PROVINCIA DE BUENOS AIRES
PROCURACIÓN GENERAL DE LA
SUPREMA CORTE DE JUSTICIA

3002-291-13-4

Especificaciones técnicas Sistema antivirus con control de acceso a dispositivos

El sistema deberá ser una única solución de software, que cubra los siguientes aspectos de seguridad, no admitiéndose soluciones que integren más de un producto y deberá contar con soporte, actualizaciones de motor y definiciones durante 3 años.

Antivirus

- Deberá proveer protección antivirus a estaciones de trabajo (clientes) y servidores
- Compatible con Windows XP, 2003/2008 Server, Vista y 7 (32 y 64 bits), 8 y 8.1 (32 y 64 bits), Symbian, Windows Mobile, Blackberry OS, Android e iOS con soporte y actualizaciones de motor y definiciones para dichos sistemas operativos durante la duración del contrato
- Detección y eliminación de virus conocidos en las estaciones clientes y/o servidores según el método de análisis seleccionado (tiempo real, demanda, programado)
    - Virus de arranques
    - Virus de archivos
    - Virus macro
    - Virus de VBScript y Java Script
    - Virus en archivos comprimidos
    - Rootkits
- Detección de virus en correo entrante y saliente
- Detección de virus por tráfico web
- Posibilidad de realizar en clientes y/o servidores los siguientes tipos de análisis:
    - Tiempo real
    - Por demanda
    - Programado
    - Remoto
    - Por unidad de disco
    - Por carpetas
    - Archivos seleccionados
- Análisis heurístico que permita la identificación de nuevas amenazas y/o código malicioso
- Ejecución automática al inicio del sistema
- Chequeo de transferencias de archivos entre clientes y/o servidores
- Protección antivirus para equipos móviles que permita actualizarse a través de Internet
- Integración con Microsoft NAP y Cisco NAC.
- Capacidad de conectar equipos vía Wake on Lan para realizar tareas, inclusive equipos que estén en diferente subred que el servidor.
- Capacidad de realizar inventario de hardware y software de todos los equipos donde se encuentre instalado.

- Capacidad de diferencias máquinas virtuales de máquinas físicas.
- Soporte para el protocolo IPv6.
- Contar con módulo IDS (detección de intrusiones) para protección contra escaneo de puertos y explotación de vulnerabilidades de software. La base de analisis debe ser actualizable automáticamente.
- Protección con contraseña que impida deshabilitar el servicio de antivirus
- Requerimiento máximo de hardware: Deberá funcionar con un equipo cliente con procesador Celeron 2.66Ghz y 1GB de RAM.

Consola de administración

- Consola de administración que permita instalarse en múltiples sitios y administración remota
- La consola de administración permitirá programar la actualización del antivirus en los equipos según criterios de selección individual, por grupo o total.
- Contar con los siguientes métodos de instalación desde la consola de administración hacia las estaciones clientes y/o servidores, habilitando la protección antivirus de forma inmediata
    - Recurso compartido de red
    - Intranet/Internet
    - Forma remota (push)
    - CD/Pendrive
    - Permitir la desinstalación automática de otros antivirus que se encuentren instalados en los equipos.
- Soporte de múltiples repositorios de actualización, permitiendo la minimización de tráfico por vínculos WAN
- Actualización desatendida (sin intervención del usuario) e incremental
- Detección de equipos sin antivirus y/o con el mismo desactualizado o fuera de servicio
- Posibilidad de realizar informes que muestren:
    - Versión de las cadenas de definición y motor de búsqueda
    - Equipos infectados
    - Histórico de infecciones
- Notificación a la consola de administración ante la detección de virus

Certificaciones y reconocimientos

- Poseer certificación ICSA Labs (www.icsalabs.com)
- Poseer certificaciones Checkmark de Westcoast Labs (www.westcoastlabs.org) en los siguientes ítems:
    - Anti-Trojan
    - Anti-Virus Desktop
    - Anti-Virus Desinfection
    - Anti-Virus Server
- Poseer calificación Advanced+ en al menos 85% de la totalidad de los test de AV-Comparatives (www.av-comparatives.org), realizados en los últimos 3 años contados a partir de la fecha de apertura de ofertas.

Control de acceso a dispositivos

- Permitir desactivar la ejecución automática de dispositivos.
- Permitir desactivar el procesamiento de los archivos autorun.inf.
- Permitir aplicar diferentes políticas cuando se está conectado a la red, cuando se accede por VPN o cuando se está desconectado.
- Detección de dispositivos no autorizados ó del uso de puertos o periféricos no autorizados.
- Monitoreo en tiempo real de los equipos.
- Capacidad de alertas y registro de eventos incluyendo mensajes personalizables, y correo electrónico.
- Bloqueo por de grupos de usuarios, usuarios, computadores, y dispositivos.
- Debe poder mantener y aplicar las políticas de seguridad en los equipos aún cuando no estén conectados a la red ó los servidores no estén disponibles.
- Aplicación de Políticas de Seguridad en Conexión en Caliente (hot-plugging) y dispositivos plug-and-play.
- Cambio dinámico de políticas
- Integración con Microsoft Active Directory y Novell eDirectory permitiendo definir políticas por usuario y/o por usuario y/o por equipo.
- Permitir definir políticas a usuarios locales.
- Módulo de reportes, búsquedas de eventos y actividades en Tiempo Real en los registros de eventos, notificaciones, acciones y auditoría.

Posibilidad de controlar al menos los siguientes dispositivos:

- Dispositivos USB – dispositivos que se conectan a través del puerto USB.
- Unidades de CD/DVD-ROM.
- Disqueteras
- Dispositivos IEEE 1394 (Firewire)
- Modems – dispositivos utilizados en sistemas de comunicación. Este tipo de dispositivos incluyen modems de discado, modems ADSL, modems de Ethernet y otros.
- Dispositivos PCMCIA
- Dispositivos COM y LPT
- Unidades de cinta – dispositivo de almacenamiento en cinta magnética.
- Dispositivos Puerto paralelo
- Dispositivos de salida. La clase comprende dispositivos para la creación de imágenes estáticas, como cámaras digitales y escáners.
- Dispositivos IRDA
- Dispositivos de Tecnología de Memoria – dispositivos de almacenamiento de datos, como tarjetas de memoria.

- Dispositivos multifunción, dispositivos combinados para almacenar y leer tarjetas de memoria, modems PCMCIA, etc.
- Lectores de tarjetas inteligentes. Esta clase incluye todo tipo de lectores de tarjetas inteligentes: tarjetas prepagas, tarjetas de crédito y otras.
- Dispositivos Windows CE USB ActiveSync – dispositivos diseñados para sincronizar datos entre un dispositivo móvil (como computadoras de bolsillo, teléfonos inteligentes, etc) y un equipo.
- Dispositivos portátiles – dispositivos con el soporte de gestión de energía (por ejemplo, iPhone).
- Dispositivos Bluetooth.