UNIVERSIDAD AUTÓNOMA DE YUCATÁN

LICITACIÓN PÚBLICA INTERNACIONAL

29021002-001-12

EQUIPO DE CÓMPUTO Y AUDIOVISUAL

C O N T R A T O

CONTRATO NÚMERO 006-2012-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, **NGN, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE**, A QUIEN EN LO SUCESIVO SE LE DENOMINARA **"EL PROVEEDOR"**, REPRESENTADO POR EL SEÑOR **AUGUSTO VÍCTOR CAMELO PÉREZ**, 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 acta número Catorce, de fecha diez de enero del año dos mil tres, otorgada en la ciudad de Mérida, Yucatán, ante la fe del Abogado Antonio Bolaños Parra, titular de la Notaría Pública número Cincuenta y Ocho del Estado de Yucatán, inscrita en el Registro Público de la Propiedad y del Comercio de dicho Estado, en el Folio Mercantil Electrónico 587 1 (quinientos ochenta y siete, uno), con fecha diez de abril del año dos mil tres;

2. Que su representante legal es el señor Mario Miguel Pérez Ruiz, en su carácter de Administrador Único, según consta en acta número Doscientos Diez, de fecha siete de enero del año dos mil seis, otorgada en la ciudad de Mérida, Yucatán, ante la fe del Abogado Carlos T. Goff Rodríguez, titular de la Notaría Pública número Noventa y Siete del Estado de Yucatán, inscrita en el Registro Público de la Propiedad y del Comercio de dicho Estado, en el Folio Mercantil Electrónico 587 1(quinientos ochenta y siete, uno), con fecha veintitrés de marzo del año dos mil seis;

3. Que en este otorgamiento comparece el señor Augusto Víctor Camelo Pérez, en su carácter de apoderado general para pleitos y cobranzas y para actos de administración de la sociedad, quien cuenta con facultades para suscribir el presente contrato, según consta en acta número mil nueve de fecha nueve de septiembre del año dos mil nueve, otorgada en la ciudad de Mérida, Yucatán, ante la fe del Abogado Luis Silveira Cuevas, titular de la Notaría Pública número Ocho del Estado de Yucatán, inscrita en el Registro Público de la Propiedad y del Comercio de dicho Estado, en el Folio Mercantil Electrónico 587 – 1 (quinientos ochenta y siete guión uno), con fecha veintitrés de marzo del año dos mil diez;

4. Que su domicilio fiscal es: Calle 20 Número 298 por 17 y 19, Colonia Miguel Alemán, Código Postal 97148, de la ciudad de Mérida, Yucatán; y

5. Que su Registro Federal de Contribuyentes es: NGN0301105Q9.

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 (**2**) equipos adquiridos en la **Licitación Pública Internacional 29021002-001-12**, relativa a **Equipo de Cómputo y Audiovisual:**

PARTIDA	EQUIPO O ARTICULO	CANT.	IMPORTE
58	Actualización de Plataforma de Seguridad marca **CHECKPOINT** modelo **12407 Appliance Smart-1 50.** Características: Actualización de la plataforma de seguridad checkpoint con que cuenta la UADY, CheckPoint SecurePlatform R75.20 o superior, con administración de cluster con gateways CheckPoint 9070, que cumpla o exceda las siguientes características: Debera incluir Gateway compatible con los componentes de la plataforma de seguridad con que cuenta la UADY, cumpliendo con los siguientes requerimientos específicos: El gateway y su administración, deben permitir adicionar nuevas funcionalidades a través de plugins o módulos, sin necesidad de realizar un upgrade completo de software o hardware. Deberá permitir operación en modo transparente y Gateway. Deberá incluir fuente de poder redundante Dual y soportar la tecnología hot-swappable. Deberá incluir 8 puertos de red 10/100/1000 BASE T. Deberá incluir 3 slots de expansión. Deberá tener no menos de 4 GB en	1	$ 1'040,333.00

	RAM. Deberá tener un estándar de montaje en rack. Deberá incluir ruteo estático. Deberá incluir ruteo dinámico de tipo vector distancia (por lo menos RIP, RIP V2). Deberá contar con una capacidad de almacenamiento mayor o igual a 500 GB. Deberá incluir métodos sesión sincronizada para el firewall y VPN. Deberá contar con sesión de conmutación por error para el enrutamiento de cambio. El gateway debe incluir Firewall, VPN, IPS, Control de aplicaciones, todas en un solo hardware, con la posibilidad de ejecutar todas las funcionalidades al mismo tiempo. Deberá contener los siguientes módulos: Firewall, IPsec VPN (Virtual Private Network), Advanced Networking & Clustering, Identity Awareness, Mobile Access for 5 concurrent users, IPS (intrusion prevention system), Application Control Software Módulos. La licencia debe ser para usuarios ilimitados de firewall e ilimitadas direcciones IP. El fabricante de hardware y del software de seguridad, debe ser el mismo. El gateway debe tener una utilidad de diagnóstico de Hardware, que permita rápidamente identificar fallas en el gateway. La herramienta debe poderse ejecutar directamente desde el LCD, sin la necesidad del uso de cables o consolas. El gateway debe ser accesible a través de SSH y de interface Web usando SSL. Debe incluir la licencia de por lo menos para 5 usuarios SSL remotos con la posibilidad de usar clientless portal en Windows, MAC, Linux, Iphone, IPAD, Android y pudiendo adicionar mas usuarios con la licencia apropiada. La restauración a la configuración de fábrica, se debe poder hacer incluso desde el LCD del gateway. Un sistema de backup/restore debe ser incluido, permitiendo al administrador programar la realización de los backups de la configuración en el tiempo deseado. Los Backups pueden ser almacenados localmente, y el administrador puede transferirlos vía TFTP o SCP. El appliance debe ser capaz de almacenar mas de una imagen, y debe permitir al administrador cambiar de una imagen a otra. Debe soportar Administración en Alta disponibilidad, sin requerir una licencia adicional. Soportar consola serial. Soportar al menos 250 VLANs. El throughput debe ser al menos 25 Gbps para firewall. El throughput del firewall e IPS activos, con tráfico mixto debe ser de al menos 12 Gbps. Debe ser capaz de manejar al menos 1.2 Millones de sesiones concurrentes, pudiendo crecerlo a 3.5 Millones de necesitarlo con solamente licenciamiento. Debe de cumplir con al menos CB/UL/cUL/CE/FCC/TUV/VCCI/C-Tick. Actualización del hardware de la consola de administración compatible con los componentes de la plataforma de seguridad con que cuenta la UADY, cumpliendo con los siguientes requerimientos específicos: Todas las funcionalidades solicitadas deberán estar integradas en uno solo equipo. La consola de administración deberá poder administrar de forma centralizada toda la solución de seguridad. Deberá ofrecer un conjunto completo de Software de gestión de seguridad. Deberá poder maximizar la eficacia con una sola consola de administración unificada, para red y seguridad de punto final. Deberá poder asegurar la continuidad operacional de los entornos más exigentes. Deberá conseguir una mayor seguridad mediante la segmentación, su gestión en múltiples dominios virtuales con varios dominios. Deberá contar con 4 puertos de 1Gb Ethernet. Deberá contar con un puerto de consola. Deberá contar con un puerto LOM (lights-out management). Deberá contar con 2 puertos USB. Deberá contar con 4 Discos duros de 1 TB con configuración de RAID 10. Deberá tener una entrada un voltaje de Entrada AC 90-264V. Deberá tener una frecuencia de 47/ 63Hz. Deberá tener una potencia máxima de alimentación: 2 x 600W. Deberá tener una Potencia máxima Consumo: 505.3W. Deberá tener una conformidad de tipo, CE, FCC Clase A, RoHS. Debe tener soporte para sistemas de almacenamiento con que cuenta la UADY, SAN DELL CX3-10. Debe tener la posibilidad de ponerse en HA sin requerimiento de licenciamiento adicional. Debe soportar al menos la administración de 50 gateways. Debe soportar 30,000 logs por segundo. Software del Gateway. Firewall. El gateway debe estar basado en la tecnología conocida como “Stateful Inspection”, el cual realiza un análisis granular de los estados de las comunicaciones y aplicaciones, para controlar el flujo del tráfico pasando a través del gateway, y de esta manera abrir dinámicamente y de una forma segura, puertos y un gran rango de protocolos. Debe permitir crear controles de acceso a por lo menos 150 aplicaciones/servicios/protocolos predefinidos. Debe proteger implementaciones de VoIP, soportando H323 v2/3/4 (incluido h.225 v.2/3/3 y h.254 v3/5/7), SIP. MGCP y SCCP. Debe incluir la posibilidad de crear NATs dinámicos (N-1 o Hide) y estáticos, permitiendo trasladar direcciones IP y puertos origen y destino, en un mismo paquete y en una sola regla. Permitir implementar reglas aplicadas a intervalos de tiempo específicos. La comunicación entre los servidores de administración y los gateways, debe ser cifrada y autenticada. El firewall debe soportar métodos de autenticación, por usuario, cliente y por sesión. Debe ser capaz de autenticar sesiones de cualquier servicio. Los siguientes esquemas de autenticación deben ser soportados por los módulos de firewall y VPN: tokens (por ejemplo, SecureID), TACACS, RADIUS, certificados digitales y dispositivos biométricos. Debe incluir una base de usuarios local que permita realizar autenticación, sin depender de un dispositivo externo. Debe soportar DHCP en modos server y relay. Debe incluir la posibilidad de que el firewall trabaje en modo transparente (bridged mode). Debe permitir el controlar el acceso a archivos compartidos de Microsoft usando CIFS, y que el administrador decida que carpetas se pueden acceder y cuales no. Debe soportar Alta Disponibilidad y Balanceo de Carga de gateways con sincronización de estados, incluyendo al menos la licencia para Alta Disponibilidad. Debe soportar la inspección de https		

	de entrada y salida, para las funcionalidades de control de aplicaciones, DLP, url filtering al menos. Debe soportar interfaces en Modo SPAN para poder escuchar tráfico de IPS o DLP sin ser intrusivo en la red. **IPsec VPN.** Deben ser soportadas tanto una CA Interna como una CA externa provista por un tercero. Deben ser soportados 3DES y AES-256 para las fases I y II de IKE. Debe soportar al menos los siguientes grupos Diffie-Hellman: Grupo 1 (768 bit), Grupo 2 (1024 bit), Grupo 5 (1536 bit), Grupo 14 (2048 bit). Debe soportar integridad de datos con md5 y sha1. Debe incluir soporte a las topologías VPNs site-to-site: Full Meshed (todos a todos), Star (Oficinas Remotas a Sitio Central) y Hub and Spoke (Sitio remoto a través del sitio central hacia otro sitio remoto). Soporte a VPNs client-to-site basadas en IPSEC. Debe tener la posibilidad de realizar VPNs clientless SSL para acceso remoto, sin necesidad de instalar un cliente. Soporte a VPNs tipo L2TP, incluyendo el soporte al cliente L2TP del Iphone. El cliente VPNs IPSEC debe soportar roaming (moverse entre diferentes redes/interfases y cambiar de dirección IP sin presentar desconexión de la VPN) y la funcionalidad de Auto-Connect. Debe incluir un método simple y central, de crear túneles permanentes entre gateways del mismo fabricante. El administrador debe poder aplicar reglas de control de tráfico, al interior de la VPN. Debe soportar VPNs tipo “domain based” y “route based”, usando al menos BGP y OSPF (requiere el blade de advanced networking). Debe incluir un mecanismo para mitigar el impacto a ataques de denegación de servicio DoS a IKE, haciendo diferencia entre conexiones conocidas y desconocidas. Debe poder establecer VPNs con gateways con direcciones IP dinámicas públicas. Soporte a compresión IP para VPNs client-to-site y site-to-site. Firewall debe soportar dispositivos móviles (USB) que se conecten de modo seguro (VPN) a través de un Escritorio Virtualizado seguro que no requiera instalación para asegurar la portabilidad y se mantenga la confidencialidad de los datos entregados vía encripción permanente de la información misma que debe estar disponible en el dispositivo móvil sin estar conectado a la VPN con la facilidad de poner aplicaciones portables. IPS. El IPS integrado, debe incluir al menos los siguientes mecanismos: Attack signatures, Protocol validation y Anomaly detection y Behavior-based detection. (requiere el blade de IPS). Los módulos de IPS Integrado y de Firewall, deben estar integrados ofreciendo de esta manera, dos líneas de defensa. El administrador debe poder configurar la inspección, solo para el tráfico entrante. El IPS debe proveer al menos dos políticas o perfiles predefinidos, para ser usados inmediatamente. Debe incluir una opción, que permita detener la inspección del IPS en el Gateway bajo condiciones de alta carga, definiendo estos límites basados en % de CPU y Memoria que el administrador decida. El IPS integrado, debe incluir la habilidad de detener temporalmente la inspección y bloqueo en el gateway, para efectos de “troubleshooting”. Este procedimiento debe realizarse de una forma fácil y rápida. El administrador debe poder activar automáticamente nuevas firmas, basados en parámetros de configuración definidos previamente (impacto en el desempeño, severidad de la amenaza, tipo de protección: server o client). Debe poder detectar y bloquear las siguientes tipos de amenazas : Protocol misuse, comunicaciones Outbound con malware, Intentos de Tunneling y ataques genéricos sin contar con firmas predefinidas. Para cada protección se debe incluir la siguiente información: Tipo de protección (cliente o server), severidad de la amenaza, Impacto en el desempeño, y nivel de confidencia. Por cada protección o por todas las protecciones soportadas, debe permitir adicionar excepciones basadas en origen, destino, servicio o la combinación de los 3 factores. Debe poder realizar captura de paquetes para protecciones específicas. Debe detectar y bloquear ataques de red y de aplicación, protegiendo al menos los siguientes servicios: Email, DNS, FTP, servicios de Windows (Microsoft Networking) y SNMP. Debe estar en capacidad de detectar y bloquear tráfico peer to peer (P2P), incluso si la aplicación utiliza cambio de puertos. El administrador debe poder definir objetos de red y servicios a excluir. Debe proteger contra ataques tipo DNS Cache Poisoning, y de esa manera prevenir a los usuarios el acceso a dominios bloqueados. Debe incluir protecciones para los protocolos POP3 e IMAP. Debe soportar y proteger protocolos de VoIP (H.323, SIP, MGP y SCCP), asegurando que todos los paquetes de VoIP son estructuralmente válidos. Debe detectar y bloquear aplicaciones que realizan control remoto, incluyendo aquellas que son capaces de hacer tunneling en tráfico HTTP. El administrador debe poder permitir chat MSN Messenger pero bloquear el Video. Debe incluir protección a vulnerabilidades Citrix ICA e implementar cumplimientos de protocolo. Debe permitir bloquear trafico entrante, saliente o ambos correspondiente a determinados paises, sin necesidad de actualizar manualmente los rangos IP correspondientes a cada pais. Seguridad Web. Debe incluir un mecanismo de detección que pueda bloquear gusanos basados en patrones conocidos. Debe proveer una interfase para adicionar nuevos patrones, así como de actualizar los nuevos liberados por el fabricante. (requiere el blade de WebSecurity). Debe incluir un mecanismo de detección que permita bloquear código ejecutable malicioso en el protocolo http, sin necesidad de requerir una forma especifica. De igual manera debe poder detectar potencialmente comportamientos maliciosos. A nivel de aplicación, debe incluir protecciones tipo Cross Site Scripting, LDAP injection, SQL Injection and Command Injection. Debe incluir una lista editable de comandos y de DN (Distinguished Names) a ser bloqueados. Debe incluir protecciones contra la revelación de la información, previniendo que un atacante pueda obtener información de un		

	website. Debe incluir al menos las siguientes protecciones: Header Spoofing, remover o cambiar un header especifico que pueda aparecer en la respuesta de http. Directory Listing prevention, identificar paginas web que contengan listas de directorio y que las pueda bloquear. Error concealment, bloquear o modificar mensajes de error en web servers en respuestas HTTP. Debe incluir al menos las siguientes inspecciones de protocolo http: HTTP Format Size enforcement, ASCII-only Request enforcement, ASCII-only Response Header enforcement, Header Rejection definitions y HTTP Method definitions. Las protecciones Web deben poderse configurarse por cada Servidor Web. Debe incluir protecciones para servicios Web tipo SOAP-based XML. Filtrado URL. El filtrado de URL debe ser basado en categorías y debe poderse incluir como un blade mas (requiere el blade de URL filtering). Debe cubrir mas de 20 millones de URLs en al menos 40 categorías incluidas las siguientes: Adult, advertisements, arts, chat, computing, criminal, drugs, education, finance, food, gambling, games, glamour & intimate apparel, government, hacking, hate speech, health, hobbies, hosting sites, job search, kids sites, lifestyle & culture, motor vehicles, news, personals & dating, photo searches, real estate, reference, religion, remote proxies, search engines, sex education, shopping, sports, streaming media, travel, Usenet news, violence, weapons, web based e-mail. Debe incluir un mecanismo de listas blancas y listas negras que permitan al administrador, negar o permitir URLs específicos, independientemente de la categoría. Debe permitir la creación de excepciones basadas en la definición de objetos de red. Debe proveer la opción de modificar la notificación de bloqueo, y redireccionar al usuario a otra página. La creación y modificación de políticas debe de ser de forma granular permitiendo usuarios del directorio activo, de la base de datos interna o identificados con un portal captivo, permitiendo tener usuarios no autenticados para que no requieran tener un usuario o password. Control de Aplicaciones. El filtrado de aplicaciones debe ser basado en categorías y debe poderse incluir como un blade mas (requiere el blade de App control). Debe cubrir mas de 4500 aplicaciones y mas de 250,000 widgets de redes sociales agrupadas en al menos 80 categorias. Debe poder alertar a los usuarios acerca del control de los usos, teniendo la posibilidad de cambiar por aplicacion o grupo de aplicaciones una pagina de bloqueo completamente customizable dentro de la misma herramienta de administracion y sin dependencia de conocimiento de HTML. Debe poder inspeccionar trafico encriptado. Advanced Networking. Debe soportar al menos los siguientes protocolos de routing: BGP, OSPF, RIPv1 y RIPv2 (requiere el blade de advanced networking). Debe soportar al memos los siguientes protocolos de multicast: IGMP, PIM-DM, PIM-SM. Weighted Fair Queuing (WFQ) debe soportarse para asignar un mínimo de ancho de banda a un grupo de conexiones o a una conexión específica. Debe soportar la asignación de pesos para la definición de prioridades en la asignación de ancho de banda. Debe poderse definir limites en el ancho de banda, para restringir aplicaciones no criticas de red. Debe soportar Low latency queuing (LLQ) e Integrated Differentiated Services (DiffServ). Debe incluir el balanceo entre servidores, de manera que no se necesite utilizar un balanceador externo para manejar tráfico de DMZ y LANs. Debe soportar al menos los siguientes métodos de balanceo: Server Load, Round Trip, Round Robin, Random and Domain. Debe soportar al menos 150 servicios/aplicaciones pre-definidos. Debe soportar Alta Disponibilidad y Balanceo de Carga de links de al menos 2 ISP, sin depender del uso de enrutamientos dinámicos o equipos externos dedicados. Aceleración & Clustering. Debe incluir balanceo de carga de gateways con sincronización de estados, sin necesidad de usar un balanceador externo, para al menos 5 gateways en un solo cluster. Debe proveer un mecanismo que permita la mejor utilización de todos los procesadores con que cuente el hardware. Administración de la Política de Red: Debe soportar diferentes perfiles de administrador, incluyendo al menos los siguientes: read/write y read/only. Las comunicaciones entre todos los componentes que pertenezcan a un solo dominio de administración (servidor de administración, gateways), deben establecer comunicaciones seguras a través del uso de certificados para el cifrado. Debe incluir una entidad CA (Certificate Authority) interna X.509, que genere certificados a los gateways y a los usuarios para una fácil autenticación en las VPNs. Debe incluir la habilidad de confiar en CAs externas, que soporten estandars PKCS#12, CAPI o Entrust. Debe incluir la opción de crear diferentes perfiles de IPS, que pueden ser aplicados a diferentes gateways. Debe incluir la opción de automáticamente habilitar nuevas protecciones de IPS basadas en: Severidad de la amenaza, Impacto de Desempeño y Nivel de Confidencia. Debe incluir una manera de marcar las protecciones de IPS para un futuro seguimiento o análisis. Debe incluir una herramienta de búsqueda, que permita fácilmente filtrar objetos de red. Debe también incluir la opción de buscar objetos duplicados (con la misma IP) y objetos no usados (en una regla o política) y una lista de las reglas en que un objeto especifico es usado. Debe incluir la opción de segmentar las reglas de acceso, usando etiquetas o títulos de sección y de esa forma organizar mejor la política. Debe incluir la opción de guardar la política completa o una especifica parte de la política. Se debe poder tener la opción de tener alta disponibilidad de administración, usando servidores de administración que se sincronizan con el servidor activo, sin necesidad de un dispositivo externo. Debe incluir un comprensivo mapa, que incluya los objetos de red y sus conexiones. Estos mapas pueden ser exportados a una imagen o a Microsoft Visio. Debe		

	incluir la habilidad de distribuir y aplicar centralizadamente nuevas versiones de software para los gateways. Debe incluir una herramienta que administre centralizadamente la licencia de todos los gateways, controlados desde la estación de administración. (requiere el blade de acceleration and clustering). Logging & Status. Los logs, deben ser parte del mismo sistema de administración (incluido en el Servidor Administración de la seguridad) y opcionalmente los administradores deben poder instalar servidores de Logs por separado. Los logs deben poder estar en el servidor de administración o en un servidor separado. Debe poder capturar paquetes automáticamente de eventos de IPS, para proveer un mejor análisis forense. Debe poderse diferenciar entre logs de usuarios regulares y los logs propios de la administración. Por cada coincidencia de una regla, se debe poder configurar alguna de las siguientes opciones: Log, Alert, Send and SNMP trap, send and email, o ejecutar un user defined script. Los logs deben ser transferidos con seguridad entre los gateways y el servidor de administración o el servidor de logs. De la misma manera desde y hacia la consola de administración del servidor. Debe incluir la opción de que dinámicamente bloquee una conexión activa desde la interfase gráfica, sin requerir la modificación de las reglas de acceso. Debe poderse exportar los logs en formato de base de datos. Debe poderse realizar un cambio automático de logs, basados en programaciones de tiempo o del tamaño del archivo. Debe permitir adicionar excepciones a las protecciones de IPS desde el log. Debe poder asociar cada IP correspondiente a usuarios internos con su correspondiente nombre de usuario y nombre de máquina, tomando esa información del Active Directory, sin necesidad de instalar ninguna aplicación en el Domain Controller ni en las PCs de los usuarios. Apartir de los logs encontrados para el IPS, se debe poder cambiar esa protección, ya sea para agregar excepciones o para cambiar la protección a modo protección. Monitoreo: Debe incluir una interfase gráfica de monitoreo, que facilite la revisión del status de los gateways. Debe proveer por lo menos la siguiente información por cada gateway: Sistema Operativo, Uso de Memoria, CPU, todas las particiones de disco y porcentaje de espacio libre en disco. Debe proveer el estatus de cada uno de los componentes de cada gateway (firewall, vpn, cluster, antivirus, etc.) Debe incluir el status de todos los túneles de VPN, site-to-site y client-to-site. Debe poderse configurar límites que tomen acciones cuando sean superados. Las acciones deben incluir: Log, alert, send an SNMP trap, send an email y execute a user defined alert. Debe incluir gráficas predefinidas de monitoreo vs la evolución del tiempo, del tráfico y los contadores del sistema: top de reglas de seguridad, top de usuarios P2P, túneles de vpn, tráfico de red, etc. Debe proveer la opción de generar gráficas personalizadas. (requiere el blade de Monitoring). Debe poderse grabar las vistas de tráfico y contadores del sistema a un archivo, para posteriormente poder verlo en cualquier momento. Debe incluir la posibilidad de agregar reglas dinamicas para temporalmente bloquear paquetes basado en origen, destino y servicio Debe poder reconocer funcionamientos inadecuados y problemas de conectividad entre dos puntos conectados a través de una VPN, y alertar y crear logs cuando el túnel de VPN se encuentre abajo. Management Portal: Debe incluir la posibilidad de ver las políticas de seguridad a través de un browser, administrar logs y usuarios dando acceso a gerentes y auditores sin necesidad de tener acceso total a la consola (requiere el blade de Management portal). Debe poderse acceder usando uno de los siguientes browsers: Internet Explorer, Firefox o Netscape. Debe incluir el soporte vía browser mediante la utilización de SSL. User Directory: Debe poderse integrar con un directorio LDAP, para autenticar y autorizar usuarios, basados en el perfil almacenado en el LDAP (requiere el blade de SmartDirectory). Debe poder hablar WMI con el directorio activo, para no requerir modificación del mismo y que nos brinde la posibilidad de crear reglas basadas en usuario, poder instalar un agente de identificación del dispositivo que soporte MAC y equipos Windows, así como contar con portal captivo para administrar invitados. Debe incluir la opción de extender el esquema de LDAP o el uso de una plantilla interna, para el uso de propiedades no almacenadas en el LDAP. Debe incluir una interfase gráfica que permita adicionar, eliminar, remover, y editar usuarios que están almacenados en el directorio LDAP. Debe incluir perfiles predefinidos para Microsoft AD, Novell and Netscape. Debe poderse realizar requerimientos a diferentes servidores LDAP, para tener un esquema de redundancia y encontrar usuarios distribuidos por múltiples servidores LDAP. IPS Event Analysis: Debe contar con una herramienta de manejo de eventos de IPS. (requiere el blade/hardware de SmartEvent). Debe permitir crear filtros basados en cualquier característica de la alerta de IPS como ip de origen y destino, servicio, tipo de evento, severidad del evento, nombre del ataque, pais de origen y destino, etc. Estos filtros deben poder ser asignados a diferentes líneas gráficas actualizadas a tiempos regulares que muestren todos los eventos que van apareciendo que cumplan con el filtro. Permitiendo asi que el operador se concentre en los eventos mas importantes para su red. Debe mostrar la distribución de eventos del IPS por paises en un mapa. Debe permitir agrupar los eventos en base a cualquier caracteristica de los mismos, pudiendo agrupar en varios niveles. Debe permitir realizar busquedas dentro del listado de eventos. Debe poder generar automaticamente pequeños gráficos o tablas de distribución de eventos, origenes y destinos, en la vista del listado de eventos. Debe incluir reportes predefinidos con los eventos detectados en la última hora, dia, semana y mes. Incluyendo al menos Eventos top, Origenes top, Destinos top, Servicios top, Origenes top con sus eventos		

	top, Destinos top con sus eventos top y Servicios top con sus eventos top Provisioning: Debe incluir la habilidad de enviar y ejecutar scripts en unos o mas gateways administrados centralizadamente. (requiere el blade de provisioning). Debe poderse programar backups en uno o mas gateways. Debe poderse administrar centralizadamente, las interfases de los gateways las rutas, los servidores DNS y demás parámetros de configuración. Debe contarse con la posibilidad de administrar cientos o miles de gateways a través del uso de perfiles, los cuales son aplicados a gateways con configuración similar, sin necesidad de crear uno para cada gateway. Control de Cambios: Debe contar con una solución que se integrare completamente al proceso de Change Management de ITIL de forma nativa (sin uso de terceros), con la capacidad establecer un proceso de revisión, audición y aprobación de cambios, todo esto desde la misma consola de administración. Debe incluir un sistema de control de cambios integrado al servidor de administración. Debe poder hacer un seguimiento visual de los cambios realizados, resaltando los cambios y listandolos. Debe poder generar reportes de cambios realizados durante una sesión, para control del administrador y de los auditores. Debe poder generar reportes de cambios realizados entre 2 sesiones diferentes, resumiendo todos los cambios realizados en el período de tiempo entre ambas sesiones. Debe contar con la opción de forzar el administrador a que deba requerir la aprobación de un gerente o supervisor antes de permitir la instalación de políticas. Correlación de Eventos y Reportes: Debe incluir una herramienta para correlacionar eventos de todas las funcionalidades del gateway y de equipos de terceras partes. Debe permitir la creación de filtros basados en cualquiera de las características del evento, tales como IP de origen y destino, servicio, tipo de evento, severidad del evento, nombre del ataque, país de origen o destino, etc. El administrador debe poder asignar estos filtros a diferentes líneas en un gráfico que sean actualizadas en intervalos regulares mostrando todos los eventos que concuerdan con ese filtro. Permitiendo que el operador se focalice en los eventos mas importantes. Debe mostrar la distribución de eventos por países en un mapa. Debe permitir agrupar los eventos en base a cualquier característica de los mismos, pudiendo agrupar en varios niveles. Debe permitir realizar búsquedas dentro del listado de eventos. Debe poder generar automáticamente pequeños gráficos o tablas de distribución de eventos, origenes y destinos, en la vista del listado de eventos. Debe detectar ataques de denegación de servicio, correlacionando eventos de todas las fuentes. Debe detectar el logueo de administradores fuera de horario regular. Debe detectar ataques para adivinar credenciales. Debe incluir reportes predefinidos con los eventos detectados en la última hora, dia, semana y mes. Incluyendo al menos Eventos top, Origenes top, Destinos top, Servicios top, Origenes top con sus eventos top, Destinos top con sus eventos top y Servicios top con sus eventos top. La herramienta de reportes debe soportar al menos 25 filtros (ej. Origen, destino, nombre del ataque, número de regla) que permita personalizar los reportes predefinidos a las necesidades del administrador (ej. Actividades web de un usuario específico). Debe soportar agendar reportes para que se ejecuten automaticamente para extraer información en periodos regulares de tiempo (diarios, semanales y mensuales). Tambien debe permitir al administrador la fecha y horario en que empezará a generar el reporte agendado. Debe soportar los siguientes formatos de reportes: HTML, CSV y MHT. Debe permitir la distribución automática de los reportes por correo electrónico, subiendolos en un servidor FTP/Web y utilizando un script externo para la distribución del reporte. El sistema de reportes debe proveer información consolidada sobre al menos: El volumen de conexiones que fueron bloqueadas por el gateway del perímetro IP de origen con más conexiones bloqueadas, con sus destinos y servicios. Reglas mas usadas por el gateway. Los ataques más detectados, determinando sus origenes y destinos. Cantidad de instalaciones y desinstalaciones de políticas. Servicios de red más usados. Actividad web, detallando los sitios más visitados y los usuarios mas frecuentes. Actividad SMTP, detallando las direcciones de origen y destino mas frecuentes. Actividad FTP, detallando los usuarios más frecuentes y los archivos más subidos y descargados. Los servicios que mas carga encriptada generaron. Usuarios VPN con las conexiones más duraderas. La plataforma de seguridad se recepcionará, por lo que el proveedor deberá considerar los demás insumos necesarios para la puesta a punto, puesta en marcha y entrega funcional del equipo requerido. La plataforma de seguridad deberá considerar la instalación, configuración, puesta a punto y puesta en marcha en las instalaciones de la UADY, por personal certificado por el fabricante. Los equipos ofertados, cuentan con garantía de refacciones por lo menos 5 años. LA plataforma de seguridad 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 UADY. EL LICITANTE GANADOR DEBERA ENTREGAR UN PLAN DE TRABAJO PRELIMINAR A LA CONSIDERACION DE LA UADY, PARA ACORDAR LOS AJUSTES DE LA VERSION FINAL QUE SE DEBERA REALIZAR. EL SISTEMA SE DEBERA ENTREGAR FUNCIONANDO, PUESTO A PUNTO Y OPTIMIZADO A SATISFACCION DEL PERSONAL RESPONSABLE DE TECNOLOGÍAS DE LA UADY. EL LICITANTE GANADOR DEBERA ENTREGAR LA MEMORIA TECNICA.		

62	Licenciamiento para Plataforma de Seguridad marca **CHECKPOINT**. Características: Licenciamiento para la plataforma de seguridad con que cuenta la UADY, CheckPoint SecurePlatform R75.20 o superior, y con administración de cluster con Appliances CheckPoint 9070. EL SIGUIENTE LICENCIAMIENTO ES PARA EL EQUIPO DE LA PARTIDA 58, POR LO CUAL DEBE DE SER COMPATIBLE CON EL MISMO. El licenciamiento requerido es el siguiente: 1 licencia para el Check Point gateway - Collaborative Enterprise Support – **Standard, por al menos 1 año**. 1 licencia para el Check Point Consola de Administración, Collaborative Enterprise Support – **Standard, por al menos 1 año.** 1 licencia para Renovación SSL- Collaborative Enterprise Support for Software Gateways, **por al menos 1año**. 2 Licencias para URL-Filtering Blade - Check Point URL Filtering Blade, **por al menos 1 año** - for mid appliances and pre-defined systems. La plataforma de seguridad deberá considerar la instalación, configuración, puesta a punto y puesta en marcha en las instalaciones de la UADY, por personal certificado por el fabricante. LA plataforma de seguridad 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 UADY. EL LICITANTE GANADOR DEBERA ENTREGAR UN PLAN DE TRABAJO PRELIMINAR A LA CONSIDERACION DE LA UADY, PARA ACORDAR LOS AJUSTES DE LA VERSION FINAL QUE SE DEBERA REALIZAR. EL SISTEMA SE DEBERA ENTREGAR FUNCIONANDO, PUESTO A PUNTO Y OPTIMIZADO A SATISFACCION DEL PERSONAL RESPONSABLE DE TECNOLOGÍAS DE LA UADY. EL LICITANTE GANADOR DEBERA ENTREGAR LA MEMORIA TECNICA.	1	$ 299,999.98
T O T A L:		**2**	**$ 1’340,332.98**

SEGUNDA.- “EL PROVEEDOR” 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 **$ 1’340,332.98 (SON: UN MILLÓN TRESCIENTOS CUARENTA MIL TRESCIENTOS TREINTA Y DOS PESOS, NOVENTA Y OCHO 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.**

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 proporcionar la capacitación para su manejo 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. 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;
b) Copia certificada del Acta en la que consta el nombramiento del Administrador Único;
c) Copia certificada del Poder que acredita la personalidad del apoderado general;
d) Copia de la identificación con fotografía del apoderado general;
e) 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;
f) Las proposiciones técnicas y económicas presentadas por **"EL PROVEEDOR"**;
g) Relación de las Dependencias donde serán entregados los equipos objeto de este contrato; y
h) Póliza de Fianza No. 88136135 00000 0000 de fecha 30 de marzo de 2012, expedida por: CHUBB DE MÉXICO, COMPAÑÍA AFIANZADORA, SOCIEDAD ANÓNIMA DE CAPITAL VARIABLE, por la cantidad de: **$ 160,839.96 (CIENTO SESENTA MIL OCHOCIENTOS TREINTA Y NUEVE PESOS, NOVENTA Y SEIS 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 TREINTA DÍAS DEL MES DE MARZO DEL AÑO DOS MIL DOCE.

POR **"LA UADY"**	POR **"EL PROVEEDOR"**
_____ **C.P. AURELIANO MARTÍNEZ CASTILLO** DIRECTOR GENERAL DE FINANZAS	_____ **SR. AUGUSTO VÍCTOR CAMELO PÉREZ** APODERADO GENERAL