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

CONTRATO NÚMERO 007-2013-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, **ALEF SOLUCIONES INTEGRALES, SOCIEDAD COOPERATIVA DE PRODUCCIÓN DE RESPONSABILIDAD LIMITADA DE CAPITAL VARIABLE,** A QUIEN EN LO SUCESIVO SE LE DENOMINARA **"EL PROVEEDOR"**, REPRESENTADO POR LA SEÑORA **MARÍA ERENDIRA RUIZ LUA**, EN SU CARÁCTER DE APODERADA 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, constituida inicialmente con la razón social de Alfa Soluciones Integrales, Sociedad Anónima de Capital Variable, por escritura pública número Treinta y Dos Mil Doscientos Cuarenta y Cuatro, de fecha dos de diciembre del año de mil novecientos noventa y tres, otorgada en la ciudad de México, Distrito Federal, ante la fe del Licenciado Manuel Enrique Oliveros Lara, titular de la Notaría Pública número Cien del Distrito Federal, inscrita en el Registro Público de Comercio de la ciudad de México, Distrito Federal, en el folio mercantil número 182583 (ciento ochenta y dos mil quinientos ochenta y tres), con fecha veintidós de diciembre del propio año de mil novecientos noventa y tres;

2. Que por escritura pública número Quince Mil Doscientos Diecinueve, de fecha veintisiete de febrero del año de mil novecientos noventa y siete, otorgada en la ciudad de México, Distrito Federal, ante la fe del Licenciado Benjamín Cervantes Cardiel, titular de la Notaría Pública número Ciento Sesenta y Siete del Distrito Federal, se protocolizó el Acta de Asamblea General Extraordinaria de Alfa Soluciones Integrales, Sociedad Anónima de Capital Variable, de fecha dieciocho de febrero del año de mil novecientos noventa y siete, celebrada en la ciudad de México, Distrito Federal, en la que se nombró como Administrador Único de la sociedad al señor Ángel Ruiz Lúa, al que se le otorgaron todas las facultades consignadas en el artículo Vigésimo de los estatutos sociales, sin limitación alguna, se nombró como apoderado general de la sociedad a la señora María Erendira Ruiz Lúa, con facultades de apoderada general para pleitos y cobranzas y actos de administración, con todas las facultades generales y aún las especiales que conforme a la Ley requieran poder o cláusula especial y se cambió la denominación de la sociedad de Alfa Soluciones Integrales, Sociedad Anónima de Capital Variable, por la de Alef Soluciones Integrales, Sociedad Anónima de Capital Variable, habiéndose inscrito esta escritura en el Registro Público de Comercio de la ciudad de México, Distrito Federal, en el folio mercantil número 182583 (ciento ochenta y dos mil quinientos ochenta y tres), con fecha veinte de mayo del propio año de mil novecientos noventa y siete;

3. Que por escritura pública número Treinta y Siete Mil Trescientos Veintinueve, de fecha veintidós de diciembre del año dos mil seis, otorgada en la ciudad de Naucalpan, Estado de México, ante la fe del Licenciado Álvaro Villalba Valdés, titular de la Notaría Pública número Sesenta y Cuatro del Estado de México y Notario del Patrimonio Inmueble Federal, con residencia en Naucalpan, se protocolizó el Acta de Asamblea General Extraordinaria de Alef Soluciones Integrales, Sociedad Anónima de Capital Variable, de fecha veintidós de diciembre del año dos mil seis, celebrada en la ciudad de México, Distrito Federal, en la que se acordó transformar la sociedad en una Sociedad Cooperativa de Responsabilidad Limitada de Capital Variable, se aprobaron las bases constitutivas de Alef Soluciones Integrales, Sociedad Cooperativa de Responsabilidad Limitada de Capital Variable, se designó como Socio Administrador al señor Ángel Ruiz Lúa, con las más amplias facultades para administrar la sociedad y se nombró como apoderada general de la sociedad a la señora María Erendira Ruiz Lúa, con facultades de apoderada general para actos de administración y con facultades de apoderada general para pleitos y cobranzas, con todas las facultades generales y aún las especiales que de acuerdo con la Ley requieran cláusula especial, habiéndose inscrito esta escritura en el Registro Público de Comercio de la ciudad de México, Distrito Federal, en el folio mercantil número 182583 (ciento ochenta y dos mil quinientos ochenta y tres), con fecha veinticuatro de mayo del año dos mil siete;

4. Que por escritura pública número Treinta y Ocho Mil Seiscientos Veinticuatro, de fecha diez de septiembre del año dos mil siete, otorgada en la ciudad de Naucalpan, Estado de México, ante la fe del Licenciado Álvaro Villalba Valdés, titular de la Notaría Pública número Sesenta y Cuatro del Estado de México y Notario del Patrimonio Inmueble Federal, con residencia en Naucalpan, se protocolizó el Acta de Asamblea General Extraordinaria de Alef Soluciones Integrales, Sociedad Cooperativa de Responsabilidad Limitada de Capital

Variable, de fecha tres de septiembre del año dos mil siete, celebrada en la ciudad de México, Distrito Federal, en la que se acordó modificar la cláusula segunda de las bases constitutivas, en virtud de que la sociedad es una Sociedad Cooperativa de Producción, la cual, sin modificar la denominación de la sociedad, quedó redactada como sigue: Segunda.- La sociedad se denominará Alef Soluciones Integrales, que irá seguida de las palabras Sociedad Cooperativa de Producción de Responsabilidad Limitada de Capital Variable o de su abreviatura S.C. de P. de R.L. de C.V, habiéndose inscrito esta escritura en el Registro Público de Comercio de la ciudad de México, Distrito Federal, en el folio mercantil número 182583 (ciento ochenta y dos mil quinientos ochenta y tres), con fecha veintiocho de marzo del año dos mil ocho;

5. Que por escritura pública número Ciento Diez Mil Doscientos Setenta y Cinco, de fecha treinta y uno de octubre del año dos mil ocho, otorgada en la ciudad de México, ante la fe del Licenciado Gerardo Correa Etchegaray, titular de la Notaría Pública Número Ochenta y Nueve del Distrito Federal, se protocolizó el Acta de Asamblea General Extraordinaria de Alef Soluciones Integrales, Sociedad Cooperativa de Producción de Responsabilidad Limitada de Capital Variable, de fecha diez de agosto del año dos mil ocho, celebrada en la ciudad de México, Distrito Federal, en la que se acordó modificar el objeto social de la sociedad y en consecuencia reformar la cláusula quinta de las bases constitutivas de la sociedad, habiéndose inscrito esta escritura en el Registro Público de Comercio de la ciudad de México, Distrito Federal, en el folio mercantil número 182583 (ciento ochenta y dos mil quinientos ochenta y tres), con fecha diecinueve de noviembre del propio año dos mil ocho;

6. Que en este otorgamiento comparece la señora María Erendira Ruiz Lúa, en su carácter de apoderada general de la sociedad con facultades para suscribir el presente contrato, nombramiento y facultades que constan en la escritura relacionada en la declaración 3 **DE "EL PROVEEDOR"**;

7. Que su domicilio fiscal es: Calle Río Nazas Número 116, entre Río Tiber y Río Poo, Colonia Cuauhtemoc, Delegación Cuauhtemoc, Código Postal 06500, de la ciudad de México, Distrito Federal; y

8. Que su Registro Federal de Contribuyentes es: ASI970227PZ4.

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**", el siguiente (**1**) equipo adquirido en la **Licitación Pública Internacional LA-931056978-I1-2013**, relativa a **Equipo de Cómputo, Audiovisual y Refrigeración:**

PARTIDA	EQUIPO O ARTICULO	CANT.	IMPORTE
77	Actualización de Software Antivirus Institucional MCafee, 1 Suite que ampara 2500 Licencias de EPS Antivirus Institucional, marca **McAffe End Point Protection Suite**; 100 Licencias para Mac Antivirus Institucional marca **McAfee Virus Scan para Mac**. Características: Renovación de la solución Antivirus institucional con que cuenta la Universidad Autónoma de Yucatán, McAfee Endpoint Protection Grant number: 5140527-NAI. La solución antivirus debe ofrecer a una protección contra código malicioso que cubra al menos contra virus, troyanos, gusanos y programas no deseados. Esta solución debe estar diseñada para funcionar en un ambiente de red, y el mismo fabricante debe proporcionar las herramientas para ser administrada de forma centralizada, tanto para la configuración, como instalación y actualizaciones. La solución antivirus deberá ser capaz de analizar en busca de código malicioso, el sistema donde esté instalado en tiempo real, cuando se acceda a un archivo o carpeta, así como los procesos que se ejecuten en memoria. La solución analizará archivos de discos locales de la computadora, unidades removibles, así como el contenido de unidades de red. La aplicación antivirus debe tener la opción de clasificar los procesos en base al riesgo que representan, y poder configurar el análisis en tiempo real en base a este parámetro. Así, debe permitir al menos tres configuraciones, alto, bajo y estándar. La solución debe realizar el análisis de archivos de comandos (scripts) mientras se están ejecutando. Dentro de los métodos de detección debe contar con la detección heurística. Deberá contar con un método de detección de amenazas en base a comportamiento. Cuando se detecta que una computadora está tratando de ser infectada a través de la red, el antivirus debe ser capaz de bloquear todas las conexiones de las computadoras que tratan de infectarla y reportar la dirección IP de tal computadora. El bloqueo puede ser por un tiempo específico o permanente. El bloqueo se terminará después de transcurrir el tiempo, manualmente desde la interface del antivirus o desde la consola de administración centralizada. Debe poder configurar un mensaje de alerta al usuario cuando se da una detección y mostrarle distintas acciones a aplicar. También permitirá aplicar acciones automáticas sin mostrar información al usuario. El antivirus deberá tener diferentes opciones para el manejo del registro de eventos de la aplicación. Entre la opciones se podrá determinar si se activa o desactiva el registro; nombre y ubicación del archivo de registro; tamaño máximo del archivo; poder ver el archivo desde la interface del antivirus. Permitirá al administrador configurar la solución para analizar todos los archivos, ó una lista de tipos de archivo predetermina por las firmas de fabricante. A esta lista de tipos de archivo el administrador podrá agregar otros tipos de archivo. El antivirus permitirá la creación de excepciones de archivos, carpetas o unidades disco para no ser analizadas. Para el análisis de archivos empacados (.zip, pkg, etc.), el antivirus permitirá habilitar o deshabilitar que se realice el análisis de los éstos. En caso de habilitarse, debe permitir fijar un tiempo máximo de análisis por cada uno de los archivos contenidos en el conjunto, y un tiempo máximo de análisis del archivo empacado completo. El sistema se integrará al sistema operativo de manera que creará opciones en el menú de contexto del explorador. Esto permitirá que apretando el botón derecho del Mouse sobre un archivo o carpeta, entre todas las opciones mostrará la de 'analizar en busca de virus'. El programa antivirus debe contar con la opción de crear análisis bajo demanda. Estos análisis se podrán configurar para realizarse inmediatamente o a una fecha y hora futura, y también se podrán configurar para realizarse una vez o repetirse a diferentes intervalos, días, semanas, meses, etc. Los análisis bajo demanda se podrán realizar a todas las unidades de la computadora o a carpetas, unidades o archivos específicos. Los análisis bajo demanda deberán dar la opción de analizar la memoria durante su ejecución en búsqueda de programas maliciosos o no deseados y terminarlos en caso de encontrarlos. Los análisis bajo demanda tendrán la opción de fijar un máximo, en porcentaje, de la utilización de recursos del sistema que se utilizarán durante el análisis. En cuanto al análisis, los análisis bajo demanda, permitirán las mismas opciones que en el análisis de tiempo real, como los tipos de archivo, tiempos de análisis, excepciones, archivos empacados, etc. La solución se debe integrar con los clientes MAPI de correo electrónico MS Outlook y Lotus Notes. Debe escanear en tiempo real el buzón de Outlook y la base de datos de Notes. También permitirá hacer escaneos bajo demanda de buzón y base de datos. Además de la integración con un sistema de administración central para el manejo de las alertas, el sistema antivirus deberá dar la opción de tener su propio sistema de alertas para generar notificaciones. Debe cubrir al menos los siguientes tipos de eventos: Análisis en tiempo real – detecciones, limpieza cuarentena, etc. Análisis bajo demanda - detecciones, limpieza cuarentena, etc. Restricción de acceso – eventos de restricción de acceso. Actualizaciones – eventos durante las actualizaciones del software. Dentro de las acciones que el programa puede realizar cuando detecta código malicioso está la de poner los archivos donde se dio la detección en cuarentena. Para manejar esta carpeta de cuarentena, se deben dar al menos las siguientes opciones: Determinar la ubicación de la carpeta de cuarentena. Eliminar los archivos de la cuarentena	1	$ 228,163.33

	automáticamente después de un periodo. Debe permitir habilitar o deshabilitar esta opción. En caso de habilitarla, se podrá fijar el número de días máximo en cuarentena. Ver el contenido en la cuarentena desde la interface del antivirus. Ver información acerca de la detección y del tiempo en cuarentena. Permitirá analizar el archivo desde esta interface; se podrá restaurar el archivo y borrar de la cuarentena. El fabricante deberá proporcionar una herramienta que permita recoger información acerca de su programa y su configuración para casos de problemas que deban ser atendidos por soporte técnico. La solución deberá contar con una herramienta que permita restablecer los valores de configuración originales en el antivirus, así como reinstalar los archivos de la aplicación. El software antivirus debe permitir al usuario cerrar (bloquear) puertos de comunicación de red, tanto de entrada como salida. En estos bloqueos puede determinar la protección contra cualquier proceso que los use o definir una lista. También permitirá la creación de una lista de excepción. Debe permitir al usuario o administrador crear una política o políticas para controlar las acciones que los procesos del sistema o de red pueden realizar sobre uno o varios archivos. Dentro de las acciones debe incluir al menos, lectura, escritura, ejecución, creación y borrado. Debe permitir al usuario o administrador crear una política o políticas para controlar las acciones que los procesos del sistema o de red pueden realizar sobre un directorio o carpeta. Dentro de las acciones debe incluir al menos, lectura, escritura, ejecución, creación y borrado. Debe permitir al usuario o administrador crear una política o políticas para controlar las acciones que los procesos del sistema o de red pueden realizar sobre un directorio o carpeta compartidos. Dentro de las acciones debe incluir al menos, lectura y escritura, aún cuando la carpeta se haya compartido con todos los permisos. Cuando se detecta que una computadora está tratando de ser infectada a través de la red, el antivirus debe ser capaz de bloquear todas las conexiones de las computadoras que tratan de infectarla. El bloque puede ser por un tiempo específico o permanente. El bloqueo se terminará después de transcurrir el tiempo, manualmente desde la interface del antivirus o desde la consola de administración centralizada. La solución antivirus también debe contar con protección y bloqueo preventivo de desbordamientos de buffer (buffer overflow) de aplicaciones. Esta protección será activada o desactivada sin afectar el proceso antivirus. Permitirá crear nuevas reglas para que el software prevenga desbordamientos de pila de otras aplicaciones. Capacidad de bloqueo de configuraciones por medio de una contraseña. Este bloqueo debe ser selectivo para partes específicas de la configuración, ó para toda la consola. Así como toda la configuración del sistema, esta contraseña de bloque debe ser configurada localmente y centralmente desde la consola de administración. El antivirus podrá instalarse de forma remota desde la consola de administración. La solución deberá contar con reglas de acceso que permitan dar protección preventiva en base a comportamiento, Las reglas deben prevenir al menos: Detener la creación y modificación remota de archivos ejecutables. Proteger el archivo con la lista de contactos. Prevenir la falsificación de proceso de Windows (spoofing). Prevenir la comunicación IRC. Prevenir el uso de ftp.exe. Prevenir que svchost ejecute programas no Windows. Prevenir contra programas de corro masivo locales. Controles contra contingencias de virus, como bloqueo de directorios compartidos. Prevenir la modificación de los archivos de la solución antivirus. Prevenir la modificación de archivos y configuración de los navegadores, Internet Explorer, Mozilla o FireFox. Prevenir la terminación del proceso antivirus. Detener programas que se intenten registrar en la 'auto-ejecución' (autorun). Detener programas que se intentan registrar como servicio. Detener la creación de archivos en carpetas importantes del sistema operativo. La solución antivirus debe prevenir que el proceso antivirus sea detenido, así como el agente de administración que le permite comunicarse con la consola central. El proveedor del software antivirus debe publicar al menos diariamente las bases de datos de firmas para la detección. La actualización de firmas debe realizarse de forma automática o manual, según la configuración del administrador. Se podrá hacer programada desde la consola central. Las actualizaciones de las firmas debe ser incremental. La solución debe contar con tecnología de detección de 'rootkits' por reglas y por comportamiento. Todas las opciones de configuración mencionadas antes, deben poderse configurar, habilitar, crear asignar desde la consola de administración central.Debe soportar sistemas operativos Windows a 64 bits. Programa contra programas espía. La solución contra programas espía (antispyware) debe ofrecer una protección contra programas no deseados. Esta solución debe estar diseñada para funcionar en un ambiente de red, y el mismo fabricante debe proporcionar las herramientas para ser administrada de forma centralizada, tanto para la configuración, como instalación y actualizaciones. El programa antispyware de integrarse con la solución antivirus. Deben usar el mismo programa de análisis y también deben usar las mismas bases de datos para la detección. Por lo tanto las actualizaciones serán con la misma frecuencia en el mismo grupo de archivos. Debe detectar al menos los siguientes tipos de programas no deseados: Programas espía (spyware). De publicidad (adware). Administración remota. Marcadores telefónicos (dialers). Descifrador contraseñas (password crakers). Bromas (jokes). Regitro de teclas (key loggers). Debe permitir configurar la misma reacción que el software antivirus, o una diferente para este tipo de programas. En la consola de administración central debe contar con un grupo de		

	reportes propios para distinguirlo de las detecciones antivirus. Deberá se capaz de hacer detección y limpieza en disco, memoria y registro de Windows. Debe detectar cookies en tiempo real para evitar que sean instaladas en el sistema. Programa de administración centralizada de aplicaciones de seguridad. Sistema de administración centralizada de las soluciones antivirus. La solución debe permitir la administración de políticas, configuración, actualización, notificaciones y respuesta a contingencias. Las tareas de administración deben poder realizarse desde una consola remota desde cualquier lugar de la organización. Los administradores pueden definir distintas políticas que contemplen todos los niveles de protección. Las características mínimas se describen a continuación. El sistema deberá ser administrado desde una interfase web, permitiendo el uso de navegadores de Internet para conectarse y trabajar con el sistema desde cualquier computadora que cuente con uno, y teniendo el usuario las credenciales de acceso necesarias. El sistema contará con tableros de control que muestren información gráfica de las funciones principales de las soluciones administradas, como detecciones, actualizaciones, eventos, y versiones de productos instalados, entre otras. El sistema permitirá que cada usuario del sistema de administración pueda generar las búsquedas necesarias para desplegar la información en el tablero de control, en base al perfil que tiene asignado. También el sistema debe permitir que cada usuario haga que sus propias búsquedas sean públicas, o de uso exclusivo. Cada usuario, según su perfil, también podrá hacer sus propios tableros de control, y organizarlos como le convenga, teniendo la opción de crear más de un tablero de control con diferentes búsquedas e información. El sistema deberá contar con un sistema propio para generar las búsquedas, para facilitar el uso de la herramienta y la obtención de la información, si necesidad de recurrir a una herramienta de terceros para generar las búsquedas que se usan para crear los tableros de control y los reportes. El sistema incluirá de fábrica reportes y búsquedas de todos los productos que maneje. Estos reportes y búsquedas se podrán modificar y copiar para que el cliente tenga sus propias búsquedas y rebotes en base a los de fábrica del producto. Es posible otorgar diferentes niveles de derechos a los usuarios asignándoles uno o más grupos de derechos. Los grupos de derechos darán acceso a los usuarios a configurar diferentes productos; por ejemplo puede permitir a un usuario configura el antivirus, pero no el agente de administración. También asignará permisos sobre diferentes grupos de equipos, así un administrador puede tener acceso a configurar o ver, ciertos equipos, y otros no. En caso de instalarse más de un servidor de administración, el sistema contará con la posibilidad de consolidar la información de todos los servidores de administración en uno sólo para generar reportes de eventos y de actualización de producto. Es posible planificar tareas para que se ejecuten en el servidor de administración seleccionado con el objeto de realizar el mantenimiento de la base de datos y del Repositorio. Asimismo, es posible comprobar el estado de cada tarea. Puede trabajar con la información, las notificaciones y los eventos de error del servidor de administración. Además, podrá ver y actualizar eventos del servidor, guardarlos en un archivo o imprimirlos. La solución permitirá la organización lógica de los equipos que serán administrados en un directorio. La organización del directorio, por ejemplo, puede ser por departamento funcional, ubicación geográfica o por dirección IP de la computadora. El directorio se podrá organizar en grupos y subgrupos; en el caso de los subgrupos se pueden especificar tantos subniveles como sea necesario dentro de cada grupo. El directorio permitirá hacer búsquedas de equipos, y tareas administrativas como moverlos entre grupos y borrarlos, entre otras. La organización por dirección IP se puede hacer basándose en la subred de los equipo o por rango de direcciones. Está organización permitirá que por medio de una tarea, los equipos sean enviados automáticamente a su grupo correspondiente por la dirección IP. El sistema permitirá la creación de etiquetas en los equipos para poder organizarlos en los grupos en base a éste criterio; para poder generar búsquedas y para filtrar reportes. Estás etiquetas se podrán generar, entre otras, en base a las siguientes características: Dirección IP, nombre del equipo, nombre del dominio, tipo de CPU, cantidad de memoria y sistema operativo. El sistema permitirá que la organización de los equipos se realice también en base al criterio de las etiquetas de forma automática. El directorio contará con un grupo donde se almacenarán los equipos para los que no se puede determinar su ubicación adecuada en el Directorio. La solución deberá utilizar las direcciones IP, los nombres de equipos, los nombres de dominio y los nombres de grupo para determinar dónde situarlos. El sistema de administración será capaz de verificar que todos los equipos del directorio tienen nombres únicos y, si ordena equipos por dirección IP, que los intervalos de direcciones IP y las máscaras de subred de IP asignadas a los sitios y los grupos en el directorio siguen las directrices de administración IP. El sistema deberá contar con métodos propios y automáticos para verificar el directorio: al menos debe ser capaz de buscar nombres de equipo duplicados y Verificar la integridad de la configuración de administración IP. El sistema de administración centralizada contará con repositorios de almacenamiento de software distribuidos, para ayudar a facilitar las descargas de software hacia los clientes finales. Debe tener al menos las siguientes características: El repositorio principal debe mantener la copia original de los paquetes, este repositorio es el servidor de administración. Cada repositorio de		

	almacenamiento distribuido mantiene una copia idéntica de los paquetes que están en el repositorio principal. Los repositorios de almacenamiento distribuidos serán creados y administrados desde el servidor central, a través de la consola. No será necesario instalar o correr ningún programa relacionado con el sistema de administración en estos servidores distribuidos, únicamente se deben copiar los paquetes de programas, no deben ser servidores dedicados a este sistema. Los repositorios distribuidos serán actualizados desde el servidor central. La descarga de los archivos hacia los clientes deberá ser al menos, dependiendo del tipo de servidor, a través de ftp, http o UNC. En caso de tener más de un repositorio distribuido, debe permitir la actualización selectiva de éstos. Cada tarea de actualización de los repositorios distribuidos se puede configurar para que sólo actualice los productos necesarios. Puede planificar tareas automáticas de descarga de actualizaciones al servidor central de administración y de réplica hacia los repositorios de almacenamiento o ejecutarlas bajo demanda. Estas tareas permiten mantener actualizados los repositorios principales y los repositorios de almacenamiento distribuidos. Las tareas se pueden crear con dependencia entre éstas, por ejemplo, se puede programar para que el servidor descargue las actualizaciones, y una vez terminada, haga la réplica de las actualizaciones los repositorios distribuidos. Puede establecer directivas de los productos (valores de configuración) antes de aplicarlas o usar directivas predeterminadas, y cambiarlas como sea necesario después de su aplicación. Estas políticas podrán aplicarse a computadoras en particular, grupos o todo el directorio. El sistema de administración debe permitir la administración de distintas aplicaciones además del antivirus de las computadoras de usuario. Debe ser capaz de administrar el antivirus de servidores Windows, NetWare, Linux, y antivirus para servidores de correo electrónico al menos. El sistema debe obtener y guardar información acerca de las computadoras que administra. La información como mínimo debe incluir el nombre del equipo, dominio, dirección IP, subred, sistema operativo, capacidad de disco duro, CPU y memoria RAM. El sistema debe permitir a los administradores crear tareas de actualización, instalación y escaneos sobre demanda para equipos específicos, grupos o todo el directorio. Las tareas serán programadas de acuerdo con, al menos, los siguientes valores: Diario, semanal, mensual, una vez, al arrancar el equipo, cuando está prendida sin usarse, inmediatamente, al firmarse y al hacer una conexión remota (dial-up). La instalación del agente se debe poder realizar desde la consola de administración, o usando herramientas de otros fabricantes, o manualmente en el equipo donde se quiere instalar. Debe contar con un medio automático por el cual el servidor de administración detecte las computadoras cuyos agentes no han mantenido comunicación con el servidor durante un tiempo y poder determinar cuales de esos agentes ya no están instalados o las computadoras ya no existen, y así poder tomar acciones al respecto. Debe permitir fijar el parámetro de tiempo (en días por ejemplo) por el cual el sistema debe determinar si un agente ya no está activo. Además de los tiempos en los que se ejecutan las instalaciones y actualizaciones de software, el agente debe mantener una comunicación constante con el servidor de administración. Este tiempo debe ser configurable e incluso poder desactivar esta comunicación, si que esto implique que el agente sea desactivado localmente. También debe permitir que administrador pueda forzar desde la consola la comunicación del agente al servidor. Esta función se podrá aplicar a un solo agente a todo un grupo, permitiendo también determinar un periodo de tiempo en el que aleatoriamente se forzará esta comunicación, en el caso de que sean muchos los agentes. El sistema deberá contar un mecanismo que permita al administrador hacer una actualización de todos los equipos en el momento que surja una actualización. Esta actualización general puede ser lanzada automáticamente en el momento que el servidor de administración encuentre una actualización en el sitio del fabricante, como una nueva firma o parche antivirus, ó manualmente el administrador la puede disparar desde la consola. También permitirá al administrador que productos se actualizarán y que tipo de actualizaciones hacer. Las actualizaciones deben cubrir todos los productos administrados desde el servidor, y dentro de cada producto incluyen nuevas versiones, actualización de firmas, parches y hot fixes. Esta actualización puede ser selectiva. El administrador podrá determinar que productos y que tipo de actualización será automática y cuales manuales, incluso poder configurar diferentes métodos o tipo dependiendo del producto o del grupo. El servidor de administración será capaz de descargar las actualizaciones desde el sitio del fabricante a través de tareas programadas. El servidor de administración generará reportes, además de la información en la consola, acerca de las versiones instaladas en los equipos, incluyendo versiones de software, parches, hotfixes, firmas de antivirus y todo lo relevante respecto a los productos administrados. Los reportes de la herramienta de administración deben generarse desde la misma consola. Los reportes permitirán generar filtros al ejecutarse y guardar plantillas de reportes. El sistema debe contar con reportes referentes a eventos del sistema. Siendo la administración del antivirus, debe contar al menos con reportes acerca de detecciones y actualizaciones antivirus, como los virus más detectados, las máquinas con más incidentes, las versiones instaladas. Debe especificar nombre del virus, tipo de virus, acción resultante. Debe permitir ir al detalle de los reportes una vez que se generó el reporte origina, así poder navegar en la información hasta llegar al		

	detalle del reporte. Debe proveer herramientas que permitan al administrador hacer tareas de la base de datos, como respaldos, restauraciones, mantenimientos y otros. Puede planificar una tarea: Sincronizar dominios para sincronizar los dominios seleccionados importados en el Directorio con sus equivalentes en la red. Esto se realiza con el fin de mantener actualizad el Directorio con la red de forma automática. El sistema de administración podrá determinar, por medio de búsquedas (escaneos), la presencia de parches de seguridad de Microsoft en los equipos administrados. Podrá crear perfiles de seguridad en case a reglas creadas por el administrador, así como plantillas predefinidas en el sistema. Estos perfiles buscarán la presencia de parches de Microsoft, algún archivo característico de una amenaza conocida, algún servicio o llave del registro. Esta función debe ser parte del sistema de administración centralizada, no una aplicación por separado. Debe contar con reportes acerca del cumplimiento de estas políticas. También debe integrarse con el módulo de notificaciones para poderlas generar en base a los resultados de estas búsquedas. El agente debe ser compatible con las versiones de 64 bits de los sistemas operativos Windows. El sistema debe permitir la importación de la información de computadoras del Directorio Activo de Microsoft. La importación se debe poder programar para que se realice periódicamente. Así el sistema reflejará las nuevas computadoras que van siendo agregadas al Directorio activo También permitirá que se puede hacer un mapeo entre los grupos del sistema de administración centralizado con los grupos del directorio activo. El sistema podrá auditar al menos las siguientes acciones: inicios de sesión en el sistema, cambio de perfiles o roles de usuarios del sistema, cambio de contraseñas, desinstalación de los agentes por eliminación, cambios en las políticas de configuración de los productos administrados, agregar o borrar componentes del directorio, renombrar componentes del directorio. Debe permitir que las computadoras sean administradas e identificadas por el nombre o por la dirección física de la tarjeta (MAC address). En el caso de computadoras que tienen más de una dirección física (MAC) - una portátil con una "dock station" por ejemplo- el sistema debe ser capaz de identificar que se trata del mismo sistema, y tratarlo como uno solo, sin duplicar la información. El sistema contará con un mecanismo para detectar máquinas que están conectadas a la red, y determinar si estas computadoras ya son administradas por el sistema central de administración del antivirus. Como acciones ante computadoras no administradas se les puede enviar la instalación del agente de administración y con ello el antivirus o enviar notificaciones al (los) administrador(es). Deberá contar también con reportes específicos de este componente. El sistema enviará notificaciones de eventos que sucedan en sus componentes. Las notificaciones serán en base a reglas definidas por el administrador. Estas reglas utilizarán al menos los siguientes parámetros: Nivel del directorio. Se podrá determinar a que nivel del directorio aplicará cada regla. Por ejemplo enviar una notificación únicamente si se detecta un virus en el grupo “dirección general”. Sistema Operativo. Producto. Por ejemplo un evento en el servidor de administración o en algún cliente. Tipo de evento. Puede ser una detección de virus, una actualización, etc. Tipo de notificación. Correo electrónico, SNMP, etc. El sistema de administración debe soportar Microsoft Clustering Services para alta disponibilidad El sistema de administración permitirá controlar las actualizaciones para maximizar la protección y minimizar el tráfico en la red. Se pueden configurar tareas de actualización por separado, para actualizar clientes con cualquier combinación de firmas de antivirus, motores y paquetes de actualización de productos en el repositorio. Sistema de prevención de intrusos para los sistemas. La solución ofrecida debe contar con un sistema de protección de intrusos para las computadoras que se integre con el sistema de administración centralizado, para su instalación y administración de actualizaciones y políticas. Está solución debe contar con las siguientes características. La solución de IPS de sistema debe ser un programa que se instala en la computadora y protege al mismo sistema. Debe contar con al menos los siguientes componentes: Prevención de intrusos (IPS). Firewall. Bloqueo de aplicaciones. En componente IPS debe contar con diferentes métodos de detección que permitan bloquear y registrar actividad maliciosa en la computadora. Debe contar con al menos los siguientes métodos: Detección por firma. Patrones de caracteres que si son detectados en el flujo de la información indican al IPS de sistema que es un ataque, con esta función se detienen los ataques conocidos. Detección por firma 2. las firmas deben estar diseñadas para aplicaciones y sistemas operativos específicos. Detección por comportamiento. Este método se basa en el comportamiento de las aplicaciones para detectar actividad maliciosa, esto permitirá detener ataques aun cuando no existe una firma específica, ataques día-cero. El IPS creará eventos en la consola central cuando detenga un ataque, en base a esta información el administrador podrá crear excepciones, que evitarán la aplicación de la regla cuando se cumplan los criterios de la excepción. También permitirá al administrador, en base esta información de los eventos, crear una lista de aplicaciones seguras, a las que no se le aplicarán las reglas de IPS. El componente Firewall debe funcionar como filtro entre la computadora y la red donde está conectada. El firewall debe utilizar al menos criterios como la dirección IP, puerto TCP o UDP y tipo de paquete para aplicar los criterios de bloquear y dejar pasar. Estos criterios deben aplicarse para tráfico entrante y saliente. El firewall debe usar tecnología de “Stateful packet		

	filtering" y "stateful packet inspection". El firewall debe permitir poner las máquinas en cuarentena, donde esta cuarentena permitirá la comunicación con otros puntos de la red, con tantas restricciones como la política determinada por el administrador lo especifique. El firewall podrá aplicar una política diferente, dependiendo en donde se encuentre conectada la computadora. Por ejemplo si la máquina de un usuario móvil está conectada a la red de la organización usará una política diferente a si está conectada a una red pública. El software será capaz de determinar cuando la máquina está conectada en diferentes redes. Para la creación de las reglas del firewall se deben basar, al menos, en los siguientes criterios. Tipo de conexión (red o inalámbrica). Protocolos IP y ni IP. Tráfico de entrada o salida o los dos. La aplicación que generó el tráfico. El puerto o servicio usado por la computadora, ya sea como receptor u origen. El puerto o servicio usado por la computadora remota, ya sea como receptor u origen. Dirección IP del origen o el receptor. El momento del día o la semana en que el paquete fue enviado o recibido. El componente de bloqueo de aplicaciones monitorea las aplicaciones que se están ejecutando y las bloque o las permite. El administrador podrá crear las reglas que permitirán o evitarán la ejecución de las aplicaciones en las máquinas cliente. El bloqueo de aplicaciones también permitirá detener aplicaciones que tratan de ligarse con otros procesos para ejecutarse, cuando estas aplicaciones son programas maliciosos. El administrador podrá determinar si se aplican los dos tipos de bloqueo, el de ejecución y el de ligado de aplicaciones, o los dos. Deberá considerar el control de dispositivos que cuente con las siguientes funcionalidades y características: Proporcionar o restringir el acceso a dispositivos USB, Floppy, CD´s y Carpetas compartidas. El módulo Antimalware deberá evitar una infección provocada por la ejecución del archivo Autorun.inf contenido en un dispositivo de USB al momento de ser conectado en la estación de trabajo. Para los dispositivos USBs, Floppy, CD´s y Carpetas compartidas, el antimalware deberá permitir al usuario hacer modificaciones en el contenido del dispositivo, permitir que el usuario tenga un control total sobre el dispositivo, permitir que el usuario únicamente tenga permisos de solo lectura sobre el dispositivo, permitir que el usuario tenga únicamente permisos de lectura y ejecución sobre el dispositivo, permitir que el usuario pueda tener acceso al contenido del dispositivo, Siendo cada una de estas configuraciones independientes para cada uno de los dispositivos a proteger. Protección de equipos MAC. Exploración en el momento del acceso para buscar virus y amenazas siempre que se acceda a un archivo. Detecta automáticamente infecciones por virus en el momento en que intentan infectar los sistemas Macintosh, PC y Unix. Además, puede verificar si existen amenazas en mensajes y adjuntos de Apple Mail. Protege sus usuarios cuando guardan o abren archivos desde unidades de red compartidas. Utiliza el análisis heurístico y la detección genérica, que toman la iniciativa de proteger contra virus nuevos y todavía desconocidos. Administración desde la consola centralizada lo cual permite la implementación, y la configuración de políticas. Capacidad de programar exploraciones completas del disco a intervalos convenientes, como durante la noche o durante las horas de menor demanda. Capacidad de programar actualizaciones automáticas diaria s o semanales, permitiendo la actualización y limpieza automáticas que protege contra descargas infectadas desde Internet y evita innumerables horas de tiempo perdido para recuperar y recrear el trabajo perdido. CERTIFICACIONES: Al menos 2 Ingenieros certificados por el fabricante en las siguientes soluciones: Certificación en McAfee ePolicy Orchestrator. Certificación en McAfee VirusScan Enterprise. Certificación en McAfee Host Intrusion Prevention. Certificación en McAfee Data Loss Prevention. El personal técnico contará con la experiencia en ambientes de seguridad informática. Avalada la experiencia en cursos de Seguridad Informática impartido por la UNAM, ITESM, ITAM. Etc. Validado por el fabricante que el proveedor es distribuidor autorizado y certificado para comercializar las soluciones propuestas.		
T O T A L:		**1**	**$ 228,163.33**

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 **$ 228,163.33 (SON: DOSCIENTOS VEINTIOCHO MIL CIENTO SESENTA Y TRES PESOS, TREINTA Y TRES 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 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;
b) Copias certificadas de las Actas en las que constan: el cambio de la denominación de la sociedad; la transformación de la misma a Sociedad Cooperativa de Responsabilidad Limitada de Capital Variable y los nombramientos del Administrador Único y de la apoderada general; el cambio a Sociedad Cooperativa de Producción; y la de modificación de su objeto social;
c) Copia de la identificación con fotografía de la apoderada 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. III-444489-RC, Serie y Folio DF204626 de fecha 27 de marzo de 2013, expedida por: FIANZAS ATLAS, SOCIEDAD ANÓNIMA, por la cantidad de: **$ 23,603.10 (VEINTITRÉS MIL SEISCIENTOS TRES PESOS, DIEZ 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	**SRA. MARÍA ERENDIRA RUIZ LÚA**
DIRECTOR GENERAL DE FINANZAS	APODERADA GENERAL