INFORME TECNICO PREVIO DE EVALUACION DE SOFTWARE N° 005-2011

1. NOMBRE DEL ÁREA

Gerencia de Tecnologías de la Información, Comunicaciones y Estadística.

2. RESPONSABLE(S) DE LA EVALUACIÓN

Freddy Alvarado Vargas
Winston Ugaz Cachay
Juan Rodríguez Calderón

3. CARGO(S)

Gerente de Tecnologías de la Información, Comunicaciones y Estadística (e)
Administrador de Redes y Comunicaciones.
Técnico en Redes e Informática.

4. FECHA

Lunes, 09 de Mayo de 2011.

5. OBJETIVO

Proveer al OISPTEL de la renovación de 367 licencias y la ampliación de 57 licencias de software de seguridad para estaciones de trabajo y servidores.

6. JUSTIFICACIÓN

Osiptel es una institución pública que para cumplir adecuadamente con sus actividades y ejecutar eficientemente sus procesos, requiere contar con una infraestructura tecnológica de redes que soporte los diversos servicios y sistemas informáticos implementados, y brinde continuidad, seguridad y flexibilidad en la administración y manejo de la información, por lo cual los equipos informáticos deben ser continuamente renovados y actualizados.

Mediante Directiva Nº009-2008-GG/OSIPTEL se aprueban las disposiciones para el "Uso y Seguridad de los Recursos Informáticos del OSIPTEL de conformidad con la Norma Técnica Peruana ISO/IEC 17999:2007 EDI "Código de Buenas Prácticas para la Gestión de la Seguridad de la Información", donde se establece que la institución deberá velar por brindar la seguridad adecuada a la información.

Mediante Adjudicación de Menor Cuantía Nº 109-2010/OSIPTEL se contrató el servicio de actualización de 367 licencias software de seguridad contra programas y tráfico de red malicioso.

OSIPTEL G.T.I.C.E. W. UGAZ

OSIPTEL G.T.I.C.E. F. ALVARADO

OSIPTEL G.T.I.C.E. J. RODRIGUEZ

Mediante Resolución de Gerencia General N°383-2010-GG/OSIPTEL de fecha 07 de octubre de 2010 se aprueba entre otros software la estandarización de Software de Seguridad McAfee.

Mediante Resolución de Presidencia N° 020 – 2011-PD/OSIPTEL de fecha 25 de febrero 2011 se aprueba el Plan Operativo Informático 2011, en el cual se considera el siguiente proyecto:

- Renovación de Soporte y Mantenimiento de Licencias de Software de Seguridad.

En este sentido se necesita proveer el servicio de renovación y soporte de 367 licencias y la adquisición de 57 licencias adicionales de software de seguridad para estaciones de trabajo y servidores del OSIPTEL.

7. DEFINICIÓN DEL PROBLEMA

Se requiere del servicio de renovación de soporte y mantenimiento de 367 licencias y la ampliación de 57 licencias de software de seguridad para estaciones de trabajo y servidores del OSIPTEL.

8. ANÁLISIS DE ALTERNATIVAS

Los productos actualmente licenciados del software de seguridad McAfee para estaciones de trabajo y servidores se detallan a continuación:

Nº	SOFTWARE	DESCRIPCIÓN	PRODUCTOS	CANTIDAD	FECHA INICIO SOPORTE	FECHA TERMINO SOPORTE
1	Software de Seguridad	McAfee Total Protection for Endpoint.[1]	VirusScan Enterprise Host Intrusion Prevention ePolicy Orchestrator GroupShield for Mail Servers SpamKiller for Mail Servers	367	16/06 /2010	15/06 /2011

El Osiptel es propietario del total de 367 licencias de software de seguridad (para estaciones de trabajo y servidores) McAfee y se desea la renovación del soporte de las 367 licencias y adicionar 53 licencias para crecimiento y futuras implementaciones de ODEs, con las características de acuerdo a las especificaciones técnicas[2].

La no renovación del servicio de mantenimiento es independiente de la continuidad de uso de los productos licenciados aun cuando no exista un contrato de soporte vigente. Por consiguiente, las alternativas a comparar son:

- **Renovación del servicio**. Bajo este escenario se puede obtener lo siguiente:

[1] Ver Anexo 1
[2] Ver Anexo 2

OSIPTEL G.T.I.C.E. W. UGAZ

OSIPTEL G.T.I.C.E. F. ALVARADO

OSIPTEL G.T.I.C.E. J. RODRIGUEZ

1. Con esto se aseguraría la información contenida en los servicios informáticos (sistema operativo, bases de datos, correo electrónico, aplicaciones, web, etc) en caso de ataque por virus informático en cualquiera de sus presentaciones (malware, spyware, troyano, etc.) mediante el acceso a soporte garantizando, actualización del producto, acceso a parches de seguridad y nuevas funcionalidades de los productos licenciados.

2. Obtener de manera eficiente y con menor costo el soporte de licenciamiento de 367 licencias de software de seguridad para estaciones de trabajo y servidores McAfee con las que cuenta el OSIPTEL, implicando esto el ahorro considerable por el pago de renovación del soporte y mantenimiento de un producto preexistente e incluir 53 licencias del mismo producto.

- **No renovación del servicio**. Bajo este escenario existe las siguientes posibilidades:

1. El riesgo de paralización de los sistemas de información en caso de ataque por virus informático en cualquiera de sus presentaciones (malware, spyware, troyano, etc.), generando una falta de garantía de recuperación efectiva y/o en el corto plazo de los servicios informáticos (sistema operativo, bases de datos, correo electrónico, aplicaciones, web, etc).

   Para poder acceder nuevamente al servicio de soporte una vez vencido el plazo de renovación, este se aplicaría a partir de la nueva fecha lo que generaría una demora en la aplicación de acciones correctivas en casos de contingencia.

2. La adquisición de un nuevo producto de software de seguridad con costos elevados por tratarse de una solución nueva, retraso en los tiempos considerando las instalaciones y configuraciones del nuevo producto, poniendo en alto riesgo los servicios (sistema operativo, bases de datos, correo electrónico, aplicaciones, web, etc.) y la información institucional.

9. ANÁLISIS COMPARATIVO TÉCNICO

Costos

a) Licenciamiento – El costo de renovación del servicio de soporte y actualización de software actualmente utilizado es el siguiente:

Proveedor	Producto	Nº Licencias	Costo
Bafing S.A.	**Endpoint Protection - Advanced Suite, (Crossgrade)+ Endpoint Protection - Advanced Suite, (Licencia Nueva)+ 03 años de McAfee Protect PlusGold Support**	420	S/82,110.30[3]

[3] Ver Anexo 3

OSIPTEL G.T.I.C.E. W. UGAZ

OSIPTEL G.T.I.C.E. E. ALVARADO

OSIPTEL G.T.I.C.E. J. RODRIGUEZ

SSG Peru S.A.C.	**McAfee Endpoint Protection - Advanced Suite –Crossgrade 1 year Support + McAfee Endpoint Protection - Advanced Suite new license 3 Years Support**	420	S/88,224.00[4]

b) Hardware necesario para su funcionamiento – La renovación de soporte no genera costos adicionales de equipamiento informático. Los productos licenciados se encuentran ya instalados y operativos.

c) Soporte y mantenimiento externo – El servicio a contratar es el de soporte y actualización de licencias con las características mencionadas en el literal a).

d) Capacitación – El servicio a contratar no genera costos adicionales en capacitación a usuarios. Información sobre el uso del servicio de soporte es provisto por McAfee a través de su sitio web.

Beneficios

Los beneficios obtenidos por la renovación del servicio son:

- Actualización de las versiones de todos los programas licenciados
- Versiones generales de mantenimiento
- Versiones determinadas de funcionalidad
- Acceso a la Web de soporte del Fabricante del Software de Seguridad.

10. CONCLUSIONES

El software de seguridad para estaciones de trabajo y servidores es requerido para proteger y preservar la información digital de la institución almacenada en medios electrónicos, asegurando su confidencialidad, integridad y disponibilidad, conforme a la Norma Técnica Peruana ISO/IEC 17799:2007

Se concluye que se requiere del servicio de renovación de 367 licencias e inclusión de 53 licencias de software de seguridad para estaciones de trabajo y servidores para garantizar la permanente disponibilidad de las versiones actualizadas del software.

[4] Ver Anexo 4

OSIPTEL G.T.I.C.E. W. UGAZ

OSIPTEL G.T.I.C.E. F. ALVARADO

OSIPTEL G.T.I.C.E. J. RODRIGUEZ

11. FIRMAS

OSIPTEL G.T.I.C.E. W. UGAZ

WINSTON UGAZ CACHAY
ADMINISTRADOR DE RED Y COMUNICACIONES

OSIPTEL G.T.I.C.E. J. RODRIGUEZ

JUAN RODRÍGUEZ CALDERÓN
TÉCNICO EN REDES E INFORMÁTICA

OSIPTEL G.T.I.C.E. F. ALVARADO

FREDDY ALVARADO VARGAS
GERENTE DE TECNOLOGÍAS DE LA INFORMACIÓN, COMUNICACIONES Y ESTADÍSTICA

OSIPTEL G.T.I.C.E. W. UGAZ

ANEXO 1 Carta de Concesión McAffe Inc para OSIPTEL

McAfee® Product Grant Letter

Carta de concesión de producto de McAfee, Inc. para Osiptel

Estado de la Carta: Final

IMPORTANTE: Esta carta constituye la autorización de sus productos de asistencia o licencia de McAfee. Es aconsejable que la conserve. Necesitará el número de concesión que aparece a continuación para poder recibir los servicios de asistencia.

Número de Concesión: 3978281-NAI
Número de Cuenta del Cliente: 636482

SKU / Descripción	Cantidad	Término de Asistencia o Licencia / Nivel de Asistencia	Número de serie de MFG / PRODUCTO	Estado
TENYFM-AA MFE Total Prtxn for Endpoint 1Yr GL[P+]	200	JUN/16/10 - JUN/15/11 GOLD		Delivered
TENYFM-AA MFE Total Prtxn for Endpoint 1Yr GL[P+]	167	JUN/16/10 - JUN/15/11 GOLD		Delivered

Esta carta de autorización de licencia contiene la confirmación de su adquisición de servicios de asistencia técnica o productos de McAfee, además de constituir una forma de acceso a la descarga electrónica de servicios de asistencia técnica y productos de software con licencia.

Esta concesión de autorización de licencia forma parte de la "Documentación" de los servicios de asistencia técnica y/o de los productos y, como tal, está incorporada en el contrato de licencia y en el contrato de asistencia técnica celebrado entre McAfee, Inc. y su organización.

La guía del servicio de asistencia técnica Gold incluye instrucciones sobre cómo plantear casos de asistencia, así como las ventajas de la asistencia Gold. Consúltela en:
http://www.mcafee.com/us/local_content/datasheets/gold_support_user_guide.pdf

Para obtener una descripción completa de la Política de mantenimiento de productos McAfee, visite este sitio Web: http://www.mcafee.com/us/enterprise/support/technical_support/maintenance_policy.html

Para obtener una descripción completa de la política de ciclo de vida de los productos McAfee, visite el sitio Web http://www.mcafee.com/us/enterprise/support/customer_service/end_life.html

OSIPTEL G.T.I.C.E. W. UGAZ

OSIPTEL G.T.I.C.E. F. ALVARADO

OSIPTEL G.T.I.C.E. J. RODRIGUEZ

ANEXO 2 *Especificaciones Técnicas*

TÉRMINOS DE REFERENCIA

"SERVICIO DE ACTUALIZACIÓN DE SOFTWARE DE SEGURIDAD MCAFFE"

1. ANTECEDENTES

OSIPTEL necesita contar con el soporte adecuado para la gestión eficiente del software de seguridad contra programas y tráfico de red maliciosos, el cual es imprescindible para mantener la seguridad de la información y las redes de comunicaciones de datos, libres de programas y tráfico de red dañinos, como los virus, spam, spyware, entre otros.

OSIPTEL actualmente cuenta con 367 licencias de uso de la solución de software de seguridad Suite McAfee Total Protection For End Point, la cual cuenta con los siguientes productos:

- VirusScan Enterprise 8.8.0i
- Desktop Firewall (Host Intrusion Prevention 6.1.0)
- ePolicy Orchestrator 6.0.2
- GroupShield for Mail Servers 6.0.2
- WebShield SMTP 4.5
- SpamKiller for Mail Servers 2.1.2
- Consola EPO 4.0

De acuerdo a la Norma Técnica Peruana ISO/IEC 17799:2007 EDI. "Código de Buenas Prácticas para la Gestión de la Seguridad de la Información", aprobada con Resolución Ministerial N° 246-2007-PCM, a la Política de Seguridad de la Información de OSIPTEL aprobada con Resolución de Gerencia General Nº 343-2006-GG/OSIPTEL y de conformidad a la Directiva del Uso y Seguridad de los Recursos Informáticos Nº009-2008-GG/OSIPTEL, la institución debe velar por brindar la seguridad adecuada a la información, por tal motivo se necesita contar con una adecuada solución de software de seguridad, que se encuentre permanentemente actualizada y con el respectivo soporte y mantenimiento que garantice la protección de la información y de los sistemas informáticos de la institución.

Asimismo mediante Resolución de Gerencia General N°383-2010-GG/OSIPTEL se estandariza el software institucional, la cual contiene entre otros el software de seguridad McAfee como producto de software estandarizado en el OSIPTEL.

2. OBJETIVO

Proteger y preservar la información digital de la institución almacenada en medios electrónicos, asegurando su confidencialidad, integridad y disponibilidad, conforme a la Norma Técnica Peruana ISO/IEC 17799:2007.

OSIPTEL G.T.I.C.E. W. UGAZ

OSIPTEL G.T.I.C.E. F. ALVARADO

OSIPTEL G.T.I.C.E. J. RODRIGUEZ

3. FINALIDAD PÚBLICA

Es necesaria la contratación del Servicio de actualización de software de seguridad McAffe, a fin de salvaguardar la información digital institucional asegurando su confidencialidad, integridad y disponibilidad, conforme a la Norma Técnica Peruana ISO/IEC 17799:2007, esto permitirá cumplir con el normal desempeño de las labores de los funcionarios del OSIPTEL, cuya labor está enfocada en la atención de temas referentes a: regulación, supervisión, fiscalización, emisión de normas, solución de controversias y atención de usuarios de telecomunicaciones en las distintas regiones del país.

4. ESPECIFICACIONES TÉCNICAS DEL SERVICIO

El servicio debe incluir la renovación de soporte y mantenimiento de 367 licencias de software de seguridad McAffe más 53 licencias adicionales (en total: 420 licencias de software de seguridad McAffe con las siguientes características:

3.1 Protección de Estaciones de Trabajo (clientes) y Servidores

El software de seguridad debe ser compatible con los sistemas operativos utilizados en el Osiptel: MS Windows a nivel cliente y servidores, Linux que incluya sistemas de 32 y 64 bits.

3.2 Función Antivirus

La función antivirus debe incluir como mínimo lo siguiente:

Permita detener la acción y eliminar proactivamente el software malicioso, extender la cobertura contra nuevos riesgos de seguridad y reduzca el tiempo de respuesta frente a epidemias. La tecnología de protección debe identificar amenazas nuevas y desconocidas.

Permita combinar tecnologías avanzadas para la prevención de intrusos, firewall y antivirus, abarcando una gran variedad de amenazas, a través de la detección heurística y genérica, que encuentre virus nuevos y desconocidos, incluso aquellos que están ocultos en archivos comprimidos.

Permita buscar exploits conocidos que atacan a las aplicaciones y servicios bloqueando amenazas que aprovechan la codificación de aplicaciones en lenguajes de programación más usados.

Permita defender los sistemas contra virus, buffer overflows (o desbordamientos de buffer) y ataques combinados.

Permita bloquear las amenazas que no escriben en el disco duro con el escaneo en memoria.

Permita evitar que se instalen rootkits y archivos ocultos.

OSIPTEL G.T.I.C.E. W. UGAZ

OSIPTEL G.T.I.C.E. F. ALVARADO

OSIPTEL G.T.I.C.E. J. RODRIGUEZ

Permita ser administrado por una consola de administración centralizada vía Web.

Permita bloquear una amplia gama de virus y amenazas de código malicioso, incluso los que están ocultos en archivos comprimidos; que descubra virus desconocidos con detección heurística y genérica.

Permita limitar el daño provocado por contagios, incluso antes de la emisión de archivos DAT; cerrar los puertos, monitorear aplicaciones y motores de correo electrónico, bloquear archivos y directorios, efectuar seguimientos y bloquear las fuentes de infección.

Permita detectar amenazas que se escriben en la memoria en lugar de hacerlo en el disco (como CodeRed y SQLSlammer)

Permita detectar y limpiar virus en cliente de correo electrónico usado en el Osiptel (cliente para Microsoft Exchange) e inclusive texto HTML y archivos adjuntos.

Permita evitar que se ejecuten amenazas que aprovechan código como java script o visual basic.

Permita adaptar las actualizaciones en terreno a ubicaciones físicas y velocidades de conexión: reanudará la actualización después de que se restablezca una conexión interrumpida.

Permita evitar que los archivos del antivirus sean modificados a través de las reglas de protección de acceso mejoradas.

Permita escanear la memoria del sistema para encontrar rootkits ya instalados, procesos ocultos y otros códigos maliciosos ocultos

3.3 Función AntiSpyware

La función antispyware debe incluir como mínimo lo siguiente:

Permita detectar los programas espía, bloqueando los programas espía antes de que se instalen y se extiendan, usando una tecnología de exploración en el momento del acceso de AntiSpyware.

Permita buscar y detener los programas espía desconocidos, con la finalidad de que no se quede esperando a recibir los archivos de firmas actualizados de programas espías; deberá usar una tecnología basada en comportamiento de AntiSpyware detectando y bloqueando los programas espía desconocidos basándose en su forma de actuar.

Permita realizar la exploración en el momento del acceso, detectando y bloqueando los programas espía antes de que se instalen y se extiendan; que explore los procesos y archivos que se ejecutan en memoria para neutralizarlos.

OSIPTEL G.T.I.C.E. W. UGAZ

OSIPTEL G.T.I.C.E. F. ALVARADO

OSIPTEL G.T.I.C.E. RODRIGUEZ

Permita realizar la detención eficiente de programas espía y virus, con la finalidad de detener tanto los programas espía como los virus integrando antispyware y antivirus en un mismo modulo; ambos programas deberán compartir un único procesador de exploración que permite reducir la sobrecarga del sistema y mejorar su rendimiento.

Permita efectuar la exploración y detección de programas espía en el registro y los archivos, bloqueando la molesta reinstalación de programas espía, para lo cual el antispyware debe explorar tanto las entradas del registro como los archivos y, con ello, eliminar las principales amenazas contra la seguridad y los anuncios emergentes.

Así mismo la funcionalidad AntiSpyware debe integrarse en el mismo software antivirus y no con programas o software adicional, además de reportar gráficamente la actividad de los componentes.

Incluya un Sistema de bloqueo de tráfico en puertos de entrada y/o salida por reglas predefinidas de fabrica y reglas adicionales definidas por el administrador.

Incluya un Sistema de aseguramiento de archivos, carpetas y elementos compartidos (shares), que permita reestablecer y/o aumentar el nivel de seguridad de los permisos afines a éstos en todos los equipos, asimismo debe prohibir el acceso local y remoto a determinadas áreas del computador.

Incluya un Sistema de protección contra desbordamiento de buffer (conocido como buffer overflow) que permita proteger de manera proactiva al Kernel del sistema operativo contra exploits o ataques informáticos conocidos y desconocidos a través de vulnerabilidades del sistema operativo o software afines.

Incluya un Sistema de detección, eliminación y/o envío a cuarentena spyware (programas espía, propaganda, otros) a través de reglas y listas predefinidas y/o personalizadas por el administrador.

3.4 Consola de Administración

La Consola de Administración debe incluir como mínimo lo siguiente:

La consola deberá permitir ser administrada vía web.

Permita desplegar, actualizar, administrar y dar soporte a la plataforma antivirus y de seguridad que debe efectuar a través de una consola de gestión de políticas de seguridad y antivirus que cubra tanto los elementos locales como remotos y móviles, incluyendo estaciones de trabajo, servidores de grupo, aplicación, y servidores de correo electrónico.

Permita que las actualizaciones se realicen de forma incremental y automática.

La consola de administración debe estar basada en una arquitectura jerárquica (dominios, grupos de elementos, elementos, otros) que permita un esquema distribuido de repositorios de instalación, que permitan un ahorro de ancho de banda a

OSIPTEL G.T.I.C.E. W. UGAZ

OSIPTEL G.T.I.C.E. J. RODRIGUEZ

OSIPTEL G.T.I.C.E. F. ALVARADO

nivel local y nacional mientras se efectúen labores de instalación, actualización y soporte.

Permita que las labores de instalación, despliegue o desinstalación no deban requerir la movilización de personal técnico hacia la estación de usuario final o equipo alguno de la red. Esta debe realizarse de forma totalmente remota desde la consola de administración, reconociendo a los equipos por su dirección o rango de direcciones IP, nombre, pertenencia a dominio, cuenta de correo electrónico, lista plana.

La consola debe permitir monitorear las estaciones de trabajo activas e inactivas de la totalidad de la red y además permitir tomar acciones en caso se detecte una estación con virus.

En caso de encontrar equipos que no cumplan con la política de seguridad establecida, que sean vulnerables o se encuentren infectados, deberá tomar las acciones necesarias para subsanar éstas deficiencias de seguridad. Asimismo, se deberá efectuar análisis en demanda de los equipos en busca de virus.

Debe permitir la configuración basada en las políticas de seguridad antivirus default o a ser desarrolladas por el Osiptel que deberá ser desplegada a toda la red. El despliegue de configuraciones deberá ser programable o activado por el administrador.

Debe permitir la recepción de los archivos de actualización se deberá efectuar a través de Internet con el fin de ponerlas a disposición de los administradores o del software involucrado para su despliegue.

Debe permitir actualizaciones, obtenida directamente de los sitios disponibles por el fabricante o a través del proveedor, cada hora, día o semanalmente, y ser aplicadas a cada uno de los productos. Las actualizaciones deberán ser totalmente constantes y auditables.

Debe permitir la lectura del estado de los equipos en forma automática y así como programada o activada por el administrador. La consola de administración deberá mantener una base de datos interna o externa en la cual se almacenará en tiempo real toda la información relacionada a actividad en la plataforma de seguridad y antivirus (despliegue, instalación, actualización, monitoreo).

Debe permitir la ejecución de reportes individuales y personalizados, relacionados a equipos y archivos afectados.

La consola deberá recoger en la base de datos otra información sobre los equipos que conforman la plataforma antivirus como CPU (velocidad y tipo), memoria, espacio total y disponible de discos duros, directorios de instalación de archivos de sistema, versiones de sistema operativo y niveles de parche, usuarios que ingresaron al sistema, entre otros, que también podrán ser materia de reporte.

Debe incluir un sistema de umbrales de seguridad que responderán con alertas emitidas por SNMP, e-mail, SMS, pager. Toda acción de la consola de administración central deberá ser totalmente transparente para el usuario final o escrita en la bitácora de funcionamiento.

OSIPTEL G.T.I.C.E. W. UGAZ

OSIPTEL G.T.I.C.E. V. RODRIGUEZ

OSIPTEL G.T.I.C.E. F. ALVARADO

La comunicación debe realizarse entre el sistema central ubicado en un servidor y agentes de comunicación instalados en los equipos. Este agente realizará tareas de gestión de políticas de seguridad, actualización de productos antivirus y envío de información hacia sistema central (éstas tareas se realizan bajo programación y configuración).

Permita el bloqueo de carpetas compartidas.

La consola deberá permitir bloquear puertos de comunicación para combatir epidemias. Así como también crear políticas de denegación de escritura en forma centralizada para evitar epidemias.

La consola de administración debe tener la capacidad de seguir o hacer un "trace" de los equipos de la red que se encuentren infectados y tener la capacidad de bloquear equipos remotamente no permitiéndoles mayor comunicación con la red.

Debe permitir la activación de múltiples modalidades de actualización incluyendo transmisión http, ftp o por UNC.

Debe poseer un módulo que reporte el estado de actualización de los parches de seguridad relacionados a Microsoft, a través de un sistema de reportes gráficos y una base de datos de información de las mejoras de seguridad disponibles.

Debe poseer un modulo que permita verificar y reportar el estado de distintas anomalías de seguridad según políticas predefinidas y personalizables por el usuario, por ejemplo, falta de parches, software de seguridad, entre otros.

Debe poseer tecnología de cliente – servidor a través de un agente, que recoja información del software y hardware de la PC guardándolo dentro de la base de datos(Sistema Operativo, Versión de sistema operativo, Número de Service Pack, Memoria RAM, Discos, Unidades lógicas de disco, Espacio total de disco, Espacio libre de disco, Dirección IP de la PC., etc)

Debe ser compatible con servidor de correo electrónico Microsoft Exchange y que soporte configuración en cluster. Asimismo que se integre como un servicio más del sistema de correo electrónico con las siguientes funcionalidades: Análisis en acceso, Análisis en demanda, Análisis en segundo plano, Análisis proactivo, Subsistema de prevención de brotes de virus y filtrado de contenido.

3.5 Detección y Prevención de Intrusos

La Detección y Prevención de intrusos debe incluir como mínimo lo siguiente:

Protección completa de los equipos, que incluya tres capas de protección (reglas de comportamiento, análisis de firmas y protección mediante firewall) que impidan las intrusiones, protejan los activos y salvaguarden los equipos de sobremesa y los portátiles. Que proteja los sistemas de escritorio contra ataques desconocidos. Y que sea fácil gestionar todos los equipos de sobremesa, sin tener en cuenta su ubicación, desde una única consola centralizada.

OSIPTEL G.T.I.C.E. W. UGAZ

OSIPTEL G.T.I.C.E. J. RODRIGUEZ

OSIPTEL G.T.I.C.E. E. ALVARADO

Protección de los equipos.- la cual gestione centralmente y que sea escalable, de modo que puede desplegarlo en toda la institución para obtener una protección global completa compatible y en varios idiomas.

Protección de vulnerabilidades, donde la actualización automática del contenido de seguridad tenga como objetivo vulnerabilidades específicas reconozca los ataques por vulnerabilidad desconocidos y evite que se ejecuten; las actualizaciones del contenido de seguridad no debe permitir el reinicio el sistema.

Evite problemas de desbordamiento del búfer, el cual utilice una tecnología de intrusión del host para evitar ataques de desbordamiento del búfer, dado que es uno de los métodos de ataque a computadoras personales más comunes.

Bloqueo sistemas USB extraíbles, con la finalidad de permitir bloquear el uso de sistemas USB extraíbles, se pueda impedir la entrada inadvertida de virus o gusanos en los equipos de sobremesa, reducir el robo de datos y aplicar las políticas de bloqueo de la institución.

Protección de firewall de computadoras personales, permitiendo que los firewall de computadoras personales puedan aplicar diferentes políticas de firewall según la conexión de su sistema a la red, permitir poner en cuarentena los sistemas incompatibles a medida que intentan conectar con la red y bloquear puertos del sistema.

3.6 Sistema de clasificación intuitivo

El Sistema de Clasificación intuitivo de intrusos debe incluir como mínimo lo siguiente:

Herramienta que permita navegar y buscar en la web de forma segura y mantenerse alejado de amenazas como programas espía, programas publicitarios, timos de phishing, etc. Que añada otra capa de protección a la vez que educa a los usuarios acerca de los peligros de navegar por Internet.

Proteger contra el software dañino basado en la web como el software publicitario, el software espía, los virus y las estafas por robo de identidad y que convierta las búsquedas y la navegación por la web en una actividad más segura.

Consola de administración, fácil de implantar, que indique qué equipos tienen instalado el producto.

Evitar que se navegue involuntariamente en paginas peligrosas cuando haga búsquedas en internet (como: Google, Yahoo MSN, AOL o Ask.com, etc.) Obteniendo una valoración de seguridad al lado del resultado de la búsqueda.

El sistema de valoración deberá estar basado en códigos de colores que permita identificar qué sitios son seguros y cuáles son peligrosos; con lo cual se identifica si el sitio que está explorando el usuario está libre de amenazas.

Avisos por adelantado que informen acerca de los sitios web dañinos, de modo que evitará correr riesgos innecesarios.

OSIPTEL G.T.I.C.E. W. UCAÑAN

OSIPTEL G.T.I.C.E. J. RODRIGUEZ

OSIPTEL G.T.I.C.E. F. ALVARADO

Señales tipo semáforo deben alertar de posibles amenazas en las páginas que visite el usuario.

Facilidad para probar los sitios para detectar un número excesivo de menús emergentes, prácticas fraudulentas y aprovechamiento de debilidades, como el software publicitario y el software espía, así como enlaces ocultos a otros sitios web dañinos.

Permita a través de un clic obtener un perfil de amenazas completo de cada sitio, incluida información acerca de cuántos correos electrónicos recibirá al mes si se registra, críticas de usuarios y molestias.

Permita ser utilizado como complemento de los navegadores usados en el OSIPTEL.

3.7 Características globales de los productos de forma independiente

a) Consola interna de productos

Todos los productos de la solución (antivirus, antispyware, etc) deberán incluir una consola propia que pueda ser configurada independientemente de la solución de gestión e incluir tareas de actualización, análisis en demanda, configuración de análisis en acceso, entre otros.

b) Actualización independiente de productos

La actualización del producto deberá efectuarse de forma independiente o "stand alone" a través de:

Una consola interna que permita mantener actualizados los productos (actualización de archivos de firma de virus y actualización de versión del software motor para todos los productos de la solución antivirus) en los clientes y servidores mediante una conexión a Internet o desde un computador previamente designado (http, ftp, UNC, ruta local o puerto definido) y de forma automática y programada o cuando el usuario lo active.

Archivos ejecutables que permita mantener actualizados los productos (actualización de archivos de firma de virus y actualización de versión del software motor para todos los productos de la solución antivirus) en los clientes y servidores mediante la ejecución de éstos de manera local.

c) Sistema de alertas independiente

Este sistema deberá especificar qué tipo de alerta emitir cuando se detecta en virus. Asimismo deberá permitir enviar una alerta de usuario, alerta por la red a otros usuarios o al administrador, alertas vía correo electrónico, así como una alerta del tipo DMI, como también la visualización de mensajes especiales de alerta y/o la ejecución de alerta sonoros. Asimismo, el sistema de alertas deberá tener la capacidad de ser administrado centralmente.

d) Sistema de reportes independiente

Este sistema deberá tener la capacidad de generar reportes locales en cada equipo referentes a todas las transacciones realizadas por cada producto. Este reporte deberá permitir ser almacenado en cualquier unidad de disco local o remota y la

OSIPTEL G.T.I.C.E. W. UCAT

OSIPTEL G.T.I.C.E. J. RODRIGUEZ

OSIPTEL G.T.I.C.E. T. ALVARADO

longitud límite de reporte es configurable por el usuario. Las actividades a registrar en el reporte, bitácora o "log" puedan ser configurables previamente.

3.8 Control de Dispositivos Removibles

El Control de Dispositivos Removibles debe incluir como mínimo lo siguiente:

Permita vigilar y regular la transferencia de datos por parte de los usuarios a dispositivos extraíbles, como unidades USB, reproductores MP3, CD, DVD y dispositivos Bluetooth, aunque los usuarios no estén conectados a la red de la empresa.

Permita especificar filtrado, vigilancia y bloqueo detallados de los datos confidenciales, basados en hardware y en contenidos, en cualquier dispositivo de almacenamiento extraíble; asegurar de que los usuarios sigan usando de forma segura los dispositivos permitidos.

La administración centralizada que defina, despliegue, administre y actualice centralmente a través de la consola administrativa las directivas y agentes de seguridad en todo su entorno; permita establecer directivas de dispositivos y datos por usuario, grupo o departamento, impidiendo la fuga de información clasificada como confidencial.

Permita supervisar los incidentes en tiempo real y que genere informes detallados para demostrar el cumplimiento de los requisitos de las normativas y directivas internas relativas a la protección de la intimidad ante auditores, miembros de la junta directiva y demás interesados.

Permita la gestión integral de dispositivos y datos, supervisando la copia de datos por parte de los usuarios de la red a unidades USB, iPods, CD y DVD grabables, dispositivos Bluetooth e infrarrojos, equipos de imagen, puertos COM y LPT, etc.; bloqueando los intentos de copia que infrinjan las directivas y que proteja todos los formatos de datos, aunque se hayan modificado.

Permita especificar qué dispositivos se pueden usar y cuáles no en función de cualquier parámetro de dispositivo del sistema operativo, como identificación de producto, identificación de proveedor, número de serie, clase de dispositivo y nombre de dispositivo; para los dispositivos que se pueden usar, especifique qué contenidos se pueden copiar y cuáles no en esos dispositivos.

Permita la generación de informes y de auditoría, que contribuya a lograr el cumplimiento con un registro detallado a nivel de usuario y de dispositivo; recoja detalles tales como dispositivo, fecha y pruebas de datos para unas auditorías puntuales y correctas

3.9 Control de Acceso a la Red

El Control de Acceso a la Red debe incluir como mínimo lo siguiente:

OSIPTEL G.T.I.C.E. W. UGAZ

Permita reducir el riesgo a través de un control de acceso a la red integral aplicable en todos los tipos de métodos de acceso a red y para todos los tipos de dispositivos: sistemas gestionados por Osiptel, sistemas invitados sin gestionar y sistemas de acceso remoto.

Permita proteger la información digital contra las últimas amenazas, además de imponer el cumplimiento de normativas; que se integre con la solución de seguridad antivirus, para crear una solución integral gestionada desde una única consola centralizada.

Permita aplicar el cumplimiento de normativas cuando los sistemas intenten entrar en la red; minimizando la congestión de la red producida por amenazas introducidas por diversos sistemas infectados, de modo que mantenga un adecuado nivel de continuidad de la red.

Permita la gestión de parches automática que facilite el cumplimiento de normas aplicando los parches a los sistemas incompatibles cuando intenten acceder a la red.

Permita supervisar a usuarios móviles, con mucha rapidez y facilidad con la finalidad de mantener un alto nivel de rendimiento y disponibilidad de la red; sólo podrán entrar los sistemas compatibles, de modo que la red se mantenga en funcionamiento y sea segura para todos los usuarios.

Permita descubrir sistemas administrados y no administrados, no compatibles que podrían provocar daños en la red y los usuarios.

Permita realizar comprobaciones exhaustivas del sistema, evaluando con rapidez y sencillez el cumplimiento de los sistemas no administrados en cuarentena con un agente a demanda.

Permita obtener una imposición de políticas incorporadas para los sistemas administrados y no administrados conectados local o remotamente (LAN, WAN, IPSec, VPN o SSL).

Permita administrar y controlar el acceso a la red, mediante una única consola de administración que defina políticas y genere informes de forma centralizada de las comprobaciones de cumplimiento erróneas y de las acciones de reparaciones en la consola.

Incluya opciones de reparación automática y que permita remitir a los usuarios a un portal de reparaciones en el que el administrador puede recomendar una acción específica.

3.10 Auditoría de políticas.

La auditoría de políticas debe incluir como mínimo lo siguiente:

Permita utilizar plantillas de directivas predefinidas que demuestran el cumplimiento de las principales normativas del sector y de las directivas internas (como por ejemplo:

OSIPTEL G.T.I.C.E. F. ALVARADO

OSIPTEL G.T.I.C.E. J. RODRIGUEZ

OSIPTEL G.T.I.C.E. M. UGAZ

DSS del PCI, SOX, GLBA, HIPAA y FISMA), y de los marcos de buenas prácticas ISO 27001 y COBIT. Incluya un panel PCI creado que ofrezca una visión consolidada del estado de cumplimiento por requisito/control del PCI.

Permita utilizar la consola McAfee ePolicy Orchestrator (ePO) para reducir el costo de propiedad al consolidar la administración de la seguridad de los endpoints y la administración del cumplimiento, facilitando el despliegue de agentes, la administración y los informes.

Permita crear reglas a partir de cualquier lenguaje de secuencias de comandos (VBScript, archivos por lotes, Perl, Python, etc) compatible con el sistema sometido a auditoría para ampliar las funciones de comprobación.

Permita establecer la frecuencia de la captura de datos para apoyar informes automatizados con datos precisos.

Permita descargar puntos de referencia de sitios fidedignos, permitiendo ver en cuestión de minutos, una orientación de seguridad detallada para confirmar el cumplimiento de las normativas o diseñar sus propias directivas internas de gobernanza basándose en las buenas prácticas de la comunidad de la seguridad.

5. CONFIGURACIÓN Y CAPACITACIÓN

La definición de la arquitectura de la solución del software de seguridad McAffe configurarse e implementarse, la instalación piloto inicial (instalación conjunta de los productos en un grupo de equipos) y el control de calidad del producto deberán estar incluidos.

Charla técnica para la instalación, administración y solución de problemas relacionados a la solución para el personal que administrará la plataforma antivirus con entrega de certificado de capacitación (01 charla de 4 horas efectivas – entregar certificado de educación)

6. SOPORTE TÉCNICO

Debe incluir el Soporte técnico On-Line, a través del Soporte Técnico por el periodo contratado, a cargo de personal propio certificado y especializado. Este soporte técnico se brindara a través de comunicación electrónica como e-mail y medios de telefonía fija o celular y tiene por objetivo absolver consultas técnicas y dar soporte a incidentes reportados.

El postor deberá incluir dentro de su propuesta técnica una carta de representación emitida por el FABRICANTE y dirigida a OSIPTEL, vigente a la fecha de presentación de la Propuesta, en donde indique que están autorizados a comercializar el producto así como contar con el soporte técnico autorizado de la marca y brindar soporte técnico con personal certificado por el fabricante.

Debe incluir asimismo el Soporte técnico telefónico, a través del servicio y soporte telefónico a la sede central y asegurar el seguimiento de solicitudes de soporte técnico hasta su completa resolución mediante sistemas de Help Desk.

OSIPTEL G.T.I.C.E. RODRIGUEZ

OSIPTEL G.T.I.C.E. W. LIGAZ

OSIPTEL G.T.I.C.E. F. ALVARADO

La Solución de seguridad McAffe, deberá contar con un servicio de Soporte Telefónico Gratuito brindado por el mismo fabricante, a través de una línea 0800, y en el idioma español (Adjuntar carta emitida por el fabricante, donde indica el soporte 0800).

7. PERFIL DE LA EMPRESA

Experiencia mínima de dos años en la venta y/o actualización de la solución de software de seguridad McAffe.

Experiencia en la venta y/o actualización de la solución de software de seguridad, por lo menos en 5 instituciones o empresas.

8. DURACIÓN DEL SERVICIO

El servicio tendrá una duración de 03 años, a partir del 16 de Junio del 2011 hasta el 15 de Junio del 2014.

9. PLAZO DE ENTREGA

El plazo máximo de entrega de la licencia del software de seguridad McAffe será de 10 días calendarios contados a partir del día siguiente de emitida la orden de servicio por parte del OSIPTEL.

El postor deberá entregar la licencia del software y la información de acceso de solicitud y/o descarga a los medios de instalación del software adquirido a OSIPTEL.

El Postor deberá entregar por mesa de partes de la institución la documentación necesaria y la carta dirigida a OSIPTEL (Anexo A) que acredite que se le otorga al ORGANISMO SUPERVISOR DE INVERSIÓN PRIVADA EN TELECOMUNICACIONES la licencia de uso del software adquirido.

10. CONFORMIDAD

El OSIPTEL, a través de la Gerencia de Tecnología de la Información, Comunicaciones y Estadística, es el responsable de efectuar la verificación de la documentación de la licencia adquirida. Para ello deberá dar conformidad de acuerdo a los parámetros establecidos en el presente documento para su respectivo pago.

11. FORMA DE PAGO

La forma del pago del servicio se realizará en tres (03) pagos, a razón de pago anual efectuado al inicio del año cubierto por el mantenimiento.

OSIPTEL G.T.I.C.E. W. UGAZ

OSIPTEL G.T.I.C.E. F. ALVARADO

OSIPTEL G.T.I.C.E. J. RODRIGUEZ

ANEXO A.- Formato de Carta de Acreditación de Licencias de software

Logo Empresa

Lima, fecha

Señores
ORGANISMO SUPERVISOR DE INVERSIÓN PRIVADA EN TELECOMUNICIONES-OSIPTEL.
Presente.-

Referencia: Entrega de Licencia de Software de Orden de Compra/ Servicio NºXXX

De nuestra consideración:
Habiendo recibido la Orden de Compra/Servicio de la referencia, tenemos a bien hacer entrega de la licencia, conforme en lo solicitado en la orden de compra/servicio.

Fabricante	Descripción	Cantidad

Por lo que se deja constancia que el ORGANISMO SUPERVISOR DE INVERSIÓN PRIVADA EN TELECOMUNICACIONES-OSIPTEL es propietario de:

Nombre de Software :
Cantidad :
Número de Autorización :
Número de Licencia/ Cuenta :
Fecha de Inicio de Soporte :
Fecha de Vencimiento de Soporte :

Para cualquier consulta o información adicional agradeceré estar en contacto a la siguiente dirección de correo electrónico nombre@dominioempresa.xx y/o al teléfono N° ######.

Sin otro particular y agradeciendo su atención a la presente, me despido cordialmente.

.....
Nombre Gerente o Representante Legal
Nombre de Empresa

OSIPTEL G.T.I.C.E. W. UGAZ

OSIPTEL G.T.I.C.E. L. RODRIGUEZ

OSIPTEL G.T.I.C.E. F. ALVARADO

ANEXO 3 *Cotización Empresa BAFING S.A.C.*

BAFING S.A.C.

McAfee SecurityAlliance ElitePartner

PROPUESTA ECONÓMICA

McAfee Endpoint Protection - Advanced Suite		
Descripción	Precio Unitario	Precio Total
Endpoint Protection - Advanced Suite, (Crossgrade) ○ PartNumber: EPACDE-DA-EA + EPAYKM-AA-EA ○ 367 licencias ○ Incluye 03 años de McAfee Protect PlusGold Support	160.00	58,720.00
Endpoint Protection - Advanced Suite, (Licencia Nueva) ○ PartNumber: EPACDE-AA-EA + EPAYKM-AA-EA ○ 53 licencias Incluye 03 años de McAfee Protect PlusGold Support	205.00	10,865.00
	Sub Total S/.	69,585.00
	IGV 18%	12,525.30
	TOTAL S/.	82,110.30

Los precios están expresados en Nuevos Soles

COBERTURA DE LA PROPUESTA

Plazo de entrega: La licencia de software entrega en 05 días.
Vigencia de la propuesta: La presente propuesta tiene una vigencia de 30 días.

OSIPTEL G.T.I.C.E. W. HUGAZ

OSIPTEL G.T.I.C.E. RODRIGUEZ

OSIPTEL G.T.I.C.E. F. ALVARADO

ANEXO 4 *Cotización Empresa SSG Perú S.A.C.*

SSG PERU S.A.C.
SOLUCIONES DE SEGURIDAD Y GESTION
SEGURIDAD INFORMATICA
VENTAS DE COMPUTADORAS
IMPRESORAS - PARTES Y PIEZAS
SUMINISTROS Y UTILES DE OFICINA
CONSULTORIAS - PAGINAS WEB

PROPUESTA ECONOMICA

PartNumber	Descripción	Cant.	Precio Unitario S/.	Precio Total S/.
EPACDE-DA-EA EPAYKM-AA-EA	**McAfee Endpoint Protection - Advanced Suite – Crossgrade 3 years Support** LICENSE: Per Node. DELIVERABLE: Download. PRODUCT CONTENT: Desktops: VirusScan Enterprise, VirusScan Command Line for DOS & Unix, Anti-Spyware Enterprise, Host Intrusion Prevention with integrated Firewall for Desktops, Device Control, SiteAdvisor Enterprise Plus & Web Filtering for Endpoint. Servers: VirusScan Enterprise & Anti-Spyware Enterprise. Groupware: McAfee Security for Email Servers with Anti-Spam for Microsoft Exchange and Lotus Domino. Compliance: Network Access Control, Policy Auditor for Desktop. Management: ePolicy Orchestrator. Designed for organizations of any size who require advanced endpoint protection, policy compliance and network access control.	367	204.00	74,868.00
EPACDE-AA-EA EPAYKM-AA-EA	**McAfee Endpoint Protection - Advanced Suite new license 3 years Support** LICENSE: Per Node. DELIVERABLE: Download. PRODUCT CONTENT: Desktops: VirusScan Enterprise, VirusScan Command Line for DOS & Unix, Anti-Spyware Enterprise, Host Intrusion Prevention with integrated Firewall for Desktops, Device Control, SiteAdvisor Enterprise Plus & Web Filtering for Endpoint. Servers: VirusScan Enterprise & Anti-Spyware Enterprise. Groupware: McAfee Security for Email Servers with Anti-Spam for Microsoft Exchange and Lotus Domino. Compliance: Network Access Control, Policy Auditor for Desktop. Management: ePolicy Orchestrator. Designed for organizations of any size who require advanced endpoint protection, policy compliance and network access control.	53	252.00	13,356.00
			TOTAL S/.	88,224.00

CONDICIONES COMERCIALES

Cuenta Corriente US$: Banco Continental: 0011-0162-0100022348 a nombre de SSG PERU SAC.
Los precios están expresados en Nuevos Soles
Los Precios incluyen el 18% del IGV.
Plazo de entrega: La licencia de software entrega en 03 días calendario.
Vigencia de la propuesta: La presente propuesta tiene una vigencia de 30 días.

OSIPTEL G.T.I.C.E. W. UGAZ

OSIPTEL G.T.I.C.E. J. RODRIGUEZ

OSIPTEL G.T.I.C.E. R. ALVARADO