escanear

GOBIERNO DEL
ESTADO DE MÉXICO

GOBIERNO QUE TRABAJA Y LOGRA
enGRANDE

FECHA DE SUSCRIPCIÓN			CONTRATO ADMINISTRATIVO DE ADQUISICIÓN DE BIENES Y/O SERVICIOS	NÚMERO DE CONTRATO
DIA 14	MES 12	AÑO 2012		SSC/DGAS/CMC/079/2012

DATOS GENERALES DEL PROVEEDOR

NOMBRE, DENOMINACIÓN O RAZÓN SOCIAL: "GRUPO EMPRESARIAL RAA", S.A. DE C.V.

INSTRUMENTO QUE ACREDITA LA CONSTITUCIÓN DE LA PERSONA MORAL COLECTIVA:
Escritura Pública Número 9,090 (Nueve mil noventa), volumen 335 ordinario (Trescientos treinta y cinco), folio 93-100, de fecha tres de Febrero del año dos mil once, pasada ante la fe del Licenciado Jesús Maldonado Camarena, Notario Público Número 132 (Ciento treinta y dos), con residencia en Zinacantepec Estado de México.

REGISTRO FEDERAL DE CONTRIBUYENTES:	CLAVE UNICA DE REGISTRO DE POBLACIÓN:	NACIONALIDAD:
GER1102031K8	[redacted]	Mexicana.

DOMICILIO FISCAL (CALLE, NÚMERO, COLONIA, CODIGO POSTAL, LOCALIDAD, MUNICIPIO Y ENTIDAD FEDERATIVA):
Paseo San Gerardo No. 134 Club de Golf San Carlos Metepec Estado de México CP 52159

DOMICILIO EN EL ESTADO DE MÉXICO (CALLE, NÚMERO, COLONIA, CODIGO POSTAL Y LOCALIDAD):
Paseo San Gerardo No. 134 Club de Golf San Carlos Metepec Estado de México CP 52159

TELEFONO: (722) 5084641	TELEFAX: (722) 5084641	CORREO ELECTRÓNICO (E-MAIL): jorgeluis.becerril@gmail.com

NOMBRE DEL REPRESENTANTE: C. JORGE LUIS BECERRIL VAZQUEZ

INSTRUMENTO QUE ACREDITA LA REPRESENTACIÓN:
Instrumento Público Número 9,772 (Nueve mil setecientos setenta y dos), volumen 352 ordinario (Trecientos cincuenta y dos), folio 146-147, de fecha diez de Julio del año dos mil doce, pasada ante la fe del Licenciado Jesús Maldonado Camarena, Notario Público Número 132 (Ciento treinta y dos), con residencia en Zinacantepec Estado de México.

DATOS GENERALES DE LA ADJUDICACIÓN

GIRO COMERCIAL: 3271 ARRENDAMIENTO DE ACTIVOS INTANGIBLES.	SUBGIRO COMERCIAL: 3271A LICENCIAS DE PROGRAMAS DE COMPUTO.

UNIDAD ADMINISTRATIVA: CENTRO DE MANDO Y COMUNICACION, DE LA SECRETARIA DE SEGURIDAD CIUDADANA.

NÚMERO DE REQUISICIÓN:	PROCEDIMIENTO ADQUISITIVO:	LEGISLACIÓN APLICADA (ESTATAL O FEDERAL):	ACUERDO O DICTAMEN DE ADJUDICACIÓN (NÚMERO Y FECHA):
SSC/SRM/DAS/086/2012	Adjudicación Directa AD/SSC/DGAS/062/2012	Estatal.	AD/SSC/DGAS/CADQ/061/2012 del 04 de Diciembre del Dos Mil Doce.

TIPO DE GASTO (CORRIENTE O DE INVERSIÓN):	ORIGEN DE LOS RECURSOS (ESTATAL, FEDERAL O CONCURRENTE):	PARTIDA PRESUPUESTAL:
Inversión	Concurrente	Oficio número 203200-AGIS-FASP-0454/12 de fecha 24 de Mayo de 2012, Partida 3271.

ELEMENTOS BÁSICOS DE LA CONTRATACIÓN

OBJETO DE LA ADQUISICIÓN: "Software antivirus corporativo con 1000 estaciones de trabajo Windows 2000/2003/XP/VISTA/7"."

PLAZO DE ENTREGA: Dentro de los 15 días hábiles posteriores a la firma del contrato, en un horario de 09:00 a 18:00 horas.

LUGAR DE ENTREGA: En las instalaciones del Centro de Mando y Comunicación, sito en Calle Marie Curie S/N, Esquina Paseo Tollocan C.P. 50140, Col. San Sebastián Toluca de Lerdo, Estado de México.

IMPORTE TOTAL DE LA ADQUISICIÓN: $199,999.66 (Ciento noventa y nueve mil novecientos noventa y nueve pesos 66/100 M.N.) incluye el Impuesto al Valor Agregado.

FORMA DE PAGO: El pago será dentro de los 20 días hábiles posteriores, a la entrega total de los bienes a entera satisfacción de la unidad usuaria y presentación de la factura en la unidad administrativa solicitante. No aplicaran intereses, ni se otorgaran anticipos.

PLAZO DEL PAGO: El pago será dentro de los 20 días hábiles posteriores, a la entrega total de los bienes a entera satisfacción de la unidad usuaria y presentación de la factura en la unidad administrativa solicitante. No aplicaran intereses, ni se otorgaran anticipos.

ANTICIPO: No hay anticipo, por lo que queda sin efectos la cláusula Quinta contenida en el reverso del presente contrato.

AJUSTE DE PRECIOS: Los precios son fijos durante la vigencia del contrato, por lo que queda sin efecto la clausula Sexta contenida en el reverso de presente contrato.

GARANTÍA DE CALIDAD DE LA ADQUISICIÓN (PLAZO): El Proveedor garantizará la calidad de los bienes y/o servicios, comprometiéndose a cumplir estrictamente con las condiciones establecidas en el presente contrato y sus anexos correspondientes.

GARANTÍA DE CUMPLIMIENTO DE CONTRATO (TIPO E IMPORTE): El Proveedor entregará a la Secretaría de Seguridad Ciudadana sito calle 28 de Octubre S/N , esq. Fidel Velázquez, Col. Vértice, Toluca, Estado de México, C.P. 50150, dentro de los diez días hábiles posteriores a la suscripción del contrato a través de fianza, cheque certificado o cheque de caja, la correspondiente garantía de cumplimiento del presente contrato, expedida a favor del Gobierno del Estado de México equivalente al **10%** del importe total del contrato, por un monto de $ 19,999.96 (Diecinueve mil novecientos noventa y nueve pesos 96/100 M.N.)

GARANTÍA CONTRA DEFECTOS O VICIOS OCULTOS: No aplica

PENAS CONVENCIONALES (INCUMPLIMIENTO Y RESCISIÓN): Las referidas al reverso del presente contrato.

ANEXOS DEL CONTRATO

ANEXO UNO: DESCRIPCIÓN DE LOS BIENES Y/O SERVICIOS.

OBSERVACIONES

Queda sin efectos la cláusula tercera del contenido al reverso del presente contrato, por no tratarse de un contrato abierto.
Queda sin efectos el párrafo segundo de la cláusula octava del contenido al reverso del presente contrato.

VALIDACIÓN DEL CONTRATO (ANVERSO Y REVERSO)

POR EL CONTRATANTE	POR EL PROVEEDOR
EDGAR RICARDO SIERRA VARELA DIRECTOR GENERAL DE ADMINISTRACIÓN Y SERVICIOS DE LA SECRETARIA DE SEGURIDAD CIUDADANA.	C. JORGE LUIS BECERRIL VAZQUEZ REPRESENTANTE LEGAL

SECRETARIA DE SEGURIDAD CIUDADANA
DIRECCIÓN GENERAL DE ADMINISTRACIÓN Y SERVICIOS

ANEXO UNO

NO. DE PARTIDA	CLAVE DE VERIFICACIÓN	ESPECIFICACIONES DE LOS BIENES O SERVICIOS	UNIDAD DE MEDIDA	CANTIDAD SOLICITADA	PRECIO (IVA INCLUIDO)	
					UNITARIO	TOTAL
1		Software Antivirus Corporativo con 1000 estaciones de trabajo Windows 2000/2003/XP/Vista/7, con al menos 1 consola de administración, bloqueo de aplicaciones en el cliente, anti spam para Exchange, soporte técnico, actualizaciones de software y definiciones de virus por un año con las siguientes especificaciones técnicas: •Ofrecer una protección contra código malicioso que cubra por lo menos ataques e intromisiones de 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 una consola de administración centralizada, tanto para la configuración, como instalación y actualizaciones en cada equipo. •Debe ser capaz de analizar o buscar el código malicioso, cuando se acceda a un archivo o carpeta, así como los procesos que se ejecuten en memoria todo esto donde esté instalado en tiempo real. •Debe tener la opción de clasificar los procesos con base en el 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. •Realizar el análisis de archivos de comandos (scripts) mientras se están ejecutando •Dentro de los métodos de detección debe contar con la detección heurística. •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 termina después de transcurrir el tiempo, manualmente desde la interfase del antivirus o desde la consola de administración centralizada. •Se puede configurar un mensaje de alerta al usuario cuando se da una detección y mostrarle distintas acciones a aplicar, así como permitir aplicar acciones automáticas sin mostrar información al usuario. •Debe tener diferentes opciones para el manejo del registro de eventos de la aplicación; entre las opciones se debe determinar si se activa o desactiva el registro; nombre y ubicación del archivo de registro; tamaño máximo del archivo, así como poder ver el archivo desde la interfase del antivirus. Debe permitir al administrador configurar la solución para analizar todos los archivos, o una lista de tipos de archivo predeterminados por las firmas de fabricante. A esta lista de tipos de archivo el administrador puede agregar otros tipos de archivo. •Debe permitir la creación de excepciones de archivos, carpetas o unidades disco para no ser analizadas. •Deber contar al menos con las siguientes categorías para protección de acceso: protección estándar antisoftware espía, protección máxima antisoftware espía, protección estándar de antivirus, protección máxima de antivirus, control contra brotes de antivirus, protección común estándar, protección común máxima y reglas definidas por el usuario.	PIEZA	1	$199,999.66	$199,999.66

NO. DE PARTIDA	CLAVE DE VERIFICACIÓN	ESPECIFICACIONES DE LOS BIENES O SERVICIOS	UNIDAD DE MEDIDA	CANTIDAD SOLICITADA	PRECIO (IVA INCLUIDO)	
					UNITARIO	TOTAL
		•Analizar archivos macros en todos los archivos adjuntos. •Para el análisis de archivos empacados (.zip, pkg, etc.), el antivirus debe permitir habilitar o deshabilitar que se realice el análisis de 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. •Se debe integrar al sistema operativo de manera que creará opciones en el menú de contexto del explorador. Esto permite que apretando el botón derecho del mouse sobre un archivo o carpeta, entre todas las opciones mostrará la de 'analizar en busca de virus' •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 debe permitir 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, debe 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 y las previstas por el software Análisis bajo demanda.- detecciones, limpieza cuarentena y las previstas por el software 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: Debe ver el contenido en la cuarentena desde la interfase del antivirus, así como ver información acerca de la detección y del tiempo en cuarentena. Debe permitir analizar el archivo desde esta interfase; se puede restaurar el archivo y borrar de la cuarentena. Debe 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. Debe 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 permitir la creación de una lista de excepción. •Debe permitir al usuario o administrador crear una o varias políticas para controlar las acciones que los procesos del sistema o de red pueden realizar sobre uno o varios archivos, directorio o carpeta. Dentro de las acciones debe incluir al menos, lectura, escritura, ejecución, aun cuando la carpeta se haya compartido con todos los permisos.				

					UNITARIO	TOTAL
		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 termina después de transcurrir el tiempo, manualmente desde la interfase del antivirus o desde la consola de administración centralizada. •Capacidad de bloqueo de configuraciones por medio de una contraseña. Este bloqueo debe ser selectivo para partes específicas de la configuración, o 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. Debe 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 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 correo masivo locales Prevenir la modificación de los archivos de la solución antivirus Prevenir la modificación de archivos y configuración de los navegadores, Internet Explorer, FireFox y actuales 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 también el agente de administración que le permite comunicarse con la consola central. El oferente del software antivirus debe publicar en su página Web actual al menos diariamente las bases de datos de firmas para la detección, con acceso autorizado. La actualización de firmas debe realizarse de forma automática o manual, según la configuración del administrador se debe 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 XP, Vista y Windows a 64 bits 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. Debe integrarse con la solución antivirus. Deben usar el mismo programa de análisis y también 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.				

NO. DE PARTIDA	CLAVE DE VERIFICACIÓN	ESPECIFICACIONES DE LOS BIENES O SERVICIOS	UNIDAD DE MEDIDA	CANTIDAD SOLICITADA	PRECIO (MN) UNITARIO	PRECIO (MN) TOTAL
		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) Registro de teclas (key loggers) •Debe permitir configurar la misma reacción que el software antivirus, o una diferente para este tipo de programas. •Debe ser capaz de hacer la detección y limpieza en disco, memoria y registro de Windows. •Sistema de administración centralizada de las soluciones antivirus. 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. •Deben incluir de fábrica reportes y búsquedas de todos los productos que maneje. Estos reportes y búsquedas se deben modificar y copiar para que el cliente tenga sus propias búsquedas y reportes en base a los de fábrica del 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, debe ver y actualizar eventos del servidor, guardarlos en un archivo o imprimirlos. •La solución debe permitir la organización lógica de los equipos que son administrados en un directorio El directorio se debe 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 debe permitir 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 debe permitir que por medio de una tarea, los equipos sean enviados automáticamente a su grupo correspondiente por la dirección IP. •El sistema debe permitir 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 deben generar, entre otras, en base a las siguientes características: Dirección IP Nombre del equipo Nombre del dominio •El directorio debe contar con un grupo donde se almacén los equipos para los que no se puede determinar su ubicación adecuada en el directorio. La solución debe utilizar las direcciones IP, los nombres de equipos, los nombres de dominio y los nombres de grupo para determinar dónde situarlos.				

NO. DE PARTIDA	CLAVE DE VERIFICACIÓN	ESPECIFICACIONES DE LOS BIENES O SERVICIOS	UNIDAD DE MEDIDA	CANTIDAD SOLICITADA	PRECIO (IVA INCLUIDO)	
					UNITARIO	TOTAL
		•El sistema de administración debe ser 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 de administración centralizada debe contar 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 Cada repositorio de almacenamiento distribuido mantiene una copia idéntica de los paquetes que están en el repositorio principal Los repositorios de almacenamiento distribuidos deben ser creados y administrados desde el servidor central, a través de la consola •No debe ser 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 debe ser actualizados desde el servidor central •La descarga de los archivos hacia los clientes debe 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. •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 deben 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 Server, Linux, y antivirus para servidores de correo electrónico al menos. •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.				

NO. DE PARTIDA	CLAVE DE VERIFICACIÓN	ESPECIFICACIONES DE LOS BIENES O SERVICIOS	UNIDAD DE MEDIDA	CANTIDAD SOLICITADA	PRECIO (IVA INCLUIDO)	
					UNITARIO	TOTAL
		•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 cuáles 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 el administrador pueda forzar desde la consola la comunicación del agente al servidor. Esta función se puede aplicar a un solo agente a todo un grupo, permitiendo también determinar un periodo de tiempo en el que aleatóriamente se forzará esta comunicación, en el caso de que sean muchos los agentes. •Debe 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, o manualmente el administrador la puede disparar desde la consola. También permitir al administrador que productos se actualizarán y qué 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 puede determinar qué productos y qué tipo de actualización debe ser automática y cuales manuales, incluso poder configurar diferentes métodos o tipo dependiendo del producto o del grupo. •Los reportes de la herramienta de administración deben generarse desde la misma consola. Los reportes permitir 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 proporcionar 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 actualizado el directorio con la red de forma automática.				

NO. DE PARTIDA	CLAVE DE VERIFICACIÓN	ESPECIFICACIONES DE LOS BIENES O SERVICIOS	UNIDAD DE MEDIDA	CANTIDAD SOLICITADA	PRECIO (IVA INCLUIDO)	
					UNITARIO	TOTAL
		•El sistema debe contar 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) así como contar también con reportes específicos de este componente. •El sistema debe enviar notificaciones de eventos que sucedan en sus componentes; las notificaciones serán en base a reglas definidas por el administrador, estas reglas que utilizan al menos los siguientes parámetros: Nivel del directorio.- se puede determinar a qué nivel del directorio debe aplicar cada regla. El sistema de administración debe permitir 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 •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 debe permitir detener ataques aún cuando no existe una firma específica, ataques día cero. •El IPS debe crear eventos en la consola central cuando detenga un ataque, en base a esta información el administrador puede crear excepciones, que eviten la aplicación de la regla cuando se cumplan los criterios de la excepción. •También debe permitir al administrador, en base esta información de los eventos, crear una lista de aplicaciones seguras, a las que no se le apliquen las reglas de IPS				

NO. DE PARTIDA	CLAVE DE VERIFICACIÓN	ESPECIFICACIONES DE LOS BIENES O SERVICIOS	UNIDAD DE MEDIDA	CANTIDAD SOLICITADA	PRECIO (IVA INCLUIDO)	
					UNITARIO	TOTAL
		•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 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 puede crear las reglas que permitan o eviten la ejecución de las aplicaciones en las máquinas cliente. •El bloqueo de aplicaciones también debe permitir detener aplicaciones que tratan de ligarse con otros procesos para ejecutarse, cuando estas aplicaciones son programas maliciosos. •El administrador puede determinar si se aplican los dos tipos de bloqueo, el de ejecución y el de ligado de aplicaciones, o los dos. •La solución debe estar certificada por ICSA Labs y West Coast Labs •Debe ofrecer protección antiphising • Debe contar con Software Antispam con las siguientes funciones mínimas: - Integración con Microsoft Exchange Standard 2010. - Comprobación de los mensajes de correo electrónico entrantes para determinar si son legítimos. El correo electrónico que se reconozca como no solicitado se deberá etiquetar y enviar a una carpeta independiente. - Impedir que el correo electrónico no solicitado entre en la bandeja de entrada. Contar con reglas de filtrado avanzadas de antispam que permitan actualizarse automáticamente para todas las cuentas de correo electrónico. Permitir la creación de filtros personalizados para definir qué buscar en un mensaje y ajustar el nivel de filtrado (de menos agresivo a más agresivo) según las necesidades. - Protección contra phishing, identificar los posibles sitios Web de phishing que solicitan información personal. Redirigir a una página segura si se intenta acceder a un sitio Web fraudulento o posiblemente fraudulento, ofrecer información acerca de las razones por las que el sitio se clasificó como sitio de phishing y permitir decidir si desea visitarlo. Agregar a una lista blanca si se considera que es un sitio seguro. - Contar con lista de amigos para recibir siempre sus mensajes de correo electrónico. - Filtro de webmail •Un año de soporte telefónico, soporte vía Web y Chat de 24 X 7 Capacitación del uso y administración del software antivirus por lo menos a 2 personas en instalaciones que el área usuaria solicitante defina.				

NO. DE PARTIDA	CLAVE DE VERIFICACIÓN	ESPECIFICACIONES DE LOS BIENES O SERVICIOS	DE MEDIDA	SOLICITADA	UNITARIO	TOTAL
		Por las características propias del software, y para garantizar el éxito del mismo, el oferente adjudicado debe: Revisar la compatibilidad e instalar, configurar, probar y poner a punto la totalidad de las licencias del presente dictamen técnico.				
					IMPORTE TOTAL	$199,999.66

VALIDACIÓN DEL ANEXO

POR EL CONTRATANTE	POR EL PROVEEDOR
EDGAR RICARDO SIERRA VARELA DIRECTOR GENERAL DE ADMINISTRACIÓN Y SERVICIOS DE LA SECRETARIA DE SEGURIDAD CIUDADANA.	C. JORGE LUIS BECERRIL VAZQUEZ REPRESENTANTE LEGAL.