INFORME Nº 001-2011- USI

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE

1. Nombre del área

La unidad asignada de la evaluación técnica para la adquisición de un software antivirus es la Unidad de Seguridad Informática de la Caja Metropolitana.

Las áreas usuarias que se estarían beneficiando en la adquisición de este producto son todas las áreas de la Caja Metropolitana.

2. Nombre y Cargo del Responsable de la evaluación

Los analistas responsables de la evaluación son los señores Jhon Alvarado y Luis Espinoza, Jefe y Asistente de la referida unidad.

3. Fecha

La fecha del presente informe es del 25 de mayo del 2011.

4. Justificación

El objetivo de este documento es especificar detalladamente las pruebas realizadas a los antivirus, los cuales estuvieron bajo estricta evaluación de acuerdo a parámetros establecidos según requerimientos finales en torno a la seguridad de la empresa.

Este documento abarca los parámetros establecidos para las pruebas, descripciones de las pruebas, fases de pruebas, prolijas descripciones de productos evaluados y conclusiones.

Al término del mes de abril la licencia del antivirus que se usa en la empresa (McAfee) ha caducado, por ello se requiere analizar la viabilidad de un cambio de software antivirus. El antivirus con el que se contó hasta la fecha señalada no ha llegado a brindar funciones primordiales en cuanto a protección de equipos y a actualizaciones. Si nos referimos al primer contexto podemos señalar que se ha llegado a comprobar que el antivirus no puede eliminar ni desinfectar algunos virus, troyanos y gusanos, como es el caso del Conficker, un conocido gusano que se caracteriza por bloquear cuentas de usuario y a propagarse de forma inmediata por la red, causando estragos en ella. A través de reportes diarios se puede observar que los ataques de este gusano se han suscitado de manera paulatina durante gran parte del año 2010 en la empresa. La eliminación de este gusano fue posible por uso de otras herramientas. Otro punto negativo a citar en McAfee es su aumento de porcentaje de registros de falsos positivos. En los meses de febrero y marzo se registraron cerca de 3500 falsos positivos, entre ellos estaban propios archivos del antivirus y herramientas que a diario se usan en diversos equipos de la empresa, como: SICMET, RAdmin, por citar algunos. Dirigiéndonos al otro contexto podemos mencionar que McAfee posee un deficiente ciclo de actualización, es decir, aproximadamente cada 2 días se actualiza y sus paquetes de instalación tienen un gran tamaño, lo que es una desventaja para la distribución de esos paquetes en la red. Podemos añadir también que el proveedor ha brindado un pésimo servicio de soporte técnico.

5. Alternativas

En un primer momento se tuvo la participación de 4 proveedores que ofrecían antivirus como: ESET Nod 32, G Data, Kaspersky y eScan. A lo largo del proceso de evaluación se canceló la evaluación de ESET por la desidia mostrada del proveedor (falta de interés, no cumplir con cronogramas) y también se canceló la evaluación de eScan porque su nueva versión –de este año- no posee un sistema de administración adecuado en su consola para las actualizaciones, por ello en el presente informe solo se observarán datos correlativos a G Data y Kaspersky. Ante tales sucesos solo se tuvieron las 2 alternativas siguientes:

- G Data
- Kaspersky

6. Análisis comparativo técnico

A lo largo de 17 días se han evaluado 2 productos, los cuales son:

- ✓ G Data 10.7.1.115 (versión 2010)
- ✓ Kaspersky Total Space Security International Edition 150-249

Para las pruebas se han tomado los siguientes parámetros a considerar:

- ✓ Consola de administración
- ✓ Capacidad de detección de malware
- ✓ Detección de falsos positivos
- ✓ Manejo de actualizaciones
- ✓ Rendimiento en equipos (Uso de CPU, uso de memoria)
- ✓ Capacidad de desinfección de malware

En base a los requerimientos de seguridad informática de la empresa se ha previsto que el software antivirus cuente con las siguientes características que se adjuntan en la tabla:

Atributo	Descripción
Características generales	• Mostrar información de la seguridad en tiempo real de todos los recursos protegidos. • La instalación del software a los computadores de los usuarios debe de ser directamente desde la Consola de Administración, además de la posibilidad de instalación mediante CD o recurso UNC. • La administración centralizada no debe requerir un servidor dedicado. • Configuración para formar grupos de equipos y aplicar distintas directivas y/o políticas del software antivirus por grupo de equipos a través de la consola de administración. • El producto debe ser capaz de bloquear, por un tiempo determinado, aquellas máquinas que traten de infectar la PC protegida mediante recursos de red. • Debe ser posible para el usuario hacer acciones de rollback de definiciones de virus, en el posible caso de que las definiciones

	puedan tener problemas con alguna aplicación específica. • El producto debe contar con tecnologías que mejoren el performance de los escaneos, mediante el uso de uso de algoritmos que en base a la firmas de virus, última vez que el archivo fue escaneado, fecha de modificación determinen si un objeto debe o no ser escaneado y su escalabilidad entre niveles de compresión de cualquier formato. • La protección en tiempo real debe tener niveles predefinidos de protección e igualmente debe permitir al usuario personalizar el nivel de protección de acuerdo a sus requerimientos. • La consola de administración deberá de ser capaz de permitir la generación de reportes gráficos y personalización de los mismos. • La solución ofertada no deberá consumir muchos recursos de memoria y procesador en los equipos usuarios • El producto debe permitir la detección y protección activa de de los dispositivos USB de las estaciones de trabajo, computadoras mono usuario y servidores y permitir el escaneo y la vacunación automática o manual de estos dispositivos de almacenamiento externo. • El producto debe contar con un modulo de protección en tiempo real para correos que debe tener las siguientes características: a. Debe poder integrarse con Microsoft Outlook. b. Debe poder escanear a través de los puertos SMTP, POP3, IMAP, NNTP. c. Debe tener niveles predefinidos de protección e igualmente debe permitir al usuario d. personalizar el nivel de protección de acuerdo a sus requerimientos e. Debe ser posible definir si se desea escanear sólo tráfico entrante, tráfico saliente o ambos. f. Debe tener la opción de no escanear archivos adjuntos. g. Debe tener la opción de poder detener el escaneo luego de un tiempo el cual se puede programar. h. Debe tener una opción de filtrado de archivos adjuntos, permitiendo especificar qué tipo de archivos serán renombrado o eliminados. i. Debe tener la capacidad de proteger al usuario de ataques tipo phishing. j. El antivirus debe ser capaz de escanear las bases de datos de correos archivados en la computadora. k. El antivirus debe tener una base de datos de enlaces URLs que tienen contenido malicioso y que deben ser bloqueados automáticamente l. Debe tener un motor heurístico para detección de posibles nuevos virus, el nivel de la heurística debe poder ser personalizable.
Estaciones de trabajo	• El software antivirus debe poder instalarse en su última versión sobre plataformas Windows 2000, XP Professional, Vista Business y Windows 7 Professional. • El antivirus también deberá soportar la instalación en plataformas de

	64 Bits. • El producto debe contar con un módulo de detección en tiempo real que proteja contra: virus, gusanos, troyanos, keyloggers, dialers, adware, spyware, hacktools, rootkits, bots, spam, herramientas de control remoto y otros programas potencialmente peligrosos. • El producto debe ser capaz de monitorear el comportamiento de aplicaciones específicas, para determinar el posible uso o intento de modificación de estas aplicaciones por agentes maliciosos y bloquear estas acciones. • El producto debe ser capaz de evitar que sus procesos, servicios, archivos o archivos de registro puedan ser detenidos, deshabilitados, eliminados o modificados, para de esta manera garantizar su funcionamiento ante cualquier tipo de ataque de virus. • El producto debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión, aplicación específica o malware específico. • El producto antivirus debe poder realizar escaneos manuales o programados, indicándose las unidades a escanear o las carpetas específicas que requieren ser escaneadas. • El producto debe pedir una contraseña ante intentos de cambio indebidos en la configuración del producto.
Servidores	• El software antivirus debe poder instalarse en su última versión, sobre plataformas Windows NT Server, Windows 2000 Server, Windows 2003 Server, Windows 2008 Server. • El antivirus también deberá soportar la instalación en plataformas de 64 Bits. • El producto debe contar con un modulo de detección en tiempo real que proteja contra: virus, gusanos, troyanos, keyloggers, dialers, adware, spyware, hacktools, rootkits, bots, herramientas de control remoto y otros programas potencialmente peligrosos • El producto debe ser capaz de evitar que sus procesos, servicios, archivos o archivos de registro puedan ser detenidos, deshabilitados, eliminados o modificados, para de esta manera garantizar su funcionamiento ante cualquier tipo de ataque de virus. • El producto debe ser capaz de crear exclusiones de escaneo ya sea por archivo, extensión, aplicación específica o malware específico. • El producto antivirus debe poder realizar escaneos manuales o programados, indicándose las unidades a escanear o las carpetas específicas que requieren ser escaneadas. • El producto debe pedir una contraseña ante intentos de cambio indebidos en la configuración del producto. • El producto debe contar con un cliente antivirus y con un agente que le permita ser administrado desde una consola centralizada. • El producto debe ser capaz de detectar el número de procesadores que tiene el servidor y en base a esto balancear la carga del trabajo del antivirus entre los procesadores. • El producto debe permitir escanear archivos comprimidos ya sea con escaneos bajo demanda y escaneos programados. • La protección en tiempo real debe contar con una opción para pausar automáticamente la revisión antivirus en base a un horario o cuando

	se ejecute determinada aplicación. • Debe tener un motor heurístico para detección de posibles nuevos virus, el nivel de la heurística debe poder ser personalizable.
Consola de administración	• La consola de administración debe permitir la configuración y administración remota de la solución antivirus instalada en las estaciones de trabajo y servidores. • La consola debe poder instalarse sobre Windows NT Server/Workstation, Windows XP Professional, Windows 2003 Server. • La solución antivirus debe poseer una consola de administración centralizada a la cual debe reportar su estado todas las soluciones antivirus instaladas en la dependencia. • El producto debe ser capaz de mostrar las PCs detectadas en la red. • El producto debe ser capaz de agregar a un grupo administrativo, automáticamente una PC nueva que ingresa a la red. • El producto debe ser capaz de automáticamente instalar el antivirus en aquellas Pc's nuevas que ingresen a la red. • La consola de administración centralizada debe tener la capacidad de mostrar los intentos de infección de virus en las PCs clientes. • El producto debe permitir al administrador visualizar características de la PC, tales como: a. Sistema Operativo y versión del mismo. b. Nombre de la PC y dirección IP c. Dominio al que pertenece. d. Usuario logueado en el equipo e. Tipo de procesador • La consola de administración debe ser capaz de poder tener múltiples políticas de seguridad, pudiendo activar, una política específica ante epidemias de virus. • La consola deberá permitir una estructura jerárquica para una mejor administración de los clientes antivirus. • Las políticas de administración de grupos deben poder heredar o no (a criterio del administrador) políticas de grupos con mayor jerarquía. • El producto debe permitir la instalación y desinstalación remota de los antivirus en los servidores y clientes antivirus. • El producto debe ser capaz de actualizar las definiciones de virus de los paquetes de instalación a enviar, para de esta manera evitar el tráfico de red, que ocurre después de la instalación del producto. • El producto debe ser capaz de crear un paquete de instalación consolidado (archivo ejecutable) que pueda ser accedido mediante la red, para la instalación de los antivirus o del agente. • El producto debe ser capaz de generación de alertas ante un evento específico mediante el envío de un correo, el envío de mensajes de red (netsend) o la ejecución de un archivo. • Las actualizaciones deben ser descargadas centralizadamente para que los clientes actualicen desde el servidor de administración sus definiciones de virus, phishing, SPAM, actualización de parches del producto entre otras.
Servidor de correo	• Protección antivirus a nivel de servidores de correo Exchange 2000, 2003, 2007 y 2010. o Escaneo de virus en el correo entrante, saliente y en el mail

	almacenado en el servidor. o Reconocimiento de spam en adjuntos utilizando tecnologías inteligentes propietarias. Escaneo en busca de virus, gusanos, hack tools, adware, spyware, en tiempo real. Capacidad de escaneo programado en background de los mensajes almacenados. o Backup del malware detectado (virus, gusanos, troyanos, spam, etc.), para hacer posible la restauración de la información si un intento de eliminación de virus falla o ante un falso positivo ocasionado por el motor antispam. o Actualización programada, independiente del motor de búsqueda de virus y del motor de búsqueda de spam. o El producto debe trabajar con firmas de SPAM y debe ser capaz de poder detectar variaciones de SPAM, que intenten evadir los controles antispam. o El producto debe ser capaz de revisar el cuerpo del mensaje y los adjuntos en busca de palabras o frases que generalmente se encuentran en los correos SPAM.

Tabla 4.1. Características con las que debe contar el software antivirus para la empresa.

a. Consola de administración

1. ***G Data:*** Su consola de administración dista de parámetros de usabilidad, no es intuitiva.

2. ***Kaspersky:*** Su consola de administración deriva de la consola de Microsoft Windows (MMC), por lo que un usuario típico de este sistema operativo se sentirá más familiarizado en cuanto a usabilidad e interacción con la interfaz de usuario.

b. Capacidad de detección de malware

Para ambos antivirus se hicieron las pruebas con los mismos virus, troyanos y gusanos. En la siguiente tabla se aprecian los resultados:

Antivirus / **Malware**	**G Data**	**Kaspersky**
Cam.Trojan.Downloader.Win32 (Genérico)	Detectó	Detectó
Hacktool.Win32 (Genérico)	Detectó	Detectó
JWGKVSQ.VMX	Detectó	Detectó
SXOLPE.exe	Detectó	Detectó
SYMDRVMN.exe	Detectó	Detectó
AMVO.exe	Detectó	Detectó
Recycler.exe	Detectó	Detectó
Facemoodssr_v.exe	Detectó	Detectó
Win32.Agent.Fbx	Detectó	Detectó

Generic joke	Detectó	No detectó

Tabla 4.2. Lista de malware sujeto a pruebas de detección.

La capacidad de detección de ambos es alta, salvo el caso de “Generic joke”, en los demás casos ambos antivirus detectaron todo. Este particular caso (Generic joke) deviene de un código fuente hecho en un simple editor de texto y convertido a archivo por lotes, está diseñado para ejecutarse cada vez que se inicie sesión. Su ejecución implica copiar réplicas en la carpeta raíz, en la carpeta de los archivos del sistema y en el escritorio.

c. Detección de falsos positivos

Solo se registró un caso de falso positivo, G Data reconocía a la aplicación SicmactAdmin.exe como un troyano, a pesar de realizar las exclusiones correspondientes en su consola, no se pudo evitar que siempre se reconozca a este ejecutable como troyano. Personal de Soporte Técnico de G Data se hizo cargo del asunto enviando una muestra a los laboratorios del antivirus, con una nueva actualización ya no se reconocía como troyano. Lo desfavorable a G Data es la inoperancia de sus exclusiones que nada pudieron hacer. Mientras tanto Kaspersky no tuvo algún problema de falso positivo con ningún archivo de los sistemas que se utilizan en la empresa. A diferencia de G Data, Kaspersky apenas se instala en un equipo tiene una heurística para prevenir situaciones de falsos positivos. Por ejemplo, McAfee siempre ha tenido problemas en excluir al software RAdmin, lo reconoce como un troyano y lo elimina, Kaspersky de por sí ya tiene agregado en su base de datos el reconocimiento a esa clase de aplicaciones, también hay una sección configurable de exclusión.

d. Manejo de actualizaciones

En la administración de actualizaciones ambos productos muestran similares características; el modelo actual de replicación y distribución de actualizaciones guiado por McAfee se adapta perfectamente a la empresa ya que se optimiza el consumo de ancho de banda por lo que la idea principal es que algunos de estos productos tenga una característica similar o incluso mejor.

Vayamos primero con G Data, acá se puede tener 2 características:

- **Centralizada:** Se tiene un nodo principal (un único servidor), del cual parten las actualizaciones. Su principal desventaja es que se consume en demasía el ancho de banda.
- **Descentralizada dependiente:** Se tiene un nodo principal y nodos secundarios, los cuales actúan como intermediarios para la actualización, estos nodos distribuyen las actualizaciones en las máquinas que estén en su misma red de área local. La desventaja es que con G Data se tienen que instalar consolas en cada nodo secundario, lo cual dista de entrar en estándares de seguridad informática porque tener entre 30 y 40 consolas implica un riesgo, muy aparte que no todos los nodos secundarios en agencias serían servidores, hay PCs que son usados día a día por usuarios y actúan como intermediarios (con McAfee a través de una carpeta compartida se distribuyen las actualizaciones).

Por otro lado, Kaspersky ofrece también una gestión centralizada, una descentralizada no dependiente y compartida. Se dice que es descentralizada no dependiente porque a diferencia de G Data, no se tienen que instalar consolas en los nodos secundarios, en este

caso se llaman agentes de actualización, que son definidos en la consola de administración. Estos agentes también pueden desplegar actualizaciones automáticas, para ello se definen los paquetes de instalación.

e. Rendimiento en equipos

Los equipos donde se probaron los antivirus tenían un estándar en cuanto a hardware. Los requisitos mínimos a considerar para pruebas fueron:

- Φ Procesador de 1.80 Ghz
- Φ Memoria RAM 956 MB

Se tomaron en cuenta los análisis locales y remotos; el rendimiento del equipo se hizo con la herramienta “Rendimiento” del sistema operativo y con la aplicación Process Explorer. Se tomaron en cuenta los siguientes parámetros: Uso del CPU e historial de memoria física. Los resultados se pueden observar en la siguiente tabla:

- Φ Uso de CPU (en porcentaje) en escaneo local:

Tiempo (min) / **Antivirus**	*5*	*10*	*15*	*20*	*25*	*30*	*35*	*40*	*45*	*50*	*55*	*60*	*Prom*
G Data	62.22	38.91	79.13	41.59	87.65	70.09	40.28	25.74	93.2	58.26	67.92	39.7	**58.72**
Kaspersky	2.81	30.82	75.23	60.42	23.11	38.71	78.40	27.36	51.14	6.84	85.28	2.05	**40.18**

- Φ Uso de CPU (en porcentaje) en escaneo remoto:

Tiempo (min) / **Antivirus**	*5*	*10*	*15*	*20*	*25*	*30*	*35*	*40*	*45*	*50*	*55*	*60*	*Prom*
G Data	77.15	33.38	82.17	46.68	83.72	76.90	51.64	31.11	89.48	65.63	74.14	58.33	**64.19**
Kaspersky	71.64	42.81	81.16	53.65	29.36	33.4	77.87	35.21	50.46	16.82	85.39	6.17	**48.66**

Φ Uso de memoria física (en Megabytes) en escaneo local:

Memoria física total = 1 017 328 Kb

Tiempo (min) / **Antivirus**	*10*	*20*	*30*	*40*	*50*	*60*	*Prom*
G Data	722.38	679.29	583.15	549.13	537.46	698.57	**628.33**
Kaspersky	488.61	573.6	419.52	382.68	605.3	426.13	**482.64**

Φ Uso de memoria física (en Megabytes) en escaneo remoto:

Memoria física total = 1 017 328 Kb

Tiempo (min) / **Antivirus**	*10*	*20*	*30*	*40*	*50*	*60*	*Prom*
G Data	769.26	592.31	743.52	661.8	746.95	674.59	**698.07**
Kaspersky	454.12	606.11	513.24	668	587.48	621.1	**575.01**

Se extrapola de los 4 cuadros que G Data consume más recursos que Kaspersky, esto tiene su motivo, G Data usa 2 motores para detección y desinfección: Motor A y Motor B. Por ejemplo para equipos no potentes se recomienda usar solo un motor. Se agrega también que los escaneos (remoto y local) se efectuaron mientras otras aplicaciones hacían uso de porción de memoria y de CPU como: Microsoft Excel 2007, Microsoft Outlook 2007, Internet Explorer 8 y SICMET. Los equipos no evidenciaron lentitud extrema (cuelgue de PC).

f. Capacidad de desinfección de malware

La desinfección parte de las pruebas de detección (ver Tabla 4.3), en ambos antivirus se configuró para que en caso registre alguna amenaza entonces proceda a la desinfección y si en caso no pueda desinfectar entonces elimine el malware hallado. Se obtuvieron los siguientes resultados:

Antivirus / **Malware**	**G Data**	**Kaspersky**
Cam.Trojan.Downloader.Win32	Desinfectó	Desinfectó

(Genérico)		
Hacktool.Win32 (Genérico)	Desinfectó	Desinfectó
JWGKVSQ.VMX	Desinfectó	Desinfectó
SXOLPE.exe	Desinfectó	Desinfectó
SYMDRVMN.exe	Desinfectó	Desinfectó
AMVO.exe	Eliminó	Eliminó
Recycler.exe	Desinfectó	Desinfectó
Facemoodssr_v.exe	Desinfectó	Desinfectó
Win32.Agent.Fbx	Desinfectó	Desinfectó
Generic joke	Eliminó	No detectó

Tabla 4.3. Lista de malware sujeto a pruebas de desinfección.

Kaspersky y G Data coinciden en casi todos los casos, a excepción de Generic joke –que Kaspersky no detectó, como se detalló en el apartado 3.2- y AMVO.exe, que atinaron solo a eliminar. Este malware fue instalado adrede junto a sus variantes en una máquina virtual, ambos antivirus lograron eliminar las variantes aunque en el registro quedaron algunas llaves. Se demuestra que ambos tienen un significativo porcentaje de efectividad en desinfección.

7. Análisis comparativo costo-beneficio

Costo: Se ha tomado como base licenciamiento por un año, la cantidad de licencias es de 650.

Software antivirus	Proveedor	Costo aproximado para 650 licencias
G Data	3W S.A.C.	S/. 32, 260.00
Kaspersky Enterprise Space Security	Business Technology	$ 9, 100.00
Kaspersky Business Space Security	PremiumSoft	$ 13, 000.00

Beneficio: El producto garantizará que las estaciones de trabajo y servidores estén protegidos y también en base a característica proactiva y heurística elimine los diversos tipos de malware.

8. Conclusiones

Como resultado de la evaluación se concluye que el producto de software antivirus más adecuado a las necesidades y que cumple a cabalidad los requerimientos propuestos es **Kaspersky**.

Para llegar a las conclusiones expuestas se ha basado en las siguientes métricas:

Ítem	Criterio	Puntuación máxima	G Data	Kaspersky
1	Desempeño de consola de administración	25	8	23
2	Capacidad de detección de malware	15	14	13

3	Detección de falsos positivos	10	5	9
4	Manejo de actualizaciones	20	10	18
5	Rendimiento en equipos	10	7	8
6	Capacidad de desinfección de malware	15	13	13
7	Control de dispositivos extraíbles	5	5	5
Puntaje total:		100	62	89

Tabla 6.1. Métricas de evaluación y puntuación de productos antivirus