**Acta de Presentación de Proposiciones Técnicas y Económicas y Apertura de Proposiciones de la Licitación Pública Nacional 00011001-021/08**

En la Ciudad de México, Distrito Federal, siendo las **12:00** horas del día **18 de julio del 2008**, en la sala de juntas de la Dirección de Adquisiciones de la Secretaría de Educación Pública, ubicada en el 2º. Piso de la Avenida Arcos de Belén No. 79, Colonia Centro, se llevó a cabo el **Acto de Presentación de Proposiciones Técnicas y Económicas y Apertura de Proposiciones de la Licitación Pública Nacional N° 00011001-021/08,** para la **Contratación Plurianual de los Servicios de Seguridad Perimetral y Antivirus,** en cumplimiento en lo dispuesto por los artículos 34 y 35 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

Los nombres, cargos y firmas de los servidores públicos que asistieron a este acto son los que se señalan a continuación:

**"Por la Secretaría"**

| Nombre | Cargo |
|---|---|
| LIC. IVAN ORLANDO PAREDES ESPINOZA | DIRECTOR DE ADQUISICIONES. |
| ING. RADAMÉS HERNÁNDEZ ALEMÁN | REPRESENTANTE DE LA DIRECCIÓN GENERAL DE TECNOLOGÍA DE LA INFORMACIÓN. |
| ING. LUIS JORGE TEJADA FIGUEROA | REPRESENTANTE DE LA DIRECCIÓN GENERAL DE TECNOLOGÍA DE LA INFORMACIÓN. |
| ING. J. CARLOS CASTRO ESPINOSA | REPRESENTANTE DE LA DIRECCIÓN GENERAL DE TECNOLOGÍA DE LA INFORMACIÓN. |
| LIC. GLORIA LILIANA LUNA FANDIÑO | REPRESENTANTE DE LA DIRECCIÓN GENERAL DE TECNOLOGÍA DE LA INFORMACIÓN. |
| NO SE PRESENTO. | REPRESENTANTE DEL ÓRGANO INTERNO DE CONTROL EN LA SECRETARÍA DE EDUCACIÓN PÚBLICA.. |
| NO SE PRESENTO. | REPRESENTANTE DE LA DIRECCIÓN GENERAL DE ASUNTOS JURÍDICOS. |

---

Asimismo, se contó con la participación de los licitantes cuyas razones sociales se señalan a continuación:

**Por las Empresas:**

| | NOMBRE | RAZÓN SOCIAL |
|---|---|---|
| 1 | FELIPE MENDOZA MENDOZA | INFORMÁTICA INTEGRAL ADMINISTRATIVA, S.A. DE C.V. EN CONSORCIO CON LA EMPRESA SECURITY |

| | NOMBRE | RAZÓN SOCIAL |
|---|---|---|
| | | ONE, S.A. DE C.V. |
| 2 | CESAR VALLARTA LEÓN | ARRENDAMIENTOS Y SERVICIOS EN COMPUTACIÓN, S.A. DE C.V. |
| 3 | CARLOS BORIS PASTRANA POLO | SCITUM, S.A. DE C.V. |
| 4 | JUAN MANUEL PEÑA ZAVALA | INTERNET ENGINE, S.A. DE C.V. |
| 5 | EDGAR MORALES SARDANETA | ONLINET, S.A. DE C.V. |
| 6 | FABIOLA MOCTEZUMA GASCA | DESARROLLOS DE TI, S.A. DE C.V. |
| 7 | JUAN ESCAREÑO FERNÁNDEZ | INFORMÁTICA EMPRESARIAL INTEGRADA, S.A. DE C.V. EN CONSORCIO CON LA EMPRESA DISEÑO DE SOLUCIONES EN ALTA SEGURIDAD INFORMÁTICA, S.A. DE C.V. |
| 8 | CARLOS ACUÑA Z. | GRUPO DE TECNOLOGÍA CIBERNÉTICA, S.A. DE C.V. EN CONSORCIO CON LA EMPRESA GRUPO ESTRATEGICO PARA TELECOMUNICACIONES, S.A. DE C.V. |

El Licenciado Iván Orlando Paredes Espinoza, Director de Adquisiciones, en nombre de la Secretaría de Educación Pública, agradeció la presencia de los participantes dando inicio al acto, presentando a los integrantes del presidium y comentó que el registro de licitantes se cerró a las **12:00** horas en punto. Señaló que el incumplimiento de cualquiera de los requisitos solicitados en las bases y su anexo sería motivo de descalificación acorde a lo previsto por el Artículo 35 Fracción I de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público y el numeral 10.1.1 de las bases concúrsales.

El Lic. Iván Orlando Paredes Espinoza, en nombre de la Secretaría de Educación Pública, preguntó si entre los asistentes al evento se cuenta con la presencia de representantes de alguna Cámara de Comercio ó de algún Organismo no Gubernamental sin que alguien contestara afirmativamente.

**Asimismo se informó que no se recibieron propuestas a través de medios remotos de comunicación electrónica (Compranet)**

Acto seguido, se procedió a la recepción de los sobres que contienen las proposiciones técnicas y económicas de los licitantes mismas que fueron abiertas en presencia de los asistentes.

Una vez abiertos los sobres que contienen las ofertas y en cumplimiento al Artículo 35 fracción III de la Ley se revisó y constató que las proposiciones presentadas contuvieran de manera cuantitativa la documentación legal, administrativa, técnica y económica solicitada en bases.

De igual forma, se informa a los licitantes participantes que de conformidad con lo establecido en el artículo 39 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, se integra a la presente acta como anexo 1, copia de las propuestas económicas presentadas por cada uno de los licitantes.

Después de la revisión aludida se informó a los licitantes que sus propuestas serán analizadas cualitativamente tanto en el aspecto legal, administrativo y técnico de acuerdo a lo señalado en la fracción lV del artículo 35 de la citada Ley.

**Acta de Presentación de Proposiciones Técnicas y Económicas y Apertura de Proposiciones de la Licitación Pública Nacional 00011001-021/08**

Con base en el artículo 35 fracción II de la Ley en la materia en este acto se firmaron todas y cada una de las hojas que conforman el apartado de las proposiciones técnicas y económicas tanto por los servidores públicos asistentes, así mismo se formo una comisión de tres de los representantes de las empresas participantes que a continuación se enlistan.

| | NOMBRE | RAZÓN SOCIAL |
|---|---|---|
| 1 | FELIPE MENDOZA MENDOZA | INFORMÁTICA INTEGRAL ADMINISTRATIVA, S.A. DE C.V. |
| 2 | CESAR VALLARTA LEÓN | ARRENDAMIENTOS Y SERVICIOS EN COMPUTACIÓN, S.A. DE C.V. |
| 3 | CARLOS BORIS PASTRANA POLO | SCITUM, S.A. DE C.V. |

Por último, se informa, que el fallo se llevará a cabo el **23 de julio de 2008 a las 17:00 horas** en la sala de juntas de la Dirección de Adquisiciones, sita en la Av. Arcos de Belén N°. 79, Esq. Av. Balderas, piso 2° colonia Centro, recomendándoles su puntual asistencia.

Copia de esta acta será fijada en el estrado de la Dirección de Adquisiciones ubicado en el 4º piso de Arcos de Belén No. 79, Colonia Centro, Delegación Cuauhtémoc, por un término no menor de cinco días hábiles, siendo de la exclusiva responsabilidad de los licitantes acudir a enterarse de su contenido y obtener, en su caso, copia de la misma. Dicho procedimiento sustituye a la notificación personal.

No habiendo otro asunto que tratar, se cierra la presente acta siendo las **15:30** horas del mismo día en que se dio inicio, firmando al margen y al calce todos los que en ésta participaron.

**“Por la Secretaría”**

| Nombre | Firma |
|---|---|
| **LIC. IVAN ORLANDO PAREDES ESPINOZA** | |
| **ING. RADAMÉS HERNÁNDEZ ALEMÁN** | |
| **LIC. GLORIA LILIANA LUNA FANDIÑO** | |

| Nombre | Firma |
|---|---|
| **ING. LUÍS JORGE TEJADA FIGUEROA** | |
| **ING. J. CARLOS CASTRO ESPINOSA** | |

**“Por las Empresas”:**

| NOMBRE Y RAZÓN SOCIAL | FIRMA |
|---|---|
| FELIPE MENDOZA MENDOZA | |
| CESAR VALLARTA LEÓN | |
| CARLOS BORIS PASTRANA POLO | |
| JUAN MANUEL PEÑA ZAVALA | |
| EDGAR MORALES SARDANETA | |
| FABIOLA MOCTEZUMA GASCA | |
| JUAN ESCAREÑO FERNÁNDEZ | |
| CARLOS ACUÑA Z. | |

---
---

**División del Norte No. 525 Desp. 301**
**Col. del Valle, México D.F. C.P. 03100**
**Tels. 5682-8702, 5682-8714 y 55439173**

0125

informática integral administrativa s.a de c.v

México D.F. a 18 de Julio de 2008

Licitación Pública Nacional No. 00011001-021/08
Para la contratación Plurianual de los Servicios de Seguridad Perimetral y Antivirus

Secretaría de Educación Pública
Oficialia Mayor
Dirección General de Recursos Materiales y Servicios
Dirección de Adquisiciones

Presente

Anexo 9 Propuesta Económica

| | DIA | MES | AÑO |
|---|---|---|---|
| FECHA | 18 | Julio | 2008 |

NOMBRE DEL LICITANTE: Informática Integral Administrativa S.A. de C.V. R.F.C IIA-990408-553
DOMICILIO: División del Norte No. 525 Despacho 301 Col. Del Valle Del. Benito Juárez CP. 03100

| TELEFONO | FAX | CORREO ELECTRÓNICO | NÚMERO DE RECIBO DE COMPRA DE BASES. |
|---|---|---|---|
| 5682-8702 | 5543-9173 | Felipe.mendoza@iia.com.mx | 154906 |

LOS SERVICIOS PROPUESTOS, SE APEGAN JUSTA, EXACTA Y CABALMENTE A LO SOLICITADO POR LA CONVOCANTE EN EL ANEXO 1 (UNO), DE LAS BASES DE LA LICITACIÓN PÚBLICA NACIONAL NÚMERO 00011001-021/08

| CONCEPTO | Costo mensual | 2008 (4 meses) | 2009 (12 meses) | 2010 (12 meses) |
|---|---|---|---|---|
| SERVICIO DE SEGURIDAD PERIMETRAL Y ANTIVIRUS | $ 993,967.00 | $ 3,975,868.00 | $ 11,927,604.00 | $ 11,927,604.00 |

| | | |
|---|---|---|
| TOTAL DEL SERVICIO | SUBTOTAL: | $ 27,831,076.00 |
| | IVA.: | $ 4,174,661.40 |
| | GRAN TOTAL: | $ 32,005,737.40 |

TOTAL EN LETRA. TREINTA Y DOS MILLONES CINCO MIL SETECIENTOS TREINTA Y SIETE PESOS 40/100 MN.

EN EL CASO QUE LA SECRETARÍA DE EDUCACIÓN PÚBLICA, ME OTORGUE LA ADJUDICACIÓN DEL CONTRATO, ME OBLIGO EN NOMBRE DE MÍ REPRESENTADA A SUSCRIBIR EL CONTRATO QUE SE DERIVE, EN LOS TÉRMINOS, CONDICIONES Y PORCENTAJE ESTABLECIDOS EN ESTAS BASES.

- PRECIOS FIJOS A PARTIR DE LA PRESENTACIÓN DE PROPOSICIONES TÉCNICAS Y ECONÓMICAS HASTA LA CONCLUSIÓN DE LA VIGENCIA DEL CONTRATO
- PRECIOS EXPRESADOS EN MONEDA NACIONAL.

Atentamente.

Felipe Mendoza Mendoza
Representante Legal

División del Norte No. 525 Desp. 301
Col. del Valle, México D.F. C.P. 03100
Tels. 5682-8702, 5682-8714 y 55439173

0124

informática integral administrativa s.a de c.v

México D.F. a 18 de Julio de 2008

Licitación Pública Nacional No. 00011001-021/08
Para la contratación Plurianual de los Servicios de Seguridad Perimetral y Antivirus

Secretaría de Educación Pública
Oficialia Mayor
Dirección General de Recursos Materiales y Servicios
Dirección de Adquisiciones

Propuesta Económica

Atentamente

Felipe Mendoza Mendoza
Representante Legal
Informática Integral Administrativa S.A. de C.V.

ASECO

ARRENDAMIENTOS Y SERVICIO EN COMPUTACION S.A DE C.V.

LICITACIÓN PÚBLICA NACIONAL NÚMERO 00011001-021/08.
**PARA LA CONTRATACIÓN PLURIANUAL DE LOS SERVICIOS DE SEGURIDAD PERIMETRAL Y ANTIVIRUS**

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

**ANEXO 9**

**FORMATO DE PROPUESTA ECONOMICA.**

| | DIA | MES | AÑO |
|---|---|---|---|
| FECHA | 18 | 07 | 2008 |

NOMBRE DEL LICITANTE: ARRENDAMIENTOS Y SERVICIO EN COMPUTACION, S.A. DE C.V.___ R.F.C: ASC930629 2X8
DOMICILIO: LEONOR 370 PB, DEPTO 2, COL. NATIVITAS
C.P. 03500, MEXICO, D.F.

| **TELEFONO** | **FAX** | **CORREO ELECTRÓNICO** | **NÚMERO DE RECIBO DE COMPRA DE BASES.** |
|---|---|---|---|
| 56986930 | 56987741 | dhernandez@aseco.com.mx | |

LOS SERVICIOS PROPUESTOS, SE APEGAN JUSTA, EXACTA Y CABALMENTE A LO SOLICITADO POR LA CONVOCANTE EN EL ANEXO 1 (UNO), DE LAS BASES DE LA LICITACIÓN PÚBLICA NACIONAL NÚMERO: 00011001-021-08

| CONCEPTO | Costo mensual | 2008 (4 meses) | 2009 (12 meses) | 2010 (12 meses) |
|---|---|---|---|---|
| A nombre de mi representada arrendamientos y Servicio en Computación, S.A. de C.V. damos a continuación, en detalle nuestra PROPUESTA ECONOMICA mediante la cual describimos los servicios que proporcionaremos si nos es adjudicado el contrato plurianual de los servicios de seguridad perimetral y antivirus.<br><br>**Servicios de Seguridad Perimetral y Antivirus**<br><br>Entregaremos una solución de seguridad integral basada en software/hardware nuevo, para proteger el perímetro de la red de datos de la Secretaría, la cual cumple como mínimo con los siguientes puntos.<br><br>➢ Se encontrara en un sitio centralizado, y protegera la confidencialidad de la información que circule a través de la red de la SEP hacia el Internet público y viceversa.<br><br>➢ Contempla una solución de seguridad robusta y redundante en los firewall para el acceso corporativo hacia Internet.<br><br>➢ Consideramos la administración de la solución de seguridad que proporcionaremos, y adicionalmente asignaremos en las instalaciones de la Secretaría de Educación Pública (en la ciudad de México) nuestro personal técnico en sitio, que se encargara del aseguramiento de las funcionalidades requeridas por la Secretaría. Proporcionaremos al menos dos ingenieros en sitio en horario de 9:00 a 18:00 hrs. de lunes a viernes, contaran con la capacidad necesaria para poder administrar, operar y dar el soporte técnico necesario en la solución robusta de seguridad perimetral y antivirus, acorde a las necesidades de la Secretaria, así como el personal adicional que consideremos sea necesario para cumplir con los niveles de servicio establecidos en el presente Anexo. De acuerdo a lo establecido en la junta de aclaraciones, la convocante proporcionara el lugar de trabajo (escritorio, acceso a internet, extensión telefónica con acceso a la red pública telefónica) en sus instalaciones para que nuestros ingenieros realicen sus labores en sitio. | $1,039,000.00 | $4,156,000.00 | $12,468,000.00 | $12,468,000.00 |

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

- Proporcionaremos la seguridad en apego a los niveles de servicio requerido por la Secretaría, mismo que se detallan en la presente propuesta técnica.
- Incluiremos todo el hardware y/o software necesarios para proporcionar al menos las siguientes funcionalidades:

1. Firewall en alta disponibilidad (soporta al menos 15,000 usuarios concurrentes). El Firewall esta dimensionado para los usuarios internos y tiene la capacidad de soportar el trafico de los usuarios externos.
2. Sistema de Prevención de intrusos (IPS) (aseguramiento de los servicios publicados por la Secretaría y red interna Institucional), así como cada una de las zonas declaradas en los firewalls.
3. Control de accesos a páginas Web (licencias para al menos 15,000 usuarios)
4. Seguridad de Correo Electrónico con antispam y antivirus (soporte 15,000 usuarios)
5. Antivirus para computadoras personales incluyendo los servicios de consolas de administración centrales (soporte 15,000 usuarios)
6. Equipo para la conectividad para la segmentación de las zonas.
7. Centro de operación de seguridad (SOC)

**LOTE 1 Firewall en alta disponibilidad**

Nuestra solución incluye todo el hardware y/o software necesario para prestación de los servicios, el cual cumple con las siguientes características y funcionalidades:

Firewall en alta disponibilidad, 2 Equipos Marca **Juniper**, Modelo **NS5400** con las siguientes características:

- ✓ Traducción de Direcciones (NAT).
- ✓ Cada característica de las herramientas de administración y configuración cuenta con interfaz gráfica (GUI).
- ✓ Configuración y administración remota por consola usando conexiones cifradas y métodos de autenticación. Capacidad de administración de varios firewalls a través de una misma consola.
- ✓ Generación de Bitácoras y reportes, registro de eventos históricos, capacidad de generar gráficos y emitir reportes orientados a diferentes perfiles (técnicos, ejecutivos). Será nuestra responsabilidad la generación de las bitácoras así como los reportes, en caso de resultar adjudicados.
- ✓ Mecanismos de alarmas y avisos, ante eventos inesperados.
- ✓ Incluye una consola central con capacidad de configurar los niveles de alerta. Capacidad de notificación en tiempo real vía SNMP (Simple Network

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

| | | | |
|---|---|---|---|
| Management Protocol), disparo de actividades.<br>✓ Implementa restricciones por dirección IP o grupos de direcciones IP.<br>✓ Capacidad de soportar hasta 15,000 usuarios activos concurrentes.<br>✓ Proporcionamos una solución de Firewall con la capacidad de desempeño de 5 Gbps, con capacidad de por lo menos 40,000 nuevas sesiones por segundo o de 20,000 nuevas sesiones con 1'500,000 sesiones concurrentes.<br>✓ Monitoreo del estado de seguridad que guarda la operación. presentando gráficamente alarmas, bitácoras e información que sirva al administrador para conocer el detalle de las políticas de seguridad implementadas.<br>✓ Cuenta con la capacidad de controlar el acceso a servicios en dispositivos conectados al firewall.<br>✓ Genera y administra remotamente las políticas de seguridad.<br>✓ Cuenta con Integración con servicios de directorio LDAP.<br>✓ Soporta a diversos esquemas de autenticación compatibles con tecnología Radius y/o TACACS.<br>✓ Cuenta con la capacidad de administración de usuarios individuales y por grupo de trabajo.<br>✓ Cuenta con alta disponibilidad (Load Balancing) de manera que se garantice la continuidad de la funcionalidad, (activo-activo).<br>Soportar entre otros los siguientes protocolos:<br>IP<br>ICMP<br>ARP<br>ICMP Router Discovery<br>CIDR<br>Rutas Estáticas<br>RIP<br>RIP versión 2<br>OSPF<br>DVMRP o PIM<br>IGMP<br>Tuneles Multicast<br>IPv6 CORE<br>Differentiated Services<br>Bootp/DHCP Relay<br>Cuenta con las siguientes funcionalidades:<br>I. Administración en Base a Roles con distintos permisos.<br>II. Acceso de Lectura/Escritura y Acceso de solo lectura propietarios o de terceros.<br>III. Lista de Control de Accesos.<br>IV. SSH (Secure Telnet y FTP)<br>V. Administración de Tráfico. | | | 0471 |

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

VI. Capacidad de realizar la tarea de Firewall, VPN y QoS.

VII. Administración y monitoreo centralizado de políticas de firewall, VPN (IPSec y SSL) y QoS, en una consola de administración central, donde los cambios pueden ser empujados a todos los puntos de la red.

VIII. Capacidad de revisión de bitácoras en tiempo real.

IX. El sistema de firewall en HA cuenta con las siguientes certificaciones:

**Certificación ICSA para el FireWall.**

**Certificación de Common Criteria EAL4 o superior para el FireWall.**

Tiene la capacidad de soportar 400 VPN'S IPSec y 200 VPN'S SSL, FireWall y QoS integrados en la misma caja con una misma arquitectura y una consola de administración.

Se incluye el diseño esquemático para los la implementación de los elementos de seguridad. En Anexo en la presente propuesta técnica.

**LOTE 2, SISTEMA DE PREVENCIÓN DE INTRUSOS (IPS),**

Entregaremos una solución de un Sistema de Prevención de Intrusos (IPS) compuesta por 8 equipos Marca **IBM Internet Security Systems**, Modelo **GX5108C**

**2.1 Objetivo general**

Se Implementará una solución de ocho IPS con 500 MBPS de Throughput cada uno, que permiten el desarrollo de un proceso de administración y protección de seguridad perimetral, permitiendo lograr la eficiencia máxima en la detección y prevención de ataques, a través de funcionalidades de detección de anomalías en protocolos de red, minimizando los falsos positivos y falsos negativos en la identificación de ataques, con una administración centralizada contra amenazas conocidas o desconocidas y ataques híbridos.

**2.2 Especificaciones del fabricante de cumplimiento obligatorio**

La solución cumple con las siguientes características:

El fabricante cuenta con un sistema de monitoreo global, que le permite conocer e identificar nuevos ataques, de manera que se pueda disponer de un indicador que demuestre la criticidad de los eventos que están ocurriendo en el mundo vía WEB, mediante X-Force, cuyas características solicitadas se muestran en la siguiente url http://xforce.iss.net/. (Anexamos impresión en nuestra propuesta técnica).

El fabricante cuenta con un grupo de investigación sobre vulnerabilidades y amenazas informáticas, denominado X-Force y cuya liga a sitio fue mostrada en párrafo anterior. **(Anexamos impresión en nuestra propuesta técnica).**

**2.3 Especificaciones técnicas de cumplimiento obligatorio**

La solución implementada cumple con las siguientes especificaciones técnicas:

La solución de prevención de intrusos cuenta con la capacidad incluida e

0472

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

integrada dentro del mismo Appliance para detección y rechazo de ataques conocidos y desconocidos,

La solución de prevención a nivel de hardware cuenta con al menos el reconocimiento NSS Group o ICSA Labs o EAL o Common Criteria, organizaciones que se encargan de la certificación y testeo de productos de seguridad informática.

Para facilidad de administración, el equipo soportar actualización automática de firmas de ataques, con opción a definir configuración de proxy de salida a internet de manera manual y actualización automática de firmas de ataques de manera calendarizada o por fechas definidas.

El sistema proporciona un mecanismo de mantenimiento de la base de datos de eventos y alertas que permite eliminar las alertas y eventos de mayor antigüedad de manera que se evite que el espacio en disco se agote garantizando la continuidad de servicio de la solución. Entendemos que no es necesario conservar los eventos de alerta de mayor antigüedad.

**2.4 Especificaciones para la prevención de intrusiones**

Así mismo cumple con las siguientes especificaciones para la prevención de intrusiones:

Con nuestra solución podemos monitorear el tráfico de red para prevenir ataques, port scanning, ataques de denegación de servicio y tráfico malicioso.

Funcionalidades Básicas:
Solución de software y hardware basado en "appliances", que tiene la capacidad de realizar su monitoreo y prevención de manera en línea además de ser de un sólo fabricante.

El sensor opera en línea sin necesidad de configurar direcciones IPs ni cambiar direccionamiento interno proporcionando un mecanismo de puenteo con base en pares de interfaces para cada segmento de red. Este mecanismo deberá permitir definir una lista de alertas para las cuales el trafico será inspeccionado y prevenido aun cuando el nivel de confianza de la alerta indique que el trafico no debería ser prevenido con el fin de poder definir excepciones a las reglas default.

El dispositivo soporta la identificación y protección de ataques en protocolos de Voice over IP (VoIP), tales como: SIP, MGCP, H.323, H.225, H.245, Q.931 y SCCP.

Implementaremos una solución de ocho IPS físicamente independientes, por cada IPS incluye un total de 5 interfaces, de las cuales:
La solución cuenta con 4 interfaces 10/100/1000 Mbps cobre, Integradas al IPS
La solución cuenta con 1 interfaz 10/100/1000 Mbps para comunicación con el sistema de administración de correlación de eventos, integrada al IPS.
Conforme a junta de aclaraciones en esta licitación no se está solicitando la infraestructura para la correlación de eventos, pero en el futuro existe la posibilidad de integrarlo como un servicio adicional.

Para una mayor eficiencia en la inspección de tráfico, se cuenta con un lenguaje abierto para la afinación de las firmas y poder así eliminar en la medida de lo posible los falsos positivos.

Por seguridad la solución no basa sus funcionalidades de protección únicamente en firmas, sino que proporciona un mecanismo de protección y análisis de tráfico a nivel aplicativo, revisando anomalías de protocolo con mecanismos que permiten identificar el tipo de aplicaciones y tipos de Sistemas operativos de manera pasiva sin tener que utilizar necesariamente un analizador de vulnerabilidades propio o de terceros, éste se encuentra soportado y amparado por el fabricante, con el fin de correlacionar la información identificada y detener

0473

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

| |
|---|
| ataques de manera dinámica como por ejemplo gusanos que pueden cambiar su código dinámicamente y que son difíciles de detener con tecnologías basadas exclusivamente en firmas. El escaneo de vulnerabilidades puede efectuarse de manera independiente al IPS. Como respuesta a la detección de un incidente. |
| La solución proporciona un mecanismo que automáticamente habilita firmas o protecciones para contener ataques que puedan ser explotados en los recursos de la red a partir de la correlación de los resultados de un escaneo de vulnerabilidades. |
| La solución permite en tiempo real, la detección de ataques desconocidos y/o variaciones de ataques conocidos. |
| La solución permite el paso del tráfico en el segmento de red sin afectar el funcionamiento de la red (Fail-Open), en caso de una falla eléctrica. |
| El sistema proporciona un mecanismo para definir reglas de firewall basadas en IP y puerto fuente, IP y puerto destino, tipo de protocolo, registro de log y acción como aceptar o rechazar o bloquear el paquete. |
| Cuenta con herramientas de análisis, el sistema otorga la posibilidad de guardar los paquetes crudos relacionados con alguna alerta desde la misma interfase de administración los cuales pueden ser abiertos de manera automática o manual por algún analizador de tráfico externo |
| El sistema proporciona un mecanismo para definir una lista de equipos clientes cuyo tráfico no será inspeccionado por el sensor y también una lista de servidores hacia los cuales el tráfico no será inspeccionado por el sensor. |
| El sistema realiza acciones a partir de las alertas generadas como bloquear el tráfico, enviar un email al administrador, envía un trap de SNMP a un sistema de gestión externo, envía la alerta a un programa externo, envía la alerta al visor de alertas |
| La solución captura tráfico para el análisis de evidencia. |
| El dispositivo soporta reset de la sesión TCP cuando se utiliza en modo pasivo y/o activo. |
| El sistema neutraliza los paquetes en tiempo real eliminando o neutralizando los paquetes con el código malicioso mientras deja pasar los paquetes legítimos. |
| El sistema soporta revisiones automatizadas de contenido seguridad y actualizaciones de productos a través de Internet. |
| El sistema soporta una consola gráfica local con acceso remoto. |
| El sistema soporta una administración centralizada con consola gráfica. |
| El sistema proporciona un mecanismo para definir una lista de alertas para las cuales el tráfico será inspeccionado y prevenido aún cuando el nivel de confianza de la alerta indique que el tráfico no debería de ser prevenida con el fin de poder definir excepciones a las reglas default. |
| El sistema proporciona un mecanismo para definir cierto tiempo durante el cual una fuente atacante será puesta en cuarentena después de que una alerta haya sido generada por dicha fuente para tráfico TCP. |
| El sistema proporciona un mecanismo que automáticamente habilita firmas o protecciones para contener ataques que puedan ser explotados en los recursos de la red a partir de la correlación de los resultados de un escaneo de vulnerabilidades. |

0474

ASECO

ARRENDAMIENTOS Y SERVICIO EN COMPUTACION S.A DE C.V.

LICITACIÓN PÚBLICA NACIONAL NÚMERO 00011001-021/08.
**PARA LA CONTRATACIÓN PLURIANUAL DE LOS SERVICIOS DE SEGURIDAD PERIMETRAL Y ANTIVIRUS**

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

**LOTE 3 Control de Accesos a páginas Web,**

Control de Acceso a Páginas Marca **IBM Internet Security Systems**, con la solución **Proventia Web Filtering**.

Ofertamos en nuestra solución, el hardware y/o software necesario que cuenta con las siguientes características para el control de acceso a páginas Web:

Control de accesos a páginas Web (licencias para 15,000 usuarios)

Software para controlar, monitorear y filtrar los accesos a sitios o páginas Web en Internet, en el nodo "INTERNET".

Cuenta con administración mediante interfaz gráfica, para cada una de sus facilidades.

Cuenta con la capacidad de generar y administrar políticas de uso, administración de accesos y obtención de reportes detallados de las funcionalidades de control del producto.

La interfaz de generación de reportes permite la programación de múltiples tareas de generación de reportes predeterminados, en horarios y días de la semana predefinidos, y podemos:
• Enviar los reportes generados por correo electrónico hacia los recipientes deseados
• Publicar los reportes generados en una página Web.
• Podrá aplicar las políticas de manera externa siempre y cuando cumpla con todos los requerimientos y especificaciones de este apartado.

Soporta Integración con múltiples firewalls, servidores Proxy, dispositivos cache, entre otros.

Tiene la capacidad de funcionar en stand alone.

Permite el sniffing a través de una única tarjeta de red (la misma tarjeta utilizada para comunicación con la red), bien como por dos o más tarjetas (tarjetas dedicadas a escuchar al tráfico desde múltiples segmentos).

Cuenta con la capacidad de generar una bitácora al entrar a diferentes sitios de internet configurable que puede incluir la información del usuario, los sitios visitados y las violaciones de las políticas de acceso definidas. Los reportes muestran el comportamiento del flujo de la información accedida, así como el tráfico y el número de violaciones por usuario.

La solución tiene la capacidad de controlar el Servicio de mensajería instantánea como Messenger de Hotmail, Messenger de Yahoo, Skype, ICQ, es decir, permite o bloquea el servicio por usuario, grupo de usuarios o a toda la red. Y conforme a junta de aclaraciones esta funcionalidad la cumplimos mediante el servicio de proxy , el cual esta descrito en el lote 4.1 que se describe en nuestra propuesta técnica-

Provee un servicio de actualización automática al menos 3 veces al día de Base de Datos predefinidas sobre sitios de Internet, categorizados para ser filtrados automáticamente y en más de 58 categorías diferentes, con capacidad de recategorizar y permitir el acceso con cuotas de tiempo, o permitir el acceso tras la aceptación de un término de responsabilidad. Se podrán agregar, eliminar, modificar sitios a criterio de los administradores.
La base de datos contiene más de 20 millones de URLs identificados y categorizados al día de hoy en diferentes idiomas. Asimismo, cuenta con funcionalidad de envío automático de URLs desconocidas o no categorizadas a nosotros como fabricante del producto, para su categorización e inclusión dentro

0475

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

| | |
|---|---|
| de la base de datos.<br><br>Sitios de phishing, spyware, adware, key loggers, inclusive aquellos sitios inocentes de otras categorías que hayan sido usados para hospedar phishing; luego de ser descontaminados, deben volver a sus categorías originales.<br><br>Garantizamos que nuevas páginas cuyo contenido represente riesgos a la seguridad sean agregadas automáticamente a la lista de URL's durante el transcurso del día después de haber sido descubiertas por el fabricante de la solución y durante el transcurso del día.<br><br>Cuenta con filtro de protocolos no-HTTP basado en listas de protocolos.<br><br>Es capaz de identificar Gusanos generados a través del puerto 25 (SMTP) y otro tipo de tráfico malicioso.<br><br>Identifica redes zombies, conocidas como redes BOTS, en el entorno y bloquea el tráfico que esto generen.<br><br>Identifica y bloquea aquel tráfico que genere spyware, addware, Malicious Mobile Code, etc.<br><br>Cuenta con la capacidad de configurar el acceso a sitios permitidos sobre la base de usuario, dirección IP, hora o día de la semana. Incluye funcionalidad para permitir a ciertos usuarios acceder a sitios normalmente restringidos por un tiempo limitado configurable.<br><br>Soporte para 15,000 licencias para usuario.<br><br>Capacidad de bloquear adicionalmente por tipo de datos (MIME) o archivo (extensión).<br><br>Posibilidad de adecuar/modificar la página HTML mostrada al ser bloqueado un URL; está modificación o adecuación se refiere a la página que se le mostrará al usuario en caso de bloquearse alguna pagina Web.<br><br>Esta solución será implementada sobre un Hardware de la marca Hewlett Packard Modelo Proliant DL 380.<br><br>**LOTE 4 Seguridad de Correo Electrónico con antispam y antivirus**<br><br>Seguridad de Correo Electrónico con antispam y antivirus, Marca **McAfee** Modelo **Secure Appliance McAfee Messaging Gateway**-<br><br>Ofrecemos 2 equipos Appliance: 1 para el correo saliente y 1 equipo para el correo entrante.<br><br>La solución de seguridad de Correo Electrónico con antispam y antivirus soporta 15,000 usuarios.<br><br>Ofrecemos en nuestra solución, el hardware y/o software necesario para poder proporcionar el siguiente servicio:<br><br>✓ Filtrado de correo electrónico malicioso o basura tanto entrante como saliente.<br>✓ Es una solución basada en hardware (Appliance) y/o con sistema | 0476 |

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

| | | |
|---|---|---|
| operativo propietario de propósito específico.<br>✓ Contamos con protección para protocolo de correo: SMTP<br>✓ Incluye detección antivirus, antispam y anti-phishing de amenazas conocidas.<br>✓ Incluye detección de amenazas desconocidas (o de día cero).<br>✓ Cuenta con un mecanismo especial para hacer la captura de SPAM en imágenes en forma efectiva.<br>✓ Cuenta con un centro de investigación Anti SPAM que genera filtros para los mensajes que contengan material indeseable.<br>✓ Contamos con un centro de control y monitoreo de amenazas y ofrecemos soluciones avanzadas para la prevención de amenazas y alertas tempranas.<br>✓ Funciona en modo transparente o como relay.<br>✓ Cuenta con actualización automática de sus firmas antivirus, antispyware y antiphishing<br>✓ El fabricante cuenta con un centro de investigación AntiSpam que genera filtros para los mensajes que contienen material indeseable. La actualización de dichos filtros debe ser frecuente y automática. (Anexamos pagina WEB)<br>✓ Incluye capacidad de crear reglas específicas para evitar correos de salida con información específica.<br>✓ Cuenta con capacidad de crear políticas para diferentes tipos de usuarios.<br>✓ Se Integra vía LDAP.<br>✓ Cuenta con actualización automática de sus firmas antivirus y antispam.<br>✓ Cuenta con la capacidad de clustering<br>✓ Proporciona esquema de cuarentena para los diversos eventos y la implementación de políticas de seguridad.<br><br>✓ Cuenta con más de una interfase de red a fin de permitir la separación y comunicación adecuada de los diversos servicios requeridos a través de las diferentes áreas de red.<br><br>✓ La administración de colas es altamente eficiente a fin de evitar cuellos de botella.<br>✓ Tiene capacidad de evitar la recepción de correos por ataques de "bounce"; sin embargo permite el regreso de bounce legítimos.<br>✓ Provee mecanismos que permitan la autenticación del correo enviado: SPF, DomainKeys o contar con mecanismos para clasificar los remitentes por su origen y tomar decisiones de flujo y volumen en | | 0477 |

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

| | | | |
|---|---|---|---|
| consecuencia.<br>✓ Puede ser monitoreado por SNMP.<br>✓ Cuenta con algún mecanismo de prevención de brotes de nuevas epidemias de virus en el Internet.<br>✓ Cuenta con la facilidad de designar ciertas fuentes de correo en grupos como listas negras, listas blancas o cualquier otro grupo al que deba aplicársele una política específica.<br>✓ En caso de resultar ganadores nuestro gestionaremos ante las instancias correspondientes el desbloqueo en las principales listas o bases de datos de spam en caso de que la Secretaría estuviera incluida en estas. | | | |
| **LOTE 4.1 Servicio de Proxy**<br><br>Servicio Proxy, Marca **TEKTON NETWOKS** Modelo Proxy Server Byteware.<br><br>Ofrecemos en nuestra solución, para el control de acceso a Internet, el hardware y software que permite acceder a varios usuarios a Internet a través de una sola conexión física, La solución Proxy esta complementada por el hardware (basado en appliance independiente a los demás equipos que forman parte de la solución) y software necesarios, estos son integralmente compatibles y el desempeño de la solución no se vea degradado y se cuenta con el respaldo técnico del fabricante de la solución<br><br>Cuenta con las siguientes características:<br><br>Establece un punto de control que permite asegurar y acelerar las aplicaciones con la que cuenta el usuario<br>Puede controlar aplicaciones P2P, Mensajería instantánea con al menos los siguientes clientes AOL IM, Yahoo IM, MSN.<br>Controla aplicaciones de streaming media para al menos las siguientes aplicaciones MS, Real, QuickTime.<br>Es una solución de tipo appliance, la solución Proxy esta complementada por el hardware (basado en appliance) y software necesario integralmente compatibles, el desempeño de la solución no se ve degradado y se cuenta con el respaldo técnico de fabricante.<br>Permite crear políticas granulares a nivel de usuarios<br>Cuenta con la funcionalidad de administración de ancho de banda.<br>Cuenta con la funcionalidad de optimización de protocolos (http)<br>Soporta al menos los siguientes protocolos http, CIFS, SSL, FTP, MAPI, Telnet (para la comunicación con el equipo proxy), SOCKS, P2P, AOL IM, YAHOO IM, Microsoft IM, MMS, RTSP, QuickTime, TCP-Tunnel, DNS. El Proxy cuenta con las características de cache server, control de políticas y reporteo. | | | 0478 |

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

| | | | |
|---|---|---|---|
| Cuenta con la funcionalidad de bloquear spyware.<br>Puede autenticar a los usuarios a través de: archivos de password locales, NTLM, LDAP (Active Directory, eDirectory, SunOne), Microsoft Kerberos, Radius y certificados.<br>Cuenta con una interfaz de administración Web.<br>Cuenta con una interfaz de línea de comandos.<br>Puede enviar alertas vía SNMP, SMTP y registrar los eventos administrativos.<br>Pueder soportar al menos 15,000 usuarios concurrentes.<br>Tiene la capacidad de controlar el Servicio de mensajería instantánea como Messenger de Hotmail, Messenger de Yahoo, Skype, ICQ, es decir, permite o bloquea el servicio por usuario, grupo de usuarios o a toda la red.<br><br>**LOTE 5 Antivirus para Computadoras personales**<br><br>**Seguridad de Antivirus para computadoras, Marca McAfee**<br>**Modelo** McAfee Total Protection for Endpoint, McAfee Linux Shield<br><br>Solución que incluye:<br>Productos para computadoras de escritorio y servidores:<br>VirusScan Enterprise<br>VirusScan Command Line for DOS & Unix (soporta Solaris)<br>Anti-Spyware Enterprise<br>Host Intrusion Prevention for Desktops.<br>Servers: VirusScan Enterprise,<br>SiteAdvisor Enterprise Plus<br>Consola de administration ePolicy Orchestrator<br><br>Antivirus para computadoras personales incluyendo los servicios de consolas de administración centrales (soporte 15,000 usuarios)<br><br>Ofrecemos a la Secretaría protección antivirus para un máximo de 50 equipos servidores con sistema operativo Solaris 10, Windows 2003 y Linux 7.3 Red Hat en modo administrado.<br><br>La instalación de los clientes de antivirus será nuestra responsabilidad, la Secretaría a través de su Dirección General de Tecnología de la Información, nos indicará la ubicación de los sitios (Distrito Federal) en que serán instaladas las licencias.<br><br>La aplicación cuenta con uno o más Motores de Rastreo para análisis y búsqueda de Virus, de contar con más de uno, éstos trabajar de manera independiente y concurrentemente para rastrear en el sistema actividades maliciosas, permitiendo escaneos más rápidos y precisos, así como un mejor rendimiento en el equipo.<br><br>La solución permite que durante la instalación sea configurable la distribución inicial.<br><br>Cuenta con la capacidad para bloquear al cliente por medio de password la desinstalación del programa antivirus.<br><br>El Software de administración permite administrar y configurar niveles de seguridad.<br><br>La solución cuenta con la protección contra rootkits; así como su detección y limpieza. | | | |

0479

ASECO

ARRENDAMIENTOS Y SERVICIO EN COMPUTACION S.A DE C.V.

LICITACIÓN PÚBLICA NACIONAL NÚMERO 00011001-021/08.
**PARA LA CONTRATACIÓN PLURIANUAL DE LOS SERVICIOS DE SEGURIDAD PERIMETRAL Y ANTIVIRUS**

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

| | | | | |
|---|---|---|---|---|
| Proporcionaremos 6 servidores con las características técnicas necesarias para la administración, actualización y monitoreo de los equipos en red con el cliente antivirus.<br>Servidores Marca Hewlett Packard Modelo Proliant ML110 | | | | |
| Se integra a Outlook y Outlook Express, revisando en tiempo real correo SMTP entrante y saliente. | | | | |
| La solución incluye una herramienta Antispyware sin reducir el desempeño de los equipos, la cual es un módulo adicional administrado por la misma consola antivirus y no reduce el desempeño de los equipos. | | | | |
| La solución se integra al sistema operativo, así como al Explorador de Windows protegiendo en tiempo real todo el tráfico de Internet esto desde la capa WinSock del sistema, y así detectar antes de que se escriba al disco duro. | | | | |
| La solución cuenta con escaneo en sector de arranque, memoria y procesos ejecutándose, así mismo puede desinfectar cualquiera de las partes mencionadas sin necesidad de escanear por completo el equipo, correr algún fix o reiniciar el sistema. | | | | |
| La solución cuenta con capacidad para detectar unidades de tipo stream, unidades CD y en unidades removibles de lectura y escritura, cuenta con la capacidad de detectar y reparar las infecciones. | | | | 0480 |
| La solución permite exportar los datos de las bitácoras a formatos de archivo TXT o CSV. | | | | |
| Detecta y limpia los virus más comunes como FunLove, Nimda, Klez, Opaserv, Sircam, Elkern, etc., regresando los archivos infectados a su estado original. | | | | |
| Limpia los archivos sin necesidad de recompilarlos, los atributos de estos se mantienen sin perder su integridad. | | | | |
| Tiene la capacidad de escaneo en background de cada archivo que el usuario o sistema acceda, sin disminuir el rendimiento del sistema, en dicho escaneo utiliza menos del 50% de rendimiento del equipo. | | | | |
| Elimina Virus en archivos compactados con los siguientes formatos: ZIP, ARJ (JAR), RAR, CAB, ACE, ZOO, GZIP (GZ), TAR, Z, TGZ, TAZ, etc. | | | | |
| La solución cuenta con motor heuristico. | | | | |

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

| | | | |
|---|---|---|---|
| Permite crear discos de reparación de emergencia que permitan el arranque (boot) y reparación del sistema, cuando el sector de arranque haya sido dañado, o bien reparar los daños sin necesidad de estas Herramientas. Es posible permitir en lugar de crear discos se pueda sustituir por dispositivos USB con comandos ejecutados desde una herramienta propietaria de nuestra solución. | | | |
| Los discos o USB de reparación trabajar con particiones FAT, FAT-32 y NTFS. | | | |
| Soporta la actualización del software antivirus, definiciones de virus motor de rastreo y programa a través de los protocolos http, esto puede realizarlo manual o automáticamente. | | | |
| Soporta todas las plataformas Windows (2000 Profesional, NT Workstation, XP y Vista), adicionalmente el uso de librería multi-lenguaje que reconoce inglés y otros idiomas automáticamente. | | | |
| Tiene la capacidad para detectar virus desconocidos y moverlos a un directorio virtual esto para prevenir que los virus desconocidos infecten el sistema. Dichos Virus son enviados al equipo de soporte del fabricante para su análisis. El reporte sera resuelto y aplicado dentro de las siguientes 24 horas. | | | 0481 |
| Las actualizaciones en los clientes podrán ser directo de la consola, vía Internet, manualmente, o descargarlas desde otros usuarios. | | | |
| La actualización en los clientes tiene la capacidad para actualizarse desde el servidor central sin la intervención del usuario. | | | |
| La consola del sistema se puede instalar en cualquier computadora con sistema operativo Windows Server o superior. | | | |
| El servicio proporciona una consola GUI vía WEB que conserve los beneficios de la consola de administración remota sin generar nuevas vulnerabilidades en el sistema. | | | |
| La solución administra todos los clientes y servidores bajo una sola consola. | | | |
| Se provee un servicio para bloquear procesos no deseados en los equipos, para poder atacar un problema de virus nuevos. | | | |
| La consola de administración cuenta con alertas o bioqueo de propagación para | | | |

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

| | | | |
|---|---|---|---|
| virus desconocidos antes de que las actualizaciones estén disponibles. | | | |
| Cuenta con políticas de Emergencia para situaciones Urgentes. | | | |
| Cuenta con información sobre puertos sospechosos como puertas traseras (Backdoor), así como puertos de control los cuales utilizan dichos "Puertos Sospechosos", intercepción de sesiones, terminación de procesos e intervención después de terminar el proceso. | | | |
| Detecta vulnerabilidades en cuentas de usuarios, red, y parches de seguridad, a través de la solución Antivirus. | | | |
| La consola permite la ejecución en tiempo real de rastreos remotos sobre las PC'S | | | |
| La consola genera notificaciones por evento, por producto, por severidad, por nodo del árbol de la red. | | | |
| La consola cuenta con administrador de privilegios de usuarios. Con la posibilidad de definir diversos perfiles tales como privilegios de administrador o de solo lectura y generación de reportes, el administrador contara con todos los privilegios | | | |
| Genera reportes automáticos del estado del cliente o agente, o reportar al administrador del sistema el estado de los equipos en la red. | | | |
| La consola recibe las actualizaciones de patrones de virus, motores de rastreo y programa, desde los servidores del fabricante a través de una conexión a Internet de forma automática. | | | |
| Cuenta con una distribución inteligente de las actualizaciones hacia los clientes y puntos remotos, esto para no afectar en el desempeño de la red. | | | |
| La solución no comparte ni una sola carpeta en el servidor. | | | |
| La solución protege y administra las carpetas compartidas con la finalidad de no permitir Infecciones. | | | |
| En caso de infección, detecta la máquina origen de la epidemia, al menos: dirección IP, nombre del equipo (si existe), nombre del usuario (si existe). | | | |
| La solución cuenta con una ventana de "información de virus" que muestre al | | | |

0482

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

menos: la hora, nombre del usuario, nombre del grupo, estado de infección, nombre del virus y nombre de los archivos infectados. El administrador podrá rastrear al usuario y el archivo infectado con esta ventana.

El administrador puede guardar tablas y gráficos en archivos, exportarlos o imprimirlos para análisis de datos y mantener acciones pro-activas frente a la constante amenaza de virus.

La consola de administración centralizada entrega las herramientas necesarias para mantener las actualizaciones al día, realizándolas mínimo tres veces a la semana, en forma automática e incremental, optimizando el ancho de banda de la organización y minimizando el tráfico en la red.

**LOTE 6 Equipo para la conectividad para la segmentación de las zonas.**

Ofrecemos una solución para la conectividad para la Segmentación de las zonas, **Marca 3Com.**

Nuestra solución incluye el equipo de conectividad separado de los servidores de la zona perimetral de servicios de Internet y a los servidores de aplicaciones internas por medio de switchos de alto rendimiento de capa tres de la Marca 3com y módulos adicionales, que permiten la aplicación de políticas de control de acceso a los servicios y programas de los mismos y tienen las siguientes capacidades y características:

Maneja diversas tecnologías de red.

La solución cuenta con fuentes redundantes.

La solución cuenta con un total de 36 puertos de Gigabit Ethernet, de los cuales 18 interfaces o puertos de fibra óptica son del tipo SX, dejando 18 puertos adicionales disponibles para cualquier crecimiento a corto plazo.

Entendemos que lo que requiere la convocante es un pacth cord de punta a punta y que la distancia los patch cords o jumpers (en su caso) será de 50 mts aproximadamente. El tipo de conector que consideraremos en el panel de interconexión de la fibra de la dependencia será del tipo LC.

Nuestra solución de conectividad cuenta con 96 puertos de UTP 10/100/1000 TX.

Los equipos cumplen con los siguientes estándares: IEEE 802.3, IEEE 802.1D, IEEE 802.1p, IEEE 802.1Q, IEEE 802.1w, IEEE 802.1s, IEEE 802.1X, IEEE 802.3ae, IEEE 802.3ad, 802.1Q VLANs, 802.1D MAC Bridges, 802.1w Rapid-reconvergence of Spanning Tree, 802.3ad Link Aggregation, Broadcast Supresión, 802.3x Flow Control, IDS Redirect,

La solución tiene una capacidad de switcheo de al menos de 40.5 Mpps y una capacidad de 54 Gbps como mínimo

**LOTE 7 Centro de operación de seguridad (SOC).**

**Gestión y Monitoreo de la Solución de Seguridad**

**Enfoque del Servicio**

0483

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

Como parte de nuestra solución general propuesta, incluimos para el proyecto de Servicios de Seguridad los servicios de un SOC (Security Operations Center) localizado en la República Mexicana, mediante el cual conforme a estándares y mejores prácticas proporcionaremos los servicios de seguridad de la información requeridos por la Secretaría, de acuerdo con los SLA's establecidos en el proyecto. Manifestamos que contamos con una experiencia mínima de 1 año en la prestación y operación de servicios del SOC en México.

En nuestra solución la conexión de las consolas al SOC serán a través de una VPN o un acceso que se integre a la solución con mecanismos de seguridad

**Objetivo**

Proporcionar un servicio de gestión y monitoreo de la solución de seguridad que forma parte de este proyecto, a través de un SOC, de tal manera que se pueda garantizar el cumplimiento de los requerimientos establecidos en las bases y junta de aclaraciones del presente proceso de licitación.

**Los objetivos que cubriremos son los siguientes:**

- Mejorar y fortalecer los niveles de servicio de la solución de seguridad con que se cuenta en la red actual de la Secretaria, partiendo de los niveles de servicio que actualmente se encuentran en operación. Los cuales en caso de que resultemos ser el licitante adjudicado,.nos comprometemos a revisar en conjunto con la Secretaria.

- Pondremos a disposición el personal de soporte necesario para atender cualquier eventualidad relacionada con los elementos de la solución de seguridad propuesta de acuerdo a los niveles de servicio.

- Contamos con una metodología de administración y operación basada en estándares internacionales como ITIL, para atender de manera oportuna los incidentes de seguridad, que se presenten en los servicios de este proyecto.

- Nuestro personal de soporte técnico cuenta con la experiencia necesaria en las soluciones de seguridad propuestas para operar el monitoreo y administración de la seguridad del proyecto en un esquema 7 x 24 durante la vigencia del contrato. Presentamos en nuestra propuesta una Carta bajo protesta de decir verdad acreditando lo anterior.

- El SOC contara con un portal vía web en donde se tendrá acceso en línea a los eventos que se han presentado, generar cambios de configuración y nuevos requerimientos, generación de reportes a partir de consultas personalizadas a la base de datos de eventos, así como interacción en línea con un ingeniero del SOC
  A través del portal web del SOC se podrán levantar tickets en nuestro sistema de mesa de ayuda y hacer el seguimiento respectivo hasta su solución.
- El soporte técnico a la solución de seguridad la podremos llevar a cabo de manera remota o en sitio, siempre cumpliendo con los SLA's establecidos.

- Aplicaremos una asesoría proactiva en el tratamiento de incidentes que involucran la aparición y/o detección de nuevas vulnerabilidades, ofreciendo información oportuna respecto a las nuevas vulnerabilidades relacionadas a la infraestructura de la Secretaria, las amenazas a las cuales puede estar expuesta y su forma de remediación. Para lo cual nos apoyaremos con información generada por organismos internacionales tan pronto como esta sea liberada.

0484

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

**Definición de Gestión y Monitoreo.**

Entendemos por gestión y monitoreo de la seguridad las siguientes tareas y/o servicios generales:

- La visualización e interacción en línea desde un punto remoto en nuestras consolas o acceso equivalente, de todos los elementos que forman parte de la solución de seguridad, observando sus funciones principales, desempeños, bitácoras, alarmas, eventos, reportes y en general cualquier parámetro informativo que según la documentación o manuales que estarán disponibles para garantizar el cumplimiento de los SLA's establecidos.

- Administración y control de las configuraciones de los elementos involucrados en su solución, incluyendo el control de cambios en dichas configuraciones.

- La atención a los requerimientos en cuanto a solicitud de cambios, reporte y atención de incidentes, así como consultas relacionadas al estado de la solución de seguridad.

- Esquemas proactivos de operación que permitan evitar ataques e incidentes de seguridad y en su caso, detectarlos, contenerlos y erradicarlos de la red de la Secretaría.

- Monitoreo 7x24 de los servidores internos de la Secretaría que cuenten ya sea con sistema operativo **Windows, Linux o Solaris**. Incluyendo el monitoreo de Ping, Puertos, Utilización de CPU, Utilización de Disco, Utilización de Memoria y de Ancho de Banda. El servicio incluirá la generación automática de alertas por falla en los servicios monitoreados. Adicionalmente en el caso de estas fallas se incluirá la capacidad de recuperación, pudiendo automáticamente reiniciar el equipo, reiniciar los servicios Windows y hasta correr scripts. Todos estos servicios aplicarán para un máximo de 50 servidores. La secretaría proporcionaría los accesos, permisos y privilegios para instalar los agentes en los sistemas operativos de los servidores.

  Tomando en consideración estas cantidades:
  20 (max) Windows 2003
  15 (max) Windows Server 2000
  15 (max) Linux 7.3 RedHat

- El servicio anterior incluirá la generación automática de alertas por falla e inclusive por degradación de servicio, es decir, que cuando alguno de los servicios monitoreados alcance ciertos umbrales (como por ejemplo: llegar al 80% de utilización del procesador) se generará automáticamente una alerta que podrá ser enviada vía correo electrónico a quienes señale la Dirección General de Tecnología de la Información de la Secretaría.

- El servicio anterior incluirá reportes en tiempo real por hora, día, semanas y meses, manteniendo un histórico. Y siendo capaz de enviar dichos reportes por correo electrónico. Presentaremos estos reportes a la Secretaría cada vez que esta los requiera.

- Incluiremos los procesos y procedimientos necesarios para mantener los niveles de disponibilidad y servicio solicitados.

0485

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

**Descripción de actividades a realizarse en el Servicio de Gestión y Monitoreo de la Seguridad.**

Ofreceremos a la Secretaría servicios de seguridad los cuales otorgaremos utilizando tecnología, prácticas y procesos por un Security Operation Center (SOC), dedicado a garantizar los niveles de seguridad que la SEP requiere.

***Estrategia a seguir para la liberación***

***Arranque***

Conforme a junta de aclaraciones el SOC operara desde la puesta en operación e implementación de los dispositivos de seguridad, por lo que se realizaremos todas las actividades necesarias para poner a punto la infraestructura de seguridad que proponemos como parte de nuestra solución, además de prepararla para su gestión y monitoreo desde el SOC.

***Actividades requeridas en la etapa de arranque***

ASECO en caso de ser el licitante ganador nos obligamos a realizar en esta etapa de la implantación las actividades de instalación y configuración de las tecnologías de seguridad para la prestación de los servicios. En esta implementación se contemplamos las siguientes actividades:

- Presentamos como parte de nuestra propuesta el diseño esquemático para la implementación de los elementos de seguridad ofertados especificando marcas y modelos de cada unos de los dispositivos de la solucion. Anexamos documento en nuestra propuesta técnica.
- Conforme a junta de aclaraciones en caso de ser el licitante ganador presentaremos la estrategia de implementación de las herramientas necesarias que forman parte de la solución de seguridad.
- Generación inicial de reglas y/o políticas de seguridad de las tecnologías a implementar. La puesta en marcha del servicio será con base en las políticas existentes en la solución de seguridad en operación, por lo que desde el momento de la asignación en caso de ser el licitante ganador la secretaria nos dará acceso en forma documental a estas políticas
- Generación de memoria técnica. ASECO en caso de ser el licitante ganador generaremos la documentación de la memoria técnica la cual incluirá el diagrama o diseño de la implementación de las tecnologías, la configuración de cada una de las herramientas instaladas, y las políticas y/o reglas de seguridad aplicadas.

***Entregables de la etapa de arranque***

Como resultado de la implantación de la solución de seguridad, generaremos al menos los siguientes entregables, los cuales entregaremos a la Secretaría a través de su Dirección General de Tecnología de la Información, considerando que los documentos mencionados a continuación solamente serán entregados por ASECO en caso de resultar adiudicados, una vez dado el fallo y conforme se cumplan las etapas de implantación de la solución de seguridad:

- Memorias técnicas de la implementación de la solución de seguridad.

Procedimientos para la operación de la gestión y monitoreo de la seguridad:

- Procedimiento de respuesta a incidentes.

0486

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

- Procedimiento de atención.
- Conjunto de reportes tipo (reportes de actividad sospechosa, vigencia de licenciamiento, reporte de vulnerabilidades, reporte de desempeño de los componentes de seguridad de la solución (uso de CPU, consumo de memoria y disponibilidad como mínimo), tendencia de comportamiento, top de hojas Web accesadas, intentos de acceso a páginas no permitidas, los anteriores como los más representativos).

***Gestión y Monitoreo***

***Servicios de arranque para la operación de la Gestión y Monitoreo de la Seguridad***

- **Definición del proceso de respuesta a incidentes.-** En caso de que ASECO sea el licitante ganador contaremos con un proceso ya definido de respuesta a incidentes de seguridad, el cual será revisado por personal de la Dirección General de Tecnología de la Información de la Secretaria y afinado por nuestro personal técnico de acuerdo a la retroalimentación recibida. Para esto, contemplamos las sesiones de trabajo necesarias para que el proceso quede totalmente adecuado a las necesidades de la Secretaria.
- **Definición del proceso de atención.-** En caso de que ASECO sea el licitante ganador documentaremos el proceso de atención a la Dirección General de Tecnología de la Información de la Secretaria para requerimientos de cambios, reporte de fallas, solución de dudas, etc. Este proceso contemplara los procedimientos y matrices de escalamiento necesarios, de común acuerdo con lo establecido con el SOC.
- **Revisión y afinación de reportes.** El proceso de operación iniciará con los reportes tipo propuestos y como resultado de la operación, se acordarán de manera conjunta las modificaciones o precisiones que se requieran a los mismos, estos cambios los realizaremos sin costo para la SEP.

ASECO en caso de ser el licitante ganador realizaremos cualquier otra actividad que se considere necesaria para garantizar que al arranque de la operación se cumplan con los niveles de servicio solicitados.

**Operación Continua**

Conforme a junta de aclaraciones el SOC operara desde la implementación de los dispositivos de seguridad, de acuerdo con los requerimientos y SLA's establecidos por la Secretaría y la Gestión y Monitoreo necesarios además de que pueda ingresar todos los servicios establecidos como parte de la solución.

El enlace por el que atraviese toda la información de las consolas hacia el centro de monitoreo será fuertemente asegurado y cifrado así como también entrar en un segmento monitoreado internamente por el SOC.

ASECO en caso de ser el licitante ganador proporcionara a la Secretaría una interfaz gráfica (GUI) o interfaz web, que formará parte de los servicios del SOC para las actividades de monitoreo en general y en específico en los equipos en los que se requiera.

0487

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

ASECO en caso de ser el licitante ganador proporcionara una persona responsable del proyecto que cubrir con las siguientes funciones:

- Ser el único punto de contacto para la secretaría.
- Coordinar la realización de los servicios solicitados.
- Asegurar que los servicios brindados sean de acuerdo a las especificaciones de los fabricantes de los productos de hardware y/o software.
- Asegurar el cumplimiento de todas las cláusulas y requerimientos del contrato.
- Informar inmediatamente al personal designado por la secretaría sobre cualquier cambio, problema o algún otro asunto que pudiera afectar el desarrollo de los servicios ofertados.
- Asistir a las juntas de coordinación que sean programadas con la secretaría
- Elaborar reportes de avance mensuales donde se indiquen los servicios brindados.
- Los niveles de servicio de monitoreo (SOC) 7X24 se medirán para cada uno de los casos mencionados a continuación de acuerdo a los datos e información con que cuente el ASECO en caso de ser el licitante ganador.

**Cumpliremos con los siguientes niveles de servicio: (SLA´s)**

| **Característica** | **Tipo de Servicio: 7x24** |
|---|---|
| Número de solicitudes de cambio mensuales | Ilimitado |
| Medios de Solicitud de cambios | Teléfono o e-Mail, 01 800 sin costo para el interior de la república |
| Tiempo de confirmación de que el caso ya está asignado y trabajándose. | 30 minutos |

Conforme a la junta de aclaraciones el **tiempo de confirmación** se refiere al tiempo transcurrido en la confirmación de que el caso ya ha sido asignado al técnico correspondiente y que está en proceso de solución

Sobre Incidentes de Operación y/o Seguridad.

| **Clasificación** | **Descripción** | **Tiempo de Respuesta** | **Penalización en caso de incumplimiento** |
|---|---|---|---|
| Prioridad 1 | Relacionada con situaciones en donde la operación esta fuera de servicio por completo. | 30 mins | 0.02% de la facturación total mensual por hora de retraso |
| Prioridad 2 | Relacionada con situaciones donde el sistema presenta fallas o inconsistencias y estas pueden regresar a condiciones iniciales de operación normal con un reinicio del sistema o dichas inconsistencias permiten la operación aunque de manera restringida. | 90 mins | 0.01% de la facturación total mensual por hora de retraso |
| Priorida | Prioridad relacionada con | 2hrs | 0.005% de la facturación total mensual |

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

| | | | |
|---|---|---|---|
| d 3 | situaciones donde se requiere la habilitación o corrección de cierta característica de funcionalidad sobre el producto para poder habilitar un nuevo servicio. En este nivel la operación no se ve afectada. | | por hora de retraso |
| Priorida d 4 | Prioridad relacionada con la solicitud de reportes o dudas. | 4hrs | 0.005% de la facturación total mensual por hora de retraso |

Conforme a junta de aclaraciones el tiempo de respuesta el tiempo de respuesta inicia al momento en que personal de la secretaría levante un ticket o el SOC detecte una falla durante el monitoreo hasta que el licitante ganador concluya el requerimiento, considerando que estos tiempos no deben exceder lo definido en la tabla sobre incidentes de operación

Sobre cambios de tipo administrativo en los productos de seguridad.

| Clasificación | Descripción | Tiempo de Respuesta | Penalización en caso de incumplimiento |
|---|---|---|---|
| Priorida d 1 | Relacionada a Agregar, Eliminar, Modificar objetos, reglas o usuarios. | 1 hr. | 0.002% de la facturación total mensual por hora de retrazo |
| Priorida d 2 | Relacionada con situaciones de VPN´s, ruteo, configuraciones finas de propiedades de seguridad que puedan implicar la afectación de la operación o el trabajo en conjunto con terceros. | 3 hr | 0.005% de la facturación total mensual por hora de retrazo |
| Priorida d 3 | Relacionadas con rastreos o análisis. | 6 hr | 0.005% de la facturación total mensual por hora de retrazo |

Conforme a junta de aclaraciones el tiempo de respuesta el tiempo de respuesta inicia al momento en que personal de la secretaría levante un ticket o el SOC detecte una falla durante el monitoreo hasta que el licitante ganador concluya el requerimiento, considerando que estos tiempos no deben exceder lo definido en la tabla sobre incidentes de operación

**Licenciamiento y Entrega de Actualizaciones**

ASECO en caso de ser el licitante ganador considerara todo el licenciamiento necesario para la correcta operación de su solución incluyendo dentro de la vigencia del servicio, los parches y actualizaciones (upgrades) relacionados con los elementos de la solución y los que permitan asegurar los SLA's solicitados por la Secretaría a través de la Dirección General de Tecnología de la Información.

Nuestro SOC cuenta con una metodología de administración y operación basada en estándares internacionales como ITIL, para atender de manera Oportuna los incidentes de seguridad, que se presenten en los servicios de este proyecto

ASECO en caso de ser el licitante ganador Observaremos e implementaremos los siguientes puntos:

0489

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

**Control de Cambios**
Administrar las modificaciones realizadas sobre la infraestructura que forme parte de la solución de seguridad, consideremos un esquema de control de cambios que permita garantizar la continuidad operativa del servicio, así como los SLA's establecidos. Lo anterior con el fin de permitir el flujo adecuado de las aplicaciones del negocio, y bloquear toda aquella actividad o flujo de datos ajeno o perjudicial para el mismo.

Cualquier modificación al ambiente de operación, sera debidamente documentada para su posterior consulta, para de esta forma mantener una base o registro actualizada al día, de las configuraciones que se tienen en los dispositivos.

**Soporte a fallas**
Teniendo como punto de contacto al SOC, llevaremos a cabo la apertura de reporte de fallas de los elementos de la solución de seguridad considerados como parte del servicio de Seguridad.
El servicio de soporte técnico será 7X24 en idioma Español durante la vigencia del servicio Ante una falla apoyaremos las actividades necesarias para restablecer el servicio o corregirla de acuerdo con los SLA's establecidos.

El servicio de soporte a fallas permitirá el levantamiento de tickets a través de los siguientes medios:

- Numero directo a las instalaciones del SOC, en la Ciudad de México
- Contara con un numero 01800 sin costo
- Vía e-mail
- A través de un sitio WEB

**Disponibilidad**
Vigilaremos que los dispositivos de seguridad administrados por ASECO en caso de ser el licitante ganador estén operando de acuerdo con los SLA's establecidos durante período de servicio y negociados previamente con el licitante ganador. ASECO en caso de ser ganador será el responsable de garantizar la continuidad operativa de los servicios y el cumplimiento de los SLA's acordados con la Dirección General de Tecnología de la Información conforme a lo establecido en la presente propuesta; en caso de cualquier falla en los elementos que formen parte de la solución de seguridad.

**Manejo de incidentes**
El manejo de incidentes tendrá por objetivo, el evitar de manera proactiva, rápida y eficiente que una actividad sospechosa se convierta en incidente de seguridad y tenga algún impacto sobre la solución de seguridad. Los procesos que forman parte de esta actividad son la identificación, contención inicial, recuperación, seguimiento y documentación.

**Entregables de la etapa de operación**
Mensualmente entregaremos a la Dirección General de Tecnología de la Información reportes detallados de los servicios de la solución de seguridad con el fin de contar con información precisa para determinar de manera proactiva riesgos sobre la solución de seguridad implantada como parte de este servicio. Estos reportes serán al menos los siguientes:

1. Reporte de la actividad de los firewalls donde se presenten los principales protocolos que circulan por estos, el tráfico generado por cada uno de ellos, el tipo de tráfico por protocolo, principales direcciones destino por protocolo, comportamiento del trafico diario las principales direcciones IP para cada una de los protocolos principales, y el tráfico total que circula por el firewall por día.

0490

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

2. Con base en el formato de reporte de fallas presentar el Reporte de estas y de eventos de soporte técnico atendidos y en caso de existir, en donde se presentan las fallas de la infraestructura de seguridad bajo contrato, con detalles como fecha y hora de inicio, fecha y hora de finalización, persona que reportó la falla, persona que atendió y la descripción de la falla misma.

3. Reporte de actividades sospechosas e incidentes de seguridad, lo anterior con base en el comportamiento del día y solo se informarán los incidentes más relevantes que el SOC manejó, especificando tipo de actividad identificada, origen y destino, cómo se identificó y cómo se trató de resolver, así como las recomendaciones para evitar futuros incidentes.

4. Reporte de requerimientos atendidos en el periodo y tiempos de respuesta donde se presente la lista de todas las solicitudes de cambio realizadas al SOC, especificando fecha y hora del requerimiento y fecha y hora de atención/solución, persona que solicitó y que atendió.

5. Resumen ejecutivo donde se presenten los aspectos más relevantes del servicio en el periodo, contemplando las conclusiones y métricas más importantes.

6. Reporte de disponibilidad de la infraestructura de seguridad; este reporte deberá presentar el porcentaje de disponibilidad de la infraestructura de seguridad

7. Reporte de eventualidades o actividad sospechosa no atendidos en el periodo establecido y de responsabilidad del personal institucional.

8. Estadísticas referentes al servicio de protección de correo electrónico.

9. El reporte de vulnerabilidades para los servidores críticos (máximo 50) a solicitud de la Dirección General de Tecnología de la Información en caso de ser necesario. Los cuales reflejen los niveles de inseguridad de los equipos, conteniendo al menos: los puertos abiertos, parches de seguridad faltantes, versiones obsoletas, etc. Estos reportes serán requeridos en cualquier momento y a solicitud expresa de la Dirección General de Tecnología de la Información.

Los reportes generados por el SOC serán accesibles vía Web mediante un portal de Internet.

ASECO incluye en su propuesta técnica, un ejemplo de cada uno de los reportes anteriores y en caso de ser el licitante ganador ajustaremos los formatos de dichos reportes a las necesidades particulares de la institución.

ASECO en caso de ser el licitante ganador proporcionara la capacitación para 7 personas por un mínimo de 120 horas dentro de los primeros 90 (noventa) días posteriores al inicio de la vigencia del contrato, necesaria para el manejo de la infraestructura y base instalada en la Secretaría.

Esta se llevará a cabo en nuestras instalaciones, cumplirá con las condiciones técnicas y ambientales necesarias, para las principales funcionalidades y el monitoreo de cada dispositivo integrado en la solución, así mismo proporcionaremos los recursos materiales, instalaciones y logística necesaria para la impartición de la capacitación.

Conforme a la junta de aclaraciones las personas que tomarán la capacitación por parte de la SEP deberán contar con los conocimientos básicos de la tecnología que se implementara.

0491

ASECO

ARRENDAMIENTOS Y SERVICIO EN COMPUTACION S.A DE C.V.

LICITACIÓN PÚBLICA NACIONAL NÚMERO 00011001-021/08.
**PARA LA CONTRATACIÓN PLURIANUAL DE LOS SERVICIOS DE SEGURIDAD PERIMETRAL Y ANTIVIRUS**

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

Periodos de instalación e inicio del servicio.

| **Inicio del servicio** | **1 de septiembre de 2008** |
|---|---|
| Instalación del equipamiento central<br><br>Firewall en alta disponibilidad<br>Sistema de prevención de intrusos (IPS<br>Control de Accesos a páginas Web<br>Seguridad de Correo Electrónico con antispam y antivirus<br>Servicio de Proxy<br>Equipo para la conectividad para la segmentación de las zonas<br>Servidores de administración para el cliente antivirus<br>Y Centro de operación de seguridad (SOC). | Hasta el 31 de agosto de 2008 |
| Instalación de antivirus para computadoras personales | Hasta el 30 de septiembre de 2008 |

0492

| | |
|---|---|
| TOTAL DEL SERVICIO | SUBTOTAL: $29,092,000.00<br>IVA.: $4,363,800.00<br>GRAN TOTAL: $33,455,800.00 |

**(Son: Treinta y tres millones cuatrocientos cincuenta y cinco mil ochocientos pesos 00/100, M.N.)**

**ARRENDAMIENTOS Y SERVICIO EN COMPUTACIÓN, S.A. DE C.V.**
**LEONOR 370 PB, DEPTO. 2, COL. NATIVITAS, DELEG. BENITO JUAREZ, C.P. 03500, MÉXICO D.F.**
**TEL/FAX 56987741 Y 56986930**

ASECO

ARRENDAMIENTOS Y SERVICIO EN COMPUTACION S.A DE C.V.

LICITACIÓN PÚBLICA NACIONAL NÚMERO 00011001-021/08.
**PARA LA CONTRATACIÓN PLURIANUAL DE LOS SERVICIOS DE SEGURIDAD PERIMETRAL Y ANTIVIRUS**

Mexico, D.F. a 18 de julio del 2008.

SECRETARÍA DE EDUCACIÓN PÚBLICA.
OFICIALÍA MAYOR.
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.
DIRECCIÓN DE ADQUISICIONES.
PRESENTE

EN EL CASO QUE LA SECRETARÍA DE EDUCACIÓN PÚBLICA, ME OTORGUE LA ADJUDICACIÓN DEL CONTRATO, ME OBLIGO EN NOMBRE DE MÍ REPRESENTADA A SUSCRIBIR EL CONTRATO QUE SE DERIVE, EN LOS TÉRMINOS, CONDICIONES Y PORCENTAJE ESTABLECIDOS EN ESTAS BASES.

0493

Atentamente,

Diana Hernandez Almeida
Representante Legal de
Arrendamientos y Servicio en
Computación, S.A. de C.V.

Scitum
Seguridad

**ANEXO 9**

## FORMATO DE PROPUESTA ECONOMICA

| | DIA | MES | AÑO |
|---|---|---|---|
| FECHA | 18 | Julio | 2008 |

NOMBRE DEL LICITANTE: **SCITUM, S.A. DE C.V.** R.F.C: **SCI 001208 M74**

DOMICILIO: **REFORMA NO 373, COL. CUAUHTEMOC, DEL. CUAUTHEMOC, MÉXICO, D.F., C.P. 06500**

| TELEFONO | FAX | CORREO ELECTRÓNICO | NÚMERO DE RECIBO DE COMPRA DE BASES |
|---|---|---|---|
| 9150-7400 | 9150-7478 | jthome@scitum.com.mx | 135725 |

LOS SERVICIOS PROPUESTOS, SE APEGAN JUSTA, EXACTA Y CABALMENTE A LO SOLICITADO POR LA CONVOCANTE EN EL **ANEXO "B" – "DESCRIPCION DE LOS SERVICIOS"**, DE LAS BASES DE LA LICITACIÓN PÚBLICA NACIONAL No. **00011001-021/08** PARA LA CONTRATACIÓN PLURIANUAL DE LOS SERVICIOS DE SEGURIDAD PERIMETRAL Y ANTIVIRUS.

| CONCEPTO | Costo mensual | 2008 (4 meses) | 2009 (12 meses) | 2010 (12 meses) |
|---|---|---|---|---|
| SERVICIO DE SEGURIDAD PERIMETRAL Y ANTIVIRUS | $746,000.00 | $2'984,000.00 | $8'952,000.00 | $8'952,000.00 |

| | | |
|---|---|---|
| TOTAL DEL SERVICIO | SUBTOTAL: | $20'888.000.00 |
| | IVA.: | $3'133.200.00 |
| | GRAN TOTAL: | $24'021,200.00 |

**PRECIOS FIJOS EN MONEDA NACIONAL.**

EN EL CASO QUE LA SECRETARÍA DE EDUCACIÓN PÚBLICA, ME OTORGUE LA ADJUDICACIÓN DEL CONTRATO, ME OBLIGO EN NOMBRE DE MÍ REPRESENTADA A SUSCRIBIR EL CONTRATO QUE SE DERIVE, EN LOS TÉRMINOS, CONDICIONES Y PORCENTAJE ESTABLECIDOS EN LAS BASES Y JUNTA DE ACLARACIONES DE ESTA LICITACIÓN. ACEPTAMOS LAS CONDICIONES DE PRECIO Y PAGO DE LAS BASES Y JUNTA DE ACLARACIONES.

C. JORGE JUAN THOME ORTIZ
REPRESENTANTE LEGAL
SCITUM, S.A. DE C.V.

MPSNet
Internet para Negocios

| PROPUESTA ECONÓMICA. | ANEXO 9 |
|---|---|

**SECRETARÍA DE EDUCACIÓN PÚBLICA.**
**OFICIALÍA MAYOR.**
**DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS.**
**DIRECCIÓN DE ADQUISICIONES.**
**LICITACIÓN PÚBLICA NACIONAL NUM. 00011001-021/08.**
**PARA LA CONTRATACIÓN PLURIANUAL DE LOS SERVICIOS DE SEGURIDAD PERIMETRAL Y ANTIVIRUS.**

| NOMBRE DEL LICITANTE: | FECHA: |
|---|---|
| INTERNET ENGINE, S.A. DE C.V. | 18-07-2008 |
| **DOMICILIO:** | **R.F.C.:** |
| AV. CUAUHTÉMOC NUM. 1217 – PH, COL. SANTA CRUZ ATOYAC, DELEGACIÓN BENITO JUÁREZ, CP 03310, MÉXICO, D.F. | IEN 990720 K23 |

| TELÉFONO | FAX | CORREO ELECTRÓNICO | NÚMERO DE RECIBO DE COMPRA DE BASES |
|---|---|---|---|
| 5604-4655 | 5601-0249 | jpena@internetengine.com.mx | 588808 |

LOS SERVICIOS PROPUESTOS, SE APEGAN JUSTA, EXACTA Y CABALMENTE A LO SOLICITADO POR LA CONVOCANTE EN EL ANEXO 1 (UNO), DE LAS BASES DE LA LICITACIÓN PÚBLICA NACIONAL NÚMERO **00011001-021/08.**

| Concepto | Costo Mensual | 2008 (4 meses) | 2009 (12 meses) | 2010 (12 meses) |
|---|---|---|---|---|
| 1. FIREWALL EN ALTA DISPONIBILIDAD | 103,860.25 | 415,440.99 | 1,246,322.98 | 1,246,322.98 |
| 2. SISTEMA DE PREVENCIÓN DE INTRUSOS (IPS) | 135,817.25 | 543,269.00 | 1,629,807.01 | 1,629,807.01 |
| 3. CONTROL DE ACCESOS A PÁGINAS WEB | 119,838.75 | 479,355.01 | 1,438,065.04 | 1,438,065.04 |
| 4. SEGURIDAD DE CORREO ELECTRÓNICO CON ANTISPAM Y ANTIVIRUS. | 199,731.25 | 798,924.99 | 2,396,774.98 | 2,396,774.98 |
| 5. ANTIVIRUS PARA COMPUTADORAS PERSONALES (15,000 LICENCIAS) | 111,849.50 | 447,397.99 | 1,342,193.96 | 1,342,193.96 |
| 6. EQUIPO PARA LA CONECTIVIDAD PARA LA SEG. DE LAS ZONAS | 71,903.25 | 287,613.02 | 862,839.05 | 862,839.05 |
| 7. CENTRO DE OPERACIÓN DE SEGURIDAD (SOC) | 55,924.75 | 223,698.99 | 671,096.98 | 671,096.98 |
| **SERVICIO DE SEGURIDAD PERIMETRAL Y ANTIVIRUS** | **798,925.00** | **3,195,700.00** | **9,587,100.00** | **9,587,100.00** |

| | | |
|---|---|---|
| | SUB TOTAL: | 22,369,900.00 |
| | IVA: | 3,355,485.00 |
| TOTAL DEL SERVICIO | GRAN TOTAL: | 25,725,385.00 |

**Nota:**

EN EL CASO QUE LA SECRETARÍA DE EDUCACIÓN PÚBLICA, ME OTORGUE LA ADJUDICACIÓN DEL CONTRATO, ME OBLIGO EN NOMBRE DE MÍ REPRESENTADA A SUSCRIBIR EL CONTRATO QUE SE DERIVE, EN LOS TÉRMINOS, CONDICIONES Y PORCENTAJE ESTABLECIDOS EN LAS BASES DE LICITACIÓN DE REFERENCIA.

**ATENTAMENTE**

JUAN MANUEL PEÑA ZAVALA
REPRESENTANTE LEGAL

Soluciones Confiables Red Segura®

SECRETARIA DE EDUCACION PÚBLICA
DIRECCIÓN GENERAL DE RECURSOS MATERIALES Y SERVICIOS
DIRECCIÓN DE ADQUISICIONES
LICITACIÓN PÚBLICA NACIONAL NUMERO 00011001-021/08
CONTRATACIÓN PLURIANUAL DE LOS SERVICIOS DE
SEGURIDAD PERIMETRAL Y ANTIVIRUS
MÉXICO D.F. A 18 DE JULIO DEL 2008

# OFERTA ECONOMICA

**ANEXO 8**

| | DIA | MES | AÑO |
|---|---|---|---|
| FECHA | 18 | Julio | 2008 |

NOMBRE DEL LICITANTE ONLINET S.A. DE C.V. R.F.C ONL 970307321
DOMICILIO CASMA 594 COLONIA LINDAVISTA MEXICO D.F.

| TELEFONO | FAX | CORREO ELECTRÓNICO | NÚMERO DE RECIBO DE COMPRA DE BASES. |
|---|---|---|---|
| 55862613 | 55862613 EXT 102 | emorales@onlinet.com.mx | |

LOS SERVICIOS PROPUESTOS, SE APEGAN JUSTA, EXACTA Y CABALMENTE A LO SOLICITADO POR LA CONVOCANTE EN EL ANEXO B, DE LAS BASES DE LA LICITACIÓN PÚBLICA NACIONAL NÚMERO 00011001-021/08

| CONCEPTO SERVICIO DE SEGURIDAD | Costo mensual | 2008 (4 meses) | 2009 (12 meses) | 2010 (12 meses) |
|---|---|---|---|---|
| SERVICIO DE SEGURIDAD PERIMETRAL Y ANTIVIRUS CONFORME A NUESTRA PROPUESTA TECNICA | $914,323.64 | $3,657,294.56 | $10,971,883.68 | $10,971,883.68 |
| | | | SUBTOTAL | $25,601,061.92 |
| | | | IVA | $3,840,159.29 |
| | | | TOTAL MONEDA NACIONAL | $29,441,221.21 |

**VEINTINUEVE MILLONES CUATROCIENTOS CUARENTA Y UN MIL DOSCIENTOS VEINTIUN PESOS 21/100 MN**

EN EL CASO QUE LA SECRETARÍA DE EDUCACIÓN PÚBLICA, ME OTORGUE LA ADJUDICACIÓN DEL CONTRATO, ME OBLIGO EN NOMBRE DE MÍ REPRESENTADA A SUSCRIBIR EL CONTRATO QUE SE DERIVE, EN LOS TÉRMINOS, CONDICIONES Y PORCENTAJE ESTABLECIDOS EN ESTAS BASES.

**ATENTAMENTE**

ING. EDGAR MORALES SARDANETA
REPRESENTANTE LEGAL

**ONLINET S.A. DE C.V.**
http:/www.onlinet.com.mx


**ZONA NORTE**
Calle del Hospital 2538-1
Piso 1 Col. Sertoma
64718 Monterrey, N.L.
Tel. (81) 1408 01 23

**OFICINAS CORPORATIVAS**
Casma 594 Col. Lindavista
Delegacion Gustavo A. Madero
México, D.F. CP 07300
Conmutador y Fax 01 55 5586 2613

**ZONA CENTRO**
Blvd. Atlixco 1 101
Fracc. San José Vistahermosa
Puebla, Pue. CP 72190
Telefono 044 222 238 3748

**ZONA BAJÍO**
Av. Arroyo CH 404
Segundo Piso Col. Alameda
Celaya, Gto. CP 38050
Telefono 01 461 613 8304

Desarrollos de
Tecnologías de Información

**ANEXO 9**

## FORMATO DE PROPUESTA ECONOMICA.

| | DIA | MES | AÑO |
|---|---|---|---|
| FECHA | 18 | 07 | 2008 |

NOMBRE DEL LICITANTE: **DESARROLLOS DE TI, S.A. DE C.V.**
R.F.C: **DTI-030320-BY7**
DOMICILIO **Tacuba 40 Piso 2-205 Col. Centro, México Distrito Federal C.P. 06010.**

| TELEFONO | FAX | CORREO ELECTRÓNICO | NÚMERO DE RECIBO DE COMPRA DE BASES. |
|---|---|---|---|
| (55)53-00-09-25 | 55)21-66-37-64 | ventas@desarrollosti.com.mx<br>fabiola.moctezuma@desarrollosti.com.mx | **Compra por Internet Referencia Bancaria Referencia Bancaria 113733** |

LOS SERVICIOS PROPUESTOS, SE APEGAN JUSTA, EXACTA Y CABALMENTE A LO SOLICITADO POR LA CONVOCANTE EN EL ANEXO B, DE LAS BASES DE LA **LICITACIÓN PÚBLICA NACIONAL NUM 00011001-021/08**

| CONCEPTO | Costo mensual | 2008 (4 meses) | 2009 (12 meses) | 2010 (12 meses) |
|---|---|---|---|---|
| SERVICIO DE SEGURIDAD PERIMETRAL Y ANTIVIRUS | $ 826,617.35 | $ 3,306,469.40 | $ 9,919,408.20 | $ 9,919,408.20 |

| | | |
|---|---|---|
| **TOTAL DEL SERVICIO** | Sub Total : | $ 23,145,285.80 |
| | I.V.A. : | $ 3,471,792.87 |
| | Total (MN) | $ 26,617,078.67 |

EN EL CASO QUE LA SECRETARÍA DE EDUCACIÓN PÚBLICA, ME OTORGUE LA ADJUDICACIÓN DEL CONTRATO, ME OBLIGO EN NOMBRE DE MÍ REPRESENTADA A SUSCRIBIR EL CONTRATO QUE SE DERIVE, EN LOS TÉRMINOS, CONDICIONES Y PORCENTAJE ESTABLECIDOS EN ESTAS BASES.

FABIOLA MOCTEZUMA GASCA
REPRESENTANTE LEGAL



**Desarrollos de TI, S.A. de C.V.**
Tacuba 40 Piso 2-205 Col. Centro, México Distrito Federal C.P. 06010
Tel: (55) 5300-0925 Fax: (55) 2166-3764 correo: ventas@desarrollosti.com.mx
http://www.desarrollosti.com.mx

Desarrollos de
Tecnologías de Información

## FORMATO DE CUADRO RESUMEN DE PROPUESTA ECONÓMICA
## LICITACIÓN PÚBLICA NACIONAL NUM 00011001-021/08

| | DÍA | MES | AÑO |
|---|---|---|---|
| FECHA | 18 | 07 | 2008 |

**NOMBRE DEL LICITANTE: DESARROLLOS DE TI, S.A. DE C.V.**
**R.F.C: DTI-030320-BY7**
FABRICANTE_____DISTRIBUIDOR ___XXX__

**NÚMERO DE RECIBO DE COMPRA DE BASES SEP: Compra por Internet Referencia Bancaria 113733**

| | | |
|---|---|---|
| NÚMERO DE SERVICIOS QUE PROPONE:<br><br>LOTE UNICO | SUMA TOTAL DEL<br>IMPORTE DEL SERVICIO PROPUESTO | $23,145,285.80 |
| (SON VEINTITRES MILLONES CIENTO CUARENTA Y CINCO MIL DOCIENTOS OCHENTA Y CINCO PESOSO 80/100 M.N.) | EL PRECIO ES ANTES DE I.V.A | |

**FABIOLA MCTEZUMA GASCA.**
**REPRESENTANTE LEGAL DEL LICITANTE.**



**Desarrollos de TI, S.A. de C.V.**
Tacuba 40 Piso 2-205 Col. Centro. México Distrito Federal C.P. 06010
Tel: (55) 5300-0925 Fax: (55) 2166-3764 correo: ventas@desarrollosti.com.mx
http://www.desarrollosti.com.mx

Informática Empresarial Integrada S.A. de C.V.
Lerma 1930
Col. Mitras Centro
64460 Monterrey, N.L.

**SECRETARÍA DE EDUCACIÓN PÚBLICA**
**LICITACIÓN PÚBLICA NACIONAL 00011001-021/08**
**CONTRATACIÓN MULTIANUAL DE LOS SERVICIOS DE SEGURIDAD PERIMETRAL Y ANTIVIRUS**

**ANEXO 9**

## FORMATO DE PROPUESTA ECONOMICA.

| | DIA | MES | AÑO |
|---|---|---|---|
| FECHA | 18 | 07 | 2008 |

NOMBRE DEL LICITANTE. **INFORMATICA EMPRESARIAL INTEGRADA, S. A. DE C.V.**
R.F.C: **IEI930820FC2**
DOMICILIO: **LERMA 1930, COL. MITRAS CENTRO MONTERREY, N.L.**

| TELEFONO | FAX | CORREO ELECTRÓNICO | NÚMERO DE RECIBO DE COMPRA DE BASES. |
|---|---|---|---|
| (81) 83330456 | (81) 83330456 | jescaren@informaticaempresarial.com.mx | COMPRANET CONSECUTIVO BANCARIO 122203 |

LOS SERVICIOS PROPUESTOS, SE APEGAN JUSTA, EXACTA Y CABALMENTE A LO SOLICITADO POR LA CONVOCANTE EN EL ANEXO 1 (UNO), DE LAS BASES DE LA LICITACIÓN PÚBLICA NACIONAL NÚMERO **00011001-021/08**

| CONCEPTO | Costo mensual | 2008 (4 meses) | 2009 (12 meses) | 2010 (12 meses) |
|---|---|---|---|---|
| **SERVICIO DE SEGURIDAD PERIMETRAL Y ANTIVIRUS** | **$1,350,000.00** | **$5,400,000.00** | **$16,200,000.00** | **$16,200,000.00** |

| | | |
|---|---|---|
| **TOTAL DEL SERVICIO** | **SUBTOTAL:** | **37,800,000.00** |
| | **IVA.:** | **5,670,000.00** |
| | **GRAN TOTAL:** | **43,470,000.00** |

EN EL CASO QUE LA SECRETARÍA DE EDUCACIÓN PÚBLICA, ME OTORGUE LA ADJUDICACIÓN DEL CONTRATO, ME OBLIGO EN NOMBRE DE MÍ REPRESENTADA A SUSCRIBIR EL CONTRATO QUE SE DERIVE, EN LOS TÉRMINOS, CONDICIONES Y PORCENTAJE ESTABLECIDOS EN ESTAS BASES.

**LIC. JUAN ESCAREÑO FERNANDEZ**
APODERADO DEL REPRESENTANTE LEGAL
INFORMATICA EMPRESARIAL INTEGRADA, S. A. DE C.V.
IEI930820FC2

GRUPO TECNO

**PROPUESTA ECONOMICA.**

| | DIA | MES | AÑO |
|---|---|---|---|
| FECHA | 18 | 07 | 2008 |

NOMBRE DEL LICITANTE: GRUPO DE TECNOLOGIA CIBERNETICA S.A. DE C.V. R.F.C GTC 980421 R4A
DOMICILIO MARTIRES DE LA CONQUISTA #105 COL. TACUBAYA, C.P. 11870, DEL. MIGUEL HIDALGO, MEXICO D.F.

| TELEFONO | FAX | CORREO ELECTRÓNICO | NÚMERO DE RECIBO DE COMPRA DE BASES. |
|---|---|---|---|
| 5278-9210 | 5278-9234 | VENTAS@TECNO.COM.MX | 00011001021081733980421941763781 66 |

LOS SERVICIOS PROPUESTOS, SE APEGAN JUSTA, EXACTA Y CABALMENTE A LO SOLICITADO POR LA CONVOCANTE EN EL ANEXO 1 (UNO), DE LAS BASES DE LA LICITACIÓN PÚBLICA NACIONAL NÚMERO 00011001-021/08

| CONCEPTO | Costo mensual | 2008 (4 meses) | 2009 (12 meses) | 2010 (12 meses) |
|---|---|---|---|---|
| SERVICIO DE SEGURIDAD PERIMETRAL Y ANTIVIRUS | $920,475.55 MN | $3,681,902.19 MN - | $11,045,706.56 MN - | $11,045,706.56 MN- |

| | |
|---|---|
| TOTAL DEL SERVICIO | SUBTOTAL: 25,773,315.31 MN<br>IVA.: $3,865,997.30 MN<br>GRAN TOTAL: $29,639,312.60 MN |

(Veintinueve millones, seiscientos treinta y nueve mil, trescientos doce 60/100 MN)

EN EL CASO QUE LA SECRETARÍA DE EDUCACIÓN PÚBLICA, ME OTORGUE LA ADJUDICACIÓN DEL CONTRATO, ME OBLIGO EN NOMBRE DE MÍ REPRESENTADA A SUSCRIBIR EL CONTRATO QUE SE DERIVE, EN LOS TÉRMINOS, CONDICIONES Y PORCENTAJE ESTABLECIDOS EN ESTAS BASES.

CARLOS JAVIER ZUBIETA GARCIA
REPRESENTANTE LEGAL