"** como patrón sustituto.

CUMPLIMIENTO DEL CONTRATO

VIGÉSIMA SEGUNDA.- Transcurridos treinta días sin que **"EL PROVEEDOR"** hubiera dado cumplimiento a lo dispuesto en la cláusula décima primera de este documento, **"LA UADY"** podrá dar por rescindido el presente contrato y en ese sentido, se hará efectiva la fianza relativa por incumplimiento del contrato señalada en la cláusula novena, esto es independiente de los gastos, daños y perjuicios que se pudieran ocasionar por el incumplimiento del mismo, igual que todos aquellos otros gastos y honorarios que se generen si fuere necesario el ejercicio de las acciones legales de los Tribunales competentes. La aplicación de la garantía será proporcional al monto de las obligaciones incumplidas. Asimismo, **"LA UADY"** podrá dar por terminado anticipadamente el presente contrato, cuando concurran razones graves o de interés general, tales como cuando **"EL PROVEEDOR"** se encuentre en situación de atraso en la entrega de los bienes o servicios, por causas imputables al mismo, respecto al incumplimiento de otro u otros contratos y hayan afectado con ello a **"LA UADY"**.

CANCELACIÓN DE LA FIANZA

VIGÉSIMA TERCERA.- Transcurrido un año, contado a partir de la fecha en que los equipos sean entregados, así como debidamente instalados y funcionando a entera satisfacción de **"LA UADY",** ésta se compromete a expedir a **"EL PROVEEDOR",** previa solicitud hecha por escrito por el mismo, una carta de conformidad para que sea cancelada la póliza de fianza entregada como garantía de cumplimiento del contrato. Dicha carta de conformidad estará firmada por el Director General de Finanzas de **"LA UADY"**.

ANEXOS

VIGÉSIMA CUARTA.- Se consideran como parte integrante del presente contrato, los anexos siguientes:

a) Copia certificada del acta constitutiva de la sociedad, en la cual consta también el nombramiento del Administrador General Único de la misma;
b) Copia certificada del poder que acredita la personalidad del apoderado general;
c) Copia de la identificación con fotografía del apoderado general de **"EL PROVEEDOR"**;
d) Copia del escrito de **"EL PROVEEDOR"**, donde manifiesta bajo protesta de decir verdad, haber presentado en tiempo y forma las declaraciones por impuestos federales y no tener determinado a su cargo créditos fiscales firmes;
e) Las proposiciones técnicas y económicas presentadas por **"EL PROVEEDOR"**;
f) Relación de las Dependencias donde serán entregados los equipos objeto de este contrato; y
g) Póliza de Fianza No. 1317095-0000 de fecha 5 de abril de 2013, expedida por: PRIMERO FIANZAS, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE, por la cantidad de: **$ 231,376.34 (DOSCIENTOS TREINTA Y UN MIL TRESCIENTOS SETENTA Y SEIS PESOS, TREINTA Y CUATRO CENTAVOS, MONEDA NACIONAL).**

TRIBUNALES COMPETENTES

VIGÉSIMA QUINTA.- Para todo lo relacionado con la interpretación de este contrato, las partes contratantes se someten expresamente a la jurisdicción de los Jueces y Tribunales competentes de esta ciudad de Mérida, Yucatán, México, renunciando expresamente a cualquier fuero que pudiera tener relación con sus domicilios presentes y futuros.

EL PRESENTE CONTRATO SE FIRMA POR DUPLICADO, EN LA CIUDAD DE MÉRIDA, CAPITAL DEL ESTADO DE YUCATÁN, ESTADOS UNIDOS MEXICANOS, A LOS CINCO DÍAS DEL MES DE ABRIL DEL AÑO DOS MIL TRECE.

POR	POR
"LA UADY"	**"EL PROVEEDOR"**
_____	_____
C.P. AURELIANO MARTÍNEZ CASTILLO	**SR. ENRIQUE ISRAEL GUTIÉRREZ GUTIÉRREZ**
DIRECTOR GENERAL DE FINANZAS	APODERADO GENERAL