



HONORABLE SENADO DE LA NACIÓN

SUBDIRECCIÓN DE COMPRAS
 H. Yrigoyen 1710 - piso 2° - Of. - 228
 Te.:4010-3250/2 fax 4010-3253
 www.senado.gov.ar

PLIEGO DE BASES Y CONDICIONES

| | | |
|---|---|----------------------|
| EXPEDIENTE HSN- 2836 / 2014 | APERTURA DE LAS OFERTAS | |
| ACTUACION: LICITACION PUBLICA N° 27 / 2014 MODALIDAD: SIN MODALIDAD | Fecha 22/12/2014 | Hora 13:00 |
| IMPRESINDIBLE PRESENTAR JUNTO CON LA OFERTA: - Precios a consumidor final en pesos - Certificado de Inscripción en la A.F.I.P. - Documento por 5% del Valor Total Cotizado - Complemento de Declaración Jurada Adjunta Firmada en Anverso y Reverso | ANUNCIO DE PREADJUDICACIÓN Y PLAZO DE IMPUGNACIÓN PUBLICADO EN CARTELETA SUBDIRECCIÓN DE COMPRAS Y EN LA PÁGINA DE INTERNET WWW.SENADO.GOV.AR C. DIRECTA: 1 día de Anuncio y 3 días de Impugnación. L. PRIVADA: 2 día de Anuncio y 3 días de Impugnación. L. PÚBLICA: 3 día de Anuncio y 3 días de Impugnación. | |
| En caso de poseer "NUMERO DE ALTA BENEFICIARIO" (SISTEMA DE CUENTA UNICA DE TESORO), implementado por el Ministerio de Economía y Obras y Servicios Públicos, se deberá adjuntar a la oferta comprobante del mismo. Para el caso de no poseerlo y resultar adjudicatario/a, se deberá proceder a su tramitación para la presentación de la factura. | | |
| VALIDEZ DE LA OFERTA: 30 DÍAS HÁBILES | | |
| PLAZO DE PRESTACIÓN : DENTRO DE LOS 60 (SESENTA) DÍAS CORRIDOS CONTADOS A PARTIR DE LA RECEPCIÓN DE LA ORDEN DE COMPRA. DEBERÁ SER CONCLUIDA LA CONSOLA DE ADMINISTRACIÓN CON LA PROVISIÓN DEL SOFTWARE SOLICITADO, DE LAS LICENCIAS Y LA INSTALACIÓN DEL SOFTWARE ANTIVIRUS EN LAS ESTACIONES DE TRABAJO. EL SERVICIO DE MANTENIMIENTO SERÁ POR EL TERMINO DE 2 (DOS) AÑOS CON OPCIÓN A PRORROGA HASTA 1 (UN) AÑO MAS A PARTIR DEL ACTA DE INICIO. | | |
| CONDICIONES DE PAGO: LA FACTURACIÓN SERÁ POR EL TOTAL DE LA ORDEN DE COMPRA Y EL PAGO DENTRO DE LOS 30 (TREINTA) DÍAS HÁBILES DE CONFECCIONADO EL CERTIFICADO DE RECEPCIÓN DEFINITIVA PREVIA ENTREGA EN LA SUBDIRECCIÓN DE COMPRAS DE UNA PÓLIZA DE SEGURO DE CAUCIÓN, CON CERTIFICACIÓN NOTARIAL Y LEGALIZADA POR EL COLEGIO DE ESCRIBANOS, A FAVOR DE ESTE H. SENADO DE LA NACIÓN POR EL TOTAL, EN CONCEPTO DE CONTRAGARANTÍA Y DE LA CORRESPONDIENTE GARANTÍA DE ADJUDICACIÓN. | | |

"IMPORTANTE"
PRESENTACIÓN DE LAS OFERTAS:

LAS OFERTAS DEBERÁN SER EN FORMULARIOS DE LA FIRMA IDENTIFICADO CON UNA "X" SEGÚN ART. 9° DE LA R.G. 3803/94, CON LA LEYENDA "DOCUMENTO NO VÁLIDO COMO FACTURA", REDACTADOS POR EL OFERENTE O SU REPRESENTANTE AUTORIZADO, POR DUPLICADO, FIRMADAS EN TODAS SUS HOJAS Y PRESENTADAS EN SOBRE COMÚN, INDICANDO LA ACTUACIÓN CORRESPONDIENTE, FECHA Y HORA DE APERTURA.

Saluda a Ud muy atentamente

SERGIO BIANCHETTI
 Jefe Depto. de Contrataciones y
 Licitaciones
 Subdirección de Compras
 H. Senado de la Nación

SEÑOR PROVEEDOR: Sírvase cotizar precio por el suministro que se indica a continuación, de acuerdo con las especificaciones que se detallan, conforme lo establecido por el Decreto 1023/01, reglamentado DP 632/02 de este H. Senado de la Nación.-

| Renglón | Cantidad | Descripción |
|---------|----------|---|
| 1 | 1 | SOLUCION DE ANTIVIRUS,ANTISPYWARE,ANTISPAM,ANTIPHISHING, FILTRADO DE CONTENIDO DE PERIMETRO SOBRE LOS PROTOCOLOS HTTP - FTP Y ANÁLISIS DE AMENAZAS DE PERÍMETRO SOBRE LOS PROTOCOLOS SMTP Y DE MENSAJERÍA INSTANTÁNEA. LA SOLUCIÓN A PROVEER INCLUIRÁ: SOFTWARE, HARDWARE, SOPORTE TÉCNICO E IMPLEMENTACIÓN INICIAL. TODO SEGÚN LOS ANEXOS I (PLIEGO DE BASES Y CONDICIONES PARA LA CONTRATACIÓN DE SUMINISTROS Y SERVICIOS) Y ANEXO II (CONSIDERACIONES PARTICULARES). |

CLAUSULAS GENERALES:

- 1- Si la oferta supera el importe de Pesos cincuenta mil (\$ 50.000) el oferente deberá poseer el **CERTIFICADO FISCAL PARA CONTRATAR** (Resolución Gral. 1814/05 de la A.F.I.P.).-
- 2- Para el caso que la garantía de oferta supere los Pesos cinco mil (\$ 5.000) el oferente no podrá presentar pagaré. En cuyo caso deberá optar por alguna de las formas o sus combinaciones, que se establecen en el Art. 34 del Decreto DP 632/02 (Reglamento para la Contratación de Bienes, Obras y Servicios del H. Senado de la Nación). En el caso que oferente presente una Póliza de Seguro de Caucción certificada por Escribano. Respecto a su legalización de la firma ante el Colegio Notarial pertinente, solo será en los casos de extraña jurisdicción, es decir que no será necesario legalizar la firma de los Escribanos registrados en la Ciudad Autónoma de Buenos Aires.
- 3- Toda vez que personal de una empresa requiera ingresar a este H. Senado de la Nación, deberá presentar la cobertura de A.R.T. (Aseguradora De Riesgo De Trabajo).
- 4- **RESPONSABILIDAD:** La adjudicataria será la única y exclusiva responsable y se obligará a reparar la

totalidad de los daños y perjuicios de cualquier naturaleza que se produzcan con motivo o en ocasión del servicio, trabajo o suministro que se realice, ya sea por su culpa, dolo o negligencia, delitos y/o cuasidelitos, actos y/o hechos del personal bajo su dependencia, o por las cosas de su propiedad y/o que se encuentren bajo su guarda o custodia.-

5- NOTA:El H. Senado de la Nación podrá rescindir el contrato por razones de oportunidad, mérito y conveniencia, sin que el contratista pudiera alegar derecho a indemnización alguna, notificándole tal decisión al domicilio constituido con una anticipación de 30 días.

6-Para asistir a presenciar el acto de apertura se deberá acreditar identidad.-

CLÁUSULAS PARTICULARES:

- 1- SOPORTE TÉCNICO Y GARANTÍA DEL BUEN FUNCIONAMIENTO: Ver Anexo II.
 - 2- CONTENIDO DE LA OFERTA: El precio del servicio aquí solicitado deberá ser cotizado en Pesos incluyendo todos los impuestos. La oferta deberá ser cotizada íntegramente, es decir, "No se admitirán cargos por instalación del servicio ofrecido". Serán declaradas inadmisibles las ofertas que modifiquen o condicionen las cláusulas del presente pliego y/o impliquen apartarse del régimen aplicado.
- Todos los requerimientos técnicos del objeto de esta licitación y enumerados en este Pliego de Bases y Condiciones Particulares, deben ser considerados mínimos, pudiendo el Oferente presentar ofertas cuyas características superen o mejoren las aquí solicitadas.

APERTURA DE OFERTAS: 22/12/2014

SUBDIRECCIÓN DE COMPRAS - H. Yrigoyen 1710 - piso 2° - Of. - 228 - CABA

VENTA DEL PLIEGO:
Desde el: 25/12/2014

Hasta el: 05/12/2014

Lugar de venta del pliego: Dirección Tesorería- H.Yrigoyen 1710, Piso 2 "219" - CABA

CONSULTAS: Hasta el día 09/12/2014

RESPUESTAS: Hasta el día 17/12/2014

LUGAR DE PRESTACIÓN : DIRECCIÓN DE INFORMÁTICA - H. YRIGOYEN 1710 3° PISO

VALOR DEL PLIEGO: Pesos diez Con 00/100 (\$ 10,00)



SERGIO BIANCHETTI
Jefe Depto. de Contrataciones y Licitaciones
Subdirección de Compras
H. Senado de la Nación

ANEXO I

PLIEGO DE BASES Y CONDICIONES PARA LA CONTRATACIÓN DE SUMINISTROS Y SERVICIOS

64

ARTÍCULO 1º: OBJETO:

El presente pliego tiene por objeto definir las bases del llamado a LICITACIÓN PÚBLICA N° 27/2014 para la contratación del servicio de Solución Antivirus para el H. Senado de la Nación.-

ARTÍCULO 2º: ADQUISICIÓN DEL PLIEGO:

El pliego correspondiente al presente llamado podrá adquirirse, desde el día 25 de NOVIEMBRE de 2014 y hasta el día 05 de DICIEMBRE de 2014, en la Dirección de Tesorería del H. Senado de la Nación, sita en Hipólito Yrigoyen N° 1.708, piso 2º, Oficina 219, en el horario de 11 a 17 hs., teniendo el mismo un costo de **PESOS DIEZ (\$10,00)**.

ARTÍCULO 3º: ACLARACIONES Y EVACUACIÓN DE CONSULTAS:

Las consultas deberán formularse por escrito, en papel membretado perteneciente a la empresa o consorcio de empresas que haya adquirido el presente pliego, hastadías hábiles anteriores a la fecha fijada para el acto de apertura correspondiente.

Si con motivo de las consultas en cuestión fuera necesario complementar, especificar y/o detallar con mayor precisión las prescripciones del Pliego, el Organismo emitirá Notas Aclaratorias que serán consideradas como partes integrantes del mismo y dará cuenta de ellas, en forma fehaciente, a todo los proponentes.

ARTÍCULO 4º: VISITA A INSTALACIONES:

Los proponentes deberán realizar la visita a las instalaciones conjuntamente con personal del área.....del H. Senado de la Nación, el díadede....., a las.....hs., quien extenderá el certificado correspondiente.

ARTÍCULO 5º: NORMATIVA APLICABLE:

Será aplicable al presente llamado y a la contratación que se celebre, la siguiente normativa, en el orden de prelación que se consigna:

1. Decreto N° 1.023/01 y su reglamentación para el H. Senado de la Nación por D.P.-632/02.
2. Pliego único de bases y condiciones generales para el H. Senado de la Nación y/o las especificaciones técnicas particulares, en caso de corresponder.
3. El contrato que se suscriba.

ARTÍCULO 6º: FORMA DE PRESENTACIÓN Y CONTENIDO DE LAS OFERTAS:

Las ofertas deberán presentarse en la Subdirección de Compras hasta el día y hora fijados por la misma para la apertura del presente llamado a LICITACIÓN PÚBLICA N° 27/2014.-

La oferta por los trabajos, suministros o servicios será expresada en **pesos**; se presentará en formulario de la firma cotizante, en el cual se indique el monto total del servicio o suministro solicitado, como así también el valor unitario de cada uno de los ítems -y/o subítems en su caso- requeridos, incluyendo la forma y el plazo de pago previstos en el presente Pliego de Bases y Condiciones; estará foliada en todas y cada una de sus hojas y rubricada por el titular de la firma o persona autorizada para tal fin, reservándose el Organismo el derecho a exigir comprobante de acreditación cuando lo considere pertinente.

La oferta se presentará dentro de un sobre cerrado, al que se denominará **sobre único**, el cual llevará en su parte exterior solamente la indicación del número y procedimiento de selección y la fecha y hora de apertura, de modo tal que ninguna de las ofertas pueda individualizarse antes del inicio del acto de apertura correspondiente. Dicho sobre contendrá la siguiente documentación:

1. Recibo de compra del pliego;
2. Recibo de garantía de oferta o Póliza de Seguro de Caución por igual concepto;
3. Certificado de visita a las instalaciones.
4. Pliego de bases y condiciones, firmado en todas sus hojas; Antecedentes societarios:
 - a) Fotocopia del estatuto o contrato social inscripto en el Registro respectivo;
 - b) Fotocopia de las Actas en las cuales conste la designación de los miembros de los órganos directivos y de fiscalización de la empresa de acuerdo al art. 60 de la Ley 19.550;
 - c) Balances Generales y Estados de Resultados, de los dos últimos ejercicios económicos vencidos a la fecha de presentación de las ofertas, certificados por Contador Público Nacional y legalizados por el Consejo Profesional de Ciencias Económicas;
5. Oferta económica por el trabajo, suministro o servicio solicitado, con indicación del precio total ofertado en pesos y discriminación del valor unitario de cada uno de los artículos o ítems requeridos en los renglones pertinentes.

ARTÍCULO 7º: PLAZO DE MANTENIMIENTO DE LAS OFERTAS:

El plazo de mantenimiento de las ofertas será de treinta (30) días hábiles a partir de la fecha del acto de apertura. Dicho plazo se considerará prorrogado automáticamente, por períodos iguales, sin necesidad de requerimiento por parte del Organismo, salvo que el oferente manifieste en forma fehaciente su voluntad de no renovar su oferta, por lo menos con diez (10) días de anticipación al vencimiento del plazo. El desistimiento del oferente fuera de esta alternativa lo hará pasible de la pérdida de la garantía de oferta.


SERGIO BIANCHETTI
Jefe Depto. de Contrataciones y

ARTÍCULO 8º: GARANTÍAS:

La garantía de la oferta tiene carácter de obligatoria para el presente llamado y será del **cinco por ciento (5%)** del valor de la oferta. Si hubiere presupuesto Oficial la garantía de oferta se calculará sobre este último.

ARTÍCULO 9º: CAUSALES DE INADMISIBILIDAD Y DE DESCALIFICACIÓN AUTOMÁTICA: Serán causales de **inadmisibilidad** de las ofertas, que implicarán la no aceptación de su presentación, las siguientes: **a)** Extemporaneidad por vencimiento del horario establecido para el día de la apertura; **b)** Pretensión de entrega en lugar distinto al consignado en el pliego de bases y condiciones; **c)** Que la leyenda consignada en el exterior del sobre no se ajuste a lo establecido en el pliego de bases y condiciones; **d)** Cualquier cotización que se aparte de las prescripciones contenidas en el artículo 6º del presente, o alteración de la forma de pago.

Serán causales de **descalificación automática** las previstas en el artículo 56 del Anexo I del D.P.-632/02, sin perjuicio de otras que pudiere merituar en su oportunidad la Junta de Evaluación.

ARTÍCULO 10º: EVALUACIÓN DE LAS OFERTAS:

La Junta de Evaluación efectuará el estudio de las mismas, labrará un Acta en la cual emitirá el dictamen, recomendando la adjudicación de aquella que a su juicio resulte más conveniente a los intereses del Organismo.

ARTÍCULO 11º: IMPUGNACIONES:

El Acta con el dictamen de la Junta de Evaluación se expondrá en la hoja que posee el H. Senado de la Nación en Internet (www.senado.gov.ar) y en la cartelera de la Subdirección de Compras por el término de TRES (3) días hábiles, pudiendo los oferentes presentar las impugnaciones que crean oportunas hasta TRES (3) días hábiles posteriores al vencimiento del plazo de los anuncios. Transcurrido dicho plazo no se admitirá impugnación alguna y se seguirá con el trámite de forma para la contratación.

De existir impugnaciones presentadas en tiempo y forma oportuna, las mismas se trasladarán a las dependencias competentes para su dictamen. En este caso, el plazo de mantenimiento de las ofertas quedará automáticamente suspendido, hasta la resolución de aquellas. El monto de la garantía de impugnación será el establecido en el art. 33, inc. d) del Anexo I del D.P.-632/02.

ARTÍCULO 12º: DOMICILIO LEGAL:

El oferente deberá constituir domicilio legal en la Ciudad Autónoma de Buenos Aires.

ARTÍCULO 13º: FIRMA Y AFIANZAMIENTO DEL CONTRATO:

Luego de la adjudicación y dentro de los ...⁵... días hábiles de la misma, se procederá a la firma del contrato respectivo entre las partes. El adjudicatario deberá concretar la constitución de la garantía del contrato, en las mismas condiciones que la garantía de la oferta, dentro de los ocho días de firmado el contrato o recibida la orden de compra. La misma será del quince por ciento (15%) del monto total del contrato.

La falta de presentación del adjudicatario, sin causa justificada, a la firma del contrato, pasados cinco (5) días de la fecha prevista al efecto, producirá la caducidad de la adjudicación y la ejecución de la garantía de la oferta.

ARTÍCULO 14º: CUIT. IMPUESTOS:

Los precios cotizados incluirán el Impuesto al Valor Agregado sin discriminar, considerando al H. Senado de la Nación como consumidor final.

ARTÍCULO 15º: MULTAS:

Será de aplicación lo dispuesto por el art. 80 del Anexo I del D.P.-632/02.

ARTÍCULO 16º: RESPONSABILIDAD:

La adjudicataria será la única y exclusiva responsable y se obligará a reparar la totalidad de los daños y perjuicios de cualquier naturaleza que se produzcan con motivo o en ocasión del servicio, trabajo o suministro que se realice, ya sea por su culpa, dolo o negligencia, delitos y/o cuasidelitos, actos y/o hechos del personal bajo su dependencia, o por las cosas de su propiedad y/o que se encuentren bajo su guarda o custodia.

ARTÍCULO 17º: SEGURO:

Es obligación de la adjudicataria tener cubierto a todo el personal que utilice para la realización del servicio, trabajo o suministro objeto del presente pliego, según corresponda con una Aseguradora de Riesgo de Trabajo, debiendo presentar la nómina completa del personal que será afectado al mismo con el certificado de la respectiva A.R.T..

ARTÍCULO 18º: FORMA DE FACTURACIÓN Y CONDICIONES DE PAGO:

La facturación será por el total de la Orden de Compra y el pago dentro de los 30 (treinta) días hábiles de confeccionado el certificado de Recepción Definitiva previa entrega en la Subdirección de Compras de una Póliza de Seguro de Caucción, con Certificación Notarial y legalizada por el Colegio de Escribanos, a favor de este H. Senado de la Nación por el total, en concepto de contragarantía y de la correspondiente garantía de adjudicación.


SERGIO BIANCHETTI
Jefe Depto. de Contrataciones y
Licitaciones
Subdirección de Compras
H. Senado de la Nación

Solución Antivirus para el HSN



Índice

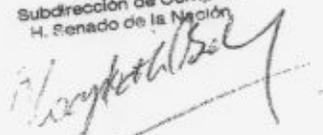
CONSIDERACIONES PARTICULARES

| | |
|--|----|
| Objeto | 1 |
| Duración del Servicio | 1 |
| Tareas del oferente | 1 |
| Equipamiento a cubrir con la solución | 1 |
| Vínculos a ser protegidos por las soluciones de borde | 1 |
| Nivel Funcional de Dominio | 1 |
| Especificaciones técnicas | 2 |
| <i>Antivirus para servidores y estaciones de trabajo</i> | 2 |
| Características | 2 |
| Mínimos Requerimientos de los clientes (32-bit): | 4 |
| Mínimos Requerimientos de los clientes (64-bit): | 4 |
| Consola de administración | 4 |
| Valoración tecnológica | 5 |
| <i>Antivirus para servidor de correo electrónico</i> | 6 |
| Características | 6 |
| Valoración tecnológica | 6 |
| <i>Filtrado de contenido en el gateway sobre los protocolos SMTP y IM (Mensajería instantánea)</i> | 7 |
| Características | 7 |
| Consola de administración | 9 |
| <i>Filtrado de contenido en el gateway sobre los protocolos HTTP y FTP</i> | 10 |
| Características | 10 |
| Consola de administración | 11 |

CONSIDERACIONES GENERALES

| | |
|--|----|
| <i>Análisis Técnico de la propuesta</i> | 12 |
| <i>Administración Centralizada de las soluciones</i> | 12 |
| <i>Recepción definitiva</i> | 12 |
| <i>Plazo, lugar y forma de entrega</i> | 13 |
| <i>Soporte técnico y garantía de buen funcionamiento</i> | 13 |
| <i>Penalidades por incumplimiento de los tiempos estipulados</i> | 14 |
| <i>Consultas, Aclaraciones y Respuestas a Consultas</i> | 14 |
| <i>Contenido de la oferta</i> | 14 |


SERGIO BIANCHETTI
Jefe Depto. de Contrataciones
Licitaciones
Subdirección de Compras
H. Senado de la Nación


Lic. GLADYS ABRAHAM,
Directora de Dirección de Informática
H. Senado de la Nación

CONSIDERACIONES PARTICULARES

Objeto

El presente llamado a licitación tiene por objeto la adquisición de una solución de Antivirus, Antispyware, Antispam, Antiphishing, Filtrado de contenido de perímetro sobre los protocolos HTTP/FTP y Análisis de amenazas de perímetro sobre los protocolos SMTP y de Mensajería Instantánea. La solución a proveer incluirá: software, hardware, soporte técnico e implementación inicial.

Duración del Servicio

El período del servicio de Mantenimiento, que incluye: actualización de los motores, definiciones de virus y el Upgrade de versiones, será por el término de 2 (dos) años con la opción de prórroga hasta 1 (un) año más.

Tareas del oferente

Corresponde al oferente:

- La desinstalación del software antivirus presente actualmente en las estaciones de trabajo y en los servidores.
- La instalación y configuración del Software de antivirus en las estaciones de trabajo y en los servidores.
- La instalación y configuración de todo el Software propio de la solución.
- La instalación y configuración de los filtros de contenido en los Gateways SMTP/IM y HTTP/FTP.

Equipamiento a cubrir con la solución

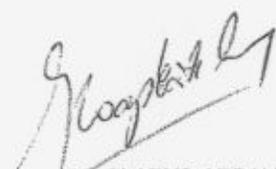
- 1300 Estaciones de trabajo Windows 7 /8.
- 5 Servidores Windows 2012 que cumplen funciones administrativas (DC, DNS, DHCP, PRINTER, etc.).
- 1 Servidor de Archivo propio del Storage EMC² VNX 5300.
- 2 Servidores de correo Exchange 2010.

Vínculos a ser protegidos por las soluciones de borde

El HSN se encuentra conectado a Internet a través de dos enlaces de 100MB cada uno.

Nivel Funcional de Dominio

En todos aquellos casos en que se requiera la integración con LDAP o Active Directory deberá ser compatible con el nivel funcional de dominio: Windows Server 2012


Lic. GLADYS ABRAHAM
Directora de Dirección de Informática
H. Senado de la Nación


SERGIO BIANCHETTI
Jefe Depto. de Contrataciones y
Licitaciones
Administración de Compras

Especificaciones técnicas

68



Antivirus para servidores y estaciones de trabajo

Características

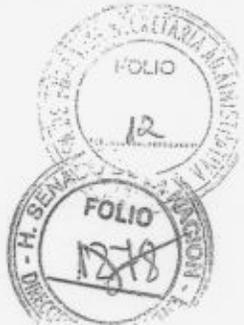
El software antivirus de los servidores y estaciones de trabajo debe contar con las siguientes características técnicas:

- Instalación y actualización en forma centralizada y desatendida, en forma transparente sin la necesidad de que intervenga el usuario final.
- Corroborar la existencia de otro Anti-Virus instalado (durante el proceso de instalación).
- Instalación, configuración y administración centralizada con opción a administrar múltiples dominios.
- Protección por contraseña en equipos cliente de la configuración y desinstalación del software antivirus.
- Contar con los siguientes métodos para la instalación:
 - En forma remota desde la consola de administración hacia las estaciones clientes y/o servidores.
 - Desde el propio cliente, a través de conexiones de red o por medio de medios extraíbles.
- Las plataformas que deberán ser soportadas en los equipos son:
 - Windows XP 32 bit / 64 bit
 - Windows Server 2003/8/12 32 bit / 64 bit (En todas sus versiones: Estándar, Enterprise, Data Center, Web Edition, R2, etc.)
 - Windows 7, Windows 8 (En todas sus versiones).
- Poseer certificación ICSA.
- Métodos de rastreo y/o detección al inicio del sistema operativo, en tiempo real, en demanda, programado y en forma remota.
- Rastreo y/o detección de amenazas en archivos, carpetas, discos y archivos compactados en distintos niveles.
- Permitir especificar los tipos de archivos a revisar en busca de amenazas:
 - Todos los archivos
 - Archivos potencialmente riesgosos, verificando en el encabezado del archivo el tipo real de archivo.
 - Extensiones riesgosas y definidas por el usuario.
- Permitir especificar la acción a tomar con los archivos infectados ante la detección de virus por cualquiera de los métodos de rastreo seleccionados.
- Acciones posibles sobre los archivos infectados:
 - Limpiarlos
 - Borrarlos
 - Ponerlos en cuarentena
 - Pasarlos por alto
- Revisión automática de la transferencia de archivos entre clientes y servidores.
- Revisión automática sobre el protocolo POP3.
- Permitir bloqueo de archivos o puertos específicos y el bloqueo de carpetas compartidas.
- Motor y firmas (patrones de búsqueda) propietario de la marca que provee la solución.
- Actualizaciones manuales y automáticas.
- Ejecución de escaneos de manera manual y programada.
- Detección y eliminación de todo tipo de virus y amenazas, conocidos y desconocidos, independientemente del nombre que se le dé en la jerga (Virus, Worms, Troyanos, Virus de red, Spywares, Graywares, Adwares, Rootkits, Dialers, Pharming, Hijacking, JokesPrograms,



Hacking tools, Remote-accesstools, Password cracking, Key loggers, Gusanos, Payload, Scam, Hoax, etc.).

- Detectar de forma heurística nuevas variantes de virus.
- Detección y eliminación de todo tipo de virus y amenazas, conocidos y desconocidos ubicados en:
 - Memoria
 - Sector de arranque
 - Archivos en General
 - Macros
 - Script
 - Java Script
 - Archivos comprimidos
 - Unidades de red
 - Bases de datos en formato PST
- Capacidad de búsqueda de código malicioso en archivos de hasta 10 capas de compresión en los siguientes formatos de compresión:
 - PKZIP, LHA, LZH, ARJ, MIME, TAR, GZIP, RAR, BZIP2, PKLITE, LZEXE, UUCODE, BINHEX.
- Capacidad de exceptuar directorios o carpetas a rastrear.
- Registro de infecciones en un registro de actividades.
- Notificación al administrador de la red ante la detección de virus, por medio de mensajes vía correo electrónico.
- Las notificaciones deben ser completamente personalizables, mediante mensajes pre-configurables.
 - Notificaciones Virus/Malware
 - Enviar notificación cuando un Virus/Malware es detectado.
 - Enviar notificación solo cuando la acción sobre Virus/Malware es insatisfactoria.
 - Notificaciones Spyware/Grayware
 - Enviar notificación cuando un Spyware/Grayware es detectado.
 - Enviar notificación solo cuando la acción sobre Spyware/Grayware es insatisfactoria.
- Opción de poder especificar qué tipos de Logs se desea guardar y cuáles no, como así también especificar cuánto tiempo de almacenamiento se dejarán.
- Administrar los siguientes tipos de logs:
 - Log de Virus/Malware.
 - Log de Spyware/Grayware.
 - Log de Firewall.
 - Log de Componentes de Actualización.
 - Log de Actualizaciones del Servidor.
 - Log de Eventos del Sistema.
- Integración con Active Directory, pudiendo detectar las pcs que no tengan protección antivirus.
- Control y bloqueo de acceso a dispositivos externos de almacenamiento y recursos de red para prevenir la fuga de información e infecciones de malware.
- Poder auto proteger sus servicios y ramas de registro donde este instalada.
- Capacidad de evitar la ejecución de aplicaciones o procesos específicos.
- Detectar y evitar cambios en los principales componentes del sistema operativo.
- Capacidad de analizar el tráfico de red entrante y saliente, con la posibilidad de crear políticas de firewall para controlarlo.
- Actualizaciones incrementales con la posibilidad de deshacer su aplicación y volver hacia una actualización anterior.



Mínimos Requerimientos de los clientes(32-bit):

- Pentium IV (1GHz para Windows Xp)
- 1GB RAM
- 260 MB disco (adicionamiento podrá utilizar 600 MB durante la instalación)

Mínimos Requerimientos de los clientes (64-bit):

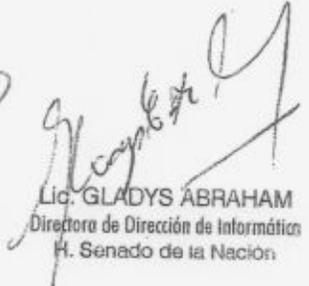
- 1 GHz con alguno de los siguientes procesadores: Intel Xeonwith Intel EM64T support, Intel Pentium IV with EM64T support, AMD 64-bit Opteron™!, AMD 64-bit Athlon™!
- 1 GB RAM
- 260 MB disco (adicionamiento podrá utilizar 600 MB durante la instalación)

Consola de administración

- Deberá contar con una consola de administración, cuarentena y control centralizado de las estaciones de trabajo y servidores.
- Con acceso desde cualquier estación de trabajo (Administración remota), por medio de Interfaz Web. Con la posibilidad de tener comunicación encriptada.
- Para ingresar a la consola se deberá ingresar una contraseña de acceso y desde la misma se podrá:

- Gestionar los clientes y servidores
- Configurar y actualizar la solución,
- Aplicar políticas globales, por grupo, o en forma individual.
- Centralizar y visualizar los logs, informes y reportes.
- Informar sobre actualizaciones, máquinas administradas.
- Suministrar la siguiente información de las estaciones de trabajo y servidores:
 - Sistema Operativo.
 - Nombre de la PC y número IP.
 - Fecha de instalación del Antivirus.
 - Lista de Virus encontrados.
 - Versión del motor de rastreo.
 - Estado.
 - Intentos de infección.
- Informes que muestren:
 - Versiones de definiciones (firmas) y motor de búsqueda.
 - Detección de Virus.
 - Tareas Programadas.
- Permitir la creación de distintos perfiles de acceso y administración, con distintos privilegios y roles.
- Programación de actualizaciones hacia todos los clientes y servidores en modo automático, centralizado y desatendido desde un repositorio ubicado en la LAN, seleccionando una estación de trabajo, un grupo de estaciones o la totalidad de las mismas. Con actualizaciones incrementales.
- Para la actualización de los motores o de la definición de virus, el producto no debe requerir el re-inicio de las estaciones de trabajo ni de los servidores.
- Proveer mecanismos de Roll Back que permitan volver a la definición de virus o versión de motor anterior, luego de una distribución.


SERGIO BIANCHETTI
 Jefe Depto. de Contrataciones y
 Uctitaciones
 Subdirección de Compras
 H. Senado de la Nación


 Lic. GLADYS ABRAHAM
 Directora de Dirección de Informática
 H. Senado de la Nación

Ing. OSCAR E. ANCELISTA
 DIRECTOR ADJUNTO
 DIRECCIÓN DE INFORMATICA
 H. SENADO DE LA NACION

41



Valoración tecnológica

Se valorarán tecnológicamente funcionalidades adicionales como ser:

- Reputación de archivos como reemplazo de la tecnología de rastreo de virus tradicional por firmas.
- Reputación web para detección de acceso a sitios maliciosos o relacionados con malware en la estación de trabajo donde se encuentre instalada la solución antivirus.
- Reputación Web con una protección adicional de ataques de phishing.



LIC. GLADYS ABRAHAM
Directora de Dirección de Informática
H. Senado de la Nación



SERGIO BIANCHETTI
Jefe Depto. de Contrataciones y
Licitaciones
Subdirección de Compras
H. Senado de la Nación



Antivirus para servidor de correo electrónico

Características

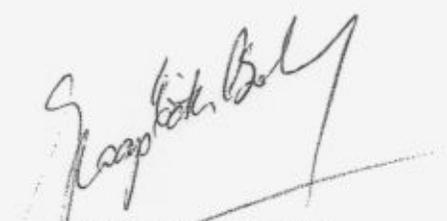
El software antivirus de los servidores de Correo Electrónico debe contar con las siguientes características técnicas:

- Operar sobre las plataformas Exchange 2010 y soportar análisis sobre los protocolos SMTP, MAPI.
- Detección y eliminación de todo tipo de virus y amenazas, conocidos y desconocidos, independientemente del nombre que se le dé en la jerga (Virus, Worms, Trojans, Virus de red, Spywares, Graywares, Adwares, Rootkits, Dialers, Phishing, Pharming, Hijacking, JokesPrograms, Hacking tools, Remote-access tools, Password cracking, Key loggers, Web Tretas, Gusanos, Payload, Scam, Hoax, etc.).
- Protección Heurística en tiempo real ante nuevas variantes de código malicioso o amenazas de día cero.
- Configuración de diferentes acciones a tomar en caso de detección de virus.
 - Limpiar los archivos infectados
 - Eliminar los archivos infectados
 - Mover los archivos infectados
- Los mensajes de correo electrónico infectados, deben llegar limpios al destinatario manteniendo al menos el cuerpo del mensaje.
- Generación automática de mensajes de alertas ante la detección de virus y correos filtrados.
- Capacidad de notificar al administrador de los eventos de virus y los eventos de sistemas que sean significativos vía Mail.
- Capacidad de elección de notificación al emisor y/o al receptor del evento de virus en el correo electrónico, pudiéndose configurar el texto del mensaje
- Capacidad de chequeo del encabezado "header" del archivo para la detección y eliminación de virus.
- Deberá tener soporte para la actualización desatendida desde una consola central y desde Internet.
- Actualizaciones incrementales y que no requieran el reinicio después de una actualización.
- Contar con servicios de cuarentena donde los usuarios finales puedan inspeccionar los mensajes, aprobar y rechazar remitentes y gestionar su propia lista de remitentes permitidos.

Valoración tecnológica

Se valorarán tecnológicamente funcionalidades adicionales como ser:

- Detección de URLs maliciosas embebidas en el correo electrónico con tecnología de reputación web.
- Detección de IPspammers según su reputación mediante consultas a base de datos externa.
- Reglas de filtrado de contenido aplicadas a usuarios o grupos de active directory.


 Lic. GLADYS ABRAHAM
 Directora de Dirección de Informática
 H. Senado de la Nación


 SERGIO BIANCHETTI
 Jefe Depto. de Contrataciones y Licitaciones
 Subdirección de Compras
 H. Senado de la Nación

Filtrado de contenido en el gateway sobre los protocolos SMTP y IM (Mensajería instantánea)

El oferente deberá proveer una solución completa. Tanto el software como el hardware necesario para implementar el filtrado en cuestión. Deberá proveer 2 (dos) equipos (compuesto por hardware y software), uno para cada enlace de modo de contar con una arquitectura tolerante a fallas. El hardware podrá ser implementado en modalidad de appliances dedicados o por medio de la provisión de servidores rackeables en no más de dos unidades cada uno. Deberá ser de primera marca y contar con discos redundantes. De requerirse licencias para sistemas operativos deberán ser incluidas en la oferta. Dado el conocimiento específico de su solución, **"el dimensionamiento del hardware necesario es responsabilidad del oferente"**. Para esto debe considerar que el H. Senado de la Nación hace uso del 100% de sus enlaces (ver: Vínculos a ser protegidos por las soluciones de borde). El oferente deberá realizar, en conjunto con el HSN, las pruebas que considere necesarias para dicho dimensionamiento. Si una vez operativo el equipamiento suministrado resultara insuficiente, el HSN exigirá al proveedor que lo reemplace, **"sin costo para el Honorable Senado de la Nación"**, por equipamiento con prestaciones acordes a las necesidades.

Características

Debe ofrecer:

- Protección tiempo real sobre los protocolos SMTP, IM.
- Protección Antivirus / Anti-Spyware / Grayware con motor y firmas (patrones de búsqueda) propietarios de la marca que provee la solución.
- Protección Anti-Phishing / Anti-Pharming mediante consultas a bases de datos de reputación de URLs / IPs propietarias de la marca que provee la solución.
- Filtrado Antispam mediante motor heurístico, que permita la identificación de correo no deseado mediante el análisis y procesamiento de los mensajes.
- Filtrado de IPs Spammers según su reputación (denegando su conexión) y mediante consultas a base de datos externas a la solución. Las bases de datos a las cuales se harán las consultas deben ser propietarias del fabricante de la solución.
- Manejo de listas negras dinámicas para bloquear Spam en tiempo real y a nivel de conectividad IP, denegando su conexión.
- Listas negras dinámicas actualizada en tiempo real.
- Deberá bloquear Spam con una efectividad del 97% y una tasa de falsos positivos de menos de 0,5%.
- Deberá bloquear IPs relacionados con :
 - Phishing
 - Virus, spyware y todo tipo de malware.
 - Robo de directorios (directoryharvestingattack)
- Filtrado de contenido permitiendo crear políticas de bloqueo de documentos, textos y tipos de extensiones de documentos.
- Protección mediante análisis del comportamiento de las IPs que conectan al MTA de la solución (IDS SMTP).
- Integración con el protocolo LDAP.
- Integración con Microsoft Active Directory.
- Integración con los MTAs líderes del mercado.
- Manejo de políticas sobre el tráfico entrante y saliente sobre los protocolos SMTP y IM. Estas políticas deben ser independientes pudiendo aplicarse sobre uno u otro protocolo y sobre uno u otro sentido (Entrante/Saliente). Estas políticas deben permitir su aplicación según: elección de remitente y receptor, excepciones de remitente y receptor. Tanto el remitente como el receptor podrán expresarse como dominio de correo o cuenta de correo
- Poder aplicar políticas con alguno de los siguientes filtros:
 - Filtro Antispam.
 - Filtro AntiPhishing.
 - Filtro por cantidad de destinatarios finales.
 - Filtro de Archivos Adjuntos por:
 - Nombre o extensión

44



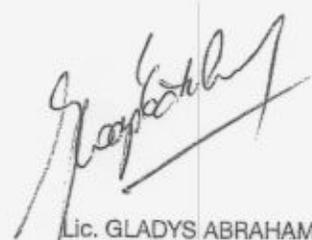
- Contenido del tipo MIME
 - Tipo real de archivo
 - Tamaño
 - Cantidad de estos
- Filtro por tamaño del mensaje.
 - Filtro de contenido por patrones de expresiones regulares en el:
 - Asunto del mensaje
 - Cuerpo del mensaje
 - Encabezado del mensaje
 - Archivos adjuntos en el mensaje
- Manejo de excepciones, listas blancas y listas negras configurables por el administrador.
 - Ante la coincidencia de un mensaje con una política la solución debe poder tomar las siguientes acciones:
 - Ninguna acción sobre el mensaje
 - Eliminar el mensaje
 - Enviar a cuarentena
 - Re direccionar los mensajes hacia otro destinatario
 - Eliminar los archivos adjuntos, todos o solamente los que coincidan con la política
 - Agregar una etiqueta en el:
 - Cuerpo del mensaje
 - Asunto del mensaje
 - Enviar una notificación al Administrador, Remitente y/o Receptor/es
 - Identificación de Spam generado a través de imágenes.
 - Identificación de Spam en URLs embebidas en el mensaje
 - Detección y eliminación de todo tipo de virus y amenazas, conocidos y desconocidos, independientemente del nombre que se le dé en la jerga (Virus, Works, Troyanos, Virus de red, Spywares, Graywares, Adwares, Rootkits, Dialers, Phishing, Pharming, Hijacking, JokesPrograms, Hacking tools, Remote-accesstools, Password cracking, Key loggers, Gusanos, Payload, Scam, etc.).
 - Protección Heurística en tiempo real ante nuevas variantes de código malicioso o amenazas de día cero.
 - Capacidad de búsqueda de código malicioso en archivos de hasta 10 capas de compresión en los siguientes formatos de compresión:
 - PKZIP, LHA, LZH, ARJ, MIME, TAR, GZIP, RAR, BZIP2, PKLITE, LZEXE, UUCODE, BINHEX.
 - Para el caso de correos infectados deberá ofrecer la posibilidad de tomar distintas acciones en función del tipo de malware (Virus, Spyware, Grayware, Virus de día Cero, etc.)
 - Acciones a tomar:
 - Ninguna acción sobre el mensaje
 - Eliminar el mensaje
 - Enviar a cuarentena
 - Re direccionar los mensajes hacia otro destinatario
 - Eliminar los archivos adjuntos, todos o solamente los que coincidan con la política
 - Agregar una etiqueta en el:
 - Cuerpo del mensaje
 - Asunto del mensaje
 - Enviar una notificación al Administrador, Remitente, Receptor/es

Sergio Bianchetti
SERGIO BIANCHETTI
 Jefe Depto. de Contrataciones
 Licitaciones

Gladys Abraham
GLADYS ABRAHAM
 Directora de Dirección de Informática

Consola de administración

- Con acceso desde cualquier estación de trabajo (Administración remota), por medio de Interfaz Web. Con la posibilidad de tener comunicación encriptada
- Para ingresar a la consola se deberá introducir una contraseña de acceso y desde la misma se podrán realizar todas las configuraciones propias de las características técnicas detalladas con anterioridad
- Entre otras tareas se podrá:
 - Configurar políticas, filtros y excepciones.
 - Administrar listas blancas y negras.
 - Configurar actualizaciones incrementales de forma automática / manual y establecer los puntos de actualización.
 - Brindar información detallada de cómo fue procesado un mensaje para un posible seguimiento de las políticas.
 - Administrar logs. permitiendo búsquedas por tipo, por fecha o periodo de tiempo. Capacidad de remover de forma manual y automática los logs determinando cada cuantos días se purgaran.
 - Acceder a la cuarentena de los mensajes de correo electrónico y permitir hacer búsquedas por Fecha, Periodo de Tiempo, Remitente, Receptor, Asunto.
 - Mostrar el estado de la solución en tiempo real, generar reportes bajo demanda y generar reportes programados.
 - Etc.



Lic. GLADYS ABRAHAM
Directora de Dirección de Informática
H. Senado de la Nación



SERGIO BIANCHETTI
Jefe Depto. de Contrataciones
Licitaciones
Subdirección de Compras.
H. Senado de la Nación



Filtrado de contenido en el gateway sobre los protocolos HTTP y FTP

El oferente deberá proveer una solución completa. Tanto el software como el hardware necesario para implementar el filtrado en cuestión. Deberá proveer 2 (dos) equipos (compuesto por hardware y software), uno para cada enlace de modo de contar con una arquitectura tolerante a fallas. El hardware podrá ser implementado en modalidad de appliances dedicados o por medio de la provisión de servidores rackeables en no más de dos unidades cada uno. Deberá ser de primera marca y contar con discos redundantes. De requerirse licencias para sistemas operativos deberán ser incluidas en la oferta. Dado el conocimiento específico de su solución, **“el dimensionamiento del hardware necesario es responsabilidad del oferente”**. Para esto debe considerar que el H. Senado de la Nación hace uso del 100% de sus enlaces (ver: Vínculos a ser protegidos por las soluciones de borde). El oferente deberá realizar, en conjunto con el HSN, las pruebas que considere necesarias para dicho dimensionamiento. Si una vez operativo el equipamiento suministrado resultara insuficiente, el HSN exigirá al proveedor que lo reemplace, **“sin costo para el Honorable Senado de la Nación”**, por equipamiento con prestaciones acordes a las necesidades.

Características

Debe ofrecer:

- Protección tiempo real sobre los protocolos HTTP – FTP
- Protección Antivirus / Anti-Spyware / Grayware con motor y firmas (patrones de búsqueda) propietarios de la marca que provee la solución.
- Protección Anti-Phishing / Anti-Pharming mediante consultas a bases de datos de reputación de URLs / IPs propietarias de la marca que provee la solución.
- Protección Heurística en tiempo real ante nuevas variantes de código malicioso o amenazas de día cero.
- Integración con Microsoft Active Directory
- Operar en modo Standalone, como Upstream Proxy, como Proxy transparente, como Router (recibir peticiones por una interface interna y reenviarlas por la externa) y como bridge (capa 2 del modelo OSI).
- Bloqueo de URLs. Configuración de URLs peligrosas y de confianza.
- Filtrado de URLs según su reputación y mediante consultas a bases de datos externas a la solución. Las bases de datos a las cuales se harán las consultas deben ser propietarias de la marca que provee la solución.
- Filtrado de URLs por categorías actualizables a través de bases de datos externas a la solución. Estas bases de datos deben ser propietarias de la marca que provee la solución y deberán contemplar más de 50 categorías.
- Por medio de categorías pre-definidas en la solución, el administrador podrá configurar en que URLs se podrá navegar y en cuáles no. También podrá definir horarios en los cuales los usuarios podrán navegar en las distintas categorías definida.
- La posibilidad de aplicar políticas de navegación por categorías a IPs, Host Name o Grupo de usuarios LDAP (Active Directory).
- La posibilidad de aplicar políticas de bloqueo de aplicaciones P2P o InstantMessaging a IPs, Host Name o Grupo de usuarios LDAP.
- La posibilidad de aplicar políticas en las cuales se definirá que IPs, Host Name o Grupo de usuarios LDAP usan cuotas de navegación.
- Capacidad para poder crear políticas sobre el tráfico entrante y saliente sobre el protocolo HTTP.
- La posibilidad de aplicar políticas específicas sobre el protocolo FTP.
- La posibilidad de especificar que archivos se escanean:
 - Todos los archivos
 - Archivos potencialmente riesgosos verificando el tipo real archivo
 - Extensiones riesgosas y definidas por el administrador.
 - Excepciones a extensiones definidas por el administrador
- Capacidad de búsqueda de código malicioso en archivos de hasta 10 capas de compresión en los siguientes formatos de compresión:
 - PKZIP, LHA, LZH, ARJ, MIME, TAR, GZIP, RAR, BZIP2, PKLITE, LZEXE, UUCODE, BINHEX.

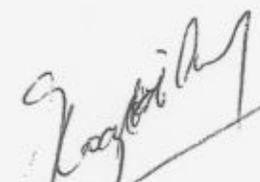
44



- Excepciones de escaneo en archivos de gran tamaño.
- La posibilidad de especificar la acción a tomar en archivos infectados. Las acciones a tomar deberán ser:
 - Limpiar
 - Eliminar
 - Enviar a cuarentena.
 - Bloquear
 - Dejar pasar
- En archivos protegidos con contraseña poder tomar acciones como:
 - Eliminar,
 - Enviar a cuarentena
 - Dejar pasar.
- La posibilidad de especificar los archivos a bloquear en el tráfico HTTP y FTP por:
 - Audio/Video (.mp3, .wav, etc.)
 - Imágenes (.gif, .jpg, etc.)
 - Archivos Comprimidos (.zip, .tar, .jar, etc.)
 - Java (.class)
 - Ejecutables (.exe, .dll, etc.)
 - Documentos de Microsoft (.doc, .xls, etc.)
 - Extensiones definidas por el administrador.

Consola de administración

- Con acceso desde cualquier estación de trabajo (Administración remota), por medio de Interfaz Web. Con la posibilidad de tener comunicación encriptada
- Para ingresar a la consola se deberá introducir una contraseña de acceso y desde la misma se podrán realizar todas las configuraciones propias de las características técnicas detalladas con anterioridad.
- Entre otras tareas se podrá:
 - Permitir la creación de distintos perfiles de acceso y administración, con distintos privilegios y roles.
 - Configurar actualizaciones de forma automática / manual y establecer los puntos de actualización.
 - Brindar información detallada de cómo fue procesada una petición HTTP para un posible seguimiento de las políticas
 - Administrar logs, permitiendo búsquedas por tipo, por fecha o periodo de tiempo. Capacidad de remover de forma manual y automática los logs determinando cada cuantos días se purgaran.
 - Mostrar el estado de la solución en tiempo real, generar reportes bajo demanda y generar reportes programados.
 - Acceder a la cuarentena de los archivos


Lic. GLADYS ABRAHAM
Directora de Dirección de Informática
H. Senado de la Nación


SERGIO BIANCHETTI
Jefe Depto. de Contrataciones
Licitaciones
Subdirección de Compras
H. Senado de la Nación

CONSIDERACIONES GENERALES

Todo el software ofertado deberá corresponder a la última versión liberada al mercado mundial por el fabricante o desarrollador a la fecha de apertura de la presente licitación.

Se deja claramente expresado que corresponde al oferente, durante el período de mantenimiento, proveer nuevas versiones del producto en caso de migración del sistema operativo en las estaciones cliente o servidores, sin costo para el H. Senado de la Nación.

Deberá presentarse una declaración jurada con el compromiso de mantener en Buenos Aires, Argentina, la capacidad técnica, suficiente para suministrar los servicios de mantenimiento preventivo y correctivo, por el periodo de garantía.

Se seleccionará la oferta más conveniente para el organismo, teniendo en cuenta el precio, la calidad, las características e idoneidad del oferente y antecedentes en el mercado.

De los productos de software objeto de la presente contratación se deberán entregar sus originales en CD-DVD con sus respectivas licencias y toda la documentación de los mismos.

Análisis Técnico de la propuesta

Con la oferta se deberán adjuntar especificaciones técnicas del equipamiento y software ofrecido, acompañadas de los folletos provistos por el fabricante, y en todos los casos se deberán consignar marca y modelo de los equipos. Para una correcta evaluación de la propuesta, No se admitirá especificar simplemente "según pliego" como identificación del cumplimiento de las características ofrecidas del hardware y software.

El análisis técnico de la propuesta estará implementado en dos etapas y será necesaria la aprobación de ambas para lograr la aprobación técnica de la solución.

1º Etapa: Se realizara un análisis detallado de la propuesta técnica contenida en la oferta del proveedor.

2º Etapa: Solo a los oferentes de las soluciones que hayan sido aprobadas en la 1º Etapa, se les solicitará por un período de prueba de 15 días, una muestra de software y hardware de idénticas características al ofrecido, debidamente instalados y la asistencia técnica necesaria. De modo tal de poder realizar una prueba en laboratorio y comprobar el cumplimiento de los requerimientos solicitados por el HSN.

Administración Centralizada de las soluciones

Se valorará tecnológicamente la solución que provea administración y actualización centralizada en una misma consola central de todas las partes que conforman la solución requerida por HSN, y que se detallan a continuación:

- Antivirus de Estaciones de trabajo y Servidores.
- Antivirus para servidor de correo electrónico.
- Filtrado de contenido en el Gateway SMTP/IM.
- Filtrado de contenido en el Gateway HTTP/FTP.

Recepción definitiva

De cumplirse satisfactoriamente las verificaciones, la Dirección de Informática del H.S.N procederá a extender el Certificado de Recepción Definitiva de los bienes.

Los tiempos de licenciamiento y mantenimiento comenzarán a correr una vez que los productos se encuentren correctamente instalados, funcionando y se haya emitido el certificado de recepción definitiva.

NOTA: La conformidad que dé, el H. Senado de la Nación, al remito de entrega de bienes emitido por el adjudicatario en oportunidad de recibir los bienes, no constituirá para el H.S.N otra obligación que la de ser simple depositario de las unidades que haya recibido.

79



Plazo, lugar y forma de entrega

La provisión del software solicitado, de las Licencias y la instalación del software antivirus en las Estaciones de trabajo, servidores, Consola de administración deberá ser concluida dentro de los 60 (sesenta) días corridos contados a partir de la entrega de la orden de compra.

La entrega de los productos y licencias será en las dependencias del H.S.N. la Dirección de Informática comunicará oportunamente los destinos a los adjudicatarios.

La recepción de los elementos y/o equipos adquiridos será realizada en el Dto. de Suministros del H.S.N.

Soporte técnico y garantía de buen funcionamiento

Los adjudicatarios deberán brindar a partir de la fecha de recepción definitiva y por el período del servicio objeto de la presente licitación, el servicio de soporte técnico, mantenimiento y garantía integral, es decir que comprenderá la reparación con provisión de repuestos y/o cambio de las partes que sean necesarias, sin cargo alguno para el HONORABLE SENADO DE LA NACIÓN, para todo el hardware y software suministrado.

Este comprenderá la reparación de todas aquellas fallas relacionadas con el hardware y software suministrado o con cualquier tipo de virus y/o amenazas que el personal del HONORABLE SENADO DE LA NACIÓN no pueda resolver en primera instancia. El tiempo de respuesta a los llamados ante fallas deberá ser de 4hs. como máximo y deberán ser solucionadas en 48 horas (considerando solo días hábiles) a partir de su fehaciente notificación y sin cargo alguno para el HONORABLE SENADO DE LA NACIÓN, con atención en el lugar de instalación. El servicio de garantía deberá ser 5 x 9. El servicio de soporte técnico y/o garantía podrá ser brindado en primera instancia telefónicamente o por control remoto, pero una vez superada esta instancia, el proveedor deberá concurrir a las dependencias del HSN y dar una solución en el sitio (atención on-site).

El proveedor garantizará que el servicio técnico será brindado o garantizado por personal especializado de la empresa fabricante de los productos ofrecidos. Es decir que la garantía de los equipos sea efectivamente garantizada por el fabricante del equipo.

Los materiales y repuestos a emplear deberán ser originales de fábrica o de calidad similar, nuevos y sin uso, debiendo presentarse la documentación que respalde las citadas características.

La propiedad de los repuestos será del HONORABLE SENADO DE LA NACION.

Las garantías deberán estar debidamente certificadas en cuanto a los tiempos del alcance y a las formas del mismo por los fabricantes de los productos.

Los materiales, repuestos, etc. que resultaren rechazados serán retirados por el proveedor a su costo, como así también los defectuosos o de buena calidad puestos en desacuerdo con las reglas del arte, estando a su cargo los gastos que demandare la inmediata sustitución de los mismos.

La relación para el cumplimiento de la garantía será directamente entre el representante del oferente y el responsable del HONORABLE SENADO DE LA NACION.

Cuando la magnitud de la avería requiera el traslado del equipamiento para su reparación en laboratorio deberá reemplazarse por uno de iguales características. El traslado y toda la operatoria necesaria para el mismo serán por cuenta y responsabilidad del adjudicatario y no generará ningún costo adicional para el HONORABLE SENADO DE LA NACION.

Si hubiera elementos o situaciones para los cuales no fuera aplicable la garantía, éstos y éstas deberán estar detallados en forma clara y explícita en la oferta. NO se aceptarán descripciones ambiguas como ser "mal uso del equipamiento". No se aceptarán posteriores adiciones a la lista explícita de elementos y/o situaciones no cubiertas por la garantía.

El proveedor deberá implementar algún mecanismo de registro y control de incidentes suministrando un número de incidente cada vez que el H. Senado de la Nación requiera de su asistencia. Indicando en su propuesta cuales son los canales de comunicación dispuestos a tal fin.



El proveedor deberá notificar al organismo acerca de la posibilidad de epidemias y los mecanismos a adoptar para evitarlas. Además deberá brindar el soporte técnico necesario para subsanarlas en el caso de ocurridas. Este soporte incluye acudir al sitio del H. Senado de la Nación con personal técnico idóneo.

Penalidades por incumplimiento de los tiempos estipulados

Cada observación al servicio no subsanada dentro de las 48 horas hábiles de su notificación, dará lugar a la aplicación de una multa del 1 por mil (1 ‰) por cada día de mora, calculada sobre el total de la facturación.

Consultas, Aclaraciones y Respuestas a Consultas

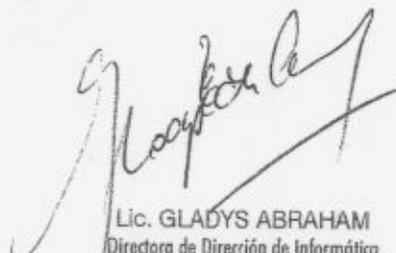
Las consultas y pedidos de aclaraciones se presentarán por escrito ante la Subdirección de compras, en el horario de 14.00 a 18.00 hs. y hasta diez (10) días hábiles antes del acto de apertura respectivo, las respuestas a dichas consultas se proporcionarán hasta setenta y dos (72) horas antes del mismo acto.

Contenido de la oferta

El precio del servicio aquí solicitado deberá ser cotizado en Pesos incluyendo todos los impuestos. La oferta deberá ser cotizada íntegramente, es decir, "No se admitirán cargos por instalación del servicio ofrecido".

Serán declaradas inadmisibles las ofertas que modifiquen o condicionen las cláusulas del presente pliego y/o impliquen apartarse del régimen aplicado.

Todos los requerimientos técnicos del objeto de esta licitación y enumerados en este Pliego de Bases y Condiciones Particulares, deben ser considerados mínimos, pudiendo el Oferente presentar ofertas cuyas características superen o mejoren las aquí solicitadas.



Lic. GLADYS ABRAHAM
Directora de Dirección de Informática
H. Senado de la Nación



SERGIO BIANCHETTI
Jefe Depto. de Contrataciones
Licitaciones
Subdirección de Compras
H. Senado de la Nación

NOTA ACLARATORIA NRO 1.-

Consultas Efectuadas sobre la Lic. Pública N° 27/2014 Servicio de Antivirus.

Consultas Generales:

- Indicar cuál es la solución (marca y versión) de antivirus actualmente instalada en servidores y estaciones de trabajo.

Trend Micro OfficeScan Client 10.6 Service Pack2

- Indicar que solución existe actualmente instalada en los servidores de Exchange.

Trend Micro Scan Mail for Microsoft Exchange versión 10.2

- Indicar que cantidad de equipos posee Windows XP. Que versión de Service pack poseen.

500 equipos con Windows XP Service pack 3.

Consulta para la solución Gateway de correo

- Indicar que solución existe actualmente en los gateways de correo.

Trend Micro InterScan Messaging Security Virtual Appliance IMSVA 8.2 SP2 Patch1 (build 1730)

- Indicar la cantidad de correos entrantes por hora (incluyendo spam, virus, etc.).
- Indicar la cantidad de correos salientes por hora.

Rango tomado 1 hora en un día corriente y en uno de los Gateway.

| Messages Processed | Total | % |
|--------------------|-------|--------|
| Total | 1188 | 100% |
| Incoming | 981 | 82.58% |
| Outgoing | 207 | 17.42% |

| Scanning Conditions | Total | % |
|---------------------|-------|--------|
| Clean email | 961 | 80.89% |
| Spam | 227 | 19.11% |

Conexiones que se deben tener en cuenta para estimar la cantidad de correos procesados.

| IP Fitering Type | Total Blocked Connections | Blocked% |
|-----------------------------|---------------------------|----------|
| Total | 949 | 100% |
| Malicious code(IP Profiler) | 0 | 0% |
| Spam(IP Profiler) | 49 | 5.16% |
| Email Reputation | 900 | 94.84% |
| DHA attack(IP Profiler) | 0 | 0% |
| Bounced mail(IP Profiler) | 0 | 0% |
| Manual(IP Profiler) | 0 | 0% |

- Indicar el tamaño promedio de los correos entrantes y salientes para las consultas anteriores.

No se cuenta con esa información.

Consulta para la solución Gateway de navegación.

- Indicar que solución existe actualmente en los gateways de navegación.

Trend Micro InterScan Web Security Virtual Appliance 5.6 IWSVA 5.6 EN Patch 2 Build 1437

- Indicar la cantidad de usuarios que navegan.

La cantidad de usuarios que navegan sería 2500 usuarios

- Indicar la cantidad de requerimientos por segundos.

Entendiendo que los requerimientos son la cantidad de conexiones concurrentes por segundos, estas son 5000.

- Indicar que funcionalidades son deseadas utilizar en el proxy.

Las funcionalidades que están citadas en las características técnicas del pliego.

Nota Aclaratoria para los oferentes

La información expresada anteriormente es dependiente de los 2 enlaces de 24 MB cada uno, con los que cuenta actualmente el HSN. La solución a proveer se deberá dimensionar para el total aprovechamiento (sin que se produzca recorte o degradación) de dos enlaces de 100 MB, como se expresa en el pliego de base y condiciones.

Teniéndose en cuenta también:

“El oferente deberá realizar, en conjunto con el HSN, las pruebas que considere necesarias para dicho dimensionamiento. Si una vez operativo el equipamiento suministrado resultara insuficiente, el HSN exigirá al proveedor que lo reemplace, “sin costo para el Honorable Senado de la Nación”, por equipamiento con prestaciones acordes a las necesidades.”

Con respecto al “equipamiento a cubrir con la solución” en el 3 ítem.

“1 Servidor de Archivo propio del Storage EMC2 VNX 5300 (CIFS Server).”

Se requiere:

- Módulos de antivirus dedicados para el servidor NAS.
- Cantidad de licencias necesarias para no degradar la performance del servidor NAS.

En la actualidad se utiliza Trend Micro Server Protect 5.80 instalado en 2 servidores virtuales para el servicio de antivirus del servidor NAS.