INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE Nº 003 GTSI

"CONTROL DE INTERFACES"

1. Nombre del Área

El área encargada de la evaluación técnica para la implementación de software que permita detectar y restringir los dispositivos por tipo, modelo o número serial individual del dispositivo, es la Gerencia de Tecnologías y Sistemas de Información (GTSI) de la Contraloría General de la República.

2. Nombre y Cargo del Responsable de la Evaluación

El encargado de realizar la evaluación es el Sr. Leoncio Rodríguez Manyari, Jefe de Soporte Técnico de la Gerencia de Tecnologías y Sistemas de Información.

3. Fecha

La fecha del presente informe es el 07 de Septiembre del 2006.

4. JUSTIFICACIÓN

Los beneficios de la integración de nuevas tecnologías como USB o WIFI por los incrementos de productividad que aportan a la organización vienen siendo usados dentro de la Contraloría General de la República cada vez más. En términos de seguridad dichas tecnologías también conllevan riesgos que se deben conocer y que pueden resumirse en tres puntos:

- **Robo y filtrado de información**

  La mayoría de la información que genera la Contraloría General se encuentra almacenada sin ningún tipo de protección en los ordenadores portátiles y en las estaciones de trabajo. En la actualidad con la proliferación de dispositivos como iPods, con una capacidad de almacenamiento de 60GB, es muy fácil que esta información sin protección pueda "escapar" fácilmente de la empresa.

- **Ataques dirigidos. Estaciones de trabajo como puertas de enlace**

  Los puertos locales y los interfaces de conexión son una de las vías principales de entrada de virus y troyanos dentro de las empresas,

C.G.R. – GERENCIA DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN – V° B°

convirtiendo la estación de trabajo en una puerta de enlace para entrar en la red corporativa. Como ejemplo, un caso reciente de espionaje empresarial que dio como resultado múltiples arrestos. El ataque fue mediante un troyano que se introdujo en la empresa mediante una presentación en CD.

Teniendo en cuenta estos aspectos, se necesitan sistemas que permitan incrementar la productividad, mediante nuevas tecnologías, a la vez que se requiere mantener de forma robusta la seguridad de la información.

5. ALTERNATIVAS

Se ha encontrado en el mercado nacional un sólo producto que cumple con las características que le permiten mitigar los riesgos de robo y filtrado de información que se encuentran en las computadoras personales y computadoras portátiles que tiene la Contraloría General de la República.

6. ANALISIS COMPARATIVO TÉCNICO Y DE COSTO-BENEFICIO

Para realizar este análisis comparativo técnico, sólo se encontró un producto que cumplía con las características solicitadas:

- SAFEND PROTECTOR

El producto cumple con elimina todos los riesgos posibles de entrada de software malicioso y fuga de información, así mismo debe mantener la privacidad mediante la definición de políticas de control que permitan gestionar todos los accesos locales, monitorizando el tráfico generado desde los puertos e interfaces de conexión.

Tiene una consola de administración que puede crear políticas de seguridad. Estas políticas se pueden aplicar a dominios, grupos, ordenadores o usuarios de la organización.

El producto tiene un agente que protege los puntos de acceso, interactuando con el sistema operativo a bajo nivel (kernel mode) demandando algunos recursos de procesador y memoria.

Características Principales

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE Nº 003 GTSI

"CONTROL DE INTERFACES"

Control de todas las interfaces locales de las estaciones de trabajo, incluyendo:

- **Interfaces Físicos**
  - USB
  - FireWire
  - PCMCIA
  - Serie
  - Paralelo
- **Interfaces Inalámbricos (Wireles)**
  - WiFi
  - Bluetooth
  - Infra Red (IrDA)
- **Almacenamiento extraible**
  - CD / DVDs
  - Flash Drives
  - Zip Drives
  - Floppy Drives
  - Tape Drives
- Control granular de redes WiFi: se pueden crear reglas con restricciones por dirección MAC, SSID o el nivel de seguridad que presenta la red inalámbrica.
- Registro de transferencia de ficheros: nuevo sistema de auditoria de los archivos que se copian y se leen desde un dispositivo de almacenamiento (CDs, pendrive, discos USB, etc) que permite obtener mayor grado de control sobre la información que entra o sale de la red corporativa.
- Control de dispositivos Keylogger: detecta y bloquea dispositivos keylooger (dispositivo que captura los datos que el usuario introduce a través del teclado) que estén conectados a puertos USB evitando, de esta forma, que se puedan utilizar sin control efectivo.
- Integración con Directorio Activo de Microsoft mejorada.
- Modo de suspensión: este modo permite suspender temporalmente la protección de un cliente. De esta forma el administrador puede realizar tareas de mantenimiento en el ordenador sin ningún tipo de restricción de los puertos.

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE Nº 003 GTSI

"CONTROL DE INTERFACES"

- Registro de eventos de Servidor, Archivos y de los clientes instalados para disponer en todo momento de la información más actualizada.
- Actualización bajo demanda de las políticas en los clientes instalados desde la consola de administración. Las políticas también se actualizan de forma automática a través del Directorio Activo.
- Administración de Clientes: a través de la consola de administración se obtiene información de los ordenadores que tienen el cliente instalado y de su configuración, por ejemplo, política asignada, política efectiva, versión de cliente, etc.

Funcionalidad de registro de transferencia de ficheros (file name logging) crea un registro forense de todos los archivos que salen y entran a la red desde dispositivos de almacenamiento removibles.

Este registro forense permite a los administradores saber no sólo que dispositivos de almacenamiento están en uso, sino qué ficheros se han copiado a y desde esos dispositivos. Es clave para analizar incidentes de seguridad y seguimiento de un potencial abuso de dispositivos de almacenamiento portátil. El registro de nombre de ficheros mejora la visibilidad que la organización tiene sobre el flujo de datos. Además ayuda a conseguir y mantener las regulaciones legales vigentes.

Licenciamiento:

LICENCIA DE SOFTWARE SAFEND PROTECTOR	**500**	**20,000.00**
01 AÑO DE MANTENIMIENTO (20%)	**01**	**4,000.00**
	TOTAL	**24,000.00**

Condiciones del servicio:

- Soporte técnico especializado para la instalación y capacitación en el uso y operación del producto de software SAFEND PROTECTOR a través del Representante de SAFEND en el Perú.
- Asistencia técnica y actualizaciones permanentes del producto de software SAFEND PROTECTOR.

V° B° C.G.R. – GERENCIA DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN

INFORME TÉCNICO PREVIO DE EVALUACIÓN DE SOFTWARE Nº 003 GTSI

"CONTROL DE INTERFACES"

7. CONCLUSIONES

Las conclusiones de la evaluación realizada son las siguientes:

- La CGR obtendrá mayor seguridad mitigando los riesgos de robo y filtrado de la información que se encuentra en las computadoras personales y portátiles.

- La información que genera la CGR son críticos y de alta importancia para las labores diarias de los usuarios, por lo que se requiere contar con una plataforma de seguridad acorde con las tecnologías y amenazas actuales existentes, que asegure a su vez el correcto funcionamiento de los sistemas institucionales.

- Por las razones expuestas anteriormente, se recomiendan adquirir e implementar las soluciones propuestas a fin de mejorar el nivel de seguridad de la información de la institución.

8. Firmas

C.G.R. – GERENCIA DE TECNOLOGÍAS Y SISTEMAS DE INFORMACIÓN
V° B°

Jesús León Lamas
Gerente
Gerencia de Tecnologías y Sistemas de Información

Leoncio Rodríguez Manyari
Jefe Soporte Técnico
Gerencia de Tecnologías y Sistemas de Información