INFORME TECNICO

ADQUISICION DEL SOFTWARE ANTIVIRUS EMPRESARIAL

Aprobado por:

JUAN PABLO NOEL ARANA
GERENTE DE INFORMATICA

CONTENIDO

I. NOMBRE DE LAS AREAS INVOLUCRADAS:

a. GERENCIA DE INFORMÁTICA
b. UNIDAD DE SOPORTE TECNICO
c. UNIDAD DE DESARROLLO Y PRODUCCION DE LA OFICNA DE INFORMATICA

II. RESPONSABLES DE LA EVALUACION:

a. JUAN PABLO NOEL – GERENTE DE INFORMÁTICA
b. PEDRO RIVERA – JEFE DE UNIDAD DE DESARROLLO Y PRODUCCION

III. FECHA

31 de Enero del 2008

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) 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, Editora Perú requiere adquirir un producto antivirus que permita brindar seguridad y control de primer para lo cual se *establecerá los atributos o características mínimas para la adquisición de dicha solución.*

V. ALTERNATIVAS

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 2007).

- SECUNIA (Lista Cronológica de Virus obtenido de los 7 principales fabricantes de productos de seguridad que reporta al fabricante que reaccionó con mayor velocidad ante la aparición de nuevos virus - (http://secunia.com/chronological_virus_list/)

- AV-TEST.ORG (Detección de malware desconocido - http://sunbeltblog.blogspot.com/2008/01/latest-antivirus-test-results-from.html)

Así mismo se han considerado los 2 fabricantes de productos de seguridad nacionales.

Los productos analizados son:

Trend Micro	:	InterScan Virus Wall 3.53
Etrust	:	eTrust Antivirus r8
Symantec	:	Symanctec Antivirus Enterprise Edition 10.1
Sophos	:	Sophos Endpoint Security and Control 7
Per Antivirus	:	Per Antivirus Suite 9.7
Hacksoft	:	The Hacker v. 6.0 para estaciones y servidores.
Mcafee	:	Total Protección Solution for Enterprise.

VI. ANALISIS COMPARATIVO TECNICO

Se realizo aplicando la parte 3 de la Guía de evaluación de Software:

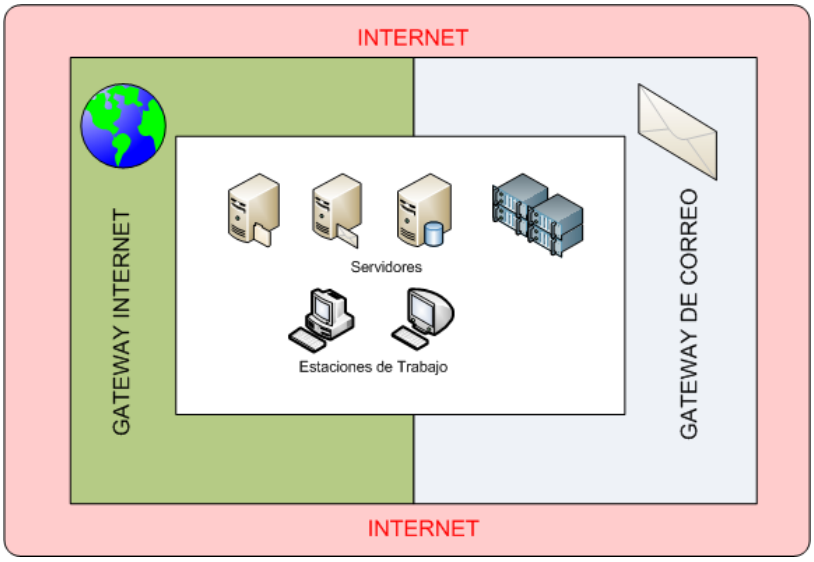
a. Propósito de la Evaluación:

Determinar los atributos o características mínimas para el Producto Final del Software 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)



b. Identificar el tipo del producto

Software de Seguridad Integrada para la protección multi-amenazas.

- anti-virus.
- anti-spyware.
- anti-adware and PUAs.
- control de aplicaciones.
- detección de intrusos de host – HIPS.
- cliente firewall.
- anti-spam
- anti-phishing.
- control del contenido de correo.
- bloqueo de sitios web maliciosos.
- filtrado de productividad web.

c. Especificación del Modelo de Calidad.

Se aplicará el Modelo de Calidad de Software descrito en la Parte I de la Guía de Evaluación de Software aprobado por Resolución Ministerial Nº 139-2004-PCM.

d. 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.

ATRIBUTOS INTERNOS		
ITEM	ATRIBUTO	DESCRIPCION
1	Sistemas Operativos Estaciones de Trabajo	▪ Windows 98/Me/2000/XP/Vista 32/64 bits ▪ Mac OS X 10.2/10.3/10.4 y 10.5 ▪ La solución deberá soportar las versiones de 32 y 64 bits.
2	Sistemas Operativos Servidores de Red	▪ Windows NT Server, Microsoft 2000 Server, Microsoft Server 2003 32/64 bits ▪ La solución deberá soportar las versiones de 32 y 64 bits
3	Actualizaciones	▪ Deben ser manuales y automáticos (programadas) del fichero de firmas de virus y del motor de búsqueda en los servidores y estaciones de trabajo desde Internet. Debe brindar la creación de repositorios distribuidos y programados. ▪ El tamaño de las actualizaciones debe ser pequeño (promedio 7Kb de tamaño). *El postor deberá certificar con información oficial del fabricante ya sea por medio de brochures 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 (pre-execution)*" y "en ejecución (on-execution)". ▪ La solución debe incluir también una tecnología de detección de intrusos de host (HIPS) que brinde protección *en acceso* embebido 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) 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 desde: 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 antivirus y el cliente Firewall en forma centralizada. o La consola debe permitir la administración simultánea de equipos y servidores Windows, Linux y Mac. o La herramienta deberá ser escalable, el cual permite activar la administración de complejas redes, permitiendo la administración de más de 250 equipos desde una sola consola. o La consola debe sincronizarse con el Directorio Activo para la instalación automática de la solución de seguridad en los equipos. o La frecuencia de actualización de firmas de virus debe ser cada 10 minutos o menos. o La administración deberá estar basada en Políticas y debe contener al menos políticas para Actualización, Antivirus, Control de Aplicaciones y Firewall. o 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. o 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. o Debe incluir la capacidad para la desinfección y limpieza remota de adware/aplicaciones potencialmente peligrosas, así como también de virus, troyanos, gusanos y spyware. o La consola debe poder utilizar al menos 3 tipos diferentes de mecanismos para detectar equipos en la red (TCP/IP, Active Directory y otros). o Se debe poder crear políticas de actualización para equipos con conexión lenta pudiendo limitarse el ancho de banda utilizado durante las actualizaciones. o 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. o La consola deberá contar con un sistema de reportes y mecanismos de notificación de eventos vía correo electrónico. o 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).	▪ La solución de seguridad para estaciones y servidores debe ser de tipo Integrada; es decir debe incluir un *único agente* que brinde protección frente a virus, spyware, adware, comportamientos sospechosos, hackers (firewall personal) y aplicaciones potencialmente peligrosas en todos los protocolos de la red . ▪ Debe contar con la capacidad de integración con las políticas de seguridad de Cisco NAC y deberá incluir un Firewall Personal del mismo fabricante. a. El firewall personal 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 para Linux debe poder realizarse desde la línea de comandos y mediante una in-

		terfaz Web en forma local y debe contar con al menos una certificación tipo RedHat Ready o Novel 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 del mismo fabricante*** 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 virus, adware y spyware 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 del fabricante 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 hacer reglas de filtrado por usuario. ▪ 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 administrado de la cuarentena por usuario que permita a su vez administrar la lista blanca y negra de cada usuario. o 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 contra con al menos con cincuenta (50) tipos de categorías organizados de acuerdo al contenido de cada sitio web. ▪ 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 Impre-

		sión de Página web oficial). ▪ Deberá contra 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 (musica, videos). ▪ Deberá contar con un plug-in para la integración con Microsoft ISA Server. ▪ 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 contenga 10 o más reportes y 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 compañía.
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 pro-

		ducto cuenta con un escaner de una vía que permita detectar malware y realizar el filtrado URL 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 numero 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 de la empresa lograr las metas específicas con exactitud e integridad, de acuerdo a las especificaciones técnicas y requerimiento de la organización.

e. 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 de software antivirus, que sirvan para una posterior comparación y evaluación.

VII. ANALISIS COMPARATIVO TECNICO DEL COSTO – BENEFICIO.

- En el Anexo II se puede apreciar un cuadro comparativo de ventajas de los productos software que fueron analizados técnicamente.
- El Análisis Tecnico costo – beneficio tiene como referencia la cantidad de licencias de software antivirus posibles de adquirir, tal como se puede apreciar en el cuadro adjunto.

ITEM	ATRIBUTOS	ESCALAS	InterScan	eTrust	Simantec	Sophos	PER	HACKER	McAfee
	ATRIBUTOS INTERNOS								
1	Sistemas Operativos Estaciones de trabajo	5	5	5	4	5	5	4	5
2	Sistemas Operativos Servidores de Red	5	5	5	5	5	5	5	5
3	Actualizaciones	6	6	6	6	6	6	6	6
4	Protección Proactiva	8	7	7	8	7	8	7	7
5	Control y Productividad en la	9	8	7	8	8	7	7	8
6	Compatibilidad	3	3	3	3	3	3	3	3
7	Instalación	5	4	5	5	5	4	4	5
	ATRIBUTOS EXTERNOS								
8	Administración	6	5	5	4	6	5	5	6
9	Defensa Integrada	6	5	5	5	6	5	5	6
10	Defensa en el Perímetro de la	9	8	9	8	9	7	8	8
11	Escaneo	6	6	6	5	6	6	6	5
	ATRIBUTOS DE USO								
12	Productividad	5	5	5	5	5	5	5	5
13	Alertas y reporte	6	6	6	6	6	6	6	6
14	Facilidad de uso	6	6	6	6	6	6	6	6
15	Soporte Técnico al usuario	7	7	7	6	7	7	7	7
16	Eficacia	8	8	8	8	7	8	8	7
	PUNTAJE TOTAL	100	94	95	92	97	93	92	95

VIII CONCLUSIONES.

- Se derteminó 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.
- El resultado identifica a SOPHOS ENDPOINT SECURITY AND CONTROL, como el software que cumple comparativamente con los requerimientos de la institución

ANEXO I
CUADRO DE ANALISIS DE SOFTWARE ANTIVIRUS.

ANTIVIRUS	CARACTERISTICAS	REQUERIMIENTO
Trend Micro: PC-Cillin	Avanzado controles paternos. Completa seguridad antivirus.	MS. Windows 98 2edition, Windows 2000Professional SP4, Windows XP

	Control de la red doméstica. Defensa anti fraudes de phishing. Detección de intrusos WI-FI Eficaz protección antipyware. Evaluación de vulnerabilidades. Mejorado filtro antispam Mejorado FIRE wall personal.	Home Edition, Professional SP1 y SP 2. MS. Windows 98SE: Intel Pentium 233Mhz o superior. MS: Windows XP: Intel Pentium 300Mhz o superior. MS Internet Explore 5.5 SP: 2 o superior. MS. Windows 98SE: 128 Mb o superior. MS: Windows XP: 128 Mb o superior. 120Mb de espacio libre en disco duro. MS Outlook Express 6.0 MS Outlook 2000. 2002, 2003 Mensajería Instantánea. MS Windows Messenger 4.7 o 5.0 o 6.2 Trend Micro AntiSpam (Herramientas AntiSpam adicionales) Windows 2000 SP4 o superior.
Symantec Antivirus Enterprise Edition	Paquete integrado de las tecnologías galardonadas Mail Security para SMTP, Mail Security para Microsoft Echange, Mail Security para Domino Antivirus Corporate Edition y Web Security de Simantec. Protección líder del mercado de servidores y estaciones de trabajo de red desde una consola central, incluso en entornos informáticos mixtos. Protección antivirus escalable y de alto rendimiento para gateways de web y correos electrónicos de Internet de gran volumen de trafico.	Servidor: Windows XP Professional, Windows Server 2003, Windows 2000 Professional Cliente: Windows XP Professional, Windows Server 2003, Windows 2000 Professional. Consola de Administración Windows XP Professional, Windows Server 2003, Windows 2000 Professional. SymantecMail Security – Servidor de Correo. Windows Server 2003, Estándar, Enterprice , Windows 2000 Server
Per Antivirus: Per Antivirus	Rutinas Inteligentes a nivel de Kernel del sistema que optimizan el filtrado	Windows 98 Windows NT Server

Aprobado por:

JUAN PABLO NOEL ARANA
GERENTE DE INFORMATICA

Suite	y detección de virus de ultima generación en as nuevas arquitecturas de hardware Hiper Threading de Intel. Tecnología Wise Heuristion, detecta y elimina nuevas especies virales, aun desconocidas. Protección contra virus de correo, Chat, ICQ, Mensajeria instantánea per to per. Integración con el Security Center de MS Windows XP.	Windows 2000 Server Windows XP Profesional Windows 2003 Server.
Hacksoft: The Hacker	Motor de búsqueda mejorado con tecnología de punta para detectar y eliminar todo tipo de virus backdoons, troyanos, strips, gusanos y aplicaciones no deseadas. Análisisde 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. Servicio de soporte técnico las 24 horas, los 365 días del año. Reinstalación del antivirus cuantas veces sea necesario.	Estaciones: Windows XP/98 Servidores: Windows 2003, NT, 2000 server

Sophos: Sophos Endpoint Security and Control 7	Control de virus, programas espía, hackers, voz sobre IP, mensajería instantánea y juegos 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. * 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 * Soporte técnico 24 horas Más seguridad y control 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) También puede controlar la instalación y el uso de programas no autorizados, como aplicaciones de voz sobre IP, mensajería instantánea, intercambio de archivos y juegos. **Consola única simplificada y automatizada.**	# Plataformas compatibles Windows Vista Windows 2003 Windows XP Windows 2000 Windows 95/98/Me y NT4 VMWare ESX 3.0 VMWare Workstation 5.0 VMWare Server 1.0 # Espacio en el disco Windows 2000/XP/2003/Vista: 120 MB Windows NT4: 90 MB Windows 95/98/Me: 90 MB # Microsoft Exchange 2000 SP3 # Microsoft Exchange 2003 SP1 # Microsoft Exchange 2007

	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 **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.	
McAfee	Una sola consola de administración: Un solo punto de administración, informaes e implementación de seguridad para una protección completa antivirus, antiespia antspam, FIRE wall para PC´s. Control de acceso a al red: Sólo permite, que accedan a la red los sistemas que cumplan las normas de seguridad. Antivirus para PC's y servidores de Archivo: Proporciona una protección avanzada contra programas malintencionados parala parte de su sistema que resulta mas difícil de de administrar. Antiespias para PC´s: Una autentica explotación en el momento del acceso identifica, bloqueos de forma preventiva y elimina de forma segura los programas potencialmente no deseados.	Procesador Intel u otra arquitectura compatible. PC: Windows NT, 2000 Professional, XP Home o Professional. Servidores: Windows NT, 2000 server, 2003 server, Enterprice Serve. Otras Plataformas compatibles: XP Table PC, Citrix, EMC RAM: 128Mb y 256Mb para servidor Servidor de Correo: 2000 server, 2003 server, Exchange 2000, etc.

	Prevención de intrusiones n PC¨s: Vigila y bloquea las instrucciones de forma preactiva combinando la protección por firmas y por comportamientos con un FIRE Wall para PC´s . Protección del correo electrónico contra Spam y virus: Bloquea y elimina virus de los correos electrónicos.	
Trend Micro InterScan Virus Wall	Actualización automática de archivos patrón de virus. Administración Centralizada a través de la Integración de otros productos de Trend Micro. Administración y configuración flexibles. Compatibilidad con los principales firewall y productos de otros fabricantes. Opciones de respuestas múltiples en contra de brotes de epidemias. Producción de tiempo real de Gateway.	MS Windows InterScan Virus Wall 3.53. Procesador Intel Pentium II 200 Mhz o mayores Windows 2000. Windows NT.4.o con sevice pack 3 instalado o versión posterior. 256 Mb de RAM. 100 – 500 Mb de espacio en disco para archivos de Intercambio.

ANEXO II
VENTAJAS DE SOFTWARE ANTIVIRUS

ANTIVIRUS	VENTAJAS
Trend Micro: InterScan Virus Wall	Provee un alto desempeño, protección completa en gateway de Internet en contra de amenazas de virus y códigos maliciosos. Opcionalmente se integra a eManager de fácil integración que ofrece a los administradores herramientas adicionales para el bloqueo de Spam, filtrado de contenido y planeación para correos electrónicos.
Trend Micro: PC-	Combina la tecnología de la seguridad antivirus con un FIRE Wall per-

Cillin	sonal para ofrecer una completa protección contra virus, troyanos, hackers. También detecta y elimina el spyware y bloquea el Spam. Incluso proporciona protección frente a los ataques de robo de identidad mediante le bloqueo de de los ataques de phishing y pharming. Además PC CILLIN protege las redes inalámbricas mediante la detección de Intrusos Wi-Fi, una función de seguridad innovadora que le avisa cuando un intruso utiliza su conexión inalámbrica.
Sophos: Sophos Endpoint Security and Control	Ofrece una protección superior unifica a un precio promedio. Una única licencia permite proteger todos los puntos vulnerables del a 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 Active Directory 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. Las políticas de seguridad se imponen automáticamente al añadir or-

	denadores nuevos a la red gracias a la sincronización con Active Directory. 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.
Symantec Antivirus Enterprise Edition	Un paquete integrado con soluciones galadornadas de Symantec Mail Security para SMTP, Mail Security para MS Exchange, Mail Security para Domino. 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. Servicio complementario Symantec Premiun AntiSpam, integrado opcional para los productos Symantec Mail.
Per Antivirus: Per Antivirus Suite	Actualización diaria automática y veloz a través de Internet, solo para usuarios de la versión vigente. Protección integral contra toda clase de virus actuales existentes en el Mundo. Protección en toda clase de medios de almacenamiento (USB, Memory Stick, etc.). Protección a todas las plataformas de MS. Per FIRE Wall Multiplataforma bloquea e impide cualquier intento de de ataque a su PC, por intrusos a través de cualquier servicio de Internet o puertos TCP /UDP e ICMP y controla el acceso a programas y servicio de Internet no autorizados.
Hacksoft: The Hacker	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 ANTISPAM para el correo electrónico no deseado, uso de listas negras, blancas, etc. Cuenta con filtros que permite reducir el ataque de los virus informáticos.

Aprobado por:

JUAN PABLO NOEL ARANA
GERENTE DE INFORMATICA