MINISTERIO DE RELACIONES EXTERIORES

INFORME PREVIO DE EVALUACIÓN DE SOFTWARE DGG Nº 010-2008

"Licenciamiento de software de protección de puntos finales (antivirus)"

1. Nombre del Área

El área encargada de la evaluación técnica para la adquisición de las licencias de software de protección de puntos finales (antivirus) es el Departamento de Comunicaciones de la Dirección General de Gestión Informática (DGG).

2. Nombre y Cargo del Responsable de la Evaluación

Jorge Armas Orbegozo, Jefe del Departamento de Comunicaciones

3. Fecha

26 de Setiembre del 2008

4. Justificación

La Dirección General de Gestión Informática del El Ministerio de Relaciones Exteriores plantea la necesidad de garantizar la adecuada protección de los sistemas informáticos, asegurando el normal desarrollo y disponibilidad de las funciones de los procesos organizacionales, procesos cada vez mas dependientes de las tecnologías informáticas, por lo que solicita la adquisición de un software que proteja los puntos finales de virus, malwares, troyanos y cualquier otro tipo de ataque que pretenda vulnerar la disponibilidad de la estación de trabajo.

El ministerio de relaciones Exteriores cuenta en la actualidad con la solución de CA Entrust, adquirida en el año 2006 mediante licitación pública realizada por la PCM en el marco de las compras corporativas

JORGE ARMAS ORBEGOZO
Jefe de Comunicaciones

5. Alternativas

Alternativa Nº 01: Renovación de licencias y mantenimiento de la marca CA.

Alternativa Nº 02: Adquisición de Licencias de Nuevo Software.

El departamento de comunicaciones ha comunicado en un informe los problemas que ha tenido con el software actualmente existente, en este sentido esta dirección considera que la alternativa 2 es la recomendada.

Para ello, se han establecido las especificaciones técnicas que servirán para la posterior evaluación de las propuestas, razón por la cual no se realizará en el presente informe una comparación de productos de software antivirus disponibles en el mercado.

6. Análisis Comparativo Técnico

El Ministerio de Relaciones Exteriores requiere 1000 licencias para ser distribuidas entre servidores, estaciones de trabajo y portátiles, siendo sus especificaciones técnicas las siguientes:

- **Servidores y Estaciones de Trabajo**

Para sistemas operativos Windows 2000/XP/2003
Debiendo realizar:

- Un solo agente
- Análisis de detección y eliminación de virus y malware
- Control de dispositivos
- Firewall personal

- **Servidor de Correo Electrónico Institucional**

Integrarse como servicio del correo Lotus Notes y Exchange 2000/2003, debiendo realizar:

- Análisis de detección y eliminación de virus y malware
- Filtrado de contenido.

- **Administración**

Deberá contar con una Consola Centralizada de Administración con acceso remoto, actualización del motor y/o firmas de Virus vía INTERNET.

- **Servicios**

Deberá proveer:

- Todas las actualizaciones y revisiones que la casa de software fabricante libere para cada uno de los productos de software licenciados.
- Mejoras y correcciones hechas a los manuales que están incluidos en los productos licenciados.
- Servicio de Reporte de Problemas, para las últimas revisiones de los productos de software licenciado. Todos los problemas reportados por el usuario se aceptarán por parte del proveedor del Servicio de Soporte.
- Una nota de aceptación indicando un número de identificación de los problemas reportados.
- Proveerá información del estado del problema reportado.
- La empresa proveedora del Servicio de Soporte proveerá de un soporte telefónico durante las 24 horas, consistente en el aislamiento y definición de problemas y ayuda en la preparación de un p roblema de so ftware reportado.
- Para situaciones que se pueden calificar como críticas, la empresa proveedora del Servicio de Soporte intentará generar un procedimiento alternativo para evitar el problema o una solución temporal en espera de una solución definitiva.

JORGE ARMAS ORBEGOZO
Jefa de Comunicaciones
Dirección General de Gestión Informática

7. Análisis Comparativo de Costo – Beneficio

- **Costos**

Para realizar el estudio de mercado se evaluaron los siguientes productos para identificar montos referenciales

Producto	Licencias	Costo Unitario US$	Costo Total US$	Costo Renovación unitario US$
TrendMicro Neatsuite 5.0	1000	48.00	48,000	19.20
Symantec multitier protection 11.2	1000	40.63	40,630	18.30
CA etrust secure	1000	36.12	36,120	16.25

- **Beneficios**

Este tipo de productos garantizará que los servidores y/o estaciones de trabajo cuenten con protección contra cualquier ataque de Virus o Software malintencionado que afecte el normal desarrollo de las actividades de la institución, requiriendo que el software de antivirus tenga una actualización permanente que le permita enfrentar los ataques, asegurando la continuidad de las labores cotidianas del Ministerio de Relaciones Exteriores.

- **Hardware Necesario**

El Ministerio de Relaciones Exteriores cuenta con el hardware necesario para implantar el producto

8. Conclusiones

Las soluciones antivirus han sido reemplazadas en la actualidad por productos más amplios tanto en capacidad como en seguridad. Las amenazas cada vez más sofisticadas deben ser enfrentadas con soluciones más complejas.

En la búsqueda de una solución de seguridad completa, esta dirección ha encontrado productos que combinan el tradicional antivirus con mecanismos de seguridad avanzados. Protección contra virus, gusanos, spyware, troyanos, amenazas de día-cero y rootkits además de funciones como Firewall personal, prevención de intrusos y control de dispositivos y aplicaciones (Bloqueo de puertos USB). Todas las funciones nombradas anteriormente son realizadas a un único agente con lo que los requerimientos de espacio en disco y memoria son reducidos.

Otro punto importante es la capacidad de estos productos para dar protección proactiva, es decir debe ser capaz de detectar, prevenir y eliminar una amenaza sin la necesidad de contar con una firma conocida. En este aspecto la solución cuenta con las siguientes tecnologías:

- Protección contra el acceso a aplicaciones, que restringe el acceso al registro, los archivos, las carpetas y los procesos (capacidad para bloquear una aplicación)
- Firmas genéricas: Protección basada en vulnerabilidades; una sola firma puede detectar cientos de amenazas nuevas.
- Bloqueo de comportamiento: Analiza el comportamiento de las aplicaciones (aplicaciones conocidas y desconocidas). El bloqueo de comportamiento ofrece una detección más precisa sin la necesidad de instalar configuraciones basadas en normas y sin tener que preocuparse de falsos positivos

La capacidad de estos productos nuevos permiten el control de acceso a dispositivos es un gran punto a favor, no solo permite disminuir el riesgo de infecciones debido al uso de memorias USB que pueden estar infectadas sino que además puede ser configurado para evitar la fuga o robo de información a través de dispositivos extraíbles.

Estos productos que combinan varias funcionalidades y que son la evolución de los productos antivirus son clasificados según el Gartner Group como productos de protección de punto final (End Point Protection plataforms), siendo Symantec, macafee y trendmicro los productos que lideran esta clasificación según el Gartner Magic Quadrant for Endpoint Protection

Por los motivos antes señalados el Ministerio de Relaciones Exteriores requiere contar con una solución de protección de puntos finales institucional, la cual debe implementarse realizando una nueva adquisición de un producto que cu mpla con las especificaciones técnicas solicitad as.

JORGE ARMAS ORBEGOZO
Jefe del Deparatamento de Comunicaciones