MUNICIPALIDAD DE LA MOLINA

INFORME TECNICO

ADQUISICION DE UNA SOLUCION DE SEGURIDAD CONTRA AMENAZAS ELECTRONICAS EN LAS ESTACIONES Y EN LAS PUERTAS DE ENLACE WEB Y CORREO

INFORME TECNICO

ADQUISICION DE UNA SOLUCION DE SEGURIDAD CONTRA AMENAZAS ELECTRONICAS EN LAS ESTACIONES Y EN LAS PUERTAS DE ENLACE WEB Y CORREO

CONTENIDO

I) NOMBRE DE LAS AREAS INVOLUCRADAS: 2
II) RESPONSABLES DE LA EVALUACION: 2
III) FECHA 2
IV) JUSTIFICACION 2
V) ALTERNATIVAS 2
VI) ANALISIS COMPARATIVO TECNICO 3
VII) ANALISIS COMPARATIVO DE COSTO – BENEFICIO. 12
VIII) MEJORAS Y CARACTERÍSTICAS TÉCNICAS ADICIONALES 18
IX) CONCLUSIONES. 19

I. NOMBRE DE LAS AREAS INVOLUCRADAS:

GERENCIA DE TECNOLOGIAS DE INFORMACION Y DE LAS COMUNICACIONES (GTIC)

II. RESPONSABLES DE LA EVALUACION:

JULIO CESAR TORRES GARCIA, Gerente de la GTIC

III. FECHA

20 de agosto de 2009

IV. JUSTIFICACION

En la actualidad los delincuentes informáticos están usando técnicas cada vez más sofisticadas para vulnerar las redes empresariales ya sea creando malware (virus, gusanos, troyanos, spyware, adware, etc.) o desplegando sus ataques haciendo uso de la ingeniería social infectando con malware y/o aplicaciones potencialmente peligrosas los mensajes de correo y sitios Web legítimos.

Así mismo con el creciente incremento de mensajes de correo basura y la necesidad de mejorar el control del uso de los recursos informáticos y de red, La Municipalidad de La Molina requiere adquirir un producto que permita brindar seguridad y control de primer nivel para lo cual se establecerá los atributos o características mínimas para la adquisición de dicha solución.

La solución que se adquiera debe proteger a la red en todos los posibles puntos de infección, los que son las estaciones y los gateways de correo y de navegación Web.

Que siendo necesario adquirir nuevas licencias de antivirus, renovar las existentes y adquirir licencias de anti-malware se justifica evaluar la oferta disponible para determinar la mejor solución para satisfacer las necesidades de la institución y que permita brindar seguridad y control de primer nivel para lo cual se establecerá los atributos o características mínimas para la adquisición de dicha solución.

V. ALTERNATIVAS

Deben ser evaluadas las alternativas de solución considerando los tres puntos vulnerables antes indicados:

a) Estaciones Cliente
b) Gateway de Correo
c) Gateway de Navegación Internet

a) Estaciones cliente:

Para la selección de los productos antivirus a analizar se han tomado en cuenta las publicaciones realizadas por empresas de investigaciones independientes y reconocidas como:

- GARTNER (Cuadrante mágico de plataformas de protección para estaciones de trabajo: 2007).

- SECUNIA Reporte de incidencias de fabricantes de productos de seguridad

    - http://secunia.com/advisories/

- AV-TEST.ORG (Detección de malware desconocido
    - http://www.virusbtn.com/news/2009/

Los productos analizados son:

Trend Micro	:	Client-Server Suite Trend Micro
Symantec	:	Symantec Multi-Tier Protection
Sophos	:	Sophos Endpoint Security and Control
McAfee	:	McAfee Total Protection for Secure Business
CA	:	CA Threat Manager Total Defense
Hacksoft	:	The Hacker v. 6.4 para estaciones y servidores.

VI. ANALISIS COMPARATIVO TECNICO

Se realizó aplicando la parte 3 de la Guía de Evaluación de Software.

Propósito de la Evaluación

Determinar los atributos o características mínimas para el Producto Final de la protección antivirus

El producto deberá proteger y controlar la seguridad en los siguientes niveles:

1) Estaciones de trabajo y servidores de red
2) En el perímetro de Internet
    a. Gateway de correo (SMTP)
    b. Gateway de Internet. (HTTP / HTTPS / FTP)

Identificar el tipo del producto

Sistema de Seguridad para la protección multi-amenazas, el que podrá ser software o software sobre appliances para las puertas de enlace de correo y Web.

Las funciones que dicho sistema deberá soportar son:

- Anti-malware, entendido como la capacidad de detección, eliminación o cuarentena de programas con virus, spyware, adware, etc.
- Aplicaciones potencialmente no deseadas (PUA), entendida como la capacidad de detectarlas, alertar sobre ellas y es deseable que las bloquee.
- Control de aplicaciones, de modo que puedan bloquearse, en forma centralizada el uso de aplicaciones que puedan ser catalogadas como de ejecución riesgosa o no productiva.
- Mecanismos de detección de intrusos de host – HIPS que incluyan, preferentemente la capacidad firewall en el cliente.
- Solución en el Gateway de correo que bloquee malware, spam y contenido no deseado.

- Solución en el Gateway de navegación Web que permita bloquear las infecciones por malware en navegación y bloqueo de websites maliciosos o no productivos.
- Anti-phishing.

Especificación del Modelo de Calidad

Se aplicará el Modelo de Calidad de Software descrito en la Parte I de la Guía de valuación de Software aprobado por Resolución Ministerial N° 139-2004-PCM.

Solución de Métricas

Las métricas fueron seleccionadas en base al análisis de la información técnica de los productos antivirus señalados en el punto "V Alternativas", como son las Características del Producto y Requerimiento de instalación.

En el Anexo I, se puede apreciar el cuadro de análisis con las características resumidas de los antivirus.

Del análisis realizado se ha determinado las siguientes características técnicas mínimas.

ANTIMALWARE		
ATRIBUTOS INTERNOS		
1	Sistemas Operativos Estaciones de Trabajo	▪ Windows 95/98/2000/XP/Vista 32/64 bits o Windows 95: xx o Windows 98: xx o Windows 98Se: xx o Windows 2000: xx o Windows XP: xx o Windows Vista: xx
2	Sistemas Operativos Servidores de Red	▪ La solución deberá soportar las versiones de 32 y 64 bits o Microsoft Server 2003: xx o Windows 2000 Server: xx o Linux Red Hat: xx o Linux xx
3	Actualizaciones	▪ Deben ser manuales y automáticas (programadas) del fichero de firmas de virus y del motor de búsqueda en los servidores y estaciones de trabajo desde Internet. ▪ Debe brindar la posibilidad de crear repositorios de firmas en forma distribuida y programable. ▪ Bajo consumo de ancho de banda para actualizaciones. El postor deberá certificar con información oficial del fabricante ya sea por medio de folletos o en la página Web del fabricante.
4	Protección Proactiva	▪ La solución debe contar con una tecnología de detección proactiva de amenazas conocidas y desconocidas que detecte malware antes de su ejecución y en ejecución. ▪ La solución debe incluir también una tecnología de detección de intrusos de host (HIPS) que brinde protección en acceso integrado en el producto. No debe requerir ejecutar agentes adicionales ni ejecutarse en forma programada.

5	Control y Productividad en la Red	▪ La solución debe contar con un sistema que permita el control de aplicaciones. ▪ Este sistema debe permitir controlar y bloquear el uso de aplicaciones que causan un impacto negativo a la productividad de los usuarios y el uso del ancho de banda en la red tales como: o Programas de mensajería (MSN, Yahoo Messenger, Google Talk y otros.) o Programas de voz sobre ip (Skype, Google Talk, etc) o Programas Peer-to-Peer (Kazaa, Imesh, Ares, etc) o Juegos en red y standalone, o Barra de Herramientas, o Herramientas de Control Remoto de Equipos (Logmein, Netcat, etc) ▪ La solución debe permitir limpiar remotamente (desinstalar) las principales aplicaciones Peer-to-peer desde la Consola de Administración.
6	Compatibilidad	▪ Carta del fabricante del software antivirus indicando la total compatibilidad con los sistemas operativos en las versiones anteriores mencionadas.
7	Instalación	▪ La instalación del software a las computadoras de los usuarios debe ser mediante: o Sincronización con el Directorio Activo de Microsoft o La consola de Administración e o Instalación mediante CD o recurso UNC
ATRIBUTOS EXTERNOS		
8	Consola de Administración	La herramienta debe contar con una Consola de Administración desde donde se pueda Administrar y controlar la solución anti-malware y sus componentes en forma centralizada. ▪ La consola debe permitir la administración simultánea de equipos y servidores Windows, Linux. ▪ La herramienta deberá ser escalable, el cual permite activar la administración de complejas redes, permitiendo la administración de más de 340 equipos desde una sola consola. ▪ La consola debe sincronizarse con el Directorio Activo para la instalación automática de la solución de seguridad en los equipos. ▪ La frecuencia de actualización de firmas de virus debe ser programable y no superior a 10 minutos. ▪ La administración deberá estar basada en Políticas cuando menos para Actualización, Antivirus, Control de Aplicaciones y Firewall. ▪ Debe contar con filtros de control que permitan detectar de forma rápida los equipos no protegidos o los que no cumplen con las políticas de seguridad.

		▪ El administrador debe poder crear políticas desde la consola para evitar el uso de aplicaciones no deseadas así como eliminar, autorizar y limpiar las mismas en los clientes. ▪ Debe incluir la capacidad para la desinfección y limpieza remota de adware/aplicaciones potencialmente peligrosas, así como también de virus, troyanos, gusanos y spyware. ▪ La consola debe poder utilizar diferentes mecanismos para detectar equipos en la red (TCP/IP, Directorio Activo y otros). ▪ Se debe poder crear políticas de actualización para equipos con conexión lenta pudiendo limitarse el ancho de banda utilizado durante las actualizaciones. ▪ La consola debe ser capaz de determinar equipos que cumplen con las políticas centrales y/o que fueron modificadas localmente. Eventualmente deberá poder "forzar" a los equipos a cumplir con las políticas centrales con tan solo un clic. ▪ La consola deberá contar con un sistema de reportes y mecanismos de notificación de eventos vía correo electrónico. ▪ Deberá almacenar un histórico de eventos de cada equipo administrado pudiéndose conocer también el Nombre del Equipo, Descripción, SO, Service Pack, IP, Grupo, Última Actualización, Eventos de error, etc. Desde la consola.
9	Defensa Integrada contra malware (Virus, Troyanos, Macro Virus, Virus Gusano, Spyware, Adware, Virus en Archivos comprimidos, PUAS – Aplicaciones Potencialmente Peligrosas).	▪ Es deseable que la solución de seguridad para estaciones y servidores debe ser de tipo Integrada, es decir que sea un único agente el que brinde protección frente a virus, spyware, adware, comportamientos sospechosos, hackers (firewall personal) y aplicaciones potencialmente peligrosas en todos los protocolos de la red, de modo que el impacto en el uso de recursos de la estación cliente sea mínimo. ▪ Deberá incluir un firewall de la estación cliente que sea ejecutado en la estación cliente. a. El firewall debe ser administrado centralizadamente. b. Debe poder bloquear y autorizar aplicaciones y puertos específicos tanto local como centralizadamente. c. El firewall debe poder trabajar en modo oculto. ▪ La solución debe tener versiones para Linux el cual debe contar con un módulo de escaneo de archivos de máximo rendimiento, estabilidad y eficacia el cual debe permitir el escaneado en acceso, en demanda y programado de unidades locales, extraíbles y compartidas (como NFS y Samba), y otros sistemas de archivos. La versión para Linux debe poder ser configurado y administrado desde la consola central.

		▪ La configuración del cliente para Linux debe poder realizarse desde la línea de comandos y mediante una interfaz Web en forma local y debe contar con al menos una certificación tipo RedHat Ready o Novell Suse Linux. ▪ La solución debe contar con una Cuarentena de usuario final que permita controlar y/o autorizar el uso de ciertas aplicaciones no deseadas. ▪ La solución tanto para Windows, Linux y Mac deberán notificar los eventos de virus, spyware, adware, aplicaciones no deseadas, intrusiones, cambios en la configuración del cliente antivirus y/o cliente firewall a la consola central. ▪ La solución debe poder actualizarse desde una consola central y desde la Web del fabricante simultáneamente con el fin de asegurar una completa protección aún cuando la consola central no se encuentre activa.
10	Defensa en el Perímetro de la Red (Gateway de Correo y Web)	▪ Se requiere una solución, preferentemente que utilice el anti-malware del mismo fabricante ofertado en las estaciones clientes, que brinde Seguridad y Control de la información entrante y saliente de la red vía los protocolos SMTP, HTTP y FTP. ▪ La solución deberá rastrear, limpiar y eliminar malware y aplicaciones potencialmente peligrosas en dichos protocolos. **GATEWAY DE CORREO (Protocolo SMTP)** ▪ Deberá tener la capacidad de configurar como Relay del correo electrónico. ▪ Deberá integrarse con el protocolo LDAP y Directorio Activo para la autenticación de usuarios y creación de políticas. ▪ Deberá incluir un filtro anti-spam del mismo fabricante que soporte descargas automáticas de políticas anti-spam. Deberá incluir varias técnicas de detección, como reputación de IP, heurística avanzada, huellas de mensajes y adjuntos, análisis de palabras clave, detección de direcciones Web, etc. ▪ El producto debe tener una efectividad de detección de SPAM fuera de caja de un mínimo del 95%. Deberá entregarse información de entidad certificadora independiente para certificar esta funcionalidad ▪ Deberá ofrecer una tecnología que permita el acceso en tiempo real a una amplia gama de información reciente contra spam. ▪ Deberá detectar ataques de robo de información (phishing), ataques de denegación de servicio (DoS) y cosecha de información (Harvest).

		▪ Deberá contar con un módulo específico para el Filtrado por Reputación que permite el bloqueo por IP's de servidores dudosos y permitir elaborar excepciones tanto a nivel MTA como a nivel de políticas de correo. Esta lista deberá residir en el servidor y deberá ser actualizado en promedio cada 10 minutos y en forma incremental. ▪ Deberá de poder detectar, eliminar y limpiar virus y spyware en los archivos adjuntos al correo electrónico y en el cuerpo del mensaje y deberá ser del mismo fabricante. ▪ Deberá de realizar el bloqueo de archivos adjuntos según el tipo de archivo y no de la extensión. ▪ Deberá de realizar el bloqueo de correos por asuntos, destinatario o texto en el cuerpo del mensaje. ▪ Deberá contar con un Editor de Políticas para filtrar el contenido del tráfico entrante y saliente. ▪ Deberá de poder establecerse reglas de filtrado por usuario o grupo LDAP. ▪ Deberá de poder hacer creaciones de lista de aceptación y negación (blanca y negra) de dominios y usuarios (cuentas de correo) confiables. ▪ Deberá de enviar notificaciones configurables al emisor, receptor y al administrador sobre mensajes electrónicos infectados y/o bloqueados. ▪ Deberá contar con un sistema de Administración vía Web Seguro (HTTPS). ▪ Debe permitir crear usuarios para la administración basada en roles para delegar ciertas funcionalidades de administración. El acceso a la interfaz de administración basada en roles debe ser vía Web seguro y debe funcionar en un puerto distinto al del Administrador principal. ▪ Deberá contar con un administrador de cuarentena central a nivel de consola. ▪ Deberá contar con un administrador de la cuarentena por usuario que permita a su vez administrar la lista blanca y negra de cada usuario. ▪ Debe poder desactivarse ciertas opciones a las cuales no se desea que los usuarios tengan acceso. ▪ Deberá contar con un sistema automático que permita realizar el backup de la cuarentena. Esta opción es configurable desde la herramienta de gestión del producto. ▪ Deberá generar un mensaje donde les informe a los usuarios finales los mensajes de correo puestos en

		cuarentena y que estos puedan recuperar todos o individualmente tan sólo con un solo clic. ▪ La herramienta debe contar con un sistema de actualización de cada parte de los componentes del producto incorporado en la herramienta de administración Web. **GATEWAY WEB (Protocolo HTTP/FTP)** ▪ El producto debe permitir bloquear programas espía (spyware), virus, pesca de información (phishing), programas maliciosos y aplicaciones no deseadas (adware, PUAS) en la puerta de enlace, y permitir un control completo del acceso a Internet para una navegación segura y productiva. ▪ Deberá ofrecer la inspección de tráfico de doble dirección (entrante y saliente) de códigos maliciosos, programas no deseados y el cumplimiento de políticas de uso de Internet. ▪ Deberá proveer un filtro de contenido (URL Filtering) del mismo fabricante y deberá estar basado en categorías. ▪ Deberá contar con al menos con cincuenta (50) tipos de categorías organizados de acuerdo al contenido de cada sitio Web. ▪ Deberá poder permitir la categorización de URL's por parte del administrador. ▪ Deberá contar con una interfaz de administración Web Segura (HTTPS). ▪ Deberá garantizar una adecuada detección con bajo impacto en la red y mínima latencia. El postor debe presentar una copia de la información pública y oficial del producto que permita certificar esta característica (Brochures y/o Impresión de Página Web oficial). ▪ Deberá contar con un sistema de administración basado en grupos con indicadores visuales y reportes en línea. ▪ Deberá incluir un proxy interno que permita ocultar la dirección IP del equipo donde esté implementado la solución. ▪ Deberá recibir actualizaciones automáticas de las firmas de virus, filtrado de contenido (URL) como mínimo cada 15 minutos. ▪ Deberá permitir crear políticas de uso de Internet por grupos de usuarios, por hora o por días. ▪ Deberá permitir controlar la descarga de aplicaciones potencialmente peligrosas incluyendo dialers, herramientas de administración remota y aplicaciones de monitoreo de PC's y archivos de streaming (música, videos).

		▪ Deberá permitir la integración con el Directorio Activo de Microsoft para la generación de políticas de seguridad y control del producto. ▪ Deberá contar con un sistema de reportes que permita conocer: o Usuarios que intentaron descargar virus. o Usuarios que intentaron visitar sitios de alto riesgo. o Usuario que intentaron descargar aplicaciones potencialmente peligrosas. o Los principales usuarios que intentaron violar las políticas de seguridad y control de la institución. o La navegación de usuarios por páginas y categorías visitadas
11	Escaneo	▪ Permitir configurar la detección sobre todos los archivos, o tipos de archivos, comprimidos (cualquier formato de comprensión, rar, zip, cab, arj, arz), ocultos y archivos en ejecución. ▪ Deberá realizar los siguientes tipos de rastreo: en tiempo real, bajo demanda, programado y remoto a través de la consola de administración. ▪ Para el escaneado en el gateway de correo y Web el producto deberá contar con un escaner de una vía que permita detectar malware y realizar el filtrado URL, deseablemente, en una sola pasada.
ATRIBUTOS DE USO		
12	Productividad	▪ No deberá consumir muchos recursos de memoria y procesador en los equipos de los usuarios.
13	Alertas y Reportes	▪ La consola de administración deberá de ser capaz de notificar los eventos de virus a través de diferentes medios (correo electrónico, alertas de registros, etc.) ▪ Además generar reportes gráficos de tipo barra, pastel, imprimibles y exportables de la cobertura de versiones, actualizaciones e infecciones. ▪ Deberá contar con un Panel de Control donde se visualice en línea y en forma automática el estado de la seguridad de la red. ▪ Deberá contar con un Panel de Control donde se visualice en línea y en forma automática el número de equipos sin protección, protegidos, con errores, que no cumplen con las políticas corporativas.
14	Facilidad de Uso	▪ Toda la solución deberá incluir capacitación a usuarios para el uso más fácil y rápido.
15	Soporte al Usuario	▪ Debe contar con soporte técnico 24/7 escalable hacia la casa matriz incluido en la licencia y en español. El postor deberá presentar un documento del fabricante donde certifique que cuenta con este tipo de soporte.

		▪ Si para el escalamiento se requiere de un código especial para el soporte desde la casa matriz el postor deberá especificarlo mediante una declaración jurada comprometiéndose a brindar dicho código el cual deberá ser emitido a nombre de la ENTIDAD al momento de la firma del contrato.
16	Eficacia	▪ Deberá ser capaz de permitir al área de TI lograr las metas específicas con exactitud e integridad, de acuerdo a las especificaciones técnicas y requerimiento de la organización.

Niveles, escalas para métricas:

ITEM	ATRIBUTOS	ESCALAS
	ATRIBUTOS INTERNOS	
1	Sistemas Operativos Estaciones de trabajo	5
2	Sistemas Operativos Servidores de Red	5
3	Actualizaciones	6
4	Protección Proactiva	8
5	Control y Productividad en la Red	9
6	Compatibilidad	3
7	Instalación	5
	ATRIBUTOS EXTERNOS	
8	Administración	6
9	Defensa Integrada contra malware (Virus, Troyanos, Macro Virus, Gusanos, Spyware, Adware, Virus en Archivos comprimidos, PUAs).	6
10	Defensa en el Perímetro de la Red (Gateway de Correo y Web)	9
11	Escaneo	6
	ATRIBUTOS DE USO	
12	Productividad	5
13	Alertas y reporte	6
14	Facilidad de uso	6
15	Soporte Técnico al usuario	7
16	Eficacia	8
	PUNTAJE TOTAL	100

No se ha comparado los productos de software antivirus, porque el objetivo es establecer características técnicas mínimas del producto a adquirir y que sirvan para una posterior comparación y evaluación.

VII. ANALISIS COMPARATIVO DE COSTO – BENEFICIO

En el Anexo II se puede apreciar un cuadro comparativo de ventajas de los productos software que fueron analizados técnicamente.

El análisis costo – beneficio tiene como referencia la cantidad de licencias de software antivirus posibles de adquirir.

Shopos Endpoint Security and Control

Producto	Cantidad	Precio Unitario. (Sin IGV)	Sub-Total (Sin IGV)
Licenciamiento Sophos Enterprise Security and Data • La solución incluye: a) Sophos Endpoint Security and Data Control b) Sophos Email Security and Data Control c) Sophos WebSecurity and Data Control • Protección para end-points, correo electrónico y filtrado Web y de correo. • Consola de administración centralizada. • Control de dispositivos. • Control de aplicaciones (MSN, P2P, Juegos, etc.). • Soporta Windows 95/98/2000/XP/2003/Vista/2008. • Integración con el Directorio Activo y otros sistemas LDAP. • Incluye versiones para Linux/Unix. • Incluye versiones para Exchange/Lotus Domino. • Permite a los usuarios usar una licencia en una PC domestica sin costo adicional. • 12 Meses Garantía. • Soporte Técnico 24x7. • Incluye instalación y capacitación.	340	S/. 90.05	S/. 30,617.00
Hardware Appliance Sophos WS500 • Protección contra malware, spyware, filtrado URL y proxy anónimos. • Permite la implementación de políticas y el filtrado URL por categoría (54 categorías).	1	S/. 13,702.00	S/. 13,702.00
		SUB-TOTAL	S/. 44,319.00
		IGV (19%)	S/. 8,420.61
		TOTAL	**S/. 52,739.61**

Nota:

- Plazo de entrega: 5 días licencias / 15 días hardware.
- Proveedor: INNOVARE E-BUSINESS S.A.C.

Symantec Multi-Tier Protection

Producto	Cantidad	Precio Unitario (Sin IGV)	Sub-Total (Sin IGV)
SYMC Multi-Tier Protection 11.0.2 • Protección para end-points y correo electrónico. • Consola de administración centralizada. • Control de dispositivos. • Soporta Windows 2000/XP/2003/Vista/2008. • Integración con el Directorio Activo y otros sistemas LDAP. • Incluye versiones para Linux. • Incluye versiones para Exchange/Lotus Domino	223	S/. 127.41	S/. 28,412.43
Appliance SMS 8340 • Incluye hardware appliance para el filtro de correo electrónico.	1	S/. 10,325.00	S/. 10,325.00
Instalación y configuración de la solución.	1	S/. 877.50	S/. 877.50
Soporte Técnico 8x5.	1	S/. 877.50	S/. 877.50
		SUB-TOTAL	S/. 40,492.43
		IGV (19%)	S/. 7,693.56
		TOTAL	**S/. 48,185.99**

Nota:

- La solución propuesta no soporta Windows 95/98, sólo se ha cotizado por 230 licencias.
- La solución propuesta no incluye filtro Web.
- No se incluye la capacitación.
- Plazo de entrega: 10 días hábiles.
- Proveedor: Cosapi Data S.A.

McAfee Total Protection for Secure Business

Producto	Cantidad	Precio Unitario (Sin IGV)	Sub-Total (Sin IGV)
McAffe Total Protection for Secure Business • Protección para end-points y correo electrónico. • Consola de administración centralizada. • Control de dispositivos. • Soporta Windows 2000/XP/2003/Vista. • Soporta servidor de correos Lotus Note Domino y Microsoft Exchange. Licenciamiento perpetuo.	340	S/. 141.94	S/. 48,259.60
McAffe Web Gateway 1100E Appliance Incluye hardware appliance para el filtro Web. • Permite el filtrado URL por categoría (54 categorías).	1	S/. 12,073.96	S/. 12,073.96
McAffe Web Gateway 1100E 1 Año Software Support & Onsite Next Business Day Hardware.	1	S/. 2,174.40	S/. 2,174.40

McAffe Web Security Gateway Edition Software.	340	S/. 58.35	S/. 19,837.78
Servicios de Ingeniería de BAFING S.A.C. • Incluye implementación y capacitación (1 sesión de 2 horas efectivas). • Soporte Técnico 24x 7 (On-Line y On-Site) por un año. • Boletín Digital de Bafing S.A.C.	1	S/. 3,020.00	S/. 3,020.00
		SUB-TOTAL	S/. 85,365.74
		IGV (19%)	S/. 16,219.49
		TOTAL	**S/. 101,585.22**

Nota:

- La solución propuesta no soporta Windows 95/98.
- La solución propuesta no incluye filtro de correo electrónico.
- Plazo de entrega: 1 día licencias / 15 días hardware.
- Proveedor: BAFING S.A.C.
- El tipo de cambio usado es de: S/. 3.02

CA Threat Manager Total Defense

Producto	Cantidad	Precio Unitario (Sin IGV)	Sub-Total (Sin IGV)
CA Threat Manager Total Defense 250-499 users – Includes Subscription License – Product plus 1 Year Value Maintenance • La solución incluye: a) CA Anti-Virus b) CA Anti-Spyware c) CA Gateway Security d) CA Threat Manager e) CA Host-Based Intrusion Prevention System • Protección para end-points, correo electrónico y filtrado Web. • Permite la implementación de políticas y el filtrado de URL. • Consola de administración centralizada. • Soporta Windows 95/98/2000/XP/2003/Vista/2008. • Soporta sistema operativo Linux/Unix.	340	S/. 120.20	S/. 40,866.64
Security Kit Olp CD-Rom • 1 año de Mantenimiento. • Instalación y Configuración, previa coordinación con el área encargada y horario a definir. • 04 horas de Capacitación en Instalación, Configuración y Administración del Producto. Soporte Técnico Telefónico 24 horas x 7 días por parte de Safe Solutions Perú, durante el año de mantenimiento. Soporte In situ de ser necesario.	1	S/. 1,510.00	S/. 1,510.00
		SUB-TOTAL	S/. 42,376.64
		IGV (19%)	S/. 8,051.56
		TOTAL	**S/. 50,428.20**

Nota:

- La solución propuesta no incluye hardware appliance.
- No brinda el control de dispositivos y aplicaciones.
- Plazo de entrega: 15 días hábiles.
- Proveedor: SAFE SOLUTIONS PERU S.A.C.
- El tipo de cambio usado es de: S/. 3.02

Client Server Suite Standard Trendmicro

Cotización 1: Client-Server Suite Trend Micro + Websense Web Filter

Producto	Cantidad	Precio Unitario (Sin IGV)	Sub-Total (Sin IGV)
Client Server Suite Standard Trendmicro • Protección para end-points y correo electrónico. • Consola de administración centralizada. • Control de dispositivos. • Soporta Windows 2000/XP/2003/Vista/2008. • Integración con el Directorio Activo. • Soporta sistema operativo Linux.	329	S/. 78.52	S/. 25,833.08
Websense Web Filter • Sólo incluye software de filtro Web. • Permite la implementación de políticas y el filtrado URL por categoría (más de 90 categorías). • Permite el control de aplicaciones y acceso Web.	350	S/. 63.42	S/. 22,197.00
Instalación y configuración de las dos soluciones.	1	S/. 2,718.00	S/. 2,718.00
Soporte Técnico 24x7 (por un año).	1	S/. 4,530.00	S/. 4,530.00
		SUB-TOTAL	S/. 55,278.08
		IGV (19%)	S/. 10,502.84
		TOTAL	**S/. 65,780.92**

Nota:

- La solución propuesta no soporta Windows 95/98. Sólo se ha cotizado por 329 licencias para end-points y 350 licencias de filtro Web.
- La solución propuesta no es una solución integrada de un solo fabricante.
- La solución propuesta no incluye hardware appliance.
- La solución propuesta no incluye el filtro de correo electrónico.
- No se incluye la capacitación.
- Plazo de entrega: 20 días licencia.
- Proveedor: TRENDCORP S.A.
- El tipo de cambio usado es de: S/. 3.02

Cotización 2: Client-Server Suite Trend Micro + Blue Coat Web Filter

Producto	Cantidad	Precio Unitario (Sin IGV)	Sub-Total (Sin IGV)
Client Server Suite Standard Trendmicro • Protección para end-points y correo electrónico. • Consola de administración centralizada. • Control de dispositivos. • Soporta Windows 2000/XP/2003/Vista/2008. • Integración con el Directorio Activo. • Soporta sistema operativo Linux.	329	S/. 78.52	S/. 25,833.08
Appliance Blue Coat SG510-10, Proxy Edition • Incluye hardware appliance para el filtro Web. • Permite la implementación de políticas y el filtrado URL por categoría (61 categorías). • Permite la clasificación dinámica en tiempo real (DRTR), organizando en forma precisa hasta el 98% de los sitios no categorizados. • Control de aplicaciones (MSN, P2P, Juegos, etc.).	1	S/. 40,407.60	S/. 40,407.60
Software Blue Coat WebFilter • Incluye mantenimiento por un año.	350	S/. 66.44	S/. 23,254.00
Instalación y configuración de las dos soluciones.	1	S/. 4,530.00	S/. 4,530.00
Soporte Técnico 24x7 (por un año).	1	S/. 9,060.00	S/. 9,060.00
		SUB-TOTAL	S/. 103,084.68
		IGV (19%)	S/. 19,586.09
		TOTAL	**S/. 122,670.77**

Nota:

- La solución propuesta no soporta Windows 95/98. Sólo se ha cotizado por 329 licencias para end-points y 350 licencias de filtro Web.
- La solución propuesta no es una solución integrada de un solo fabricante.
- No se incluye la capacitación.
- Plazo de entrega: 20 días licencia / 30 días hardware.
- Proveedor: TRENDCORP S.A.
- El tipo de cambio usado es de: S/. 3.02

Cotización 3: Client-Server Suite Trend Micro + Interscan Web Protect Trend Micro

Producto	Cantidad	Precio Unitario (Sin IGV)	Sub-Total (Sin IGV)
Client Server Suite Standard Trendmicro • Protección para end-points y correo electrónico. • Consola de administración centralizada. • Control de dispositivos. • Soporta Windows 2000/XP/2003/Vista/2008. • Integración con el Directorio Activo. • Soporta sistema operativo Linux.	329	S/. 78.52	S/. 25,833.08
Interscan Web Protect Trend Micro • Sólo incluye software de filtro Web. • Permite la implementación de políticas y el filtrado URL por categoría (más de 90 categorías). • Permite el control de aplicaciones y el acceso a sitios Web.	350	S/. 30.20	S/. 10,570.00
Instalación y configuración de las dos soluciones.	1	S/. 2,718.00	S/. 2,718.00
Soporte Técnico 24x7 (por un año).	1	S/. 4,530.00	S/. 4,530.00
		SUB-TOTAL	S/. 43,651.08
		IGV (19%)	S/. 8,293.71
		TOTAL	**S/. 51,944.79**

Nota:

- La solución propuesta no soporta Windows 95/98. Sólo se ha cotizado por 329 licencias para end-points y 350 licencias de filtro Web.
- La solución propuesta no incluye hardware appliance.
- La solución propuesta no incluye el filtro de correo electrónico.
- No se incluye la capacitación.
- Plazo de entrega: 15 días licencia.
- Proveedor: TRENDCORP S.A.
- El tipo de cambio usado es de: S/. 3.02

VIII. MEJORAS Y CARACTERÍSTICAS TÉCNICAS ADICIONALES

Estas mejoras y características técnicas adicionales servirán para adquirir un producto que nos otorgue mayores beneficios sin necesidad de incurrir en gastos adicionales para la institución. Es decir, con la inversión que se realice en software antivirus cubrir otras áreas de protección y control de la red.

MEJORA O CARACTERÍSTICA ADICIONAL	PUNTAJE
MOTOR ANTIVIRUS	
I) La solución de protección ofertada para el Control del Uso de Aplicaciones está:	
a) Incorporado en el mismo motor antivirus	10
b) Es un producto del mismo fabricante que requiere ejecutar un engine adicional	5
II) Las categorías de aplicaciones de la solución para el Control del Uso de Aplicaciones es mantenida y creada por:	
a) El fabricante	10
b) El Administrador de la red	5
III) Cuenta con un agente que se integre con el sistema de correo de la institución (MailEnable) que brinde bajo consumo de memoria y cpu (máx. 10% de CPU en cada escaneo) y sea 20 veces más rápido que un scaner ejecutado por línea de comandos.	
a) SI	10
b) NO	0
IV) Portabilidad de la licencia en computadoras personales de uso domestico de los usuarios con el producto instalado en la municipalidad.	
a) SI, sin costo	10
b) SI, con costo adicional	5
c) NO	0
GATEWAY DE CORREO Y WEB	
I) El producto tiene un ratio de detección de spam.	
a) Del 98% a más.	20
b) Del 96% al 97%	5
II) El postor cuenta con un hardware específico del mismo fabricante para la solución Web que brinde al menos: o Monitoreo del funcionamiento de la protección. o Tarjeta fail-over en caso de fallas del equipo. o Asistencia remota bajo demanda.	
a) SI	20
b) NO	0

IX. CONCLUSIONES

- Se determinó los atributos o características técnicas mínimas que deben ser considerados para una evaluación de software antivirus, asimismo se estableció la valoración cuantitativa de cada característica.

- Se estableció algunas mejoras y características técnicas adicionales a tomar en cuenta durante el proceso de evaluación los cuales nos permitirán obtener un **"Retorno a la Inversión – ROI"** al adquirir el software antivirus.

ANEXO I

CUADRO DE ANALISIS DE SOFTWARE ANTIVIRUS.

ANTIVIRUS	CARACTERISTICAS	REQUERIMIENTO
Trend Micro: Client-Server Suite Trend Micro	Solución de seguridad completa para clientes y servidores que cuenta con la nueva protección frente a amenazas Web dedicada. Bloquea el acceso a sitios maliciosos además ofrece funciones mejoradas de protección antivirus y anti-spyware • Excelente protección anti-malware • Protege frente al malware de Internet, robo de datos, tiempos de inactividad • Facilidad de uso • Reducción de los costes de TI	# Plataformas compatibles **Estaciones de Trabajo** • Windows: 2000/XP/Vista **Servidores** • Windows: 2000 Server/ Sever 2003(32 y 64 bits) • Linux: Red Hat Enterprise 4,5/Novell Suse Enterprise server 10 # Espacio en el disco **Estaciones de Trabajo** • 350 MB # Memoria **Estaciones de Trabajo** • 256 MB
Symantec: Symantec Multi-Tier Protection	Paquete integrado que combina sin problemas las principales tecnologías de seguridad, como antivirus, anti-spyware, firewall, prevención de intrusiones y control de aplicaciones y dispositivos, en un solo agente y una sola consola de administración, lo cual brinda una mejor protección además contribuye a reducir el costo total de propiedad. Solución completa diseñado para proteger los activos de la empresa disminuyendo los riesgos gracias a la protección contra software malicioso para redes empresariales multiplataforma, servidores y gateway de correo electrónico. • Protección completa que integra las mejores tecnologías para detener todo tipo de amenazas • Protección proactiva de amenazas • Un agente única y una sola consola de administración • Control de las aplicaciones y dispositivos • Defensa de varios niveles • Fácil de implementar	# Protección de puntos finales **Symantec Endpoint Proteccion Client** • Windows: 2000 /XP/2003/Vista • Linux: Red Hat Enterprise, Suse Linux Enterprise, Novell Enterprise Server, VMWare ESX • Mac: Mac OS X 10.2 **Symantec Endpoint Protection Manager** • Windows: 2000 /XP/2003 **Symantec Endpoint Manager Console** • Windows: 2000 /XP/2003/Vista # Protección de correo electrónico **Symantec Mail Security** • Exchange: Windows 2000Server/Server 2003/2000/XP • Domino: Lotus Domino Server 6.5.x y 7.x # Espacio en el disco **Symantec Endpoint Proteccion Client** • 4 GB # Memoria **Symantec Endpoint Proteccion Client** • 256 MB **Symantec Mail Security** • 2 GB como mínimo

Sophos: Sophos Endpoint Security and Control 7	Seguridad y control para ordenadores, portátiles, servidores y dispositivos móviles en diferentes plataformas. Sophos ofrece protección completa contra virus, programas espía y publicitarios, y controla aplicaciones de voz sobre IP, mensajería instantánea, intercambio de archivos y juegos. No es necesario utilizar varios productos de administración para evitar amenazas diferentes. Nuestro programa unificado protege contra virus, programas espía, programas publicitarios y aplicaciones no deseadas (PUA). **Consola única simplificada y automatizada.** Gestión de miles de ordenadores Windows, Mac OS X y Linux desde una sola consola, que ofrece una visibilidad única del estado de seguridad de toda la red. Protección automática de ordenadores nuevos. **Sophos Email Security and Control** Protege contra amenazas entrantes y salientes con efectividad y sencillez sin igual, ofreciendo seguridad de alto nivel contra spam, pesca de información, virus, programas espía y programas maliciosos. • Protección antivirus, contra programas espía y cortafuegos • Protege Windows, Macs y Linux • Automatice la gestión con una consola • Restricción de VoIP, mensajería instantánea, P2P y juegos • Bloqueo de correo no deseado, phishing, programas maliciosos y aplicaciones no deseadas. • Protección más rápida y de bajo impacto • Protección preventiva que reduce el riesgo de infección • Soporte técnico 24 horas	# Plataformas compatibles **Sophos Anti-virus** • Windows(32/64 bits): 95/98/NT/2000/XP Home y Pro/Server 2003/Vista/Server 2008/Mobile 5/6 • VMWare: ESX/Workstation/Server • Otras Plataformas: Mac OS X/UNIX/NetApp Storage Systems/EMC/Open VMS/NetWare **Enterprise Console** Servidor de Administración • Windows: 2000 Server/Server 2003 y R2/Server 2008 • VMWare: ESX/Workstation/Server Consola Remota • Windows: 2000 Pro y Server/Server 2003 y R2/XP Pro • VMWare: ESX/Workstation/Server Plataformas administradas • Windows: 95/98/NT/2000/XP Home y Pro/Server 2003/Vista/Server 2008 • Mac OS X • Linux • UNIX **Sophos NAC** • Windows: 2000/XP/Vista **Sophos Client Firewall** • Windows: 2000 Pro/XP Home y Pro/Vista # Espacio en el disco **Sophos Anti-virus** • Windows 2000/XP/2003/Vista: 120 MB • Windows 95/98/NT4: 90 MB **Sophos Client Firewall** • Mínimo de 20 MB libres **Enterprise Console** • Mínimo 150 MB más espacio de base de datos # Memoria **Sophos Anti-virus** • Windows 2000/XP/2003/Vista/NT4: Recomendada 256 MB • Windows 95/98: 128 MB **Sophos Client Firewall** • Recomendada 256 MB **Enterprise Console** • Mínimo 512 MB

McAfee: McAfee Total Protection for Secure Business	Solución que integra los galardonados productos de seguridad de McAffe para end-points, correo electrónico, Web y datos. Ofrece una defensa más sólida contra las amenazas conocidas y las amenazas que se avecinan. Plataforma de gestión unificada, con una sola consola de administración, que ayuda a incrementar la eficiencia de las operaciones mediante la implementación y configuración centralizadas y el monitoreo detallado de la situación de seguridad de toda la empresa • Administración simplificada con una sola consola de administración • Protección proactiva de los end-points. • Antivirus para estaciones de trabajo y servidores multiplataforma. • Encriptación de datos para evitar su pérdida. • Escaneo de correo electrónico • Bloqueo de spam, virus, ataques de fraude electrónico y contenido inadecuado.	# Plataformas compatibles **Estaciones de Trabajo** • Windows: NT/2000/XP Home o Professional/Vista **Servidores** • Windows: NT/2000 Server/2003 Server Enterprise Server • Novell: Novell NetWare 6.5/6.0/5.1 **Otras plataformas compatibles** • XP Tablet PC, Citrix, EMC # Protección de correo electrónico **Servidor de Correos** • Microsoft Exchange 2000, 2000 Server, 2003 Server • Domino: Lotus Domino Server 5+,6+ # Memoria • Se recomienda 128 MB y 256 MB para servidores
CA: CA Threat Manager Total Defense	Paquete de seguridad que combina las mejores soluciones ofreciendo una protección de múltiples capas para la detección, el análisis, el bloqueo y la eliminación de amenazas múltiples minimizando riesgos y ataques a la información confidencial. • Protección frente a las amenazas de la Web y envío de datos en forma segura. • Impide la ejecución de código malintencionado con la protección de antivirus y anti-spyware. • Detecta las intrusiones en el sistema y ayuda a proteger los dispositivos de red. • Permite la generación de informes personalizables.	# Plataformas compatibles **CA Antivirus** • Windows: 95/98/ME/NT 4.0/2000/XP(32/64 bits) • Linux: Red Hat Enterprise/Suse Linux Enterprise • Unix: Sun Solaris 8/HP-UX 11.0 y 11.11 **CA Gateway Security** • Windows: Server 2003 /2000/XP/Vista/ Server 2008 **CA HIPS** • Windows: 2000/XP/Vista/2000 Server/Server 2003/Server 2008 # Espacio en el disco **CA Antivirus** • 256 MB # Memoria **CA Antivirus** • 512 MB

Hacksoft: The Hacker v6.4	• Motor de búsqueda mejorado con tecnología de punta para detectar y eliminar todo tipo de virus backdoons, troyanos, gusanos y aplicaciones no deseadas. • Análisis de procesos activos en memoria y del inicio. Velos, fácil de instalar y usar. • Actualizaciones inteligentes (se actualiza automáticamente y mantiene su PC siempre protegida). • Total integración con Windows Security Center de Windows XP. • Licencia especial para organizaciones, incluye una consola de de administración remota (PC y Servidor) que actualiza y monitorea el antivirus desde una sola central. • Implementa el concepto de tareas para la creación de procesos automáticos. • The Hacker en Servidores de Correo, eficaz combinación de protección antivirus, detectando y eliminando los virus en los mensajes antes que sean filtrados hacia la bandeja de los usuarios. Incluye filtrado de contenidos y módulos anti-spam • Servicio de soporte técnico las 24 horas, los 365 días del año.	# Plataformas compatibles **Estaciones** • Windows: /98/XP **Servidores** • Windows: 2000/NT/Server 2003

ANEXO II

VENTAJAS DE SOFTWARE ANTIVIRUS

ANTIVIRUS	VENTAJAS
Trend Micro: Client-Server Suite Trend Micro	Solución unificada que protege los servidores de red, equipos de sobremesa y portátiles. Ofrece una defensa por capas frente a virus, spyware, rootkits y amenazas combinadas. Además brinda protección frente al malware basado en Web, el robo de datos y la pérdida de ingresos; gracias al nuevo servicio de reputación Web en Internet. Permite la protección frente a amenazas Web mediante el bloqueo del acceso a sitios maliciosos.
Symantec: Symantec Multi-Tier Protection	Paquete integrado que combina Symantec Antivirus con una avanzada prevención de amenazas y ofrece una defensa inigualable contra programas maliciosos en equipos portátiles, de escritorio y servidores. Avanzada protección contra virus y monitoreo de toda la empresa desde una sola consola de administración. La protección de Symantec contra manipulaciones defiende frente a los accesos no autorizados y a los ataques, a la vez que mantiene alejados a los virus que intentan desactivar las medidas de seguridad. Protección contra amenazas de red la cual incluye un motor de firewall basado en reglas un sistema genérico de bloqueo de puntos vulnerables. Ofrece una protección de alto rendimiento para el correo electrónico contra amenazas de virus, spam y riesgos a la seguridad. La tecnología avanzada Symantec Global Intelligence Network brinda una protección proactiva frente a las amenazas de Internet permitiendo calificar comportamientos buenos y malos de las aplicaciones desconocidas. Brinda protección en varios niveles para end-point y servidor de correo. Fácil de instalar, configurar y administrar.
Sophos: Sophos Endpoint Security and Control	Ofrece una protección superior unifica a un precio promedio. Una única licencia permite proteger todos los puntos vulnerables de la red. La licencia es altamente flexible, permite el uso de los dispositivos de seguridad tan solo al comprar el hardware necesario. No hay costes ocultos. Líder en el Cuadrante Mágico de Gartner de Protección de punto final 2007. Con Enterprise Console versión 3.0, la gestión de la seguridad es aún más fácil. Enterprise Console sincroniza con Directorio Activo para garantizar la aplicación automática de la política de seguridad elegida en los ordenadores nuevos que se añaden a la red. Sophos Email Security and Control protege contra amenazas entrantes y salientes con efectividad y sencillez sin igual, ofreciendo seguridad de alto nivel contra spam al 98% de detección, pesca de información, virus, programas espía y programas maliciosos. Defensa SXL contra spam en tiempo real. La exclusiva inspección del tráfico Web en dos direcciones observa las solicitudes entrantes, salientes y el contenido activo en busca de intenciones maliciosas. Este método impone políticas de uso aceptable e identifica y bloquea programas maliciosos y aplicaciones no deseadas, impidiendo su entrada en la red a través del navegador Web. Con un solo escaneado, el programa antivirus detecta virus, programas espía y publicitarios, archivos y comportamientos sospechosos, aplicaciones no autorizadas de voz sobre IP, mensajería instantánea, P2P y juegos, eliminando la dependencia de productos independientes. Permite crear y actualizar rápidamente políticas de seguridad. Las políticas de seguridad se imponen automáticamente al añadir ordenadores nuevos a la red gracias a la sincronización con Directorio Activo. Así se elimina el riesgo de que los ordenadores sin protección pongan en peligro la seguridad. La exclusiva tecnología Behavioral Genotype® protege contra amenazas nuevas y conocidas analizando el comportamiento antes de la ejecución. Las tecnologías integradas de prevención contra intrusiones detectan programas maliciosos, archivos y comportamientos sospechosos y ofrecen una protección completa y proactiva de

	fácil instalación y configuración. Actualizaciones del producto sin límite y sin preguntas, sin gastos ocultos. No es necesaria la intervención del usuario o del administrador, ya que funciona de forma similar a las actualizaciones regulares. Las actualizaciones se ejecutan automáticamente cada 5 minutos. Provee además una amplia gama de informes gráficos personalizados sobre alertas de virus, infecciones y estado de la protección Incluye soporte durante las 24 horas, todos los días del año, mientras dure la licencia.
McAfee: McAfee Total Protection for Secure Business	Solución de seguridad que proteja la red en todo nivel a largo plazo, brinda protección integral sin riesgos. La implementación de seguridad integral fácil y eficiente, gracias a la consola de administración de seguridad única y centralizada de Total Protection. Gestión de seguridad simplificada con una sola consola brindando protección total de su empresa además de mantenerle informado con informes gráficos. Protección preventiva de sus sistemas impidiendo que programas malintencionados, espías y otros no deseados se instalen en sus equipos. Exploración de correo electrónico para detectar spam, contenidos inapropiados y virus, poniéndolos en cuarentena antes de que entren o salgan de la red. Permite la creación de reglas de filtro de contenido. Previene la pérdida de datos gracias a la encriptación completa de datos, niega el acceso no autorizado a aquellos datos considerados como delicados, dejándolos inutilizables en caso de pérdida o robo de su equipo de trabajo. Permite el uso de la Web con confianza gracias a la protección de tres capas que incluye filtro de URL ayudándolo a supervisar y controlar el uso de la Web. Además permite la creación de políticas de uso aceptable
CA: CA Threat Manager Total Defense	Combina las mejores soluciones de protección: CA Antivirus, CA Anti-Spyware, CA Gateway Security y CA Host-Based Intrusión Prevention System. Ofreciendo una protección dinámica ante amenazas conocidas y los ataques de día cero, un firewall independiente con detección de intrusiones y medidas de prevención además de una solución de puerta de enlace unificada. Permite además la implementación de políticas de seguridad y el filtrado de URL.
Hacksoft: The Hacker v6.4	Protección antivirus y anti-spam para servidores de correo, plataforma Linux Proporciona una protección antivirus 100% eficaz, impidiendo que los virus lleguen a su sistema por intermedio del correo electrónico, poniendo en riesgo la seguridad de los sistemas informáticos de la empresa. Integración con nuevas tecnologías anti-spam para el correo electrónico no deseado, uso de listas negras, blancas, etc. Cuenta con filtros que permite reducir el ataque de los virus informáticos. Disponible para servidores Windows, Linux y Novell Netware