
**BASES DE PARTICIPACIÓN**

**LICITACIÓN SIMPLIFICADA Nº LS-CEV-012-08**
RELATIVA AL SOPORTE, ACTUALIZACIÓN Y ADQUISICIÓN DE LICENCIA DE SOFTWARE PARA ANTIVIRUS Y ANTISPYWARE

El Congreso del Estado de Veracruz de Ignacio de la Llave a través de la Secretaría General, con fundamento en lo dispuesto en los artículos 20 y 33 fracción V de la Constitución Política del Estado de Veracruz de Ignacio de la Llave; 18 fracción V, 54, 55, 57 fracción IV, 60 fracción IV y 61 fracción VI de la Ley Orgánica del Poder Legislativo del Estado de Veracruz de Ignacio de la Llave y aplicando los preceptos establecidos en la Ley de Adquisiciones, Arrendamientos, Administración y Enajenación de Bienes Muebles del Estado de Veracruz de Ignacio de la Llave, formula atenta invitación para participar en la **LICITACIÓN SIMPLIFICADA N° LS-CEV-012-08 RELATIVA AL SOPORTE, ACTUALIZACIÓN Y ADQUISICIÓN DE LICENCIAS DE SOFTWARE PARA ANTIVIRUS Y ANTISPYWARE,** debiendo los interesados sujetarse a las siguientes:

# B A S E S

## CAPÍTULO I
## DESCRIPCIÓN GENERAL DE LA LICITACIÓN

**PRIMERA.-** El objeto de la presente licitación lo constituye el soporte, actualización y adquisición de licencias de software para antivirus y antispyware, por lo que deberá de cotizarse en apego a las especificaciones establecidas en las presentes bases y de conformidad con el anexo técnico.

**SEGUNDA.-** Los interesados podrán participar en esta licitación **por una, varias o el total de las partidas en concurso**, admitiéndose una sola opción de proposición técnica y económica por participante; las partidas serán adjudicadas **a quien(es)** garantice(n) las mejores condiciones al Congreso, previo análisis de conveniencia de adjudicación, **siendo obligatorio ofertar la totalidad de las características solicitadas en cada una de las partidas, la omisión de alguna característica será motivo de descalificación en la licitación que nos ocupa.**

**TERCERA.- Plazo, lugar y condiciones:** Quien resulte adjudicado deberá considerar que el periodo que cubrirán las licencias será del **26 de septiembre del 2008 al 31 de diciembre de 2009.**

**Para las tres partidas** se deberá realizar la entrega de la **documentación comprobatoria que soporte la autorización por parte del fabricante** sobre la adquisición de la licencia, la contratación del servicio **y medios en Cd de los productos**, **a mas tardar un día hábil antes de la fecha del inicio de la vigencia, es decir el 25 de septiembre del 2008**.

La entrega de la documentación comprobatoria y medios en CD sobre la adquisición de las licencias y la contratación del servicio, deberá ser de conformidad con lo estipulado en estas bases y en el anexo técnico, **libre a bordo en la Coordinación de Informática del Congreso,** ubicada en Avenida Encanto s/n esquina Avenida Lázaro Cárdenas, Colonia El Mirador, en esta ciudad de Xalapa, Veracruz, en un horario de 9:00 a 15:00 y de 16:00 a 18:00 hrs. en días hábiles de lunes a viernes.

**CUARTA.-** De observarse alguna deficiencia y/o irregularidad en base a lo solicitado en las partidas, el Congreso lo notificará a la empresa adjudicada, quien deberá atender el requerimiento y proceder a subsanarlas, sin cargo alguno para el Congreso, reuniendo las especificaciones técnicas y la calidad requerida; el tiempo de respuesta No deberá ser mayor a **2 horas y para la solución de problemas no deberá exceder un plazo máximo de 24 horas,** considerando la hora en la que la empresa adjudicada recibió el aviso.

**QUINTA.- El pago** se realizará en pesos mexicanos, mediante depósito en la cuenta bancaria o cheque nominativo, a **crédito dentro de los 10 (diez) días hábiles posteriores a la entrega de la factura original debidamente requisitada**, debiendo presentar dicha factura en la Caja del Congreso, ubicada en Avenida Encanto s/n Esquina con Avenida Lázaro Cárdenas, Colonia El Mirador de esta Ciudad de Xalapa, Veracruz en un horario de 9:30 a 14:00 y de 17:00 a 19:00 hrs. en días hábiles de lunes a viernes **y en el entendido de la previa recepción de la documentación comprobatoria** que soporte la autorización por parte del fabricante sobre la adquisición de las licencias, entrega de los medios en CD y la contratación del servicio, a entera conformidad del Congreso.

En caso de que no se presente en el tiempo señalado la documentación requerida debidamente requisitada para el trámite de pago, **la fecha de pago se correrá el mismo número de días que dure el retraso.**

**SEXTA.-**Las partidas deberán estar garantizadas contra cualquier deficiencia y/o irregularidad, durante todo el tiempo que duren las licencias, el soporte y la actualización del servicio, a entera satisfacción del Congreso.

**SÉPTIMA.-** Quien resulte adjudicado, elaborará la facturación con los siguientes datos fiscales:

- **Nombre :**
  Congreso del Estado de Veracruz.
- **Domicilio fiscal :**
  Avenida Encanto s/n Esquina Avenida Lázaro Cárdenas
  Colonia el Mirador
  C.P. 91170
  Xalapa, Veracruz
- **R.F.C. :**
  CEV-950725-2M0

**OCTAVA.-** Todos los costos que erogue el participante en la preparación y presentación de su proposición serán totalmente a su cargo, liberando al Congreso de la obligación de reintegrarlos, cualquiera que sea el resultado de la licitación.

**NOVENA.-** Para los efectos de la presente licitación se entenderá por:
I.- Congreso: Al Congreso del Estado de Veracruz de Ignacio de la Llave.
II.- Ley de Adquisiciones: Ley de Adquisiciones, Arrendamientos, Administración y Enajenación de Bienes Muebles del Estado de Veracruz de Ignacio de la Llave.

## CAPÍTULO II
## DESIGNACIÓN Y ATRIBUCIONES DE LA COMISIÓN QUE TENDRÁ A CARGO EL PROCEDIMIENTO DE LA LICITACIÓN

**DÉCIMA.-** El Congreso constituirá una Comisión para hacerse cargo de la presente licitación, la cual tendrá atribuciones entre otras, la de vigilar que se cumpla con los procedimientos de contratación y la evaluación de las proposiciones técnicas y económicas presentadas por los licitantes y estará conformada por el Secretario General, el Secretario de Servicios Administrativos y Financieros, el Director de Recursos Materiales y Servicios Generales, el Director de Asuntos Jurídicos, el Coordinador de Informática, el Jefe del Departamento de Recursos Materiales y el Jefe del Departamento de Adquisiciones.

La Comisión de licitación tendrá amplias facultades para aplicar las presentes bases y las leyes que sean relativas a la licitación y podrá realizar aclaraciones y/o modificaciones al contenido de estas bases, las cuales serán consideradas como parte de ellas, debiendo dar aviso a los participantes por escrito.

## CAPÍTULO III
## INSTRUCCIONES PARA LA ELABORACIÓN DE PROPOSICIONES

**DÉCIMA PRIMERA.-** La proposición se presentará por escrito, mecanografiada en papel membretado del licitante, sin tachaduras o enmendaduras, en idioma español y a precios fijos en moneda nacional (PESOS), **en dos sobres cerrados de manera inviolable, que contendrán: uno, la proposición técnica y el otro la proposición económica.**

**Los documentos que integren las proposiciones serán firmados de manera autógrafa por la persona facultada para suscribir documentos de esta naturaleza y que se encuentre previamente registrado en el padrón de proveedores del Congreso del Estado de Veracruz.**

I. El sobre de la **PROPOSICIÓN TÉCNICA** contendrá los siguientes documentos:

a) La documentación técnica en donde se describan las especificaciones de lo que oferten, señalando como mínimo las descripciones contenidas en el **Anexo técnico** de las presentes bases. Para todas las partidas será obligatoria la presentación de **catálogos, folletos,** ilustraciones y/o demás datos que se consideren necesarios, que respalden y/o muestren los aspectos técnicos de lo propuesto, **la omisión de alguno de ellos será motivo de descalificación,** debiendo especificar claramente el número de cada una de las partidas y que los datos coincidan con **la proposición técnica**.

b) Escrito bajo protesta de decir verdad que cuenta con facultades para suscribir proposiciones a nombre de su representada, de acuerdo al **Anexo No. 1** de las presentes bases.

c) Escrito bajo protesta de decir verdad, en el que manifieste conocer las disposiciones de la Ley de Adquisiciones y señalar que no se encuentra bajo los supuestos del artículo 45 del citado ordenamiento legal, de igual manera indicar que la empresa No está inhabilitada por parte de la Secretaría de la Función Pública, de la Contraloría General del Gobierno del Estado de Veracruz y demás Instituciones Gubernamentales, de acuerdo al **Anexo No. 2** de las presentes bases.

d) Copia fotostática de identificación oficial vigente con fotografía del representante legal de la persona moral o persona física participante: credencial de elector, cartilla del servicio militar, pasaporte o cédula profesional.

e) En caso de que asista a la junta de presentación y apertura de proposiciones técnicas y económicas, persona distinta al representante legal de la persona moral o de la persona física participante, deberá presentar carta poder simple en original y copia de identificación oficial vigente con fotografía: credencial de elector, cartilla del servicio militar, pasaporte o cédula profesional.

f) Carta compromiso de garantía en sitio que soporte la capacidad de respuesta a las solicitudes en un tiempo no mayor de 2 horas y para la solución a problemas no deberá exceder un plazo máximo de 24 horas, a entera satisfacción del Congreso.

g) Documentación comprobatoria vigente (ejercicio 2008) por parte del fabricante donde la empresa participante en la licitación se avala como distribuidor autorizado.

h) Presentar certificados del personal del proveedor, que realizará el soporte, avalando que tienen conocimiento de la suite propuesta al Congreso, la falta de esta información será causa de descalificación.

II. En el sobre que se presente la **PROPOSICIÓN ECONÓMICA,** contendrá los siguientes documentos:

a) Documento en el que se describa en forma detallada el precio unitario, fijo y global en moneda nacional de lo ofertado, desglosando el Impuesto al Valor Agregado, (**en el precio de la proposición económica incluir todo lo necesario, así como gastos de fletes, seguros y si se ofrecieran descuentos o cualquier otro concepto, reflejarlos en la oferta sin necesidad de desglose)** estipulando la forma de pago, tiempo, lugar, vigencia de precios, sobre todo en el caso de que éstas resulten ser favorables para el Congreso que las señaladas originalmente en éstas bases, (según modelo presentado en el **Anexo Nº 3.**

b) Con el propósito de agilizar la elaboración del cuadro comparativo, la proposición económica podrá presentarse capturada en un archivo en disquete o en Cd, conforme a lo establecido en el **Anexo N° 3**, coincidiendo con la presentada en forma escrita. (Verificar que el archivo no contenga virus).

c) Escrito en donde manifieste que sostendrá su proposición técnica y económica, así como precio unitario contenido en la proposición económica, aún en el caso de errores aritméticos al calcular el importe total de su proposición, de acuerdo al **Anexo Nº 4** de las presentes bases.

d) **Preferentemente** podrá presentar escrito donde manifieste estar de acuerdo en que el pago se realice mediante depósito bancario, de conformidad con el **Anexo N° 5** de las presentes bases.

III. La recepción de la documentación contenida en los sobres de las proposiciones técnicas y económicas, proporcionados por los licitantes, los recibe el Congreso para analizar y verificar que cumplan con lo establecido en las presentes bases y anexos, sin que implique necesariamente compromiso alguno de contratación a su cargo, aceptándose para revisión y análisis posterior.

IV. Los licitantes sostendrán sus precios durante todo el tiempo que dure el soporte y actualización de las partidas.

## CAPÍTULO IV
## JUNTA DE PRESENTACIÓN Y APERTURA DE PROPOSICIONES TÉCNICAS Y ECONÓMICAS

**DÉCIMA SEGUNDA.-** La junta de presentación y apertura de proposiciones técnicas y económicas **se llevará a cabo el día 11 de septiembre de 2008 a las 11:00 horas**, en la Sala de Juntas **"Jesús Reyes Heroles"** adjunta a la Biblioteca, ubicada en el edificio "A" en planta alta del Congreso, sita en Avenida Encanto s/n esquina con Avenida Lázaro Cárdenas, Colonia El Mirador de esta ciudad de Xalapa, Veracruz, ante la presencia de la Comisión de Licitación y el representante de la Secretaría de Fiscalización del Congreso.

**DÉCIMA TERCERA.-** Los sobres con las proposiciones se entregarán en el día, lugar y hora señalado para tal efecto o entregarse directamente en el **Departamento de Adquisiciones** o en su caso enviarse a través del servicio postal o mensajería certificada; en el entendido de que toda proposición **recibida posterior a la fecha y hora señaladas** para la junta de presentación y apertura de proposiciones técnicas y económicas, **no será admitida** para participar en la licitación que nos ocupa.

**DÉCIMA CUARTA.-** El resultado de la junta de la presentación y apertura de proposiciones técnicas y económicas, se hará constar en acta circunstanciada, la cual precisará las proposiciones aceptadas, así como las que fueron desechadas, asentándose las razones para su valoración; de ser necesario el Comité designará una comisión técnica para el análisis de las proposiciones recibidas, para que emita el dictamen correspondiente.

**DÉCIMA QUINTA.-** La Comisión de Licitación, creada para evaluar la presente Licitación, a través de la Dirección de Recursos Materiales y Servicios Generales será la autoridad facultada para desechar cualquier proposición que no sea presentada conforme a lo dispuesto por las presentes bases y sus anexos y sobre los acuerdos o modificaciones que se deriven, así como para aplicar los ordenamientos legales inherentes y solucionar las controversias que se susciten en el procedimiento.

## CAPÍTULO V
## ELABORACIÓN DEL DICTAMEN

**DÉCIMA SEXTA.-** La Comisión de Licitación conforme al análisis técnico y económico y en base al presupuesto autorizado, elaborará por escrito el **Dictamen Técnico-Económico** que contendrá los puntos resolutivos, en el que se harán constar las proposiciones admitidas y las desechadas; asimismo expresará cual de los licitantes reúne las mejores condiciones en cuanto a precio, calidad, servicio y demás estipulaciones favorables para el Congreso, indicando también las razones y causas por las que en su caso se descalifique a alguno de los participantes.

**DÉCIMA SÉPTIMA.-** Se podrá ajustar la duración, cantidad y características de las partidas, en tal caso el Congreso lo hará saber de manera oportuna y por escrito a los participantes, o en su caso será señalado en el Dictamen correspondiente.

**DÉCIMA OCTAVA.-** Para la adjudicación se podrá dar preferencia al que oferte tecnología y calidad superior a las especificaciones mínimas requeridas, aún cuando exista un diferencial no mayor al 10% (diez por ciento) entre la oferta de mejor calidad y la cotización inmediata inferior calificada, siempre que con ello no se rebase la disponibilidad presupuestal.

## CAPÍTULO VI
## NOTIFICACIÓN DE FALLO

**DÉCIMA NOVENA.-** La notificación de fallo se comunicará a los licitantes mediante escrito y con acuse de recibo **en un plazo máximo de 3 (tres) días hábiles posteriores** a la junta de presentación y apertura de proposiciones. Asimismo se le comunicará el resultado del fallo a la Secretaría de Fiscalización del Congreso y se hará público vía Internet en la página del Congreso, siendo la dirección www.legisver.gob.mx en el apartado del Departamento de Adquisiciones.

## CAPÍTULO VII
## SUSCRIPCIÓN DEL CONTRATO Y/O PEDIDO

**VIGÉSIMA**.- **Dentro del término de los 5 (cinco) días hábiles siguientes** a la fecha de notificación de fallo, quien resulte adjudicado deberá presentarse ante el Departamento de Adquisiciones del Congreso, para firmar el contrato y/o pedido, que será a través de la persona facultada para suscribir documentos de esta naturaleza y que esté registrada en el Padrón de Proveedores del Congreso; en caso de que los datos asentados en dicho padrón hayan sufrido cambios, deberán presentar los documentos actualizados en copia fotostática y original para cotejo, en apego a lo estipulado en la Ley de Adquisiciones.

**VIGÉSIMA PRIMERA.-** La empresa adjudicada con la finalidad de garantizar el cumplimiento de las obligaciones derivadas del contrato que se celebre y de lo ofertado en la licitación, deberá entregar **original de póliza de fianza** expedida por Institución de Fianzas legalmente autorizada para ello, cuando menos por el importe del 10% (diez por ciento) sobre la obligación total del contrato, sin incluir el Impuesto al Valor Agregado (I.V.A.), de acuerdo al **Anexo No. 6** de las presentes bases, debiendo **presentarla dentro de los 3 (tres) días hábiles posteriores a la suscripción del contrato**; si ésta no se presenta será causa de rescisión del contrato.

**VIGÉSIMA SEGUNDA.-** De no comparecer en el plazo indicado para la suscripción del contrato y/o pedido, se procederá a celebrarlo con el licitante que haya ocupado la segunda mejor opción, siempre que la diferencia en precio con respecto a la proposición que inicialmente hubiera resultado ganadora, no sea superior al 10 % (diez por ciento) y si resulta favorable a los intereses del Congreso.

**VIGÉSIMA TERCERA**- Se podrá pactar con la empresa adjudicada la ampliación mediante Adendum del contrato formalizado, siempre y cuando ésta no represente más del 20% (veinte por ciento) del monto total de las partidas que se amplíen y que la empresa sostenga en la ampliación el precio pactado originalmente.
Igual porcentaje se aplicará a las prórrogas que se hagan respecto de la vigencia del contrato.

**VIGÉSIMA CUARTA.-** El Congreso podrá rescindir administrativamente el contrato y seguir el procedimiento previamente establecido en la Ley de Adquisiciones.

**VIGÉSIMA QUINTA.-** Las contribuciones que se causen por motivo de la celebración del contrato y/o pedido, correrán a cargo de la empresa adjudicada; el Congreso únicamente pagará el Impuesto al Valor Agregado.

**VIGÉSIMA SEXTA.-** La empresa adjudicada se responsabiliza expresamente en los casos que se infrinjan derechos de autor, patentes o marcas, o algún otro derecho de exclusividad, quedando liberado totalmente de ello el Congreso.

## CAPÍTULO VIII
## DECLARACIÓN DEL CONCURSO DESIERTO

**VIGÉSIMA SÉPTIMA.-** El Congreso podrá declarar desierta la presente licitación, en los siguientes casos:

I.- No haya licitantes;
II.- Se acredite de manera fehaciente que los precios de mercado son inferiores a las mejores ofertas recibidas;
III.- Los licitantes incumplan con los requisitos establecidos en estas bases;
IV.- No lo permita el presupuesto;
V.- Los montos de las ofertas económicas excedan lo autorizado; y
VI.- Se presente caso fortuito o fuerza mayor.

A este respecto, la declaración que haga el Congreso de considerar desierta la licitación, se comunicará por escrito a los participantes.

**VIGÉSIMA OCTAVA.-** Cuando sólo se cuente con una proposición, el Congreso procederá a realizar una investigación de mercado, para determinar la conveniencia de adjudicación al licitante único.

## CAPÍTULO IX
## DEL RECURSO DE REVOCACIÓN

**VIGÉSIMA NOVENA.-** Los actos o resoluciones definitivos dictados dentro del procedimiento de contratación podrán ser impugnados por el proveedor agraviado. El recurso de revocación por parte de los licitantes se hará valer por escrito ante la Secretaría de Fiscalización del Congreso, por los actos que contravengan las disposiciones de la Ley que regula la presente licitación, siendo el término para interponerlo de cinco días hábiles a partir del día siguiente a aquel en que surta sus efectos la notificación de los actos o resoluciones; sin perjuicio de que se manifieste previamente ante la Secretaría de Servicios Administrativos y Financieros, quienes resolverán lo procedente conforme a lo estipulado en la legislación aplicable.

## CAPÍTULO X
## DE LAS INFRACCIONES Y SANCIONES

**TRIGÉSIMA.-** A los proveedores o licitantes que infrinjan la Ley de Adquisiciones se les aplicarán las sanciones siguientes:

**I.-** Multa de cien a mil días de salario mínimo general diario, vigente en la capital del estado, en la fecha que se cometa la infracción; y
**II.-** Prohibición para participar en los procesos de licitación durante dos años.

**TRIGÉSIMA PRIMERA.-** Cuando el participante ganador una vez celebrado el contrato y/o pedido se atrase en la entrega de la documentación comprobatoria que soporte la autorización del inicio por parte del fabricante sobre la adquisición de las licencias, la contratación del servicio y medios en cd de los productos, se aplicará una pena convencional consistente en una **SANCIÓN** calculada por el importe correspondiente de **TRES AL MILLAR POR CADA DÍA NATURAL DE ATRASO,** respecto de lo No entregado y prestado de manera oportuna y sobre lo cual se incurra en incumplimiento, sin considerar el Impuesto al Valor Agregado; tomando en cuenta para el efecto a partir del día natural siguiente señalado para cumplir regularmente con la entrega y prestación de acuerdo a lo pactado. Dicha pena no excederá del monto de la fianza del cumplimiento respectivo. El monto de la sanción deberá ser pagada al Congreso.

**TRIGÉSIMA SEGUNDA.-** La empresa adjudicada se compromete a pagar como pena convencional por alguna situación irregular que se detecte por los daños y perjuicios ocasionados por la misma, así como cuando No se haya atendido de manera adecuada y oportuna, además los gastos que se generen por la contratación con un tercero por causas imputables a la empresa adjudicada.

**TRIGÉSIMA TERCERA.-** Se harán efectivas las garantías de cumplimiento del contrato y/o pedido, cuando no se cumplan con las condiciones y características de lo adjudicado, sin causa justificada por parte del proveedor.

**TRIGÉSIMA CUARTA.-** Los proveedores y licitantes, se conducirán de conformidad con la buena fe y prudencia debida. Son infracciones:

I. Proporcionar a la Institución información falsa o documentación alterada;
II. Incumplir con los términos del contrato;
III. Lesionar el interés público o la economía de las Instituciones;
IV. Declararse en quiebra una vez formalizado el contrato;
V. Realizar prácticas desleales para con la Institución o demás licitantes;
VI. Injustificadamente y por causas que les sean imputables, no formalicen el contrato adjudicado por el Congreso;
VII. No sostener sus proposiciones técnicas y económicas presentadas en la licitación; y
VIII. Las demás previstas por la Ley de Adquisiciones o en otros ordenamientos aplicables.

**TRIGÉSIMA QUINTA.-** Ninguna de las condiciones contenidas en las bases de la presente licitación o en las proposiciones presentadas por los licitantes podrán ser negociadas y será causa de descalificación el incumplimiento por parte del licitante de alguno de los requisitos, y/o si se comprueba la existencia de otras irregularidades graves; así mismo queda prohibido entre los licitantes concertar posturas entre sí.

## CAPÍTULO XI
## ACLARACIONES

**TRIGÉSIMA SEXTA.-** Cualquier duda o aclaración respecto a las bases y los anexos de la presente licitación, presentarlos **por escrito,** a mas tardar **el día 05 de septiembre de 2008 a las 11:00 hrs.** a efecto de estar en posibilidad de dar respuesta a los mismos. La forma de envío puede ser presentándolas directamente en el Departamento de Adquisiciones ó remitirlas por correo electrónico a la dirección licitaciones@legisver.gob.mx ó al fax directo (01-228) 8-42-05-11 o 8-42-05-12, para el caso del envío al fax o al correo electrónico deberá confirmarse la recepción y cualquier duda comunicarse al 8-42-05-00 extensiones de la 3151 a la 3156.

**Xalapa, Veracruz a 02 de septiembre de 2008**

**A T E N T A M E N T E**

**LIC. FRANCISCO JAVIER LOYO RAMOS**
SECRETARIO GENERAL DEL CONGRESO DEL ESTADO
DE VERACRUZ DE IGNACIO DE LA LLAVE

# A N E X O  N° 1
(FORMATO)

**C. LIC. FRANCISCO JAVIER LOYO RAMOS**
SECRETARIO GENERAL DEL CONGRESO
DEL ESTADO DE VERACRUZ
DE IGNACIO DE LA LLAVE
P R E S E N T E

(Nombre) manifiesto bajo protesta de decir verdad, que los datos aquí asentados, son ciertos y han sido debidamente verificados, así como que cuento con facultades suficientes para suscribir las proposiciones concernientes a la **LICITACIÓN SIMPLIFICADA N° LS-CEV-012-08 RELATIVA AL SOPORTE, ACTUALIZACIÓN Y ADQUISICIÓN DE LICENCIAS DE SOFTWARE PARA ANTIVIRUS Y ANTISPYWARE,** en nombre y representación de: **(nombre o razón social de la persona Moral o persona Física participante).**

| | | |
|---|---|---|
| Registro Federal de Contribuyentes: | | |
| Domicilio: | | |
| Calle y número: | | |
| Colonia: | Delegación o Municipio: | |
| Código Postal: | Entidad federativa: | |
| Teléfonos: | Fax: | Correo Electrónico: |
| Descripción del objeto social: | | |
| *Nº de la escritura pública en la que consta su acta constitutiva: | Fecha: | |
| *Nombre, número y lugar del Notario Público ante el cual se dió fe de la misma: | | |
| *N° de inscripción en el registro público de la propiedad | Fecha: | |
| *Relación de accionistas: Apellido Paterno: | Apellido Materno: | Nombre (s): |
| *Reformas al acta constitutiva: | | |

| |
|---|
| Nombre del apoderado o representante legal que suscribirá el contrato y/o pedido, en caso de que la empresa resulte ganadora: |
| Datos del documento mediante el cual acredita su personalidad y facultades: |
| Escritura pública número: Fecha: |
| N° de inscripción en el registro público de la propiedad Fecha: |
| Nombre, número y lugar del Notario Público ante el cual se otorgó: |

(Nombre y firma)

*** Aplicable solo en caso de Personas Morales**

**Nota:** El presente formato se firmará por el representante legal de la Persona Moral o de la Persona Física participante, presentándose en original en papel membretado de la empresa, respetando preferentemente su contenido, forma y orden indicado.

**A N E X O No. 2**

**ESCRITO DE MANIFESTACIÓN**

**C. LIC. FRANCISCO JAVIER LOYO RAMOS**
SECRETARIO GENERAL DEL CONGRESO
DEL ESTADO DE VERACRUZ
DE IGNACIO DE LA LLAVE
P R E S E N T E

En relación a la **LICITACIÓN SIMPLIFICADA N° LS-CEV-012-08 RELATIVA AL SOPORTE, ACTUALIZACIÓN Y ADQUISICIÓN DE LICENCIAS DE SOFTWARE PARA ANTIVIRUS Y ANTISPYWARE** y en cumplimiento a las bases establecidas para participar en este concurso, por la empresa **(nombre o razón social de la persona moral o persona física participante)**, manifiesto a usted bajo protesta de decir verdad lo siguiente:

**1.-Conocer** el contenido y alcance de **la Ley de Adquisiciones**, Arrendamientos, Administración y Enajenación de Bienes Muebles del Estado de Veracruz de Ignacio de la Llave, **señalando que mi representada no se encuentra en los supuestos que establece el Artículo 45** del citado ordenamiento, que le impidan participar en la licitación en cuestión, o celebrar pedidos y/o contratos derivados de ella.

**2.-**Que la empresa **NO se encuentra inhabilitada** por parte de la Secretaría de la Función Pública, por la Contraloría General del Gobierno del Estado de Veracruz y demás Instituciones Gubernamentales.

(Lugar y fecha)

**A T E N T A M E N T E**

_____
(Nombre y firma)

**Nota:** El presente formato se firmará por el representante legal de la Persona Moral o de la Persona Física participante, presentándose en original en papel membretado de la empresa, respetando preferentemente su contenido, forma y orden indicado.

## ANEXO Nº 3
## MODELO PARA LA PRESENTACIÓN DE LA PROPOSICIÓN ECONÓMICA

- **Instrucciones de llenado:**

1. La proposición económica que se solicita podrá ser presentada preferentemente capturada en disquete de 3.5" (90mm.) o en Cd y es adicional a la presentada en forma escrita.
2. Elaborarla y presentarla en formato **Excel a partir de la versión 95 en adelante,** letra Arial No. 10 **y sin combinación de celdas**, **utilizando una fila para cada partida**, tomando para ello el presente modelo.
3. Para las partidas sometidas a concurso, **considerar únicamente el nombre genérico**. (Se pueden omitir las especificaciones técnicas únicamente para el modelo a utilizarse en la Proposición Económica, pero **cabe mencionar que en la Proposición Técnica se deberán señalar todas y cada una de las especificaciones técnicas señaladas en el Anexo Técnico).**
4. En las OBSERVACIONES señalar las particularidades correspondientes a su proposición. En caso de atender lo requerido en Bases, insertar la leyenda **"de acuerdo a bases", en caso contrario especificar lo propuesto.**

**EJEMPLO/GUÍA** del modelo para Proposición Económica:

**LICITACIÓN SIMPLIFICADA No. LS-CEV-012-08**

| Nº Partida | Cant. | U.M. | Descripción | NOMBRE Y/O RAZÓN SOCIAL DE LA EMPRESA | |
|---|---|---|---|---|---|
| | | | | P.UNIT. | IMPORTE TOTAL |
| 1 | 1 | Actualización de Licencia Corporativa para 358 computadoras | Solución integral de seguridad para escritorios y servidores | $ | $ |
| 2 | 1 | Adquisición de Licencia Corporativa para 42 computadoras | Solución integral de seguridad para escritorios y servidores | $ | $ |
| 3 | 1 | Adquisición de Licencia Corporativa para 101 computadoras | Solución de cifrado de alta seguridad, autenticación, prevención de pérdida de datos y controles de seguridad por políticas para evitar el acceso y la transferencia ilegal de información confidencial. | $ | $ |
| | | | | **SUB-TOTAL** | $ |
| | | | | **I.V.A.** | $ |
| | | | **(IMPORTE CON LETRA)** | **TOTAL** | **$** |

### OBSERVACIONES:

| | |
|---|---|
| FORMA DE PAGO: | En pesos mexicanos mediante deposito en la cuenta bancaria o cheque nominativo, **a crédito dentro de los 10 (diez) días hábiles posteriores** a la entrega de la factura original debidamente requisitada y en el entendido de la previa recepción de la documentación comprobatoria que soporte la autorización de las licencias por parte del fabricante, así como los medios en CD sobre la adquisición de las licencias y la contratación del servicio respectivo, a entera conformidad del Congreso. |
| TIEMPO DE ENTREGA Y PRESTACIÓN DEL SERVICIO: | El periodo que cubrirán las licencias será del 26 de septiembre del 2008 al 31 de diciembre del 2009, realizándose la entrega de la documentación comprobatoria que soporte la autorización por parte del fabricante sobre la adquisición de las licencias, la contratación del servicio y medios en Cd de los productos, a más tardar un día hábil antes de la fecha del inicio de la vigencia, es decir el 25 de septiembre del 2008. |
| LUGAR DE ENTREGA Y PRESTACIÓN DEL SERVICIO: | Libre a Bordo en las oficinas del Congreso, en el área de la Coordinación de Informática. |
| VIGENCIA DE PRECIOS: | Hasta la terminación de la prestación del servicio. |
| GARANTÍA: | Durante el tiempo que dure el soporte y actualización de las partidas. |
| NOTA Y/O OBSERVACIONES: | Las demás que se consideren pertinentes. |

(Lugar y fecha)

_____

(Nombre y firma)

**Nota:** El formato arriba indicado es únicamente un ejemplo que se señala como guía para su llenado y se firmará por el representante legal de la Persona Moral o de la Persona Física participante, presentándose en original en papel membretado de la empresa, respetando preferentemente su contenido, forma y orden indicado.

## ANEXO Nº 4

## CARTA DE SOSTENIMIENTO DE PROPOSICIONES TÉCNICAS Y ECONÓMICAS Y PRECIOS UNITARIOS

**C. LIC. FRANCISCO JAVIER LOYO RAMOS**
SECRETARIO GENERAL
DEL CONGRESO DEL ESTADO DE VERACRUZ
DE IGNACIO DE LA LLAVE
P R E S E N T E

En relación a la **LICITACIÓN SIMPLIFICADA N° LS-CEV-012-08 RELATIVA AL SOPORTE, ACTUALIZACIÓN Y ADQUISICIÓN DE LICENCIAS DE SOFTWARE PARA ANTIVIRUS Y ANTISPYWARE** y en cumplimento a las bases establecidas para participar en este concurso, la empresa **(nombre o razón social de la persona moral o persona física participante)**, otorga su compromiso formal de sostener su proposición técnica y económica, así como los precios unitarios contenidos en su proposición económica en caso de errores aritméticos al calcular el importe total de su proposición, asumiendo la responsabilidad que pudiese derivarse con motivo de la adjudicación que pueda realizarse a favor de mi representada.

(Lugar y fecha)

**A T E N T A M E N T E**

_____
(Nombre y firma)

**Nota:** El presente formato se firmará por el representante legal de la Persona Moral o de la Persona Física participante, presentándose en original en papel membretado de la empresa, respetando preferentemente su contenido, forma y orden indicado.

**A N E X O Nº 5**
**CONSENTIMIENTO DE DEPÓSITO BANCARIO**

**LIC. ANA ROSA VALDES SALAZAR**
ENCARGADA DE TESORERÍA
DEL CONGRESO DEL ESTADO DE VERACRUZ
DE IGNACIO DE LA LLAVE
P R E S E N T E

Por este conducto le manifiesto a Usted mi consentimiento para que en caso de resultar adjudicado en la **LICITACIÓN SIMPLIFICADA N° LS-CEV-012-08 RELATIVA AL SOPORTE, ACTUALIZACIÓN Y ADQUISICIÓN DE LICENCIAS DE SOFTWARE PARA ANTIVIRUS Y ANTISPYWARE,** se proceda a efectuar los pagos correspondientes a través de depósito bancario de conformidad a los datos siguientes:

| |
|---|
| NOMBRE DEL TITULAR DE LA CUENTA:<br>(nombre o razón social de la Persona Moral o Persona Física participante) |
| BANCO: |
| N° DE CUENTA: |
| SUCURSAL: |
| POBLACIÓN: |
| NOMBRE DE LA PERSONA QUE AUTORIZA:<br>**(A)** |
| PUESTO O CARGO EN LA EMPRESA: |

(Lugar y fecha)

_____

(Nombre y firma)

**(A) DEBERA TENER FIRMA AUTORIZADA EN LA CUENTA DE REFERENCIA**

El presente formato se firmará por el representante legal de la Persona Moral o de la Persona Física participante, presentándose en original en papel membretado de la empresa, respetando preferentemente su contenido, forma y orden indicado.

## ANEXO Nº 6

## FIANZA DE GARANTÍA DE CUMPLIMIENTO DE CONTRATO

TEXTO QUE CONTIENE LAS DISPOSICIONES QUE DEBERÁN INCLUIRSE EN LA PÓLIZA DE FIANZA SOLICITADAS PARA EL CUMPLIMIENTO DEL CONTRATO.

**Ante: el Gobierno del Estado de Veracruz de Ignacio de la Llave.**

Para garantizar por: (**Nombre o razón social de la Persona Moral o Persona Física participante),** hasta por la expresada cantidad de: $ (número y letra)_____, para el cumplimiento de todas y cada una de las obligaciones estipuladas en el contrato N° _____ de fecha dd/mm/aa , celebrado con el Congreso del Estado de Veracruz de Ignacio de la Llave, derivado de la **LICITACIÓN SIMPLIFICADA N° LS-CEV-012-08 RELATIVA AL SOPORTE, ACTUALIZACIÓN Y ADQUISICIÓN DE LICENCIAS DE SOFTWARE PARA ANTIVIRUS Y ANTISPYWARE** ----------
---

Esta Fianza garantiza la calidad, vicios ocultos, deficiencias y/o irregularidades, pago de daños y perjuicios ocasionados por su incumplimiento, pago de las penas convencionales, así como el cumplimiento de las obligaciones derivadas del contrato celebrado respecto de lo adjudicado durante **(como mínimo durante todo el tiempo que dure el soporte y actualización de las licencias),** a entera satisfacción del Congreso del Estado de Veracruz de Ignacio de la Llave.----------

La Institución de Fianzas **(Razón Social de la afianzadora)** acepta expresamente continuar garantizando las obligaciones a que esta póliza se refiere, aún en el caso de que se otorguen prórrogas o esperas al deudor para el cumplimiento de las obligaciones que se afianzan.----------

La Institución de Fianzas se somete al procedimiento administrativo de ejecución que establecen los artículos 95, 95 Bis y 118 de la Ley Federal de Instituciones de Fianzas con exclusión de cualquier otro.----------

Esta fianza sólo podrá ser cancelada mediante autorización por escrito de la Secretaría de Finanzas y Planeación del Gobierno del Estado de Veracruz de Ignacio de la Llave.

**ANEXO TÉCNICO**

| PARTIDA | CANTIDAD | U.M. | DESCRIPCIÓN |
|---|---|---|---|
| **1** | 1 | Actualización de Licencia Corporativa para 358 computadoras | SOLUCIÓN INTEGRAL DE SEGURIDAD PARA ESCRITORIOS Y SERVIDORES |

| Características Requeridas | Especificaciones Requeridas |
|---|---|
| **Producto** | **Soporte y Actualización de licenciamiento para 358 computadoras sobre cualquier nueva versión, actualización o mejora que realice el fabricante en cualquier** producto de la suite. |
| | **Antivirus:** La solución antivirus debe ofrecer al H. Congreso del Estado de Veracruz, una protección contra código malicioso que cubra al menos virus, troyanos, gusanos y programas no deseados. Esta solución debe estar diseñada para funcionar en un ambiente de red y el mismo fabricante debe proporcionar las herramientas para ser administrada de forma centralizada, tanto para la configuración, como instalación y actualizaciones.<br>La solución antivirus deberá ser capaz de analizar en busca de código malicioso (lo llamaremos analizar de aquí en adelante), el sistema donde esté instalado en tiempo real, cuando se acceda a un archivo o carpeta, así como los procesos que se ejecuten en memoria.<br>La solución analizará archivos de discos locales de la computadora, unidades removibles, así como el contenido de unidades de red.<br>La aplicación antivirus debe tener la opción de clasificar los procesos en base al riesgo que representan y poder configurar el análisis en tiempo real en base a este parámetro. Así, debe permitir al menos tres configuraciones, alto, bajo y estándar.<br>La solución debe realizar el análisis de archivos de comandos (scripts) mientras se están ejecutando.<br>Dentro de los métodos de detección debe contar con la detección heurística.<br>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 que tratan de infectarla y reportar la dirección IP de tal computadora. El bloqueo puede ser por un tiempo específico o permanente. El bloqueo se terminará después de transcurrir el tiempo, manualmente desde la interfase del antivirus o desde la consola de administración centralizada.<br>El antivirus dará la opción para analizar sectores de arranque y analizar unidades de disco de 3.5” cuando se apaga el equipo.<br>Debe poder configurar un mensaje de alerta al usuario cuando se da una detección y mostrarle distintas acciones a aplicar. |

| | |
|---|---|
| | También permitirá aplicar acciones automáticas sin mostrar información al usuario.<br><br>El antivirus deberá tener diferentes opciones para el manejo del registro de eventos de la aplicación. Entre la opciones se podrá determinar si se activa o desactiva el registro; nombre y ubicación del archivo de registro; tamaño máximo del archivo; poder ver el archivo desde la interfase del antivirus.<br>Permitirá al administrador configurar la solución para analizar todos los archivos ó una lista de tipos de archivo predetermina por las firmas de fabricante. A esta lista de tipos de archivo el administrador podrá agregar otros tipos de archivo.<br>El antivirus permitirá la creación de excepciones de archivos, carpetas o unidades de disco, para no ser analizadas.<br>Para el análisis de archivos empacados (.zip, pkg, etc.), el antivirus permitirá 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.<br>El sistema se integrará al sistema operativo de manera que creará opciones en el menú de contexto del explorador. Esto permitirá que apretando el botón derecho del Mouse sobre un archivo o carpeta, entre todas las opciones mostrará la de 'analizar en busca de virus'.<br><br>El programa antivirus debe contar con la opción de crear análisis bajo demanda. Estos análisis se podrán configurar para realizarse inmediatamente o a una fecha y hora futura, y también se podrán configurar para realizarse una vez o repetirse a diferentes intervalos, días, semanas, meses, etc.<br>Los análisis bajo demanda se podrán realizar a todas las unidades de la computadora o a carpetas, unidades o archivos específicos.<br>Los análisis bajo demanda deberán dar la opción de analizar la memoria durante su ejecución en búsqueda de programas maliciosos o no deseados y terminarlos en caso de encontrarlos.<br>Los análisis bajo demanda tendrán la opción de fijar un máximo, en porcentaje, de la utilización de recursos del sistema que se utilizarán durante el análisis.<br>En cuanto al análisis, los análisis bajo demanda, permitirán las mismas opciones que en el análisis de tiempo real, como los tipos de archivo, tiempos de análisis, excepciones, archivos empacados, etc.<br>La solución se debe integrar con los clientes MAPI de correo |

| | |
|---|---|
| | electrónico MS Outlook y Lotus Notes. Debe escanear en tiempo real el buzón de Outlook y la base de datos de Notes. También permitirá hacer escaneos bajo demanda de buzón y base de datos.<br><br>Además de la integración con un sistema de administración central para el manejo de las alertas, el sistema antivirus deberá dar la opción de tener su propio sistema de alertas para generar notificaciones. Debe cubrir al menos los siguientes tipos de eventos:<br><br>Análisis en tiempo real – detecciones, limpieza cuarentena, etc.<br>Análisis bajo demanda - detecciones, limpieza cuarentena, etc.<br>Restricción de acceso – eventos de restricción de acceso<br>Actualizaciones – eventos durante las actualizaciones del software.<br>Dentro de las acciones que el programa puede realizar cuando detecte 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:<br>Determinar la ubicación de la carpeta de cuarentena<br>Eliminar los archivos de la cuarentena automáticamente después de un periodo. Debe permitir habilitar o deshabilitar esta opción. En caso de habilitarla, se podrá fijar el número de días máximo en cuarentena.<br>Ver el contenido en la cuarentena desde la interfaz del antivirus.<br>Ver información acerca de la detección y del tiempo en cuarentena.<br><br>Permitirá analizar el archivo desde esta interfaz; se podrá restaurar el archivo y borrar de la cuarentena.<br>El fabricante deberá proporcionar una herramienta que permita recoger información acerca de su programa y su configuración para casos de problemas que deban ser atendidos por soporte técnico.<br><br>La solución deberá contar con una herramienta que permita restablecer los valores de configuración originales en el antivirus, así como reinstalar los archivos de la aplicación.<br>El software antivirus debe permitir al usuario cerrar (bloquear) puertos de comunicación de red, tanto de entrada como salida. En estos bloqueos puede determinar la protección contra cualquier proceso que los use o definir una lista. También permitirá la creación de una lista de excepción.<br>Debe permitir al usuario o administrador crear una política o políticas para controlar las acciones que los procesos del sistema o de red pueden realizar sobre uno o varios archivos. Dentro de las acciones debe incluir al menos, lectura, escritura, ejecución, creación y borrado. |

| | |
|---|---|
| | Debe permitir al usuario o administrador crear una política o políticas para controlar las acciones que los procesos del sistema o de red pueden realizar sobre un directorio o carpeta. Dentro de las acciones debe incluir al menos, lectura, escritura, ejecución, creación y borrado.<br>Debe permitir al usuario o administrador crear una política o políticas para controlar las acciones que los procesos del sistema o de red pueden realizar sobre un directorio o carpeta compartidos. Dentro de las acciones debe incluir al menos, lectura y escritura, aún cuando la carpeta se haya compartido con todos los permisos.<br>Cuando se detecta que una computadora está tratando de ser infectada a través de la red, el antivirus debe ser capaz de bloquear todas las conexiones de las computadoras que tratan de infectarla. El bloque puede ser por un tiempo específico o permanente. El bloqueo se terminará después de transcurrir el tiempo, manualmente desde la interfase del antivirus o desde la consola de administración centralizada.<br>La solución antivirus también debe contar con protección y bloqueo preventivo de desbordamientos de buffer (buffer overflow) de aplicaciones. Esta protección será activada o desactivada sin afectar el proceso antivirus. Permitirá crear nuevas reglas para que el software prevenga desbordamientos de pila de otras aplicaciones.<br>Capacidad de bloqueo de configuraciones por medio de una contraseña. Este bloqueo debe ser selectivo para partes específicas de la configuración, ó para toda la consola. Así como toda la configuración del sistema, esta contraseña de bloque debe ser configurada localmente y centralmente desde la consola de administración.<br>El antivirus podrá instalarse de forma remota desde la consola de administración.<br>La solución deberá contar con reglas de acceso que permitan dar protección preventiva en base a comportamiento, Las reglas deben prevenir al menos:<br>Detener la creación y modificación remota de archivos ejecutables.<br>Proteger el archivo con la lista de contactos.<br>Prevenir la falsificación de proceso de Windows (spoofing).<br>Prevenir la comunicación IRC.<br>Prevenir el uso de ftp<br>Prevenir que svchost ejecute programas no Windows<br>Prevenir contra programas de correo masivo locales<br>Controles contra contingencias de virus, como bloqueo de directorios compartidos.<br>Prevenir la modificación de los archivos de la solución antivirus.<br>Prevenir la modificación de archivos y configuración de los navegadores, Internet Explorer, Mozilla o FireFox<br>Prevenir la terminación del proceso antivirus. |

| | |
|---|---|
| | Detener programas que se intenten registrar en la 'auto-ejecución' (autorun).<br>Detener programas que se intentan registrar como servicio.<br>Detener la creación de archivos en carpetas importantes del sistema operativo.<br>La solución antivirus debe prevenir que el proceso antivirus sea detenido, así como el agente de administración que le permite comunicarse con la consola central.<br>El proveedor del software antivirus debe publicar al menos diariamente las bases de datos de firmas para la detección.<br>La actualización de firmas debe realizarse de forma automática o manual, según la configuración del administrador. Se podrá hacer programada desde la consola central.<br>Las actualizaciones de las firmas deben ser incrementales.<br>La solución debe contar con tecnología de detección de 'rootkits' por reglas y por comportamiento.<br>Todas las opciones de configuración mencionadas antes, deben poderse configurar, habilitar, crear y asignar desde la consola de administración central.<br>Debe soportar sistemas operativos Windows a 64 bits. |
| | **Programa contra programas espía:** La solución contra programas espía (antispyware) debe ofrecer a (CLIENTE) 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.<br>El programa antispyware de integrarse con la solución antivirus. Deben usar el mismo programa de análisis y también deben usar las mismas bases de datos para la detección. Por lo tanto las actualizaciones serán con la misma frecuencia en el mismo grupo de archivos.<br>Debe detectar al menos los siguientes tipos de programas no deseados:<br>Programas espía (spyware)<br>De publicidad (adware)<br>Administración remota<br>Marcadores telefónicos (dialers)<br>Descifrador contraseñas (password crakers)<br>Bromas (jokes)<br>Registro de teclas (key loggers)<br>Debe permitir configurar la misma reacción que el software antivirus, o una diferente para este tipo de programas.<br>En la consola de administración central debe contar con un grupo de reportes propios para distinguirlo de las detecciones antivirus.<br>Deberá ser capaz de hacer detección y limpieza en disco, memoria y registro de Windows.<br>Debe detectar cookies en tiempo real para evitar que sean instaladas en el sistema. |

**CONTINUACION PARTIDA N° 1**

| | |
|---|---|
| | **Consola de Administración:** Sistema de administración centralizada de las soluciones antivirus. La solución debe permitir la administración de políticas, configuración, actualización, notificaciones y respuesta a contingencias. Las tareas de administración deben poder realizarse desde una consola remota desde cualquier lugar de la organización. Los administradores pueden definir distintas políticas que contemplen todos los niveles de protección, Las características mínimas se describen a continuación.<br>El sistema deberá ser administrado desde una interfaz web, permitiendo el uso de navegadores de Internet para conectarse y trabajar con el sistema desde cualquier computadora que cuente con uno, y teniendo el usuario las credenciales de acceso necesarias.<br>El sistema contará con tableros de control que muestren información gráfica de las funciones principales de las soluciones administradas, como detecciones, actualizaciones, eventos, y versiones de productos instalados, entre otras.<br>El sistema permitirá que cada usuario del sistema de administración pueda generar las búsquedas necesarias para desplegar la información en el tablero de control, en base al perfil que tiene asignado. También el sistema debe permitir que cada usuario haga que sus propias búsquedas sean públicas, o de uso exclusivo.<br>Cada usuarios, según su perfil, también podrá hacer sus propios tableros de control, y organizarlos como le convenga, teniendo la opción de crear más de un tablero de control con diferentes búsquedas e información.<br>El sistema deberá contar con un sistema propio para generar las búsquedas, para facilitar el uso de la herramienta y la obtención de la información, si necesidad de recurrir a una herramienta de terceros para generar las búsquedas que se usan para crear los tableros de control y los reportes.<br>El sistema incluirá de fábrica reportes y búsquedas de todos los productos que maneje. Estos reportes y búsquedas se podrán modificar y copiar para que el cliente tenga sus propias búsquedas y repotes en base a los de fábrica del producto.<br>Es posible otorgar diferentes niveles de derechos a los usuarios asignándoles uno o más grupos de derechos. Los grupos de derechos darán acceso a los usuarios a configurar diferentes productos; por ejemplo puede permitir a un usuario configura el antivirus, pero no el agente de administración. También asignará permisos sobre diferentes grupos de equipos, así un administrador puede tener acceso a configurar o ver, ciertos equipos, y otros no.<br>En caso de instalarse más de un servidor de administración, el sistema contará con la posibilidad de consolidar la información de todos los servidores de administración en uno sólo para generar reportes de eventos y de actualización de producto. |

| | |
|---|---|
| | Es posible planificar tareas para que se ejecuten en el servidor de administración seleccionado con el objeto de realizar el mantenimiento de la base de datos y del Repositorio. Asimismo, es posible comprobar el estado de cada tarea<br>Puede trabajar con la información, las notificaciones y los eventos de error del servidor de administración. Además, podrá ver y actualizar eventos del servidor, guardarlos en un archivo o imprimirlos.<br>La solución permitirá la organización lógica de los equipos que serán administrados en un directorio. La organización del directorio, por ejemplo, puede ser por departamento funcional, ubicación geográfica o por dirección IP de la computadora. El directorio se podrá organizar en grupos y subgrupos; en el caso de los subgrupos se pueden especificar tantos subniveles como sea necesario dentro de cada grupo. El directorio permitirá hacer búsquedas de equipos, y tareas administrativas como moverlos entre grupos y borrarlos, entre otras.<br>La organización por dirección IP se puede hacer basándose en la subred de los equipo o por rango de direcciones. Está organización permitirá que por medio de una tarea, los equipos sean enviados automáticamente a su grupo correspondiente por la dirección IP<br><br>El sistema permitirá la creación de etiquetas en los equipos para poder organizarlos en los grupos en base a éste criterio; para poder generar búsquedas y para filtrar reportes. Estás etiquetas se podrán generar, entre otras, en base a las siguientes características:<br>Dirección IP, nombre del equipo, nombre del dominio, tipo de CPU, cantidad de memoria y sistema operativo.<br>El sistema permitirá que la organización de los equipos se realice también en base al criterio de las etiquetas de forma automática.<br>El directorio contará con un grupo donde se almacenarán los equipos para los que no se puede determinar su ubicación adecuada en el Directorio. La solución deberá utilizar las direcciones IP, los nombres de equipos, los nombres de dominio y los nombres de grupo para determinar dónde situarlos.<br>El sistema de administración será capaz de verificar que todos los equipos del directorio tienen nombres únicos y, si ordena equipos por dirección IP, que los intervalos de direcciones IP y las máscaras de subred de IP asignadas a los sitios y los grupos en el directorio siguen las directrices de administración IP. El sistema deberá contar con métodos propios y automáticos para verificar el directorio: al menos debe ser capaz de buscar nombres de equipo duplicados y Verificar la integridad de la configuración de administración IP. |

| | |
|---|---|
| | El sistema de administración centralizada contará con repositorios de almacenamiento de software distribuidos, para ayudar a facilitar las descargas de software hacia los clientes finales. Debe tener al menos las siguientes características:<br>El repositorio principal debe mantener la copia original de los paquetes, este repositorio es el servidor de administración.<br>Cada repositorio de almacenamiento distribuido mantiene una copia idéntica de los paquetes que están en el repositorio principal.<br>Los repositorios de almacenamiento distribuidos serán creados y administrados desde el servidor central, a través de la consola.<br>No será necesario instalar o correr ningún programa relacionado con el sistema de administración en estos servidores distribuidos, únicamente se deben copiar los paquetes de programas, no deben ser servidores dedicados a este sistema.<br>Los repositorios distribuidos serán actualizados desde el servidor central.<br>La descarga de los archivos hacia los clientes deberá ser al menos, dependiendo del tipo de servidor, a través de ftp, http o UNC.<br>En caso de tener más de un repositorio distribuido, debe permitir la actualización selectiva de éstos.<br>Cada tarea de actualización de los repositorios distribuidos se puede configurar para que sólo actualice el producto necesario.<br>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.<br>Las tareas se pueden crear con dependencia entre éstas, por ejemplo, se puede programar para que el servidor descargue las actualizaciones, y una vez terminada, haga la réplica de las actualizaciones los repositorios distribuidos.<br>Puede establecer directivas de los productos (valores de configuración) antes de aplicarlas o usar directivas predeterminadas, y cambiarlas como sea necesario después de su aplicación. Estas políticas podrán aplicarse a computadoras en particular, grupos o todo el directorio.<br>El sistema de administración debe permitir la administración de distintas aplicaciones además del antivirus de las computadoras de usuario. Debe ser capaz de administrar el antivirus de servidores Windows, NetWare, Linux, y antivirus para servidores de correo electrónico al menos.<br>El sistema debe obtener y guardar información acerca de las computadoras que administra. La información como mínimo debe incluir el nombre del equipo, dominio, dirección IP, subred, sistema operativo, capacidad de disco duro, CPU y memoria |

| | |
|---|---|
| | RAM.<br>El sistema debe permitir a los administradores crear tareas de actualización, instalación y escaneos sobre demanda para equipos específicos, grupos o todo el directorio.<br>Las tareas serán programadas de acuerdo con, al menos, los siguientes valores: Diario, semanal, mensual, una vez, al arrancar el equipo, cuando está prendida sin usarse, inmediatamente, al firmarse y al hacer una conexión remota (dial-up).<br>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.<br>Debe contar con un medio automático por el cual el servidor de administración detecte las computadoras cuyos agentes no han mantenido comunicación con el servidor durante un tiempo y poder determinar cuales de esos agentes ya no está instalado 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<br>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.<br>También debe permitir que administrador pueda forzar desde la consola la comunicación del agente al servidor. Esta función se podrá aplicar a un solo agente a todo un grupo, permitiendo también determinar un periodo de tiempo en el que aleatóriamente se forzará esta comunicación, en el caso de que sean muchos los agentes.<br>El sistema deberá contar un mecanismo que permita al administrador hacer una actualización de todos los equipos en el momento que surja una actualización. Esta actualización general puede ser lanzada automáticamente en el momento que el servidor de administración encuentre una actualización en el sitio del fabricante, como una nueva firma o parche antivirus, ó manualmente el administrador la puede disparar desde la consola. También permitirá al administrador que productos se actualicen y que tipo de actualizaciones hacer.<br>Las actualizaciones deben cubrir todos los productos administrados desde el servidor, y dentro de cada producto incluyen nuevas versiones, actualización de firmas, parches y hot fixes. Esta actualización puede ser selectiva. El administrador podrá determinar que productos y que tipo de actualización será automática y cuales manuales, incluso poder configurar diferentes métodos o tipo dependiendo del producto o del grupo. |

| | |
|---|---|
| | El servidor de administración será capaz de descargar las actualizaciones desde el sitio del fabricante a través de tareas programadas.<br>El servidor de administración generará reportes, además de la información en la consola, acerca de las versiones instaladas en los equipos, incluyendo versiones de software, parches, hotfixes, firmas de antivirus y todo lo relevante respecto a los productos administrados.<br>Los reportes de la herramienta de administración deben generarse desde la misma consola. Los reportes permitirán generar filtros al ejecutarse y guardar plantillas de reportes. El sistema debe contar con reportes referentes a eventos del sistema. Siendo la administración del antivirus, debe contar al menos con reportes acerca de detecciones y actualizaciones antivirus, como los virus más detectados, las máquinas con más incidentes, las versiones instaladas. Debe especificar nombre del virus, tipo de virus, acción resultante. Debe permitir ir al detalle de los reportes una vez que se generó el reporte origina, así poder navegar en la información hasta llegar al detalle del reporte.<br>Debe proveer herramientas que permitan al administrador hacer tareas de la base de datos, como respaldos, restauraciones, mantenimientos y otros.<br>Puede planificar una tarea: Sincronizar dominios para sincronizar los dominios seleccionados importados en el Directorio con sus equivalentes en la red. Esto se realiza con el fin de mantener actualizad el Directorio con la red de forma automática.<br>El sistema de administración podrá determinar, por medio de búsquedas (escaneos), la presencia de parches de seguridad de Microsoft en los equipos administrados. Podrá crear perfiles de seguridad en case a reglas creadas por el administrador, así como plantillas predefinidas en el sistema. Estos perfiles buscarán la presencia de parches de Microsoft, algún archivo característico de una amenaza conocida, algún servicio o llave del registro. Esta función debe ser parte del sistema de administración centralizada, no una aplicación por separado. Debe contar con reportes acerca del cumplimiento de estas políticas. También debe integrarse con el módulo de notificaciones para poderlas generar en base a los resultados de estas búsquedas<br>El agente debe ser compatible con las versiones de 64 bits de los sistemas operativos Windows.<br>El sistema debe permitir la importación de la información de computadoras del Directorio Activo de Microsoft. La importación se debe poder programar para que se realice periódicamente. Así el sistema reflejará las nuevas computadoras que van siendo agregadas al Directorio activo También permitirá que se puede hacer un mapeo entre los grupos del sistema de administración centralizado con los grupos del directorio activo. |

| | |
|---|---|
| | El sistema podrá auditar al menos las siguientes acciones: inicios de sesión en el sistema, cambio de perfiles o roles de usuarios del sistema, cambio de contraseñas, desinstalación de los agentes por eliminación, cambios en las políticas de configuración de los productos administrados, agregar o borrar componentes del directorio, renombrar componentes del directorio.<br>Debe permitir que las computadoras sean administradas e identificadas por el nombre o por la dirección física de la tarjeta (MAC address).<br>En el caso de computadoras que tienen más de una dirección física (MAC) - una portátil con una "dock station" por ejemplo- el sistema debe ser capaz de identificar que se trata del mismo sistema, y tratarlo como uno solo, sin duplicar la información.<br>El sistema contará con un mecanismo para detectar máquinas que están conectadas a la red, y determinar si estas computadoras ya son administradas por el sistema central de administración del antivirus. Como acciones ante computadoras no administradas se les puede enviar la instalación del agente de administración y con ello el antivirus o enviar notificaciones al (los) administrador(es). Deberá contar también con reportes específicos de este componente.<br>El sistema enviará notificaciones de eventos que sucedan en sus componentes. Las notificaciones serán en base a reglas definidas por el administrador. Estas reglas utilizarán al menos los siguientes parámetros:<br>Nivel del directorio. Se podrá determinar a que nivel del directorio aplicará cada regla. Por ejemplo enviar una notificación únicamente si se detecta un virus en el grupo “dirección general”.<br>Sistema Operativo.<br>Producto. Por ejemplo un evento en el servidor de administración o en algún cliente.<br>Tipo de evento. Puede ser una detección de virus, una actualización, etc.<br>Tipo de notificación. Correo electrónico, SNMP, etc.<br>El sistema de administración debe soportar Microsoft Clustering Services para alta disponibilidad<br>El sistema de administración permitirá controlar las actualizaciones para maximizar la protección y minimizar el tráfico en la red. Se pueden configurar tareas de actualización por separado, para actualizar clientes con cualquier combinación de firmas de antivirus, motores y paquetes de actualización de productos en el repositorio. |
| | **Protección de Intrusos y Firewall:** La solución ofrecida debe contar con un sistema de protección de intrusos para las computadoras que se integre con el sistema de administración centralizado, para su instalación y administración de actualizaciones y políticas. Está solución debe contar con las siguientes características |

| | |
|---|---|
| | La solución de IPS de sistema debe ser un programa que se instala en la computadora y protege al mismo sistema.<br>Debe contar con al menos los siguientes componentes:<br>Prevención de intrusos (IPS)<br>Firewall<br>Bloqueo de aplicaciones<br>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:<br>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.<br>Detección por firma 2. Las firmas deben estar diseñadas para aplicaciones y sistemas operativos específicos.<br>Detección por comportamiento. Este método se basa en el comportamiento de las aplicaciones para detectar actividad maliciosa, esto permitirá detener ataques aún cuando no existe una firma específica, ataques día-cero.<br>El IPS creará eventos en la consola central cuando detenga un ataque, en base a esta información el administrador podrá crear excepciones, que evitarán la aplicación de la regla cuando se cumplan los criterios de la excepción.<br>También permitirá al administrador, en base esta información de los eventos, crear una lista de aplicaciones seguras, a las que no se le aplicarán las reglas de IPS.<br>El componente Firewall debe funcionar como filtro entre la computadora y la red donde está conectada.<br>El firewall debe utilizar al menos criterios como la dirección IP, puerto TCP o UDP y tipo de paquete para aplicar los criterios de bloquear y dejar pasar. Estos criterios deben aplicarse para tráfico entrante y saliente.<br>El firewall debe usar tecnología de “Stateful packet filtering” y “stateful packet inspection”.<br>El firewall debe permitir poner las máquinas en cuarentena, donde esta cuarentena permitirá la comunicación con otros puntos de la red, con tantas restricciones como la política determinada por el administrador lo especifique.<br>El firewall podrá aplicar una política diferente, dependiendo en donde se encuentre conectada la computadora. Por ejemplo si la máquina de un usuario móvil está conectada a la red de la organización usará una política diferente a si está conectada a una red pública. El software será capaz de determinar cuando la máquina está conectada en diferentes redes.<br>Para la creación de las reglas del firewall se deben basar, al menos, en los siguientes criterios.<br>Tipo de conexión (red o inalámbrica).<br>Protocolos IP y ni IP.<br>Tráfico de entrada o salida o los dos. |

| | |
|---|---|
| | La aplicación que generó el tráfico.<br>El puerto o servicio usado por la computadora, ya sea como receptor u origen.<br>El puerto o servicio usado por la computadora remota, ya sea como receptor u origen.<br>Dirección IP del origen o el receptor<br>El momento del día o la semana en que el paquete fue enviado o recibido.<br>El componente de bloqueo de aplicaciones monitorea las aplicaciones que se están ejecutando y las bloque o las permite.<br>El administrador podrá crear las reglas que permitirán o evitarán la ejecución de las aplicaciones en las máquinas cliente.<br>El bloqueo de aplicaciones también permitirá detener aplicaciones que tratan de ligarse con otros procesos para ejecutarse, cuando estas aplicaciones son programas maliciosos.<br>El administrador podrá determinar si se aplican los dos tipos de bloqueo, el de ejecución y el de ligado de aplicaciones, o los dos. |
| | **Protección de Antivirus para Servidores Exchange:**<br>Protección antivirus y control de contenido para servidores Microsoft Exchange<br>El sistema proporcionará una solución antivirus y de control de contenidos para servidores de correo electrónico Microsoft Exchange, con las siguientes características<br>Debe integrarse con el sistema de administración de las otras soluciones, para su administración y reporteo de eventos.<br>Capacidad de manejar el análisis o escaneo en tiempo real de los correos. Puede analizar correos o archivos cuando el usuario o sistema los lee o escribe.<br>Capacidad de llevar acabo análisis bajo demanda de forma manual o planificada para que se analicen todos los buzones, carpetas y bases de datos por virus o contenido no deseado.<br>Capacidad para analizar en busca de virus dentro de todo los diferentes tipos de archivos comprimidos como .zip, .rar, etc.<br>Capacidad para bloquear o detener correos con contenido inapropiado como palabra o frases, asunto y cuerpo del mensaje.<br>La tecnología permitirá descargar las actualizaciones de definición (DAT) y de motor de forma manual o planificada.<br>Capacidad de crear políticas globales o por grupos los cuales se pueden importar de un directorio LDAP o creados manualmente<br>Capacidad de especificar los nombres, tipos y tamaños de archivos que se deben bloquear mediante reglas de filtrado de archivos.<br>Capaz de detectar y eliminar archivos de broma y sospechosos |

| | |
|---|---|
| | como utilidades de acceso remoto, decodificadores de contraseña, etc.<br>Capaz de detener o eliminar los archivos adjuntos dañados, corruptos o de cero bytes.<br>Capaz de manejar una cuarentena, sí se desea aislar o poner en cuarentena archivos infectados o sospechosos infectados.<br>Capaz de detectar virus conocidos y desconocidos a través de comportamiento o patrones similares a los de un virus en todos los archivos.<br>Capacidad de manejar varios tipos de alertas para la notificación de eventos como infecciones. Capaz de enviar mensajes SNMP, Email, pager, etc.<br>Detectar y reaccionar ante los brotes de virus. Debe ofrecer protección basada en una selección de reglas predefinidas y especificadas por el administrador para evitar una propagación mayor, por ejemplo, dejar de mandar correo si se detectan 10000 correos infectados por el mismo virus en X segundos.<br>Capaz de permitir o denegar el acceso a los correos o archivos cifrados y de eliminar o romper las firmas digitales.<br>Capacidad para crear registros, incluyendo con reportes gráficos (A través de ePO) para diagnóstico de posibles fallas y análisis de eventos.<br>El sistema antivirus del correo electrónico debe contar con un motor de detección de SPAM, que cuente, al menos, con las siguientes características:<br>Capacidad de analizar todos los correos entrantes y salientes en tiempo real por contenido SPAM o no deseado.<br>El sistema asignará una calificación a los correos para determinar el nivel de certeza de que es spam, así, una calificación más alta asegura que el contenido del correo es más seguro de ser SPAM.<br>En base a las calificaciones permitirá asignar diferentes acciones para diferentes calificaciones de SPAM.<br>Las acciones deben incluir, al menos: bloquear, poner en cuarentena o marcar el asunto de correo con una frase alusiva al SPAM (“posible spam” por ejemplo), así como las correspondientes a notificaciones a destinatario, remitente o administrador.<br>Capacidad de crear listas negras/blancas generales para el bloqueo de dominio, email, palabras, etc.<br>Capacidad de crear listas negras/blancas individuales por el usuario del correo.<br>Debe contar un grupo de reglas predeterminadas para identificar el SPAM, estas reglas se actualizarán y ajustarán constantemente.<br>Capacidad de reenviar los correos basura (SPAM) a una carpeta creada por el mismo Spamkiller en el buzón de los usuarios o en un buzón o carpeta basura (JUNK) del sistema de correo.<br>Capaz de analizar los correos y sus adjuntos en busca de |

| | |
|---|---|
| | contenido no deseado. Se pueden crear reglas que establezcan que palabras o frases no están permitidas en ningún mensaje o adjunto. |
| | El proveedor debe presentar carta de fabricante que es distribuidor autorizado de la solución propuesta. Documentación comprobatoria vigente (ejercicio 2008). |
| | El proveedor deberá presentar certificados de su personal que avalen que tienen conocimiento de la suite propuesta al congreso, la falta de esta información será causante de descalificación. |
| ***Servicios*** | |
| | ***Incluirá los siguientes servicios**:* |
| 1 | Soporte telefónico ilimitado 24X7 para recibir ayuda respecto a la instalación configuración y funcionalidad de los productos. |
| 2 | Capacitación necesaria para la administración y manejo de la solución completa, curso de por lo menos 16 hrs. Deberá anexar material informativo sobre el curso en el idioma español y contenido del mismo para ser evaluado. El no presentar el presente documento será motivo de descalificación del licitante. |
| 3 | Servicios de actualización con acceso desde Internet a:<br>a) soluciones técnicas desde la base de conocimientos técnicos.<br>b) documentación técnica como guías, FAQ's y release notes.<br>c) envío de incidentes de manera electrónica.<br>d) Mejoras al software que incluyen updates y upgrades de documentación y SW. |
| 4 | Incluye el servicio de soporte y actualización del producto durante la duración del mismo, sobre cualquier nueva versión, actualización o mejora que realice el fabricante en cualquier producto de la suite. |
| 5 | Instalación, configuración, implementación y puesta a punto en sitio por personal certificado técnicamente por la marca del software, además de contar con al menos 3 ingenieros certificados durante la duración del servicio, mismos que deberán realizar las revisiones pertinentes a fin de garantizar el desempeño al 100% del software. |

**ANEXO TÉCNICO**

| PARTIDA | CANTIDAD | U.M. | DESCRIPCIÓN |
|---|---|---|---|
| **2** | 1 | Adquisición de Licencia Corporativa para 42 computadoras | SOLUCIÓN INTEGRAL DE SEGURIDAD PARA ESCRITORIOS Y SERVIDORES |

| Características Requeridas | Especificaciones Requeridas |
|---|---|
| **Producto** | **Soporte de licenciamiento de antivirus para 42 computadoras** |
| | **Antivirus:** La solución antivirus debe ofrecer a H. Congreso del Estado de Veracruz una protección contra código malicioso que cubra al menos contra virus, troyanos, gusanos y programas no deseados. Esta solución debe estar diseñada para funcionar en un ambiente de red, y el mismo fabricante debe proporcionar las herramientas para ser administrada de forma centralizada, tanto para la configuración, como instalación y actualizaciones.<br>La solución antivirus deberá ser capaz de analizar en busca de código malicioso (lo llamaremos analizar de aquí en adelante), el sistema donde esté instalado en tiempo real, cuando se acceda a un archivo o carpeta, así como los procesos que se ejecuten en memoria.<br>La solución analizará archivos de discos locales de la computadora, unidades removibles, así como el contenido de unidades de red.<br>La aplicación antivirus debe tener la opción de clasificar los procesos en base al riesgo que representan, y poder configurar el análisis en tiempo real en base a este parámetro. Así, debe permitir al menos tres configuraciones, alto, bajo y estándar.<br>La solución debe realizar el análisis de archivos de comandos (scripts) mientras se están ejecutando.<br>Dentro de los métodos de detección debe contar con la detección heurística.<br>Cuando se detecta que una computadora está tratando de ser infectada a través de la red, el antivirus debe ser capaz de bloquear todas las conexiones de las computadoras que tratan de infectarla y reportar la dirección IP de tal computadora. El bloqueo puede ser por un tiempo específico o permanente. El bloqueo se terminará después de transcurrir el tiempo, manualmente desde la interfase del antivirus o desde la consola de administración centralizada.<br>El antivirus dará la opción para analizar sectores de arranque y analizar unidades de disco de 3.5” cuando se apaga el equipo.<br>Debe poder configurar un mensaje de alerta al usuario cuando se da una detección y mostrarle distintas acciones a aplicar. También permitirá aplicar acciones automáticas sin mostrar información al usuario.<br>El antivirus deberá tener diferentes opciones para el manejo del registro de eventos de la aplicación. Entre la opciones se podrá |

| | |
|---|---|
| | determinar si se activa o desactiva el registro; nombre y ubicación del archivo de registro; tamaño máximo del archivo; poder ver el archivo desde la interfase del antivirus.<br>Permitirá al administrador configurar la solución para analizar todos los archivos, ó una lista de tipos de archivo predetermina por las firmas de fabricante. A esta lista de tipos de archivo el administrador podrá agregar otros tipos de archivo.<br>El antivirus permitirá la creación de excepciones de archivos, carpetas o unidades disco para no ser analizadas.<br>Para el análisis de archivos empacados (.zip, pkg, etc.), el antivirus permitirá habilitar o deshabilitar que se realice el análisis de los éstos. En caso de habilitarse, debe permitir fijar un tiempo máximo de análisis por cada uno de los archivos contenidos en el conjunto, y un tiempo máximo de análisis del archivo empacado completo.<br>El sistema se integrará al sistema operativo de manera que creará opciones en el menú de contexto del explorador. Esto permitirá que apretando el botón derecho del Mouse sobre un archivo o carpeta, entre todas las opciones mostrará la de 'analizar en busca de virus'.<br><br>El programa antivirus debe contar con la opción de crear análisis bajo demanda. Estos análisis se podrán configurar para realizarse inmediatamente o a una fecha y hora futura, y también se podrán configurar para realizarse una vez o repetirse a diferentes intervalos, días, semanas, meses, etc.<br>Los análisis bajo demanda se podrán realizar a todas las unidades de la computadora o a carpetas, unidades o archivos específicos.<br>Los análisis bajo demanda deberán dar la opción de analizar la memoria durante su ejecución en búsqueda de programas maliciosos o no deseados y terminarlos en caso de encontrarlos.<br>Los análisis bajo demanda tendrán la opción de fijar un máximo, en porcentaje, de la utilización de recursos del sistema que se utilizarán durante el análisis.<br>En cuanto al análisis, los análisis bajo demanda, permitirán las mismas opciones que en el análisis de tiempo real, como los tipos de archivo, tiempos de análisis, excepciones, archivos empacados, etc.<br>La solución se debe integrar con los clientes MAPI de correo electrónico MS Outlook y Lotus Notes. Debe escanear en tiempo real el buzón de Outlook y la base de datos de Notes. También permitirá hacer escaneos bajo demanda de buzón y base de datos.<br>Además de la integración con un sistema de administración central para el manejo de las alertas, el sistema antivirus deberá dar la opción de tener su propio sistema de alertas para generar notificaciones. Debe cubrir al menos los siguientes tipos de eventos: |

| | |
|---|---|
| | Análisis en tiempo real – detecciones, limpieza cuarentena, etc.<br>Análisis bajo demanda - detecciones, limpieza cuarentena, etc.<br>Restricción de acceso – eventos de restricción de acceso<br>Actualizaciones – eventos durante las actualizaciones del software.<br>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:<br>Determinar la ubicación de la carpeta de cuarentena<br>Eliminar los archivos de la cuarentena automáticamente después de un periodo. Debe permitir habilitar o deshabilitar esta opción. En caso de habilitarla, se podrá fijar el número de días máximo en cuarentena.<br>Ver el contenido en la cuarentena desde la interfase del antivirus. Ver información acerca de la detección y del tiempo en cuarentena.<br>Permitirá analizar el archivo desde esta interfase; se podrá restaurar el archivo y borrar de la cuarentena.<br>El fabricante deberá proporcionar una herramienta que permita recoger información acerca de su programa y su configuración para casos de problemas que deban ser atendidos por soporte técnico.<br>La solución deberá contar con una herramienta que permita restablecer los valores de configuración originales en el antivirus, así como reinstalar los archivos de la aplicación.<br>El software antivirus debe permitir al usuario cerrar (bloquear) puertos de comunicación de red, tanto de entrada como salida. En estos bloqueos puede determinar la protección contra cualquier proceso que los use o definir una lista. También permitirá la creación de una lista de excepción.<br>Debe permitir al usuario o administrador crear una política o políticas para controlar las acciones que los procesos del sistema o de red pueden realizar sobre uno o varios archivos. Dentro de las acciones debe incluir al menos, lectura, escritura, ejecución, creación y borrado.<br>Debe permitir al usuario o administrador crear una política o políticas para controlar las acciones que los procesos del sistema o de red pueden realizar sobre un directorio o carpeta. Dentro de las acciones debe incluir al menos, lectura, escritura, ejecución, creación y borrado.<br>Debe permitir al usuario o administrador crear una política o políticas para controlar las acciones que los procesos del sistema o de red pueden realizar sobre un directorio o carpeta compartidos. Dentro de las acciones debe incluir al menos, lectura y escritura, aún cuando la carpeta se haya compartido con todos los permisos.<br>Cuando se detecta que una computadora está tratando de ser infectada a través de la red, el antivirus debe ser capaz de bloquear todas las conexiones de las computadoras que tratan |

| | |
|---|---|
| | de infectarla. El bloque puede ser por un tiempo específico o permanente. El bloqueo se terminará después de transcurrir el tiempo, manualmente desde la interfase del antivirus o desde la consola de administración centralizada.<br>La solución antivirus también debe contar con protección y bloqueo preventivo de desbordamientos de buffer (buffer overflow) de aplicaciones. Esta protección será activada o desactivada sin afectar el proceso antivirus. Permitirá crear nuevas reglas para que el software prevenga desbordamientos de pila de otras aplicaciones.<br>Capacidad de bloqueo de configuraciones por medio de una contraseña. Este bloqueo debe ser selectivo para partes específicas de la configuración, ó para toda la consola. Así como toda la configuración del sistema, esta contraseña de bloque debe ser configurada localmente y centralmente desde la consola de administración.<br>El antivirus podrá instalarse de forma remota desde la consola de administración.<br>La solución deberá contar con reglas de acceso que permitan dar protección preventiva en base a comportamiento, Las reglas deben prevenir al menos:<br>Detener la creación y modificación remota de archivos ejecutables.<br>Proteger el archivo con la lista de contactos.<br>Prevenir la falsificación de proceso de Windows (spoofing).<br>Prevenir la comunicación IRC.<br>Prevenir el uso de ftp.<br>Prevenir que svchost ejecute programas no Windows<br>Prevenir contra programas de corro masivo locales<br>Controles contra contingencias de virus, como bloqueo de directorios compartidos.<br>Prevenir la modificación de los archivos de la solución antivirus.<br>Prevenir la modificación de archivos y configuración de los navegadores, Internet Explorer, Mozilla o FireFox<br>Prevenir la terminación del proceso antivirus.<br>Detener programas que se intenten registrar en la 'auto-ejecución' (autorun).<br>Detener programas que se intentan registrar como servicio.<br>Detener la creación de archivos en carpetas importantes del sistema operativo.<br>La solución antivirus debe prevenir que el proceso antivirus sea detenido, así como el agente de administración que le permite comunicarse con la consola central.<br>El proveedor del software antivirus debe publicar al menos diariamente las bases de datos de firmas para la detección.<br>La actualización de firmas debe realizarse de forma automática o manual, según la configuración del administrador. Se podrá hacer programada desde la consola central.<br>Las actualizaciones de las firmas deben ser incrementales.<br>La solución debe contar con tecnología de detección de |

| | |
|---|---|
| | 'rootkits' por reglas y por comportamiento.<br>Todas las opciones de configuración mencionadas antes, deben poderse configurar, habilitar, crear asignar desde la consola de administración central.<br>Debe soportar sistemas operativos Windows a 64 bits. |
| | Programa contra programas espía: La solución contra programas espía (antispyware) debe ofrecer a (CLIENTE) 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.<br>El programa antispyware de integrarse con la solución antivirus. Deben usar el mismo programa de análisis y también deben usar las mismas bases de datos para la detección. Por lo tanto las actualizaciones serán con la misma frecuencia en el mismo grupo de archivos.<br>Debe detectar al menos los siguientes tipos de programas no deseados:<br>Programas espía (spyware)<br>De publicidad (adware)<br>Administración remota<br>Marcadores telefónicos (dialers)<br>Descifrador contraseñas (password crakers)<br>Bromas (jokes)<br>Regitro de teclas (key loggers)<br>Debe permitir configurar la misma reacción que el software antivirus, o una diferente para este tipo de programas.<br>En la consola de administración central debe contar con un grupo de reportes propios para distinguirlo de las detecciones antivirus.<br>Deberá se capaz de hacer detección y limpieza en disco, memoria y registro de Windows.<br>Debe detectar cookies en tiempo real para evitar que sean instaladas en el sistema. |
| | **Consola de Administración:** Sistema de administración centralizada de las soluciones antivirus. La solución debe permitir la administración de políticas, configuración, actualización, notificaciones y respuesta a contingencias. Las tareas de administración deben poder realizarse desde una consola remota desde cualquier lugar de la organización. Los administradores pueden definir distintas políticas que contemplen todos los niveles de protección, Las características mínimas se describen a continuación.<br>El sistema deberá ser administrado desde una interfase web, permitiendo el uso de navegadores de Internet para conectarse y trabajar con el sistema desde cualquier computadora que cuente con uno, y teniendo el usuario las credenciales de |

| | |
|---|---|
| | acceso necesarias.<br>El sistema contará con tableros de control que muestren información gráfica de las funciones principales de las soluciones administradas, como detecciones, actualizaciones, eventos, y versiones de productos instalados, entre otras.<br>El sistema permitirá que cada usuario del sistema de administración pueda generar las búsquedas necesarias para desplegar la información en el tablero de control, en base al perfil que tiene asignado. También el sistema debe permitir que cada usuario haga que sus propias búsquedas sean públicas, o de uso exclusivo.<br>Cada usuarios, según su perfil, también podrá hacer sus propios tableros de control, y organizarlos como le convenga, teniendo la opción de crear más de un tablero de control con diferentes búsquedas e información.<br>El sistema deberá contar con un sistema propio para generar las búsquedas, para facilitar el uso de la herramienta y la obtención de la información, si necesidad de recurrir a una herramienta de terceros para generar las búsquedas que se usan para crear los tableros de control y los reportes.<br>El sistema incluirá de fábrica reportes y búsquedas de todos los productos que maneje. Estos reportes y búsquedas se podrán modificar y copiar para que el cliente tenga sus propias búsquedas y repotes en base a los de fábrica del producto.<br>Es posible otorgar diferentes niveles de derechos a los usuarios asignándoles uno o más grupos de derechos. Los grupos de derechos darán acceso a los usuarios a configurar diferentes productos; por ejemplo puede permitir a un usuario configura el antivirus, pero no el agente de administración. También asignará permisos sobre diferentes grupos de equipos, así un administrador puede tener acceso a configurar o ver, ciertos equipos, y otros no.<br>En caso de instalarse más de un servidor de administración, el sistema contará con la posibilidad de consolidar la información de todos los servidores de administración en uno sólo para generar reportes de eventos y de actualización de producto.<br>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<br>Puede trabajar con la información, las notificaciones y los eventos de error del servidor de administración. Además, podrá ver y actualizar eventos del servidor, guardarlos en un archivo o imprimirlos.<br>La solución permitirá la organización lógica de los equipos que serán administrados en un directorio. La organización del directorio, por ejemplo, puede ser por departamento funcional, ubicación geográfica o por dirección IP de la computadora. El directorio se podrá organizar en grupos y subgrupos; en el caso de los subgrupos se pueden especificar tantos subniveles como |

| | |
|---|---|
| | sea necesario dentro de cada grupo. El directorio permitirá hacer búsquedas de equipos, y tareas administrativas como moverlos entre grupos y borrarlos, entre otras.<br>La organización por dirección IP se puede hacer basándose en la subred de los equipo o por rango de direcciones. Está organización permitirá que por medio de una tarea, los equipos sean enviados automáticamente a su grupo correspondiente por la dirección IP<br>El sistema permitirá la creación de etiquetas en los equipos para poder organizarlos en los grupos en base a éste criterio; para poder generar búsquedas y para filtrar reportes. Estás etiquetas se podrán generar, entre otras, en base a las siguientes características:<br>Dirección IP, nombre del equipo, nombre del dominio, tipo de CPU, cantidad de memoria y sistema operativo.<br>El sistema permitirá que la organización de los equipos se realice también en base al criterio de las etiquetas de forma automática.<br>El directorio contará con un grupo donde se almacenarán los equipos para los que no se puede determinar su ubicación adecuada en el Directorio. La solución deberá utilizar las direcciones IP, los nombres de equipos, los nombres de dominio y los nombres de grupo para determinar dónde situarlos.<br>El sistema de administración será capaz de verificar que todos los equipos del directorio tienen nombres únicos y, si ordena equipos por dirección IP, que los intervalos de direcciones IP y las máscaras de subred de IP asignadas a los sitios y los grupos en el directorio siguen las directrices de administración IP. El sistema deberá contar con métodos propios y automáticos para verificar el directorio: al menos debe ser capaz de buscar nombres de equipo duplicados y Verificar la integridad de la configuración de administración IP.<br>El sistema de administración centralizada contará con repositorios de almacenamiento de software distribuidos, para ayudar a facilitar las descargas de software hacia los clientes finales. Debe tener al menos las siguientes características:<br>El repositorio principal debe mantener la copia original de los paquetes, este repositorio es el servidor de administración.<br>Cada repositorio de almacenamiento distribuido mantiene una copia idéntica de los paquetes que están en el repositorio principal.<br>Los repositorios de almacenamiento distribuidos serán creados y administrados desde el servidor central, a través de la consola.<br>No será necesario instalar o correr ningún programa relacionado con el sistema de administración en estos servidores distribuidos, únicamente se deben copiar los paquetes de programas, no deben ser servidores dedicados a este sistema. |

| | |
|---|---|
| | Los repositorios distribuidos serán actualizados desde el servidor central.<br>La descarga de los archivos hacia los clientes deberá ser al menos, dependiendo del tipo de servidor, a través de ftp, http o UNC.<br>En caso de tener más de un repositorio distribuido, debe permitir la actualización selectiva de éstos.<br>Cada tarea de actualización de los repositorios distribuidos se puede configurar para que sólo actualice los productos necesarios.<br>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.<br>Las tareas se pueden crear con dependencia entre éstas, por ejemplo, se puede programar para que el servidor descargue las actualizaciones, y una vez terminada, haga la réplica de las actualizaciones los repositorios distribuidos.<br>Puede establecer directivas de los productos (valores de configuración) antes de aplicarlas o usar directivas predeterminadas, y cambiarlas como sea necesario después de su aplicación. Estas políticas podrán aplicarse a computadoras en particular, grupos o todo el directorio.<br>El sistema de administración debe permitir la administración de distintas aplicaciones además del antivirus de las computadoras de usuario. Debe ser capaz de administrar el antivirus de servidores Windows, NetWare, Linux, y antivirus para servidores de correo electrónico al menos.<br>El sistema debe obtener y guardar información acerca de las computadoras que administra. La información como mínimo debe incluir el nombre del equipo, dominio, dirección IP, subred, sistema operativo, capacidad de disco duro, CPU y memoria RAM.<br>El sistema debe permitir a los administradores crear tareas de actualización, instalación y escaneos sobre demanda para equipos específicos, grupos o todo el directorio.<br>Las tareas serán programadas de acuerdo con, al menos, los siguientes valores: Diario, semanal, mensual, una vez, al arrancar el equipo, cuando está prendida sin usarse, inmediatamente, al firmarse y al hacer una conexión remota (dial-up).<br>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.<br>Debe contar con un medio automático por el cual el servidor de administración detecte las computadoras cuyos agentes no han mantenido comunicación con el servidor durante un tiempo y |

| | |
|---|---|
| | poder determinar cuales de esos agentes ya no está instalado 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<br>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.<br>También debe permitir que administrador pueda forzar desde la consola la comunicación del agente al servidor. Esta función se podrá aplicar a un solo agente a todo un grupo, permitiendo también determinar un periodo de tiempo en el que aleatóriamente se forzará esta comunicación, en el caso de que sean muchos los agentes.<br>El sistema deberá contar un mecanismo que permita al administrador hacer una actualización de todos los equipos en el momento que surja una actualización. Esta actualización general puede ser lanzada automáticamente en el momento que el servidor de administración encuentre una actualización en el sitio del fabricante, como una nueva firma o parche antivirus, ó manualmente el administrador la puede disparar desde la consola. También permitirá al administrador que productos se actualicen y que tipo de actualizaciones hacer.<br>Las actualizaciones deben cubrir todos los productos administrados desde el servidor, y dentro de cada producto incluyen nuevas versiones, actualización de firmas, parches y hot fixes. Esta actualización puede ser selectiva. El administrador podrá determinar que productos y que tipo de actualización será automática y cuales manuales, incluso poder configurar diferentes métodos o tipo dependiendo del producto o del grupo.<br>El servidor de administración será capaz de descargar las actualizaciones desde el sitio del fabricante a través de tareas programadas.<br>El servidor de administración generará reportes, además de la información en la consola, acerca de las versiones instaladas en los equipos, incluyendo versiones de software, parches, hotfixes, firmas de antivirus y todo lo relevante respecto a los productos administrados.<br>Los reportes de la herramienta de administración deben generarse desde la misma consola. Los reportes permitirán generar filtros al ejecutarse y guardar plantillas de reportes. El sistema debe contar con reportes referentes a eventos del sistema. Siendo la administración del antivirus, debe contar al menos con reportes acerca de detecciones y actualizaciones antivirus, como los virus más detectados, las máquinas con más incidentes, las versiones instaladas. Debe especificar |

| | |
|---|---|
| | nombre del virus, tipo de virus, acción resultante. Debe permitir ir al detalle de los reportes una vez que se generó el reporte origina, así poder navegar en la información hasta llegar al detalle del reporte.<br>Debe proveer herramientas que permitan al administrador hacer tareas de la base de datos, como respaldos, restauraciones, mantenimientos y otros.<br>Puede planificar una tarea: Sincronizar dominios para sincronizar los dominios seleccionados importados en el Directorio con sus equivalentes en la red. Esto se realiza con el fin de mantener actualizad el Directorio con la red de forma automática.<br>El sistema de administración podrá determinar, por medio de búsquedas (escaneos), la presencia de parches de seguridad de Microsoft en los equipos administrados. Podrá crear perfiles de seguridad en case a reglas creadas por el administrador, así como plantillas predefinidas en el sistema. Estos perfiles buscarán la presencia de parches de Microsoft, algún archivo característico de una amenaza conocida, algún servicio o llave del registro. Esta función debe ser parte del sistema de administración centralizada, no una aplicación por separado. Debe contar con reportes acerca del cumplimiento de estas políticas. También debe integrarse con el módulo de notificaciones para poderlas generar en base a los resultados de estas búsquedas<br>El agente debe ser compatible con las versiones de 64 bits de los sistemas operativos Windows.<br>El sistema debe permitir la importación de la información de computadoras del Directorio Activo de Microsoft. La importación se debe poder programar para que se realice periódicamente. Así el sistema reflejará las nuevas computadoras que van siendo agregadas al Directorio activo También permitirá que se puede hacer un mapeo entre los grupos del sistema de administración centralizado con los grupos del directorio activo.<br>El sistema podrá auditar al menos las siguientes acciones: inicios de sesión en el sistema, cambio de perfiles o roles de usuarios del sistema, cambio de contraseñas, desinstalación de los agentes por eliminación, cambios en las políticas de configuración de los productos administrados, agregar o borrar componentes del directorio, renombrar componentes del directorio.<br>Debe permitir que las computadoras sean administradas e identificadas por el nombre o por la dirección física de la tarjeta (MAC address).<br>En el caso de computadoras que tienen más de una dirección física (MAC) - una portátil con una "dock station" por ejemplo- el sistema debe ser capaz de identificar que se trata del mismo sistema, y tratarlo como uno solo, sin duplicar la información.<br>El sistema contará con un mecanismo para detectar máquinas que están conectadas a la red, y determinar si estas |

| | |
|---|---|
| | computadoras ya son administradas por el sistema central de administración del antivirus. Como acciones ante computadoras no administradas se les puede enviar la instalación del agente de administración y con ello el antivirus o enviar notificaciones al (los) administrador(es). Deberá contar también con reportes específicos de este componente.<br>El sistema enviará notificaciones de eventos que sucedan en sus componentes. Las notificaciones serán en base a reglas definidas por el administrador. Estas reglas utilizarán al menos los siguientes parámetros:<br>Nivel del directorio. Se podrá determinar a que nivel del directorio aplicará cada regla. Por ejemplo enviar una notificación únicamente si se detecta un virus en el grupo "dirección general".<br>Sistema Operativo.<br>Producto. Por ejemplo un evento en el servidor de administración o en algún cliente.<br>Tipo de evento. Puede ser una detección de virus, una actualización, etc.<br>Tipo de notificación. Correo electrónico, SNMP, etc.<br>El sistema de administración debe soportar Microsoft Clustering Services para alta disponibilidad<br>El sistema de administración permitirá controlar las actualizaciones para maximizar la protección y minimizar el tráfico en la red. Se pueden configurar tareas de actualización por separado, para actualizar clientes con cualquier combinación de firmas de antivirus, motores y paquetes de actualización de productos en el repositorio. |
| | **Protección de Intrusos y Firewall:** 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<br>La solución de IPS de sistema debe ser un programa que se instala en la computadora y protege al mismo sistema.<br>Debe contar con al menos los siguientes componentes:<br>Prevención de intrusos (IPS)<br>Firewall<br>Bloqueo de aplicaciones<br>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:<br>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.<br>Detección por firma 2. Las firmas deben estar diseñadas para aplicaciones y sistemas operativos específicos. |

| | |
|---|---|
| | Detección por comportamiento. Este método se basa en el comportamiento de las aplicaciones para detectar actividad maliciosa, esto permitirá detener ataques aún cuando no existe una firma específica, ataques día-cero.<br>El IPS creará eventos en la consola central cuando detenga un ataque, en base a esta información el administrador podrá crear excepciones, que evitarán la aplicación de la regla cuando se cumplan los criterios de la excepción.<br>También permitirá al administrador, en base esta información de los eventos, crear una lista de aplicaciones seguras, a las que no se le aplicarán las reglas de IPS.<br>El componente Firewall debe funcionar como filtro entre la computadora y la red donde está conectada.<br>El firewall debe utilizar al menos criterios como la dirección IP, puerto TCP o UDP y tipo de paquete para aplicar los criterios de bloquear y dejar pasar. Estos criterios deben aplicarse para tráfico entrante y saliente.<br>El firewall debe usar tecnología de “Stateful packet filtering” y “stateful packet inspection”.<br>El firewall debe permitir poner las máquinas en cuarentena, donde esta cuarentena permitirá la comunicación con otros puntos de la red, con tantas restricciones como la política determinada por el administrador lo especifique.<br>El firewall podrá aplicar una política diferente, dependiendo en donde se encuentre conectada la computadora. Por ejemplo si la máquina de un usuario móvil está conectada a la red de la organización usará una política diferente a si está conectada a una red pública. El software será capaz de determinar cuando la máquina está conectada en diferentes redes.<br>Para la creación de las reglas del firewall se deben basar, al menos, en los siguientes criterios.<br>Tipo de conexión (red o inalámbrica).<br>Protocolos IP y ni IP.<br>Tráfico de entrada o salida o los dos.<br>La aplicación que generó el tráfico.<br>El puerto o servicio usado por la computadora, ya sea como receptor u origen.<br>El puerto o servicio usado por la computadora remota, ya sea como receptor u origen.<br>Dirección IP del origen o el receptor<br>El momento del día o la semana en que el paquete fue enviado o recibido.<br>El componente de bloqueo de aplicaciones monitorea las aplicaciones que se están ejecutando y las bloque o las permite.<br>El administrador podrá crear las reglas que permitirán o evitarán la ejecución de las aplicaciones en las máquinas cliente.<br>El bloqueo de aplicaciones también permitirá detener aplicaciones que tratan de ligarse con otros procesos para |

| | |
|---|---|
| | ejecutarse, cuando estas aplicaciones son programas maliciosos.<br>El administrador podrá determinar si se aplican los dos tipos de bloqueo, el de ejecución y el de ligado de aplicaciones, o los dos. |
| | **Protección de Antivirus para Servidores Exchange:**<br>Protección antivirus y control de contenido para servidores Microsoft Exchange<br>El sistema proporcionará una solución antivirus y de control de contenidos para servidores de correo electrónico Miscrosoft Exchange, con las siguientes características<br>Debe integrarse con el sistema de administración de las otras soluciones, para su administración y reporteo de eventos.<br>Capacidad de manejar el análisis o escaneo en tiempo real de los correos. Puede analizar correos o archivos cuando el usuario o sistema los lee o escribe.<br>Capacidad de llevar acabo análisis bajo demanda de forma manual o planificada para que se analicen todos los buzones, carpetas y bases de datos por virus o contenido no deseado.<br>Capacidad para analizar en busca de virus dentro de todos los diferentes tipos archivos comprimidos como .zip, rar, etc.<br>Capacidad para bloquear o detener correos con contenido inapropiado como palabra o frases, asunto y cuerpo del mensaje.<br>La tecnología permitirá descargar las actualizaciones de definición (DAT) y de motor de forma manual o planificada.<br>Capacidad de crear políticas globales o por grupos los cuales se pueden importar de un directorio LDAP o creados manualmente<br>Capacidad de especificar los nombres, tipos y tamaños de archivos que se deben bloquear mediante reglas de filtrado de archivos.<br>Capaz de detectar y eliminar archivos de broma y sospechosos como utilidades de acceso remoto, decodificadores de contraseña, etc.<br>Capaz de detener o eliminar los archivos adjuntos dañados, corruptos o de cero bytes.<br>Capaz de manejar una cuarentena, sí se desea aislar o poner en cuarentena archivos infectados o sospechosos infectados.<br>Capaz de detectar virus conocidos y desconocidos a través de comportamiento o patrones similares a los de un virus en todos los archivos.<br>Capacidad de manejar varios tipos de alertas para la notificación de eventos como infecciones. Capaz de enviar mensajes SNMP, Email, pager, etc.<br>Detectar y reaccionar ante los brotes de virus. Debe ofrecer protección basada en una selección de reglas predefinidas y especificadas por el administrador para evitar una propagación mayor, por ejemplo, dejar de mandar correo si se detectan |

**CONTINUACION PARTIDA N° 2**

| | |
|---|---|
| | 10000 correos infectados por el mismo virus en X segundos.<br>Capaz de permitir o denegar el acceso a los correos o archivos cifrados y de eliminar o romper las firmas digitales.<br>Capacidad para crear registros, incluyendo con reportes gráficos (A través de ePO) para diagnóstico de posibles fallas y análisis de eventos.<br>El sistema antivirus del correo electrónico debe contar con un motor de detección de SPAM, que cuente, al menos, con las siguientes características:<br>Capacidad de analizar todos los correos entrantes y salientes en tiempo real por contenido SPAM o no deseado.<br>El sistema asignará una calificación a los correos para determinar el nivel de certeza de que es spam, así, una calificación más alta asegura que el contenido del correo es más seguro de ser SPAM.<br>En base a las calificaciones permitirá asignar diferentes acciones para diferentes calificaciones de SPAM.<br>Las acciones deben incluir, al menos: bloquear, poner en cuarentena o marcar el asunto de correo con una frase alusiva al SPAM ("posible spam" por ejemplo), así como las correspondientes a notificaciones a destinatario, remitente o administrador.<br>Capacidad de crear listas negras/blancas generales para el bloqueo de dominio, email, palabras, etc.<br>Capacidad de crear listas negras/blancas individuales por el usuario del correo.<br>Debe contar un grupo de reglas predeterminadas para identificar el SPAM, estas reglas se actualizarán y ajustarán constantemente.<br>Capacidad de reenviar los correos basura (SPAM) a una carpeta creada por el mismo Spamkiller en el buzón de los usuarios o en un buzón o carpeta basura (JUNK) del sistema de correo.<br>Capaz de analizar los correos y sus adjuntos en busca de contenido no deseado. Se pueden crear reglas que establezcan que palabras o frases no están permitidas en ningún mensaje o adjunto. |
| | El proveedor debe presentar carta de fabricante que es distribuidor autorizado de la solución propuesta. Documentación comprobatoria vigente (ejercicio 2008). |
| | El proveedor deberá presentar certificados de su personal que avalen que tienen conocimiento de la suite propuesta al congreso, la falta de esta información será causante de descalificación. |
| ***Servicios*** | |
| | ***Incluirá los siguientes servicios:*** |
| 1 | Soporte telefónico ilimitado 24X7 para recibir ayuda respecto a la instalación configuración y funcionalidad de los productos. |

**CONTINUACION PARTIDA N° 2**

| | |
|---|---|
| 2 | Capacitación necesaria para la administración y manejo de la solución completa, curso de por lo menos 16 hrs. Deberá anexar material informativo sobre el curso en el idioma español y contenido del mismo para ser evaluado. El no presentar el presente documento será motivo de descalificación del licitante. |
| 3 | Servicios de actualización con acceso desde Internet a:<br>a) soluciones técnicas desde la base de conocimientos técnicos.<br>b) documentación técnica como guías, FAQ's y release notes.<br>c) envío de incidentes de manera electrónica.<br>d) Mejoras al software que incluyen updates y upgrades de documentación y SW. |
| 4 | Incluye el servicio de soporte y actualización del producto durante la duración del mismo, sobre cualquier nueva versión, actualización o mejora que realice el fabricante en cualquier producto de la suite. |
| 5 | Instalación, configuración, implementación y puesta a punto en sitio por personal certificado técnicamente por la marca del software, además de contar con al menos 3 ingenieros certificados durante la duración del servicio, mismos que deberán realizar las revisiones pertinentes a fin de garantizar el desempeño al 100% del software. |

**ANEXO TÉCNICO**

| PARTIDA | CANTIDAD | U.M. | DESCRIPCIÓN |
|---|---|---|---|
| **3** | 1 | Adquisición de Licencia Corporativa para 101 computadoras | SOLUCIÓN DE CIFRADO DE ALTA SEGURIDAD, AUTENTICACIÓN, PREVENCIÓN DE PÉRDIDA DE DATOS Y CONTROLES DE SEGURIDAD POR POLÍTICAS PARA EVITAR EL ACCESO Y LA TRANSFERENCIA ILEGAL DE INFORMACIÓN CONFIDENCIAL |

| Características Requeridas | Especificaciones Requeridas |
|---|---|
| **Producto** | **La solución debe tener soporte nativo para las plataformas de Microsoft Windows NT4, 2000 y 2003 Server**<br>**La solución deberá soportar nativamente plataformas de Microsoft Windows XP, 2000, 2003, Vista 32/64 bits.**<br>**La solución debe soportar plataformas móviles.**<br>**La solución deberá soportar la integración con Microsoft Active Directory**<br>La solución protegida deberá trabajar con múltiples árboles de dominio de Microsoft Active Directory.<br>La solución deberá soportar y se debe integrar con otros tipos de servicios y directorio de Microsoft Active Directory.<br>La solución debe estar diseñada para trabajar con diferentes tipos de servicio de directorio.<br>La solución soportará y facilitará la integración con procesos ya existentes y provee mecanismos de automatización.<br>La solución de administración permitirá el login de varios administradores y permite definir diferentes niveles de esos administradores.<br>La instalación de la solución podrá ser a través de la red.<br>La solución deberá controlar los archivos o las carpetas que serán cifrados. Debe permitir a los administradores especificar que el contenido de ciertas carpetas, archivos creados por determinadas aplicaciones o archivos de un cierto tipo sean cifrados. Además, grupos de usuarios reciben derechos de acceso a ciertos archivos y carpetas, pudiendo compartirlos con Seguridad en toda la red.<br>Debe contar con tecnología de encriptación persistente para que los datos sigan cifrados dondequiera se guarden o se transfieran. Si un usuario no autorizado intenta guardar un archivo en un dispositivo de almacenamiento no aprobado, ese documento deberá quedar cifrado e ilegible.<br>Confirmación del usuario y del equipo antes de la inicialización de la PC, a través de autenticación bifactorial y por contraseña<br>Protección con cifrado líder de mercado, utilizando los algoritmos AES-256 y RC5-1024<br>Cifrado imperceptible de dispositivos, sin ningún impacto sobre las actividades diarias y que interfiera a los usuarios finales<br>Seguimiento retrospectivo completo, eximiendo la divulgación obligatoria en caso de pérdida de una portátil o de un dispositivo USB |

| | |
|---|---|
| | Creación y fiscalización de políticas obligatorias de seguridad Deberá utilizar FIPS 140-2 y la certificación Common Criteria EAL4 Deberá sincronizarse e integrarse con Active Directory, Novell, LDAP y PKI<br>Requisito de sistema<br>Desktop, laptop y tablet<br>Sistemas operativos<br>• Microsoft Vista (todas las versiones de 32 y 64 bits)<br>• Microsoft Windows XP<br>• Microsoft Windows 2000<br>• Microsoft Windows Server 2003<br>Hardware<br>• CPU: compatible con Pentium<br>• RAM: mínimo de 128 MB<br>• Espacio en disco: 5–35 MB disponibles, dependiendo de la ubicación y del número de dispositivos<br>• Conexión de red: TCP/IP para acceso remoto<br>Terminales móviles<br>Sistemas operativos<br>• Microsoft Windows Mobile 6.0 for Smartphone<br>• Microsoft Windows Mobile 6.0 for PDA<br>• Microsoft Windows Mobile 5,0 for Smartphone<br>• Microsoft Windows Mobile 5.0 for Pocket PC<br>Hardware<br>• CPU: mínimo de 195 MHz<br>• RAM: mínimo de 64 MB<br>• Conexión de red: TCP/IP para administración remota y Activesync 4.5 o superior para instalación/actualizaciones de políticas por la red interna<br>Administración centralizada<br>Sistemas operativos<br>• Microsoft Windows 2000<br>• Microsoft Windows XP<br>• Microsoft Windows Server 2003<br>Hardware<br>• RAM: 128 MB (512 MB recomendado)<br>• Espacio en disco: 200 MB<br>• CPU: compatible con Pentium<br>La solución deberá contar con una herramienta que controle la |

| | |
|---|---|
| | transferencia de datos en la red y de cualquier dispositivo y que controle el modo con el cual los usuarios acceden, imprimen y envían datos confidenciales por la red y dispositivos de entrada/salida; y también la transferencia de datos confidenciales por e-mail, webmail, aplicaciones P2P, IM, Skype, HTTP, HTTPS, FTP, Wi-Fi, USB, CD, DVD, impresoras, fax y almacenamiento removible.<br>Deberá monitorear (permitir la transferencia de datos)<br>Deberá impedir (bloquear la transferencia de datos)<br>Deberá colocar en cuarentena (aguardar autorización)<br>Deberá criptografiar (garantizar la criptografía antes de transferir los datos)<br>Deberá alertar (notificar a los administradores y usuarios finales)<br>La solución deberá controlar y bloquear los datos confidenciales copiados en dispositivos USB, unidades flash, iPod y otros dispositivos de almacenamiento removibles<br>Deberá especificar y clasificar los dispositivos que pueden ser usados con base en Windows®, tales como ID del producto y del proveedor, clase y nombres de dispositivos, números de serie y otros.<br>Dar acceso a las políticas centralizadas y al monitoreo de eventos con la consola de administración de la solución de antivirus solicitada en la partida 1 y 2 la integración con la consola de administración deberá permitir una administración avanzada por la Web y ofrecer recursos de emisión de informes/auditoria. |
| | El proveedor debe presentar carta de fabricante que es distribuidor autorizado de la solución propuesta. Documentación comprobatoria vigente (ejercicio 2008). |
| | El proveedor deberá presentar certificados de su personal que avalen que tienen conocimiento de la suite propuesta al congreso, la falta de esta información será causante de descalificación. |
| ***Servicios*** | |
| | *Incluirá los siguientes servicios:* |
| 1 | Soporte telefónico ilimitado 24X7 para recibir ayuda respecto a la instalación configuración y funcionalidad de los productos. |
| 2 | Capacitación necesaria para la administración y manejo de la solución completa, curso de por lo menos 16 hrs. Deberá anexar material informativo sobre el curso en el idioma español y contenido del mismo para ser evaluado. El no presentar el presente documento será motivo de descalificación del licitante. |
| 3 | Servicios de actualización con acceso desde Internet a:<br>a) soluciones técnicas desde la base de conocimientos técnicos.<br>b) documentación técnica como guías, FAQ's y release notes.<br>c) envío de incidentes de manera electrónica.<br>d) Mejoras al software que incluyen updates y upgrades de documentación y SW. |

| | |
|---|---|
| 4 | Incluye el servicio de soporte y actualización del producto durante la duración del mismo, sobre cualquier nueva versión, actualización o mejora que realice el fabricante en cualquier producto de la suite. |
| 5 | Instalación, configuración, implementación y puesta a punto en sitio por personal certificado técnicamente por la marca del software, además de contar con al menos 3 ingenieros certificados, mismo que deberá realizar las revisiones pertinentes a fin de garantizar el desempeño al 100% del software. |