Universidad de Costa Rica
Vicerrectoría de Administración
Oficina de Suministros
Teléfono: 2511-5027 Fax: 2511-4161

LICITACIÓN ABREVIADA No. 2012LA-000007-UADQ
" RENOVACIÓN O ADQUISICIÓN DE LICENCIAS ANTIVIRUS Y ANTISPYWARE 2012"

En cumplimiento de lo dispuesto en los artículos Nº 7, 8 y 9 de la Ley de la Contratación Administrativa y en los artículos Nº 9, 10 y 11 del Reglamento General de la Contratación Administrativa.

RESULTANDO QUE,

1. Que la Unidad de Adquisiciones de la Oficina de Suministros. recibe la solicitud Geco No. 2012-758 del Centro de Informática
2. De conformidad con lo que establecen los artículos 7 de la Ley de Contratación Administrativa y 8 del Reglamento de Contratación Administrativa, la unidad solicitante emite la solicitud indicada con su respectiva decisión inicial.

CONSIDERANDO QUE

1. Se estima esta contratación en la suma de ¢35.000.035,27 (Treinta y cinco millones treinta y cinco colones con 27/100).
2. Se dispone de contenido presupuestario aprobado por un monto de ¢35.000.035,27 (Treinta y cinco millones treinta y cinco colones con 27/100).
3. Que el requerimiento de la unidad solicitante, resulta congruente con el Programa de Adquisiciones de la Institución, publicado por la Universidad de Costa Rica en la Gaceta No. 17 el día 24 de enero del año 2012.
4. Se cuenta con el recurso humano y la infraestructura administrativa suficiente para verificar el fiel cumplimiento del objeto de la contratación.

POR TANTO

Esta oficina dispone iniciar los trámites utilizando la modalidad de Licitación Abreviada, de conformidad con lo que establece el artículo 44 de la ley de Contratación Administrativa y el artículo 97 del Reglamento de la ley de Contratación Administrativa y a los límites de contratación establecidos por la Contraloría General de la República, publicados en el Diario Oficial La Gaceta No.41 del viernes 27 de febrero el 2012.

Sabanilla de Montes de Oca, a los 12 días del mes de marzo del 2012.

MBA. Rosibel González Cordero
Jefe, Unidad de Adquisiciones

Universidad de Costa Rica
Vicerrectoría de Administración
Oficina de Suministros
Teléfono: 2511-5027 Fax: 2511-4161

LICITACIÓN ABREVIADA No. 2012LA-000007-UADQ
" RENOVACIÓN O ADQUISICIÓN DE LICENCIAS ANTIVIRUS Y ANTISPYWARE 2012"

La Oficina de Suministros, recibirá ofertas por escrito hasta **las 10:00 horas del día 19 de marzo del 2012**, para la contratación indicada.

Los interesados podrán obtener el cartel mediante las siguientes páginas de internet http://osum.ucr.ac.cr/ Módulo Licitaciones ó **http:// www.merlink.co.cr, cejilla concursos, consulta de concursos fuera de línea.** . O bien podrán retirarlo en la Oficina de Suministros de la Universidad de Costa Rica, ubicada en Sabanilla de Montes de Oca , de las Instalaciones Deportivas 250 metros al este y 400 metros al norte.

Los interesados en participar que adquieran el cartel por este medio, deberán enviar al fax: 2511-3785 los datos de la empresa, número telefónico, fax y el nombre de la persona a quien contactar en caso necesario, el incumplimiento de este requisito exonera a la Unidad de Adquisiciones la no comunicación de prórrogas, modificaciones o aclaraciones al concurso.

Sabanilla de Montes de Oca, 12 de marzo del 2012.

MBA. Rosibel González Cordero.
Jefe, Unidad de Adquisiciones.

Universidad de Costa Rica
Vicerrectoría de Administración
Oficina de Suministros
Teléfono: 2511-5027 Fax: 2511-4161

LICITACIÓN ABREVIADA No. 2012LA-000007-UADQ
" RENOVACIÓN O ADQUISICIÓN DE LICENCIAS ANTIVIRUS Y ANTISPYWARE 2012"

La Oficina de Suministros, recibirá ofertas por escrito **hasta las 10:00 horas del día 19 de marzo del 2012**, para la contratación indicada.

1. Objetivo de la Contratación.

Las licencias institucionales de antivirus, con que cuenta actualmente la Universidad de Costa Rica, deben ser renovadas a partir del año 2012. Esta renovación es de gran importancia ya que provee a la Universidad de herramientas de protección antivirus y antispyware. La modalidad de protección antivirus con que cuenta la UCR en la actualidad, es la de consola centralizada, la cual brinda adecuadas posibilidades de administración y descentralización, por lo que se desea continuar con esta modalidad de administración de antivirus para este nuevo período.

1.1. Objetivos específicos:

Renovación o adquisición de 4002 licencias y soporte de antivirus tipo corporativo, con consola de administración de Antivirus, Anti-spyware, y software para prevención de intrusos (Host Intrusion Prevention - HIPS), realizando la instalación del antivirus en estaciones por medio de agentes, con una vigencia de dos (2) años de licenciamiento, y dos (2) años de soporte técnico local.

La adjudicación se realizará en un único renglón.

2. Fiscalizador Técnico de la contratación:
Para la ejecución del objeto de contratación, la Universidad de Costa Rica designa al Centro de Informática como Fiscalizador Técnico. Una vez adjudicado el proceso se dará a conocer el nombre del Profesional responsable por parte del Centro de Informática.

3. Obligaciones de los oferentes:

3.1 Deberán presentar las ofertas en forma ordenada, separando la información legal, técnica y de precios en forma clara, además deberán presentarse en formato digital tipo PDF.

3.2 La empresa contratada no podrá ceder o transferir los derechos u obligaciones derivados del contrato, ni los términos y condiciones aplicables.

4. Derechos y prerrogativas de la Universidad de Costa Rica:
Queda a criterio de la Universidad de Costa Rica durante el plazo de estudio de las ofertas, solicitar a los participantes las aclaraciones que se consideren necesarias.

5. Especificaciones Técnicas

5.1 Renglón Único: Renovación o adquisición de cuatro mil dos (4002) licencias con una vigencia de dos (2) años de licenciamiento, y dos (2) años de soporte técnico local, de antivirus tipo corporativo, con consola de administración de Antivirus, Anti-spyware, y software para Prevención de Intrusos (Host Intrusion Prevention - HIPS), y con instalación de antivirus en estaciones por medio de agentes.
El proveedor deberá indicar por separado el precio de las licencias y el costo del soporte técnico local.

5.1.1 Características Básicas

El adjudicatario acepta entregar licencias nuevas de la última versión del software antivirus corporativo (Antivirus, Anti-spyware y Prevención de Intrusos) en modalidad consola, para la renovación o sustitución de las actuales, y ofrecerlas con una vigencia de dos (2) años de licenciamiento y dos (2) años de soporte técnico local, y todas con la misma fecha de vencimiento. Los derechos de uso de las licencias del Software deberán ser perpetuos.

Las licencias de Antivirus y Antispyware con que cuenta actualmente la Universidad son 4002 licencias de antivirus y antispyware Trend Micro administradas a través de una consola centralizada denominada “Control Manager”.

5.1.2 Requerimientos técnicos mínimos para la Consola de Administración de Antivirus

La Consola Antivirus deberá cumplir con las siguientes características técnicas **mínimas:**

5.1.2.1 Consola para administración centralizada de los clientes Antivirus, Anti-Spyware, y software para prevención de intrusos (Host Intrusion Prevention – HIPS).

5.1.2.2 La consola de administración no debe requerir el uso de MMC (*Microsoft Management Console*), como requisito indispensable para su instalación.

5.1.2.3 La consola de administración no debe requerir el uso de Microsoft Data Access Components (MDAC) o Windows DAC como requisito para su operación.

5.1.2.4 Consola central compatible con los siguientes sistemas operativos: Microsoft Windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows Server 2008 x64 SP1, Microsoft Windows XP Professional SP2 o superior, Microsoft Windows Vista SP1, Microsoft Windows Vista x64 SP1, Microsoft Windows 7, Microsoft Windows 7 x64

5.1.2.5 La consola de administración no debe requerir el uso de la infraestructura de mensajería denominada “Microsoft Message Queue”, como requisito para su instalación.

5.1.2.6 La consola debe estar en capacidad de administrar en forma integrada, la solución de seguridad para dispositivos móviles Symbian, Windows Mobile, y Android.

5.1.2.7 Incluir un agente que se instale en cada computadora de escritorio, computadora portátil y servidor, y que sirva como medio de comunicación entre las estaciones y la consola de antivirus.

5.1.2.8 Capacidad para la instalación por web del agente, o por medio de un login script ejecutable vía remota.

5.1.2.9 La Consola de Administración debe poseer su propio gestor de Base de Datos, para lo cual no debe requerir licencias adicionales en el servidor de administración o cualquier computadora personal dentro o fuera de la red de la UCR.

5.1.2.10 Almacenar todos los informes sobre la detección de virus, spyware, o spam, en su propia base de datos.

5.1.2.11 El software debe permitir la instalación de un número ilimitado de servidores, consolas remotas o descentralizadas, y repositorios, a fin de facilitar la administración.

5.1.2.12 Las consolas descentralizadas deberán permitir su instalación en los siguientes sistemas operativos: Microsoft Windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows Server 2008 x64 SP1, Microsoft Windows XP Professional SP2 o superior, Microsoft Windows Vista SP1, Microsoft Windows Vista x64 SP1, Microsoft Windows 7, Microsoft Windows 7 x64

5.1.2.13 Permitir agregar usuarios de tipo administrador global, administrador de grupo, revisor global, revisor del sitio. Los revisores solo deben tener acceso de lectura.

5.1.2.14 Los administradores de la consola globales o grupales, podrán realizar las siguientes acciones: Conexiones al servidor de antivirus, cambio de perfiles o roles, cambio de contraseñas, desinstalación de los agentes, cambios de políticas, agregar o borrar sitios, grupos, computadoras o cuentas, renombrar sitios, grupos o máquinas.

5.1.2.15 Las estaciones se podrán actualizar y comunicar con la consola antivirus por medio de nombres (DNS), o por direcciones IP ubicadas en diferentes subredes.

5.1.2.16 La consola debe funcionar en un ambiente en el cual los equipos de cómputo, no se encuentren registrados en un dominio Active Directory de Microsoft.

5.1.2.17 Permitir la inclusión y eliminación en la consola, de equipos que no pertenezcan a ningún dominio windows.

5.1.2.18 Posibilidad de clasificar las computadoras por rangos de dirección IP, máscara de red, u otras características comunes como equipos sin antivirus o equipos no actualizados.

5.1.2.19 Capacidad para convertir un cliente instalado en un repositorio remoto de actualizaciones, para poder actualizar otros clientes desde él o poder extraer los archivos de actualización y trasladarlos manualmente a otros clientes, minimizando así el uso del ancho de banda. Sin necesidad de instalar módulos adicionales para tales fines.

5.1.2.20 Permitir la replicación del software en forma manual o automática, a través de tareas, para las actualizaciones e instalaciones.

5.1.2.21 Permitir la creación de configuraciones de políticas por grupo, dominio o maquina individual.

5.1.2.22 Permitir ver el catálogo de políticas por cada producto, y obtener una copia a la política de cada producto, para generar una nueva sin afectar la política original.

5.1.2.23 La configuración establecida para un determinado cliente debe poder ser exportada, tanto desde la Consola Central, como desde el mismo cliente, a fin de ser importada hacia otros clientes, en caso necesario.

5.1.2.24 Capacidad para recopilar la información de inventario básica sobre el hardware de cada computadora. (Ejemplos: Procesador, memoria ram, sistema operativo).

5.1.2.25 Detectar cualquier equipo nuevo que se conecte a la red.

5.1.2.26 Deberá ofrecer la siguiente información mínima sobre los equipos administrados: Nombre del equipo, Sistema operativo, Dirección IP asignada o MAC Address, Antivirus instalado, Cantidad de virus encontrados

5.1.2.27 La Consola de Administración deberá visualizar las amenazas que se han presentado en cada uno de los clientes, brindando el nombre de archivo donde fue detectada y la acción que el Producto tomó para anular la amenaza.

5.1.2.28 Verificar si una computadora tiene agente o antivirus, y permitir tomar una acción al respecto, como por ejemplo enviar una instalación de antivirus.

5.1.2.29 Capacidad para generar notificaciones a través de correo electrónico.

5.1.2.30 Generar reportes, sobre cobertura de Anti-virus, Anti-Spyware, Prevención de intrusos, y Control de Acceso a la Red, indicando información tal como clientes con mayor porcentaje de alertas, comparativas de alertas (diarias, mensuales o anuales), porcentajes de alertas de las respectivas amenazas, y amenazas con mayor intento de incidencia. Cada reporte debe tener la opción de efectuar consultas por equipos, virus, horas o fechas. Los reportes deben poder exportarse al menos hacia alguno de los siguientes formatos: XML, PDF, HTML.

5.1.2.31 El agente deberá efectuar la instalación del software antivirus, antispyware y de prevención de intrusos (HIPS), de forma automática sin interrupción del usuario

5.1.2.32 Debe permitir proteger con contraseña la configuracion del antivirus para que no sea alterada. Esta configuración deberá estar disponible, en el momento de ingresar la contraseña en el cliente.

5.1.2.33 Capacidad para crear políticas para usuarios móviles, a fin de ofrecer una protección diferente cuando este fuera de la red corporativa

5.1.2.34 Capacidad para definir políticas de configuración por grupo de equipos, con la posibilidad de configurar la función de herencia en subgrupos.

5.1.2.35 Capacidad para relacionar las consolas descentralizadas en una jerarquía administrativa, para generar reportes de uno o varios niveles de la estructura

5.1.2.36 Capacidad para heredar tareas y políticas en la estructura jerárquica de consolas descentralizadas.

5.1.2.37 La consola debe permitir la importación o exportación de las configuración de los clientes a través de archivos XML, a fin de facilitar su transportabilidad.

5.1.2.38 A fin de prevenir la fuga de información, la consola debe poseer un modulo que active o desactive el funcionamiento de los dispositivos de almacenamiento removible, o de comunicación externos. (Ej. Unidades de CD/DVD, llaves USB, adaptadores de red externos, etc.). Sin necesidad de módulos adicionales para su operación.

5.1.3 Requerimientos técnicos mínimos para el software Antivirus en estaciones de trabajo, computadoras portátiles y servidores.

El antivirus que se adquiera deberá cumplir con las siguientes características técnicas **mínimas**:

5.1.3.1 Sistemas Operativos Microsoft en los que debe funcionar: Microsoft Windows XP/Vista/7, Windows Server 2000/2003/2008.

5.1.3.2 Sistemas operativos Mac en los que debe funcionar: MacOS X 10.4 o posterior.

5.1.3.3 Sistemas operativos Linux en los que debe funcionar: Linux RHEL 5/6, Suse Enterprise Server.

5.1.3.4 Debe prevenir posibles infecciones a través de dispositivos de almacenamiento USB, archivos accesibles vía internet, correo electrónico, archivos compartidos, discos compactos y otros dispositivos de almacenamiento externo.

5.1.3.5 Brindar protección antivirus contra archivos maliciosos, verificando cualquier archivo creado, accedido o modificado

5.1.3.6 Brindar protección antivirus de WEB verificando el tráfico entrante y saliente de los navegadores, a través de filtros para los protocolos de red.

5.1.3.7 Brindar protección antivirus de correo electrónico, que verifique los correos recibidos y enviados asi como los archivos adjuntos. Debe verificar los siguientes protocolos POP3, SMTP, IMAP. Asi como conexiones seguras POP3 SSL, SMTP SSL e IMAP SSL.

5.1.3.8 Brindar protección antivirus de mensajería instantánea, verificando este tipo de comunicación establecida a través de Google Talk, MSN, o Yahoo Messenger.

5.1.3.9 Brindar protección antivirus en archivos compactados, sin importar el número de niveles de compresión, en los siguientes formatos: .zip, .rar, .arj, .cab, .lzh, .tar, .gz, ace, izh, y upx

5.1.3.10 Brindar auto-protección a los servicios y procesos del antivirus.

5.1.3.11 El antivirus debe contar con un programa residente en la memoria que verifique todos los archivos, para detectar virus en el momento en que son accesados a través de la red o en forma local, tanto archivos comprimidos como archivos tipo “macro”, incluidos en documentos.

5.1.3.12 El antivirus debe estar en capacidad para tomar distintas acciones cuando sea detectado un virus, ataque o programa no deseado: preguntar al usuario, bloquear el acceso al mismo, intentar desinfectar o borrar el archivo de acuerdo a la configuración previamente establecida, en caso positivo de desinfección restaurar el objeto, o en caso negativo de desinfección moverlo a cuarentena y/o borrarlo.

5.1.3.13 El antivirus debe estar en capacidad de crear una copia de seguridad del objeto, antes de intentar desinfectarlo o borrarlo.

5.1.3.14 El procedimiento de actualización debe utilizar la tecnología tipo incremental, a fin de minimizar el ancho de banda consumida por la misma.

5.1.3.15 Las actualizaciones diarias de los componentes del producto se deben realizar en tiempo real desde Internet o a través de un repositorio distribuido, en forma automática y sin necesidad de intervención del usuario.

5.1.3.16 Permitir actualizar de forma manual todos sus componentes y definiciones de virus, en computadoras sin ningún tipo de conectividad a red; es decir, en status “stand-alone”.

5.1.3.17 Deberá brindar protección contra intrusos de puertos, archivos y carpetas compartidas, bloqueando el acceso hacia ellos.

5.1.3.18 Cuando se detecte un ataque hacia una carpeta, debe ser capaz de bloquear las conexiones de computadoras infectadas que traten de contaminar dicha carpeta.

5.1.3.19 Capacidad de protección y bloqueo proactivo contra desbordamientos de buffer.

5.1.3.20 Integración de la protección tanto para servidores como para estaciones de trabajo, con funciones de Firewall y de Detección de Intrusos (IDS)

5.1.3.21 Deberá ser capaz de explorar un sistema en tiempo real, cuando sea accesado un archivo o una carpeta, así como los procesos que se ejecuten en memoria.

5.1.3.22 Capacidad de verificar solo archivos nuevos o modificados

5.1.3.23 Capacidad para bloquear las configuraciones por medio de una contraseña.

5.1.3.24 Capacidad para programar tareas de exploración a demanda. Estas exploraciones deben ser configurables y ofrecer la opción de seleccionar el objeto a explorar (archivos o carpetas, programas no deseados, memoria, disco, etc).

5.1.3.25 Capacidad para detectar programas no deseados, como Spyware o Adware y de tomar acciones cuando haya una detección.

5.1.3.26 Capacidad para detectar la dirección IP de una posible computadora atacante.

5.1.3.27 Capacidad para detectar, prevenir y eliminar el ingreso de código potencialmente malicioso tipo JAVA, Activex y VBSCript

5.1.3.28 El motor de exploración deberá utilizar distintas tecnologías de detección antivirus: Exploración de firmas y exploración heurística. La exploración de firmas busca un conjunto de código hexadecimal característico de cada virus y la exploración heurística busca patrones de comportamiento de virus conocidos para la detección de virus desconocidos.

5.1.3.29 Capacidad para poder instalarse y ser administrado remotamente, desde un servidor de antivirus o desde otra consola del mismo producto.

5.1.3.30 Creación de logs para cada uno de los eventos que realice dependiendo de la tarea (exploración, actualización, y bloqueos).

5.1.3.31 Capacidad para limitar la lectura y escritura en dispositivos de almacenamiento externo.

5.1.3.32 Capacidad de bloquear la ejecución de aplicaciones en dispositivos de almacenamiento removible.

5.1.3.33 Debe proporcionar control de acceso a los dispositivos tipo USB.

5.1.3.34 Capacidad de limitar el acceso o los privilegios de las aplicaciones, a los recursos del sistema por ejemplo, llaves de registro, archivos o folders del sistema.

5.1.3.35 Capacidad para reportar y controlar la aplicación de parches de seguridad (hotfix) de Microsoft Windows. Este control debe permitir el reporte de diferentes niveles de actualización.

5.1.3.36 El cliente de antivirus debe tener la capacidad para ejecutarse en máquinas virtuales de las siguientes plataformas: VMware, Virtual PC, Virtual Box.

5.1.3.37 Capacidad para generar un caso de soporte, a través de la interfaz gráfica, sin necesidad de módulos adicionales para su operación.

5.1.4 Requerimientos técnicos mínimos para el software Antivirus en dispositivos móviles.

El antivirus que se adquiera deberá cumplir con las siguientes características técnicas **mínimas**:

5.1.4.1. Sistemas Operativos en los que debe funcionar: Windows Mobile 5/6, Symbian 9.1 o superior, Android 2.1 o superior.

5.1.4.2. Debe brindar proteccion en tiempo real al sistema de archivos del dispositivo, interceptando y analizando:

5.1.4.2.1. Todos los objetos transmitidos usando conexiones inalámbricas (infrarojo, bluetooth) o mensajes SMS, durante el proceso de sincronización o al realizar una descarga.

5.1.4.2.2. Todos los archivos abiertos en el dispositivo móvil.

5.1.4.2.3. Todos los programas instalados usando la interfaz grafica del dispositivo.

5.1.4.3. Tener capacidad para realizar un análisis de objetos en la memoria interna y en las tarjetas de expansión

5.1.4.4. Debe contar con un área de cuarentena para aislar archivos

5.1.4.5. Debe poder crear una lista para bloquear llamadas o mensajes de SMS

5.1.4.6. Deberá contar con un firewall personal.

5.1.5 Requerimientos técnicos mínimos para el software AntiSpyware

El producto que se adquiera deberá cumplir con las siguientes características técnicas **mínimas**:

5.1.5.1 Sistemas Operativos Microsoft en los que debe funcionar: Microsoft Windows XP/Vista/7, Windows Server 2000/2003/2008

5.1.5.2 Sistemas operativos Mac en los que debe funcionar: MacOS X 10.4 o posterior.

5.1.5.3 Sistemas operativos Linux en los que debe funcionar: Linux RHEL 5/6, Suse Enterprise Server.

5.1.5.4 Debe identificar programas que puedan observar, grabar y transmitir hacia afuera información confidencial de la empresa o afectar negativamente a la productividad de los usuarios.

5.1.5.5 Debe permitir integrarse a la Consola Central de Antivirus, y enviar la instalación de forma automática a todas las computadoras de la red.

5.1.5.6 Debe prevenir posibles intrusiones a través de dispositivos de almacenamiento USB, archivos accesibles vía internet, correo electrónico, archivos compartidos, discos compactos y otros dispositivos de almacenamiento externo.

5.1.5.7 Deberá detectar, bloquear y eliminar cualquier tipo de Malware; incluyendo virus, gusanos, troyanos, spyware, phishing, rootkit, adware, riskware,

keyloggers y otros códigos maliciosos. Principalmente, que lo anterior NO debe depender de que el Sistema Operativo cliente tenga las actualizaciones y Service Pack al dia.

5.1.5.8 El software debe tener la opción de bloquear procesos maliciosos, borrar llaves en el registro de Windows, limpiar y borrar archivos referentes o señuelos del malware sin necesidad de contar con los componentes o firmas requeridos para la detección, utilizando como referencia la variante del malware y los accesos de las llaves de registro.

5.1.5.9 Debe poseer una base de datos de adware, programas espías, programas de captura de tecleo y otros programas potencialmente indeseables.

5.1.5.10 El software debe poseer el recurso de actualización automática incremental, manteniendo actualizado el software de seguridad y las características de los PUPs (Potentially Unwanted Program).

5.1.5.11 Deberá escanear llaves del registro y eliminar las llaves creadas por los spyware o cualquier PUP sin afectar la estructura del registro a nivel de Sistema Operativo.

5.1.5.12 Deberá proveer reportes desde la consola de administración centralizada, los cuales deben poder exportarse al menos hacia alguno de los siguientes formatos: XML, PDF, HTML.

5.1.5.13 Capacidad para actualizarse automáticamente desde un sitio Centralizado.

5.1.5.14 Debe permitir realizar una limpieza completa tanto a nivel de escaneos en memoria, archivos y entradas o llaves de registro.

5.1.5.15 Debe permitir la desinstalación de forma manual o remotamente desde la consola de administración.

5.1.6 Requerimientos técnicos mínimos para el software de Prevención de Intrusos (HIPs)

El producto que se adquiera deberá cumplir con las siguientes características técnicas **mínimas**:

5.1.6.1 Debe contar con un modulo de IDS (Intrusion Detection System), para protección contra escaneo de puertos

5.1.6.2 El producto debe ser administrado desde la misma consola central que administra todas las soluciones de Antivirus y Anti-Spyware.

5.1.6.3 Debe permitir la creación de usuarios con privilegios para la administración de la consola Ejemplo: Usuario para crear reportes (Report user), Usuario de Solo lectura (Read only user), Usuario administrador (Administrator user).

5.1.6.4 Capacidad de manejar varios niveles de seguridad que puedan ser Monitoreados.

5.1.6.5 Debe poder generar reportes de ataques, eventos de firewall, logs de auditoria de la consola referente a cambios en políticas. Estos reportes deben poder ser exportados al menos hacia alguno de los siguientes formatos: XML, PDF, HTML.

5.1.6.6 El producto debe llevar un log o historial de todos los cambios que se han hecho en la consola y poder verificar si otro administrador modificó alguna regla o exclusión

5.1.6.7 Detección y bloqueo de ataques del tipo “denegación de servicios”, que exploten vulnerabilidades de los Sistema Operativos instalados en las estaciones y servidores.

5.1.6.8 La herramienta deberá analizar cuando una aplicación efectúe comandos fuera de lo común, como escrituras a registro y/o conexiones externas

5.1.6.9 Detectar automáticamente los parches de seguridad de Sistemas Operativos, que no están instalados en las máquinas de trabajo,

5.1.6.10 Recibir notificaciones por correo electrónico cuando se detectó un ataque a una vulnerabilidad específica en un sistema, permitiendo detectar la fuente del ataque.

5.1.6.11 Crear reglas personalizadas de prevención de intrusos para las estaciones de trabajo.

5.1.6.12 Debe tener la capacidad de detectar tráfico malicioso oculto usando protocolos sobre puertos no estándar.

5.1.7 Condiciones mínimas del soporte para Antivirus y AntiSpyware

5.1.7.1 El soporte técnico debe brindarse tanto en la Sede Central de la UCR, como en las Sedes Regionales, Recintos, y otras unidades de Investigación de la UCR.

5.1.7.2 El proveedor debe brindar 2 (dos) años de soporte técnico local, en la herramienta de software (24 horas al día, 7 días a la semana, 365 días), tanto en forma preventiva como correctiva.

5.1.7.3 Mientras esté en vigencia el soporte y el mantenimiento del software, el adjudicatario debe garantizar el correcto funcionamiento del software antivirus y antispyware, instalando todas las actualizaciones del producto cuando sea necesario, así como las nuevas versiones del software cuando éstas sean liberadas, sin costo adicional para la UCR, y en coordinación con el ente técnico que designe la UCR.

5.1.7.4 El proveedor debe brindar acceso a soporte internacional a través de Internet o por vía telefónica, en caso necesario. Esta clase de acceso debe realizarse a través de un código de usuario debidamente registrado, que esté en capacidad de utilizar todos los servicios disponibles para un adecuado soporte técnico de los productos.

5.1.7.5 El soporte técnico en la herramienta debe incluir como mínimo los siguientes aspectos:

- 5.1.7.5.1 Instalación y configuración presencial o remota, de la consola centralizada de administración del antivirus, así como del software AntiSpyware y de Protección de Intrusos.
- 5.1.7.5.2 Resolución de consultas en el sitio.
- 5.1.7.5.3 Resolución de consultas telefónicas.
- 5.1.7.5.4 Resolución de consultas por chat.
- 5.1.7.5.5 Atención de problemas de funcionamiento de la consola de administración.
- 5.1.7.5.6 Atención de emergencias provocadas por virus, y programas espías (spyware), o intrusos.
- 5.1.7.5.7 Asesoría en la elaboración de reportes.
- 5.1.7.5.8 Mantenimiento, instalación y control de actualizaciones del producto.
- 5.1.7.5.9 Brindar un buen servicio gratuito de alertas preventivas y correctivas, a través del correo electrónico u otro medio.
- 5.1.7.5.10 Brindar un adecuado sistema de soporte en línea.

5.1.7.6 El tiempo de respuesta para la resolución de consultas telefónicas no deberá ser mayor de 4 horas.

5.1.7.7 El tiempo de respuesta para la resolución de consultas en el sitio, no deberá ser mayor de 12 horas.

5.1.7.8 El tiempo de respuesta para la resolución de emergencias provocadas por virus, no deberá ser mayor de 3 horas.

5.1.7.9 Se debe indicar en la oferta del proveedor, los alcances y limitaciones del soporte técnico local descrito anteriormente.

5.1.8 Condiciones mínimas de la migración del software.

5.1.8.1 En caso necesario, la empresa proveedora deberá encargarse con su propio personal, de realizar el proceso de migración del software antivirus actual que posee la UCR, hacia el nuevo software. Para completar esta tarea la empresa proveedora debe contemplar las pruebas que sean necesarias así como las tareas de implementación. Este proceso deberá realizarse en todas las dependencias de la UCR, tanto en la Sede Central de la UCR, como en las Sedes Regionales, Recintos, y otras unidades de Investigación de la UCR.

5.1.8.2 Debe incluir, la migración de la estructura de consola central y de las consolas descentralizadas, de la Universidad de Costa Rica.

5.1.8.3 Debe incluir también la migración del software antivirus y antispyware en las estaciones de trabajo, de la Universidad de Costa Rica.

LICITACIÓN ABREVIADA No. 2012LA-000007-UADQ
" RENOVACIÓN O ADQUISICIÓN DE LICENCIAS ANTIVIRUS Y ANTISPYWARE 2012"

Condiciones Invariables

a) Aspectos Generales

1. Vigencia de las ofertas
Las ofertas deberán tener una vigencia no menor de **45 días hábiles.**

2. Monto y plazo de la garantía de cumplimiento
Se requiere un **5%** sobre el valor total adjudicado, con una vigencia de 60 días adicionales, a partir de la fecha probable de aceptación de los equipos y accesorios a satisfacción de la Universidad de Costa Rica.

3. Plazo para adjudicar
La Universidad tomará hasta 10 días hábiles para adjudicar.

4. Plazo de entrega
El plazo de entrega será de **15 días naturales** posterior a la entrega de la orden de compra.

5. Lugar de entrega
Centro de Informática.

b) Requisitos y Condiciones Especiales

1. Documentación imprescindible: Declaración Jurada
El oferente debe aportar la siguiente declaración jurada indicando que:
1.1 Existe compatibilidad total del software ofrecido con los sistemas operativos que se indiquen.
1.2 El fabricante respaldará el tiempo de garantía que el oferente proporciona en el software ofertado.
1.3 El oferente está adscrito a un esquema de soporte y servicio directamente con el fabricante.

2. Documentación imprescindible: Certificaciones
2.1 El oferente debe aportar copia del certificado vigente como Distribuidor Autorizado directo del fabricante, que asegure la efectiva "Garantía de Fábrica" del software ofrecido.
El fabricante debe indicar el conocimiento y experiencia en productos y servicios de la empresa, adquiridos a través de certificaciones técnicas y comerciales, así como el grado de compromiso que existe con la empresa como distribuidor autorizado directo.
Esta certificación debe ser dirigida a la Universidad de Costa Rica e incluir el software que es ofrecido, con una antigüedad no mayor de 3 meses de emitida.

2.2 Una lista de los clientes en el **sector público** que hayan adquirido licencias del software solicitado en las modalidades de instalación individual y por consola, durante los últimos dieciocho meses, incluyendo el número de licencias compradas por cada cliente. Puede hacer mención de proyectos con estos clientes si los hubiere. Esta información debe completarse según el siguiente cuadro:

Institución o Empresa	Contacto *	Software	Cantidad de licencias	Fecha de la venta

* En el espacio para el contacto debe incluirse la persona para constatar la información, este debe incluir teléfono, fax, correo electrónico.

2.3 El oferente debe contar con **al menos 4** ingenieros certificados en la **última versión** del producto por adquirir, y que tengan conocimientos en:

2.3.1. Antivirus
2.3.2. Control de accesos a la red
2.3.3. Detectores de Intrusos (Tecnología IPS)
2.3.4. Análisis y administración de vulnerabilidades
2.3.5. Antispam y filtrado de web

Para demostrar este punto se deberá presentar el **certificado de examen** o una nota del fabricante donde se indique la acreditación correspondiente para cada técnico.

NOTA ACLARATORIA:

Los oferentes que hayan aportado la siguiente documentación imprescindible en contrataciones anteriores, pueden indicar: número y nombre de la contratación, con el fin de no duplicar la información solicitada:

1. **DOCUMENTACIÓN IMPRESCINDIBLE : DECLARACION JURADA**
2. **DOCUMENTACIÓN IMPRESCINDIBLE : CERTIFICACIONES**

Cabe aclarar que esta documentación debe ser válida para este proceso.

3. Garantía del Software y Soporte Técnico:

3.1 La garantía mínima del software y del soporte técnico deberá ser de 24 meses, contados a partir del recibido conforme y por escrito por parte de la Universidad de Costa Rica. El adjudicatario debe entregar el certificado de garantía original o copia autenticada por la autoridad competente del fabricante, esta certificación deberá ser firmada por el representante legal autorizado para tal acción. No se aceptan firmas de vendedores o encargados de cuenta. La Universidad de Costa Rica se reserva el derecho de verificar los certificados de garantía con el fabricante. Durante el período de garantía los costos correrán por cuenta de la empresa.

3.2 El oferente deberá especificar los beneficios de la garantía del software y deberá especificar también las exclusiones. Las exclusiones que no queden explícitas en la oferta no serán válidas.

3.3 De presentarse fallas en los medios de almacenamiento electrónico del software adquirido compatible con los equipos de hardware de la institución (CD-ROM, DVD-ROM, USB) o encontrarse errores en los manuales del software, el adjudicatario deberá proceder, bajo su costo y responsabilidad, bajo la supervisión de la Universidad de Costa Rica, a sustituirlos por nuevos.

3.4 El oferente debe contar con personal técnico con experiencia mínima de un año, para solventar cualquier solicitud de falla en el Software y disponer de todas las herramientas especializadas necesarias para dar su servicio durante el período de garantía del Software.

3.5 El soporte técnico deberá ser respaldado por la casa matriz, de forma que se garantice que en caso de desaparición de la empresa proveedora adjudicada, el soporte técnico deberá ser asumido por el fabricante.

4. Presentación de Oferta Base y Oferta Alternativa

En caso de que el oferente presente varias ofertas, debe indicar claramente cual es su oferta base, cual es su oferta alternativa y se deben garantizar los siguientes puntos:

4.1 La(s) **Oferta(s) Base** serán aquellas que cumplen con todas las especificaciones técnicas incluidas en los requerimientos mínimos solicitados en el cartel.

4.2 La(s) **Oferta(s) Alternativa(s)** existe siempre en función y dependencia de la oferta base, y, si bien puede mejorar en todos los aspectos esta última; la posibilidad de adjudicar una oferta alternativa se dará solamente cuando la misma empresa haya ganado de previo con la oferta base. Se considerará como una oferta base si la misma no ofrece mejora o ventajas mayores a las requeridas en el cartel.

5 Recepción de objeto actualizado

El adjudicatario está obligado de entregar a la Universidad de Costa Rica el software actualizado tecnológicamente según lo señalado en el artículo 197 del Reglamento de la Ley de Contratación Administrativa. Como actualización tecnológica se entenderá, entre otras cosas, que el bien esté en línea de producción al momento de la entrega o como la última versión del fabricante y ésta haya sido conocida en el mercado al menos un mes antes de la entrega de la solicitud de pedido por parte de la Universidad. Para estos efectos, la entidad podrá pedir al adjudicatario que respalde el ofrecimiento con certificación emitida directamente por el fabricante.

6 Elementos de adjudicación y metodología de comparación de ofertas:

Para la evaluación del software ofertado, por los técnicos del Centro de Informática, se tomara en cuenta el siguiente factor:

TABLA 1
FACTORES A EVALUAR

	Factor	***Porcentaje***
A.	Precio de las licencias	70%
B.	Precio del soporte	20%
C.	Certificación de distribuidor autorizado de alto nivel en Seguridad de Sistemas y manejo de riesgos.	10%
	TOTAL	100%

A. Precio de las licencias (70 puntos)
Se calificará el precio según la siguiente fórmula:

$$PP = \left(\frac{P_{\min}}{P_{oferta}} \right) * PT$$

donde:

PP: Puntaje por Precio.
P_{oferta} Precio de la oferta en estudio.
P_{min} Menor precio ofrecido de los equipos elegibles
PT Máximo “puntaje por precio alcanzable” (Ver fila A.)

B. Precio del soporte (20 puntos)
El puntaje asignado para el factor “Precio del soporte” se asignará de acuerdo a la siguiente fórmula:

$$PP = \left(\frac{P_{\min}}{P_{oferta}} \right) * PT$$

donde:

PP: Puntaje por Precio.
P_{oferta} Precio de la oferta en estudio.
P_{min} Menor precio ofrecido de los equipos elegibles
PT Máximo “puntaje por precio alcanzable” (Ver fila B.)

C. Certificación de distribuidor autorizado del más alto nivel, en Seguridad de Sistemas y Manejo de Riesgos (10 puntos)

Se asignarán 10 puntos a la empresa que presente una certificación del fabricante que lo faculte como distribuidor autorizado del **más alto nivel en Seguridad de Sistemas y Manejo de riesgos**, con una antigüedad no mayor a 3 meses de emitida.
En esta certificación se deberá indicar por parte del fabricante, cuales son los niveles que puede alcanzar un distribuidor en el software ofertado, y también cual es el nivel actual que tiene el proveedor que está ofertando el producto.

7 Aspectos generales de la evaluación

7.1 Base de calificación

La máxima cantidad que pueda obtener un oferente es de 100 puntos. La oferta elegible que obtenga el mayor puntaje será la adjudicada.

7.2 Porcentaje mínimo de adjudicación

La oferta válida para ser adjudicada debe obtener como mínimo un porcentaje de 85%, en caso contrario la oferta será ser descartada.

7.3 Criterios para el redondeo

Para los cálculos de puntaje se utilizarán dos decimales.

7.4 Criterio de desempate

En caso de presentarse empate se utilizará como criterio de desempate los siguientes puntos:

7.4.1 La oferta que ofrece menor precio por soporte técnico local.
(Ver punto 5.1.7.Condiciones mínimas del soporte para Antivirus y AntiSpyware en las Especificaciones técnicas)

7.4.2 En caso de persistir empate, la Administración convocará por escrito con tres días de antelación a la fecha en que se resolverá el desempate, a los representantes legales de los oferentes que se encuentren en situación de empate, para efectuar una rifa y así seleccionar el adjudicatario, la cual será efectuada en la Oficina de Suministros por el Proveedor Institucional. Cada oferente tomará al azar un papel donde en uno de ellos se detallará la palabra “adjudicatario”, el resto estarán en blanco; el oferente que tenga el papel con la palabra antes indicada, será el adjudicatario.
La no asistencia de las partes no impedirá la realización de la rifa.
De lo actuado se levantará un acta que se incorporará al expediente.

8 Diagnóstico técnico de resultados

Luego de finalizada la evaluación de acuerdo a los requerimientos solicitados, calidades del Software y lo especificado en el apartado de evaluación, el Centro de Informática, confeccionará y enviará los resultados de su respectivo diagnóstico técnico a la Oficina de Suministros para ser incluidos en el correspondiente Expediente Administrativo.

9 De la evaluación del software adjudicado

La empresa adjudicataria debe entregar la documentación necesaria para la instalación o las licencias respectivas en CD´s, DVD’s o/y otros para ser reinstalado en caso necesario.
La evaluación se realizará la siguiente manera:

A. Se comprobará el cumplimiento de los requerimientos solicitados y adjudicados en el cartel.

B. En caso de haberse entregado medios, se comprobarán las buenas calidades del medio de almacenamiento físico del software adquirido compatible con los equipos de hardware de la institución (CD-ROM, DVD-ROM, USB).

C. En caso necesario, se instalará un laboratorio de verificación en el Centro de Informática, donde se comprobará el cumplimiento de las características técnicas del software ofertado.

10 Aceptación o Rechazo del software adjudicado

Luego de finalizada la evaluación del software, se determinará lo siguiente:

10.1 Si el software cumple con los requerimientos solicitados y adjudicados, se confeccionará y enviará los resultados de su respectivo diagnóstico técnico a la Oficina de Suministros para ser incluidos en el correspondiente Expediente Administrativo, como un recibido conforme, de parte del Centro de Informática como la Oficina de apoyo Técnico.

10.2 Si el software no cumple con los requerimientos solicitados y/o las buenas calidades del medio de almacenamiento (en caso de haberse entregado), se solicitará a la empresa su cumplimiento en un plazo máximo de 3 días hábiles.

11 Manuales de servicio

El adjudicatario deberá entregar los manuales de servicio, utilización e instalación del software en idioma español preferiblemente o en inglés. En caso de errores en los manuales, el adjudicatario deberá reemplazarlos en un plazo máximo de 3 días.

12 Curso de capacitación técnica

El adjudicatario está obligado a impartir un curso de capacitación a los técnicos que el Centro de Informática designe sobre los conceptos básicos del uso del software y en la administración de las consolas locales, en los 30 días naturales posteriores a la entrega del software.

El curso debe ser teórico-práctico, para 4 grupos de un máximo de 20 personas cada uno. Debe ser impartido por un especialista calificado en el software (adjuntar atestados) y deberá tener una duración mínima de 8 horas.

El lugar de capacitación será en las instalaciones de la Sede Central de la Universidad de Costa Rica.

Debe entregarse un folleto de al menos 10 hojas con el contenido de la capacitación, más la presentación en formato digital.

13. Prórroga

La Universidad de Costa Rica se reserva el derecho de realizar la prórroga de este Contrato siempre y cuando satisfaga el interés institucional.

14. Multas por Mora (cláusula penal)

Se aplicará una multa del 0.1% sobre el monto de adjudicación del servicio por cada día de atraso, (con respecto al plazo ofrecido), hasta un máximo del 25% (veinticinco por ciento) del importe total del contrato. En caso de que el adjudicatario no deposite el monto de la multa, la

Universidad queda autorizada para que esta suma sea deducida de las facturas presentadas para su pago o retenciones efectuadas, lo anterior, se hará conforme a las disposiciones que para tal efecto se tienen en la Ley y Reglamento de Contratación Administrativa.

15. Forma de pago

Descripción	Porcentaje de pago
Licencias de software	40%
Instalación, pruebas y migración	40%
Capacitación finalizada	20%
Total	**100%**

LICITACIÓN ABREVIADA No. 2012LA-000007-UADQ
" RENOVACIÓN O ADQUISICIÓN DE LICENCIAS ANTIVIRUS Y ANTISPYWARE 2012"

Condiciones Generales:

1. **Presentación de la oferta:**
   La recepción de ofertas será en la Oficina de Suministros, ubicada en Sabanilla de Montes de Oca, de las Instalaciones Deportivas, 250 metros este y 400 metros norte, en la fecha y hora que indique la invitación.

   La oferta deberá presentarse por escrito, en sobre cerrado rotulado con el número y el objeto de la Licitación. Toda oferta deberá presentarse en papel corriente, en original y una copia idéntica en CD , con la firma del oferente o de su representante legal, sin tachaduras ni borrones. Cualquier corrección debe ser hecha mediante nota.

   Igualmente se acompañaran fotocopias de los documentos complementarios de la oferta.

2. Debe adherir a la oferta un timbre de la Ciudad de las Niñas de ¢20,00 y un timbre de ¢200,00 del Colegio de Profesionales en Ciencias Económicas.

3. **Documentos que deben entregarse:**

   3.1 Certificación sobre la personería jurídica de la sociedad mercantil o copia de la cédula de identidad en caso de persona física.

   3.2 Cuando el oferente fuere una sociedad mercantil costarricense, deberá acompañar con su propuesta una certificación pública con la naturaleza y propiedad de sus cuotas y acciones. Si las cuotas o acciones fueran nominativas y estas pertenecieran a otra sociedad deberá igualmente aportarse certificación pública respecto a esta última en cuanto a la naturaleza de sus acciones. Las certificaciones serán emitidas: a) En cuanto a la naturaleza de las cuotas y acciones, por el Registro Público o por un Notario Público con vista en los libros de Registro, y b) En cuanto a la propiedad de las cuotas y acciones, con vista de los libros de la sociedad por un Notario Público o Contador Público autorizado. No obstante, si se tratare de una sociedad inscrita dentro del año anterior al requerimiento de la certificación, o modificada a acciones nominativas dentro del período indicado, la certificación sobre ambos extremos, podría ser extendida por el Registro Público o por un Notario Público.

   3.2.1. En tanto se declare en la oferta que la propiedad de las cuotas o acciones se mantiene invariable, la certificación original o una copia certificada de la misma, serán admitidas a los indicados efectos hasta un año después de su emisión. Si la certificación o copia certificada hubiere sido presentada en una diligencia anterior y el oferente lo manifieste así en su oferta, deberá indicar claramente el número de Licitación en que fue presentada o una copia del recibido por parte de la Oficina de Suministros, así como la declaración de que permanece invariable.

3.3. El oferente debe presentar una certificación indicando que se encuentra al día con las obligaciones obrero-patronales de la C.C.S.S., o bien, que tiene un arreglo de pago aprobado por ésta, vigente al momento de la apertura de las ofertas. (art. 65.c) Reglamento a la Ley de Contratación Administrativa.

3.4. Declaración jurada que el oferente no está afectado por ninguna causal de prohibición.

3.5. Declaración jurada que no le alcanzan, al oferente, las prohibiciones para contratar con la Universidad de Costa Rica, a que se refiere el numeral 22 de la Ley de Contratación Administrativa y en los artículos 19 y 20 del Reglamento.

3.6 Declaración jurada que el oferente se encuentra al día en el pago de todo tipo de impuestos nacionales de conformidad con lo dispuesto en el art no. 65 a del Reglamento.

3.7 Cualesquiera otros documentos que se considere oportuno acompañar, según la naturaleza del objeto licitado y el tipo de licitación que se haya promovido.

Cuando los documentos originales vigentes, se encuentren en el Registro de Proveedores, deberá manifestarse expresamente, indicar el número de proveedor y se aportará copia simple de los documentos que se indican.

4. Contenido de la oferta: Debe contener por lo menos:

4.1 Nombre y dirección de la casa oferente y según sea el caso, del exportador, del apoderado, del representante o distribuidor en Costa Rica, con indicación del nombre, cédula, dirección y posición del firmante dentro de la empresa.

4.2 Número de cédula jurídica.

4.3 El oferente debe indicar en su oferta un número de fax, para recibir notificaciones, caso contrario, se tendrá por notificado en el transcurso de 24 horas.

4.4 Descripción completa del bien indicando marca, modelo, garantía.

4.5 El precio total cotizado deberá presentarse en números y en letras coincidentes. en caso de divergencia entre ambas formas prevalecerá la consignada en letras**. (**Art. 25 del Reglamento)

5. Regulaciones que deben observarse:
Los participantes deberán cumplir con lo que establece la Ley de la Contratación Administrativa, el Reglamento a la Ley de Contratación Administrativa y otras leyes pertinentes.

6. Precios

6.1 Oferentes extranjeros:

6.1.1 Deberán indicar el precio FOB Miami y desglosar fletes y otros gastos hasta integrar el precio C&F San José. Asimismo, el oferente o su representante deberán indicar las instrucciones necesarias (factor, porcentaje u otro) para que, en caso de adjudicación parcial y para efectos de comparación entre las ofertas, los precios puedan convertirse en C&F San José, Costa Rica, por cada línea cotizada.

6.1.2 La institución no se hará cargo del pago de bodegaje atribuible al adjudicatario por incumplimiento en la entrega de documentos.

6.1.3 Los bienes ofertados por oferentes extranjeros deben cotizarse sin seguro pues todos los pedidos de la Universidad de Costa Rica están cubiertos por la póliza abierta #12239 del Instituto Nacional de Seguros.

6.2 Oferentes Nacionales:

6.2.1 Los bienes ofertados por proveedores nacionales se entenderán puesto en almacenes de la Universidad de Costa Rica. Deben incluir el desalmacenaje.

6.2.2 La Universidad de Costa Rica dará solo la exoneración de impuestos.

7. Deben cotizarse separadamente, además, los costos de instalación de los equipos, si los hubiera, y el costo del contrato de mantenimiento, cuando expresamente se solicite.

8. Impuestos:
Los oferentes nacionales deberán señalar por aparte los impuestos que los afectan. La Universidad está exenta de impuestos según Ley #7293, artículo #6, publicada en La Gaceta #63 del 31 de marzo de 1992; por lo que, se tramitará la exoneración correspondiente. No se exonerarán materiales o servicios adquiridos por subcontratistas.

9. Los oferentes extranjeros deben indicar claramente lo siguiente:

9.1 La descripción de la mercadería debe venir en idioma español o con la respectiva traducción.

9.2 El nombre de la persona a contactar encargada de brindar información sobre el estado de despacho de la mercadería, con quien podamos comunicarnos directamente para cualquier consulta, así como sus números de teléfono y fax.

9.3 Si el equipo o material cotizado requiere de accesorios adicionales para su funcionamiento, favor indicarlo y cotizarlo por separado. caso contrario, se considerará que el precio incluye todo lo necesario para la puesta en marcha el mismo.

9.4 El adjudicatario está obligado a entregar los manuales de operación y a brindar el entrenamiento necesario, para la adecuada operación del equipo u otro bien.

9.5 Favor consignar claramente en su oferta forma si corresponde, los costos adicionales por transporte internacional de mercadería peligrosa. La Universidad de Costa Rica no asumirá costos adicionales una vez que la Orden de Compra quede en firme.

10. Forma de Pago:

10.1 Oferentes Extranjeros

10.1.1 Pago contra entrega de Mercadería en nuestros Almacenes, mediante Giro Bancario Internacional a nombre de la Casa Proveedora.

10.1.2 Cobranza Bancaria Documentaria.

10.1.3 Carta de Crédito

Notas:

- En los casos en los cuales se realizará el pago mediante transferencia bancaria, el adjudicatario, deberá remitir toda la información bancaria necesaria.

- Todas las comisiones y gastos bancarios de cualquier índole dentro y fuera de Costa Rica serán asumidas por el adjudicatario o su representante.

10.2 Oferentes Nacionales:

El pago se realizará 30 días naturales siguientes al recibido conforme por parte del usuario final. Las facturas deberán presentarse en el tipo de moneda cotizada, cuando se trate de una moneda distinta al colón, el pago se realizará en colones costarricenses y de acuerdo a lo establecido en el artículo 25 del Reglamento a la Ley de Contratación Administrativa.

Se pagará en colones costarricenses dentro de los treinta (30) días naturales siguientes a la presentación de las facturas en la Oficina de Administración Financiera.

10.3 Cuando la oferta se presente en dólares, la factura se cancelará en colones costarricenses, al Tipo de Cambio promedio o valor comercial efectivo a la fecha en que se emita el cheque. La Universidad de Costa Rica no asumirá el diferencial cambiario por entrega tardía imputable al adjudicatario o por entrega de facturas para pago después de 5 días de entregado el bien.

10.4 La Orden de Pago (autorización de pago) la emitirá la Unidad de Desalmacenajes y Almacenamiento, dentro de los 5 días posteriores, previo recibido conforme por escrito de los usuarios o técnicos correspondientes.

11. Plazo de Entrega:

11.1 El plazo de entrega que indique el oferente en su propuesta se contará a partir del momento en que reciba la Orden de Compra, sea en forma personal o vía fax.

11.2 Si la entrega estuviere sujeta al trámite de exoneración, el oferente deberá indicar en su propuesta el plazo en que presentará los documentos necesarios para realizar la exoneración y el plazo que tardará en desalmacenar y entregar la mercadería. Los oferentes deberán entregar en la solicitud de exoneración la siguiente información.

11.2.1 Monto C.I.F.
11.2.2 Número de guía.
11.2.3 Consignatario
11.2.4 Aduana de desalmacenaje.
11.2.5 Lugar de procedencia.
11.2.6 Peso de la mercadería en kilogramos.
11.2.7 Factura comercial.
11.2.8 Cantidad y clase de mercadería.
11.2.9 Lista de empaque.

11.3 El oferente indicará el plazo de entrega de los bienes. Si el oferente no indica el plazo de entrega se considerará entrega inmediata. Cuando el oferente no indique la naturaleza de los días, se entenderán días naturales.

11.4 La entrega inmediata se considerará 1 día hábil después de recibida la Orden de Compra.

11.5 Los Oferentes Extranjeros deben indicar en forma desglosada el plazo de despacho y el plazo de entrega en aduana.

12. Lugar de Entrega:

El oferente deberá indicar el lugar de entrega de los bienes, en caso de omisión se entenderá que los bienes son puestos en la Universidad de Costa Rica.

13. Aspectos Generales de la Evaluación:

13.1 En los casos en que se evalúa el plazo de entrega y el oferente indica en su oferta que el plazo de entrega se cuenta a partir de la fecha en que reciban la nota de exoneración aprobada, se incluirán en la ponderación los siguientes plazos:

- El plazo en que entregará el oferente los documentos para exonerar.
- 10 días hábiles (confección y trámite ante el Ministerio de Hacienda)
- Plazo en que entregarán los bienes después de recibida la exoneración.

13.2 Tipo Cambio

Para efecto de verificación presupuestaria y comparación de precios en igualdad de condiciones, se considerará el tipo de cambio proyectado considerando el plazo para emitir la adjudicación, el plazo de entrega y plazo de pago.

14. Obligaciones del adjudicatario:

14.1 Documentación de importación.

El representante del adjudicatario extranjero se compromete a suministrar a la Unidad de Licitaciones, dentro de los 2 días posteriores al arribo a puerto de la mercadería, tres juegos de facturas, listas de empaque y conocimiento de embarque, con todos los requisitos legales que exigen las aduanas del país, para cumplir con los trámites de exoneración y permisos varios que posteriormente permitan un expedito desalmacenaje de los equipos. Si el adjudicatario incumple esta disposición, la Administración cobrará los días de bodegaje equivalentes al mismo número de días en que se retrase la llegada de los citados documentos. Si el adjudicatario no deposita el monto correspondiente al bodegaje, se deducirá del monto de la factura, previo debido proceso.

14.2 Pesos y volumen.

Los adjudicatarios de materiales y/o equipos para importación deberán indicar el peso bruto y volumen por cada línea ofrecida, y se requiere la utilización de las unidades y medidas del sistema internacional de unidades, basado en el Sistema Métrico Decimal, conforme lo requerido en el Numeral 52 inciso “g” del Reglamento de la Contratación Administrativa.

14.3 Partidas Arancelarias.

El adjudicatario deberá indicar las Partidas Arancelarias por línea adjudicada.

15. Comisiones y gastos bancarios:

Todas las comisiones y gastos bancarios tanto internas como externas, serán pagados por el vendedor o por su representante.

16. Muestras del material ofrecido cuando así se solicite expresamente en las Condiciones Especiales., estas muestras se utilizarán para corroborar las características de los bienes ofrecidos. Los oferentes no adjudicatarios quedan obligados al retiro de las mismas que no se hubiesen inutilizado en pruebas efectuadas dentro de los treinta (30) días naturales siguientes al acto de adjudicación en firme. Las muestras dejadas en custodia para comprobar la correcta ejecución del contrato se devolverán en un plazo máximo de 30 días hábiles a partir del recibido conforme. Las muestras que no fuesen retiradas dentro del indicado plazo, pasarán a propiedad de la Universidad de Costa Rica.

17. Garantías:

17.1 Garantía de cumplimiento

Todo adjudicatario deberá rendir una garantía de cumplimiento con el objeto de garantizar la calidad, confección, funcionamiento adecuado de los equipos, así como el tiempo de entrega convenido y cláusulas de la presente licitación y de las

ofertas adjudicadas, todo esto a plena satisfacción de la Universidad. La misma deberá rendirse dentro de los cinco (5) días hábiles siguientes a la adjudicación en firme. Su inobservancia dentro de dicho plazo dejará sin efecto el acto de adjudicación y autorizará a la administración para readjudicar el concurso a la segunda mejor oferta calificada, sin perjuicio de la ejecución de la garantía de participación rendida y toda otra acción tendiente a resarcir los daños y perjuicios ocasionados a la Administración por el adjudicatario renuente.

17.2 Forma de rendir las garantías.

Las garantías deberán rendirse independientemente para cada negocio (Por concurso) mediante depósito de bono de garantía de instituciones aseguradoras reconocidas en el país, o de uno de los bancos del Sistema Bancario Nacional o el Banco Popular y de Desarrollo Comunal, certificados de depósitos a plazo, bonos del Estado o de sus instituciones, cheques certificados de un banco del Sistema Bancario Nacional, dinero en efectivo y en general, conforme se estipula en el artículo No.37 del Reglamento General de la Contratación Administrativa.

17.3 Sitio donde se depositan las garantías.

Deberán ser depositadas directamente en la Oficina de Administración Financiera (O.A.F.); sita en el Edificio Administrativo “A”, Ciudad Universitaria Rodrigo Facio. El respectivo recibo deberá entregarse junto con la oferta y copia del documento depositado en la Oficina de Administración Financiera.

17.4 Devolución de la garantía

Los interesados deberán solicitar la autorización de la devolución de la garantía mediante nota dirigida a la Unidad de Ejecución Contractual, en la cual indicarán el número de concurso, número de recibo, monto y tipo de garantía. Dicha solicitud debe venir firmada por la persona que suscribió la oferta, caso contrario deberá aportar certificación de personería de quien está firmando.

Para efectos de devolución de garantías depositadas en efectivo, únicamente se devolverá con la presentación del recibo original del comprobante de ingreso de la Oficina de Administración Financiera.

Será devuelta dentro de los 30 días hábiles siguientes a la fecha en que la Universidad tenga por definitivamente ejecutado el contrato a satisfacción y se haya rendido el informe correspondiente.

17.5 Garantías Vencidas:

Las garantías (cartas de garantías, depósito a plazo, efectivo, cheque, etc.) que se encuentren vencidas y que no hayan sido retiradas, pasarán a poder de la administración 30 días después de su vencimiento, por lo que no se autorizará su devolución.