LiveCall Suite
Manual de Referencia

HAURI Incorporated
Abril 30, 2004

Para los Lectores

Este manual es para los clientes de Hauri que usen los servicios de LiveCall Suite. Recomendamos fehacientemente al usuario que lea este manual cuidadosamente antes de usar LiveCall Suite para asegurar su uso apropiado.
Este manual puede ser levemente diferente al programa debido a la incorporación de mejoras en sus funciones

Composición del Manual

Este manual está dividido en dos capítulos principales.
El Capítulo I puntualiza las características de las funciones principales, cómo instalar y usar LiveCall Suite. El Capítulo II describe en detalle cada función.

Marcas de Contenido

Tabla de Contenidos

Índice

I. Introducción a LiveCall Suite

LiveCall Suite es una herramienta de seguridad integrada, con una interfase intuitiva, pero también con un gran y rápido desempeño para ofrecer un ambiente seguro al usuario que navega en Internet.

1. Características

LiveCall Suite es una herramienta que provee de un ambiente computacional seguro para el usuario que navega en Internet. Se instala automáticamente en la PC del usuario. Detecta y remueve herramientas piratas dentro de la memoria, protege las pulsaciones de teclado, monitorea accesos remotos a través de una interfase amigable. Es una solución de seguridad en línea para mantener su computadora a salvo: no sólo asegura la integridad del sistema, sino también analiza brechas en la seguridad de Sistema Operativo

Función de seguridad de soporte integrado usando Internet

LiveCall Suite es un producto de seguridad en línea para usar cómodamente desde cualquier lugar conectado a Internet

Detección poderosa, función de reparación después de una instalación simple

LiveCall Suite se instala automáticamente cuando el usuario hace clic en SI en el cuadro de certificación de Advertencia de Seguridad de Hauri. En ese momento, se descarga el último módulo.

Prevención contra la exposición de información privada a través de Internet o archivos compartidos.

Con una función de seguridad poderosa para el teclado y su capacidad de monitorear el acceso a Internet, LiveCall Suite previene cualquier exposición peligrosa a la información privada. También es capaz de detectar un virus y reparar su daño

2. Funciones Principales

Funciones Principales	Descripción
Función de seguridad del teclado en tiempo real	La información privada puede ser protegida totalmente contra la explotación de un pirata o de un espía y provee una función poderosa en tiempo real de seguridad del teclado para interceptar cualquier exposición de la información privada importante cuando se usan los servicios en línea de bancos, compras Web o negocios
Control de acceso en tiempo real	Cualquier intento de controlar en forma remota un programa o un sistema puede ser interceptado. LiveCall Suite detecta cualquier ataque al sistema o cualquier proceso ilegal no autorizado por el usuario, a través de la política de control de acceso, la que puede ser corregida por el usuario, en tiempo real**.**
Detección de Troyanos, Backdoors, detecta y remueve herramientas piratas usando el escaneo de memoria	Detecta herramientas pirata que traten de acceder a la información personal, como Troyanos y Backdoors, cuando LiveCall Suite está en ejecución. Estas funciones previenen cualquier daño de virus o ataque de una herramienta pirata desconocida
Descargar y comprobar parches de	LiveCall Suite es capaz de obtener información importante sobre parches de seguridad y permite descargarlos a una PC, ya que ahora los programas maliciosos que se aprovechan de las brechas

seguridad del Sistema Operativo	de seguridad de un Sistema Operativo están aumentando considerablemente.
Manejo de carpetas compartidas	LiveCall Suite lo mantiene informado acerca de los recursos compartidos de su sistema, para protegerlo contra cualquier virus o código maliciosos que se aprovecha de la vulnerabilidad que implica un recurso compartido.
Poderoso desempeño de nuestra solución en línea en la detección de virus y reparación de daños	LiveCall es una función antivirus en línea basada en la técnica única de Hauri, certificada internacionalmente. Los virus que se ejecutan en el computador pueden ser detectados y reparados con el uso de la actualización más reciente, sin la necesidad de tener un antivirus instalado al momento de usar LiveCall Suite.
Función de actualización automática de la última versión de virus	Cuando se ejecuta el LiveCall Suite en la PC de un usuario, la última actualización de virus es automáticamente descargada, de manera que siempre el software esta actualizado.
Fácil de instalar y ejecutar	Cuando el usuario selecciona [Si] en el cuadro de Advertencia de Seguridad, LiveCall Suite se instala automáticamente y se ejecuta.

II. Usando LiveCall Suite

1. Requerimientos de Sistema

Para hacer funcionar LiveCall Suite, se necesita lo siguiente:

Sistema Operativo

❖ Windows 95 / 98 / 98SE / Me

❖Windows NT Workstation 4.0 / NT Server 4.0 / 2000 Professional

❖ Windows 2000 Server / 2000 Advanced Server

❖ Windows XP Home / Professional

CPU

❖ Pentium III recomendado (por lo menos Pentium 133 MHz)

Memoria

❖ 64MB o más

HDD

❖ Por lo menos 10MB de espacio libre del disco duro

Misceláneo

❖ Internet Explorer 5.5 o mayor

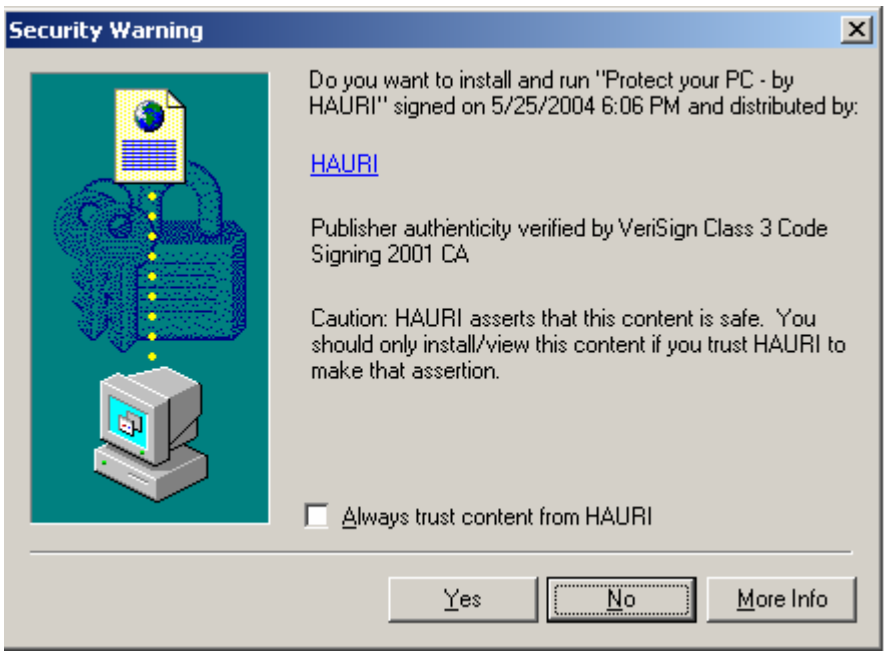
❖ Red, Mouse

1. Instalación y Desinstalación (programa Uninstall)

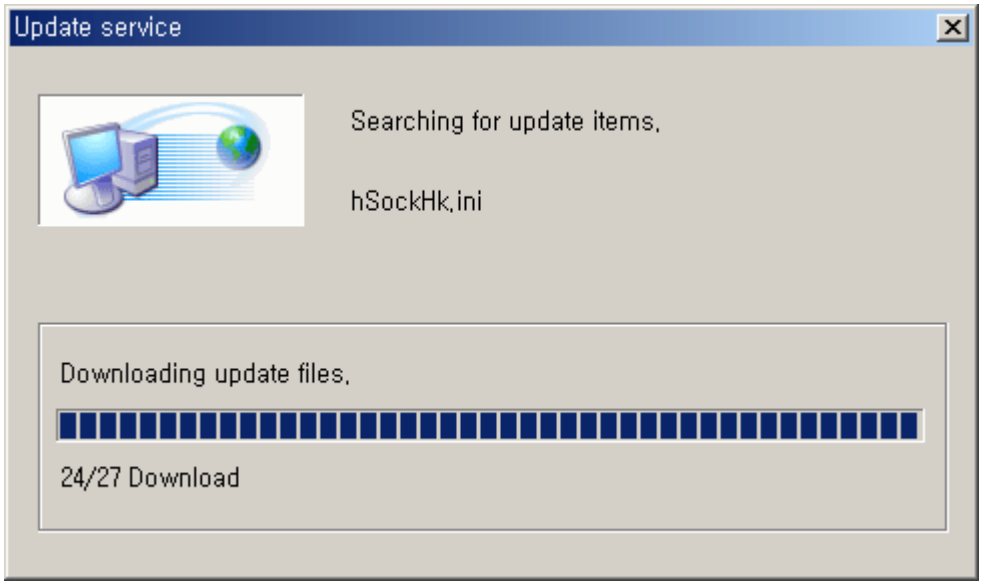
Instalación

LiveCall Suite es fácil de instalar. Se activa en minutos.

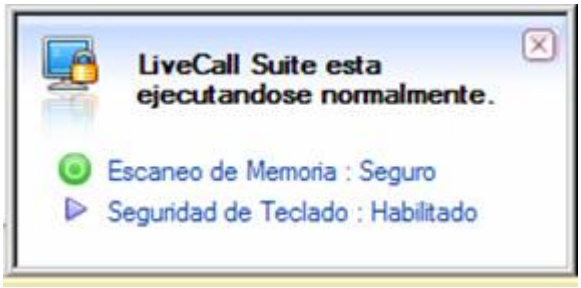
Para ejecutar LiveCall Suite, sólo vaya a la página Web relacionada. Cuando esté conectado, la ventana de seguridad aparece, le preguntará si descarga o no los archivos necesarios para ejecutar el LiveCall Suite. Haga clic en [Si] para proceder. (si elige [No], LiveCall Suite no se instala y se cierra)



En el cuadro siguiente, LiveCall Suite se ejecuta.



Una vez instalado, aparece el siguiente mensaje.
“LiveCall Suite está ejecutándose normalmente"



Cuando la aplicación se activa , el icono ( ) aparece en la esquina derecha de la barra de tareas.

3. Comenzando con LiveCall Suite

Entender LiveCall Suite

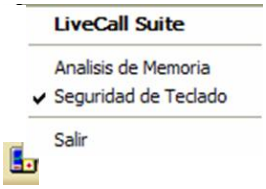
LiveCall Suite fue desarrollado para ofrecer una protección efectiva a nuestros clientes contra cualquier posible amenaza cuando están conectados a Internet.

Amenazas	Funciones de LiveCall Suite
Están en ejecución algunos virus conocidos	Cuando se ejecuta LiveCall Suite, detecta y remueve los virus de la memoria del sistema si es que están en ejecución.
Están en ejecución herramientas piratas conocidas, Troyanos, y Backdoors.	Cuando se ejecuta LiveCall Suite, detecta y remueve amenazas piratas, Troyanos y Backdoors de la memoria del sistema.
Se ejecuta un Key Logger	Cuando se ejecuta LiveCall Suite, detecta y remueve cualquier agente pirata (key logger) conocido de la memoria del sistema actual.
Están en ejecución herramientas piratas desconocidas, Troyanos, y Backdoors.	La función BOIP de LiveCall Suite muestra un mensaje de aviso cuando alguna aplicación envía información hacia Internet.
Se ejecuta un Key Logger desconocido.	La función de seguridad del teclado de LiveCall Suite protege la información personal contra la explotación por un Key Logger desconocido.
Vulnerabilidades	LiveCall Suite comprueba la instalación de los parches de seguridad del sistema y entrega un informe
Carpetas compartidas	LiveCall Suite comprueba carpetas compartidas por el sistema y entrega un informe.
Puertos abiertos	LiveCall Suite comprueba los puertos abiertos por el sistema actual y envía un informe.

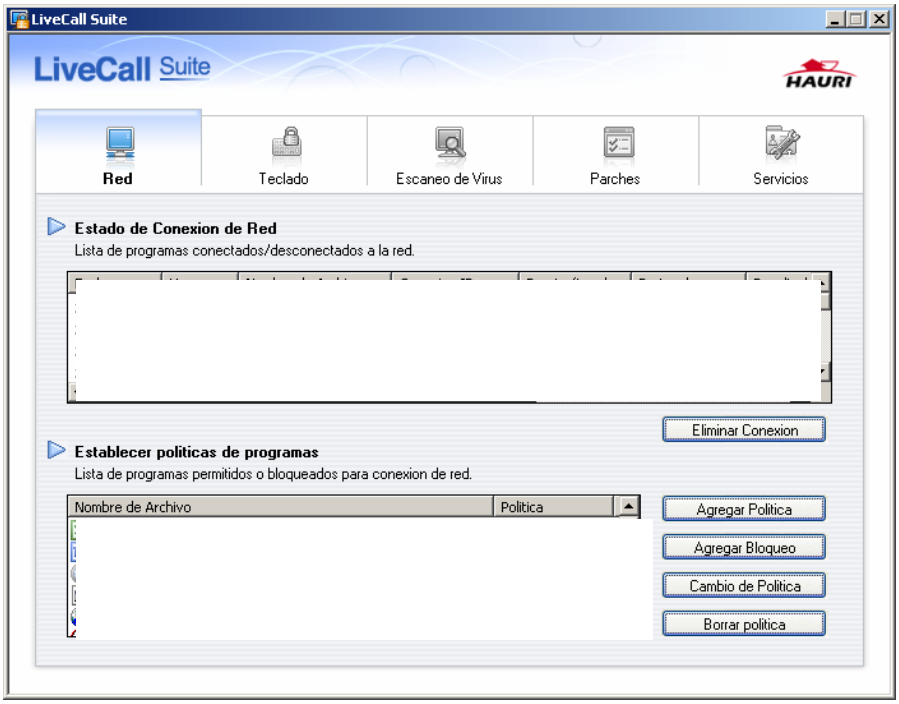
Ejecutar del LiveCall Suite

LiveCall Suite puede ser ejecutado con los siguientes métodos:

1. Doble clic en el icono LiveCall Suite de la barra de tareas. ( ).
2. Use el botón derecho del mouse para hacer clic en el icono del LiveCall Suite en la barra de tareas. En ese momento, si la ventana del menú aparece, elija “LiveCall Suite”



Cuando LiveCall Suite se encuentre ejecutándose, aparecerá el siguiente cuadro.



4. Usando LiveCall Suite

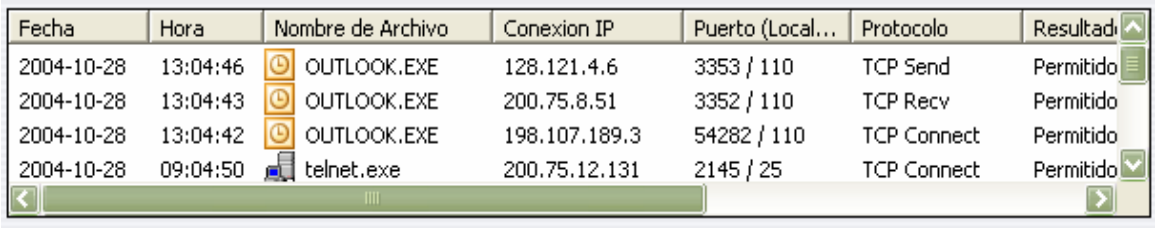
Cuando se ejecuta LiveCall Suite por primera vez, empieza a detectar Troyanos, Backdoors, Key Loggers, así como herramientas piratas dentro de la memoria del sistema .

LiveCall Suite ofrece las siguientes funciones.

Funciones	Descripción
	BOIP (Block Off Internet Process) Cuando un programa específico trata de enviar alguna información a través de Internet, usted puede bloquear el proceso.
	Comienza o detiene la función de seguridad del teclado.
	La detección de virus se puede activar por programas actualmente en uso. Con LiveCall Suite toda clase de archivos pueden ser escaneados en línea.
	Comprueba los parches de seguridad que todavía no han sido instalados en el sistema.
	Maneja cualquier carpeta compartida, tanto como puertos en uso.

Red : BOIP(Block Off Internet Process)

Esta funcionalidad de LiveCall Suite permite o intercepta (detiene) programas que comparten información con otros PCS o servidores.
El siguiente cuadro de diálogo se muestra en la esquina inferior derecha. Cuando el programa específico envía información a otra PC o a otro servidor o a Internet, un mensaje de advertencia aparece de la barra de tareas. En ese momento, sólo elija Bloquear o Permitido, para tomar una acción.

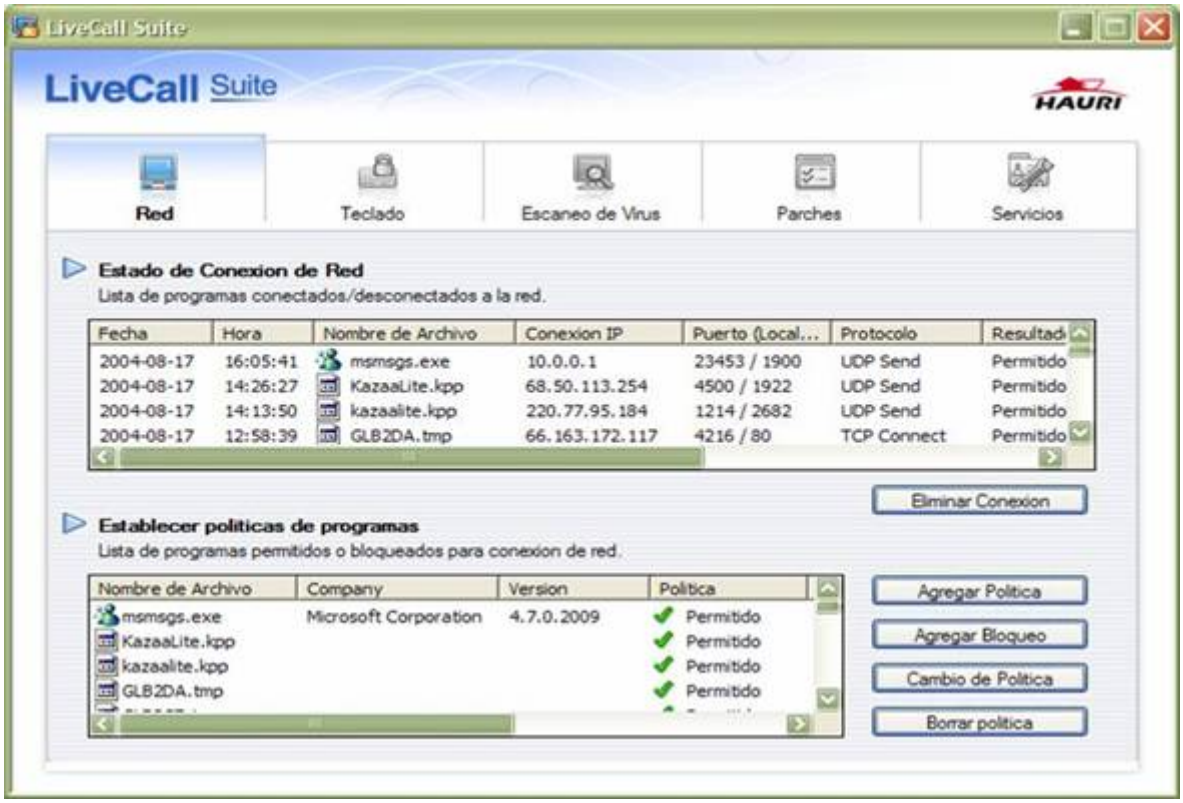


Fecha	Hora	Nombre de Archivo	Conexion IP	Puerto (Local...	Protocolo	Resultad
2004-10-28	13:04:46	OUTLOOK.EXE	128.121.4.6	3353 / 110	TCP Send	Permitido
2004-10-28	13:04:43	OUTLOOK.EXE	200.75.8.51	3352 / 110	TCP Recv	Permitido
2004-10-28	13:04:42	OUTLOOK.EXE	198.107.189.3	54282 / 110	TCP Connect	Permitido
2004-10-28	09:04:50	telnet.exe	200.75.12.131	2145 / 25	TCP Connect	Permitido

Ítem	Descripción
Nombre del Programa	El programa intenta conectarse al exterior.
Protocolo	Protocolo para enviar información al exterior.
Conexión IP	Direcciones de PC o servidores tratando de conectarse al exterior.
Puerto	Número de puerto en uso para enviar información a un lugar remoto.

Estado	Descripción
Bloquear	Bloquea programas específicos que envían información al exterior.
Permitido	Permite a programas específicos enviar información al exterior
Finalizar después de interceptar	Intercepta el programa específico que envía información al exterior y termina su uso.

Con el BOIP(Block Off Internet Process) el usuario puede permitir a un programa conectarse o no con Internet. Comprueba el proceso en Tiempo-Real con la función de monitoreo.
La información personal se puede proteger de una exposición peligrosa causada por cualquier programa específico.



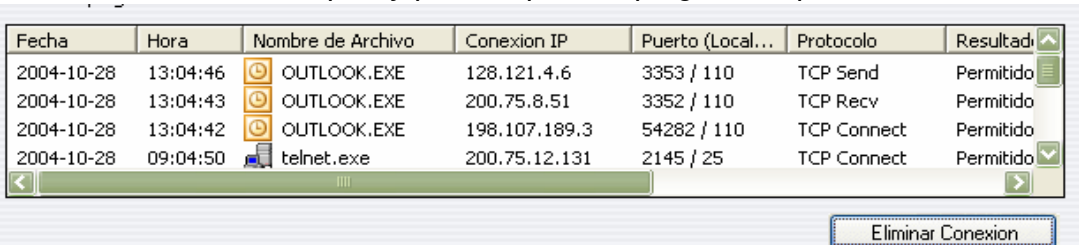
El programa bloqueado / permitido puede verse en la política de programas.

Intercepción y Permiso de LiveCall Suite

Cuando se ejecuta LiveCall Suite los programas que tratan de enviar información son monitoreados. Por lo tanto, el permiso y el bloqueo se pueden confirmar.

Usando la opción [lista de remover], usted puede suprimir la lista grabada de los programas que tratan de enviar información al exterior.

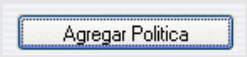
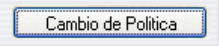
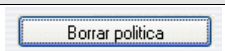
Mientras configura las reglas del programa, usted puede manejar el bloqueo y permiso para un programa específico.



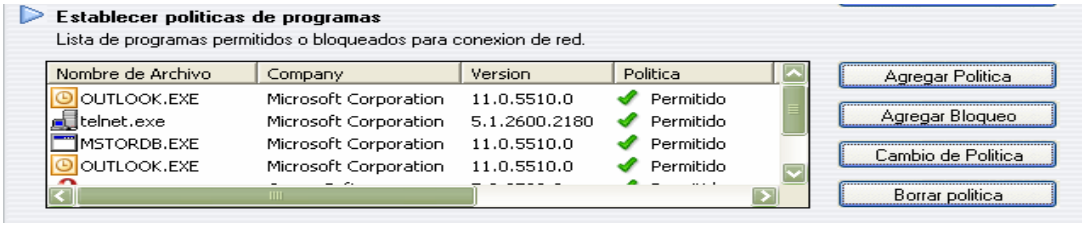
Seleccione el archivo a suprimir y haga clic [lista de remover]. Presione “Crtl” o “Shift” y haga clic en el mouse al mismo tiempo para eliminar una regla parcial o totalmente.

Preparando una política de programa

Cuando prepara una política de programa, usted puede permitir/ interceptar un programa específico. (A continuación se describe un método detallado para configurar una política de programa)

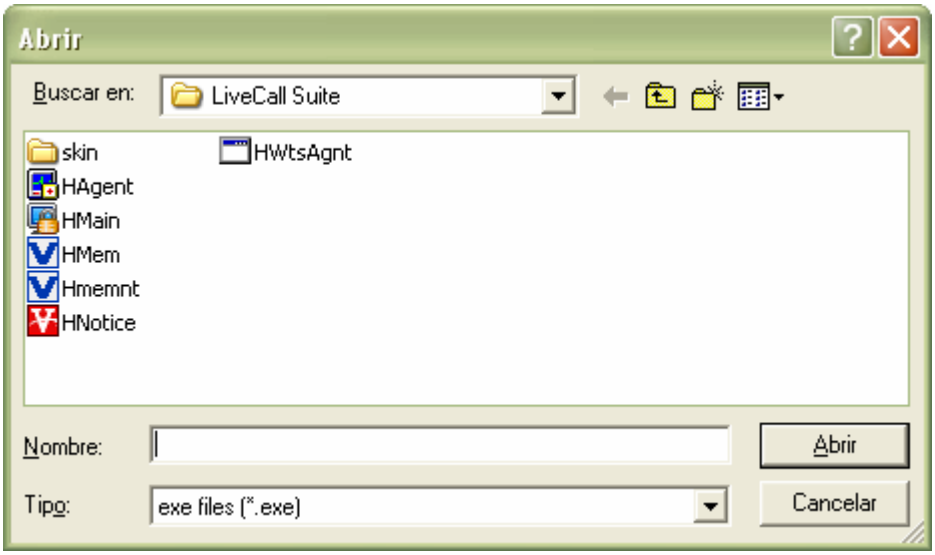
Ítem	Descripción
	Permite la transmisión de datos por un programa específico. Solo encuentre y seleccione el archivo a enviar, permita o no.
	Intercepta la transmisión de datos de algún programa
	En caso de una política de intercepción de transmisión de datos, para un programa específico, cambie de permiso a bloqueo.
	Elimine la política de permiso o bloqueo para un programa específico. Si el programa trata de enviar datos, confirme de nuevo su elección: permiso o bloqueo.

Agregar un programa a la lista de permisos

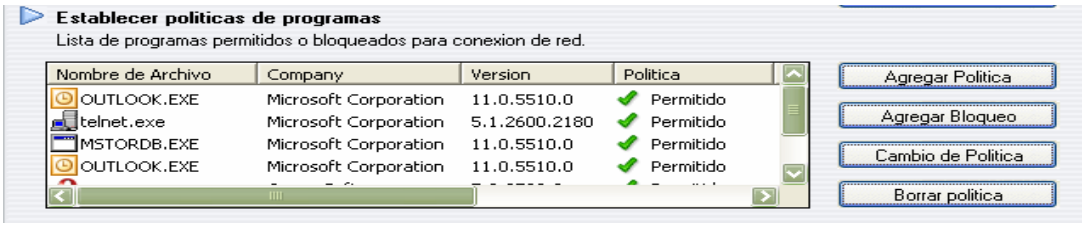


Cuando haya elegido el botón [agregar política] vaya a la ruta del programa elegido en la siguiente ventana.

Seleccione el programa y haga clic en [Abrir]



En el cuadro siguiente, la política “permiso/bloqueo” está preparada en la lista de programas.

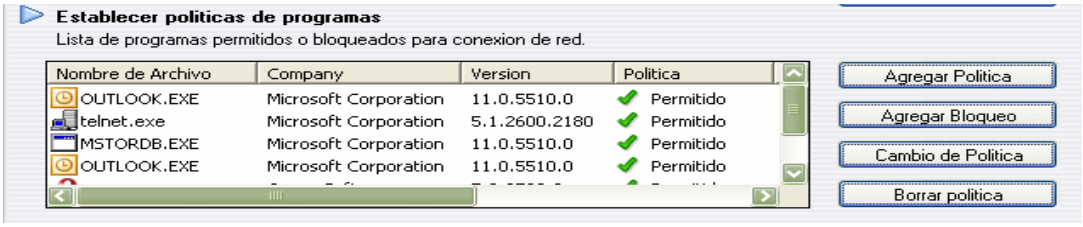


Agregar el programa que intercepta

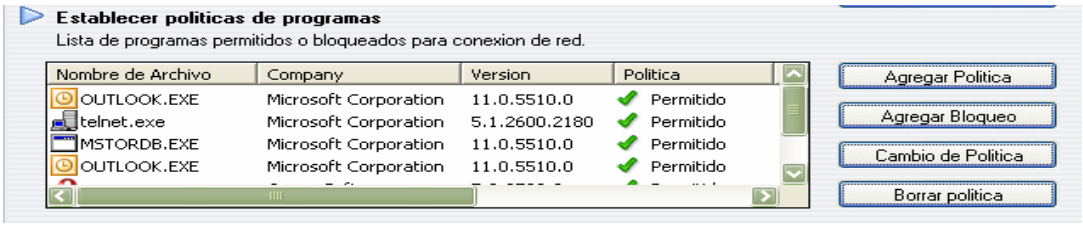
Proceda igual al método descrito en “agregar política”, mencionado arriba.

Corrija la política de programa

Haga su elección en la lista y después haga clic en el botón “cambio de política”.

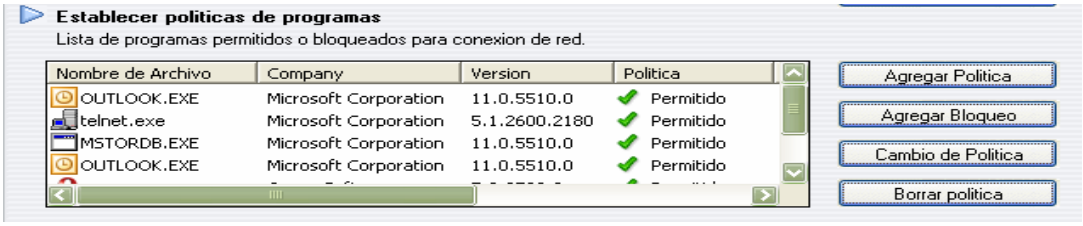


Cuando usted hace clic en [Cambio de política], la opción "permitido" cambia a "bloqueo", mientras que "interceptar" se cambia a "permitido"

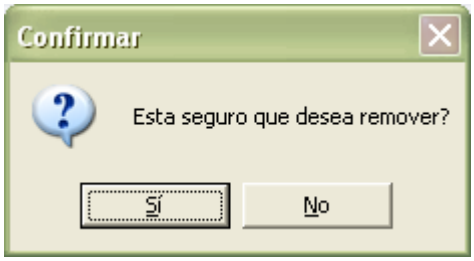


Suprima una política de programa

Una vez que el programa a eliminar haya sido elegido, haga clic en el botón [borrar política].



En el cuadro siguiente, el usuario confirma o no su elección.

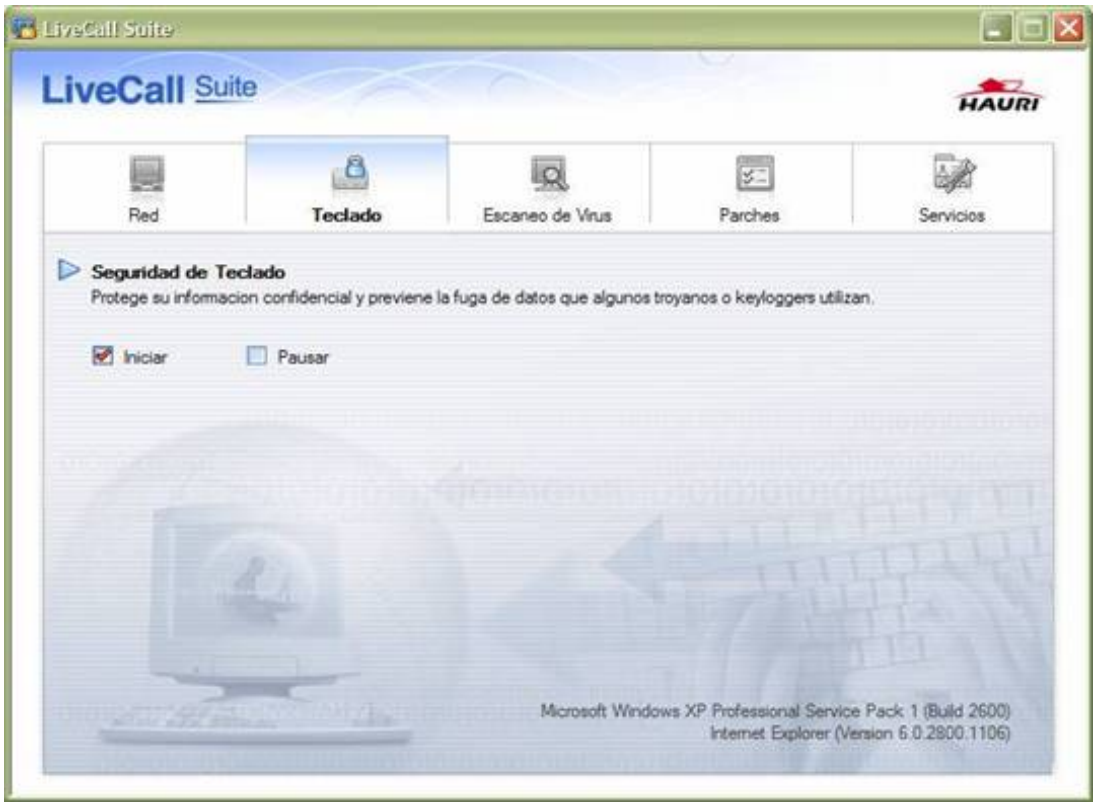


[Si] la política es eliminada efectivamente. [No] la política permanece sin cambio.

Seguridad del Teclado

La función de Seguridad del Teclado protege la información privada del usuario cuando se usa el teclado. Previene de cualquier exposición inesperada a los Troyanos y otros capturadores de pulsaciones del teclado.

Mientras se ejecuta el Servicio de Seguridad del Teclado en LiveCall Suite, toda la información entrante es protegida de manera que cualquier información privada no pueda ser interceptada.

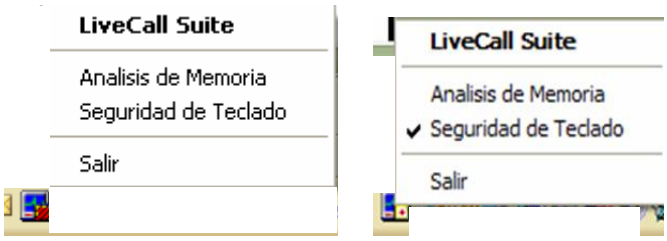


La ejecución de seguridad del teclado puede ser confirmada mediante el icono de la bandeja

Seguridad del teclado habilitada :

Seguridad del teclado inhabilitada:

ⓘ Si la seguridad del teclado no está (operando), proceda de la siguiente manera:
Con el botón derecho del mouse, seleccione el icono LiveCall Suite en la bandeja del sistema. Retire la opción seguridad del teclado en el menú de seguridad del teclado. Como puede ver debajo, el icono cambia



Si tiene que deshabilitar la función de seguridad del teclado, contacte a soporte de servicio al cliente.

ⓘ Cuando use VMWare, haga favor de usar después de deshabilitar la función de seguridad del teclado.

Virus Scan

Los Troyanos y otros agentes piratas no pueden reproducirse solos, a diferencia de los virus. Ellos generalmente se esconden en otros archivos, como juegos, contenidos de adultos, etc. Cuando se ejecutan, se generan algunos problemas de funcionamiento y es probable que algunos datos privados sean expuestos al exterior.
Una vez ejecutado, LiveCall Suite examina la memoria del sistema y si esta infectada, la repara.

Un virus se reproduce solo, de manera que cuando se ejecuta LiveCall Suite lo repara indefinidamente porque el virus continúa infectando usando una ruta específica. .

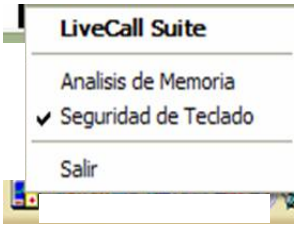
Después de ejecutar LiveCall Suite, el programa en uso puede ser escaneado usando [Revisar Memoria], y la información del virus puede ser removida usando el botón [lista de borrado].

Escanear Memoria

Hay dos maneras de escanear la memoria a) escanear desde la barra de tareas y b) escanear desde la ventana principal

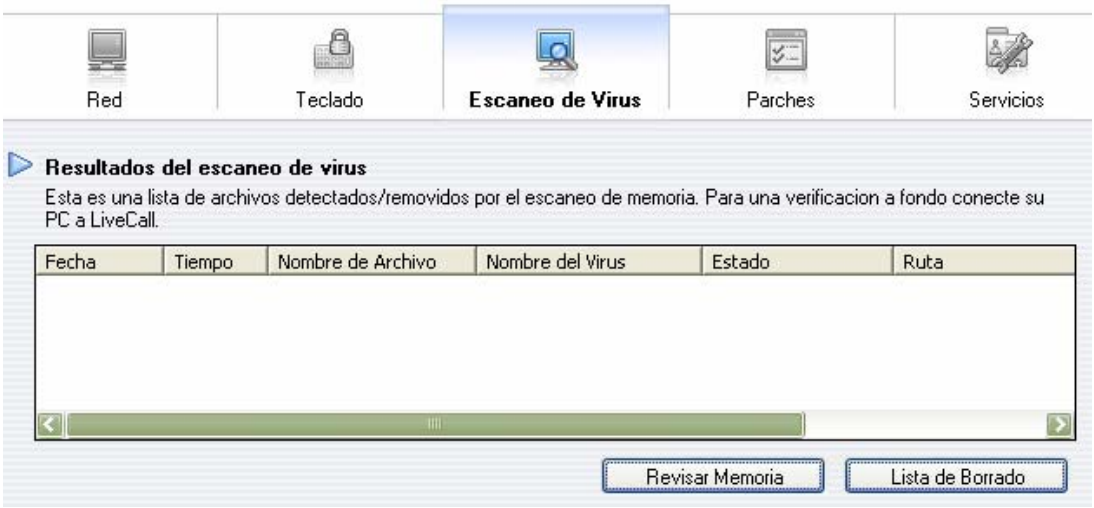
Escanear desde la barra de tareas

Con el botón derecho del mouse, elija el icono de la barra de tareas. El menú LiveCall Suite se despliega. Elija “Análisis de Memoria”



Escanear la memoria una vez que LiveCall Suite se ejecuta

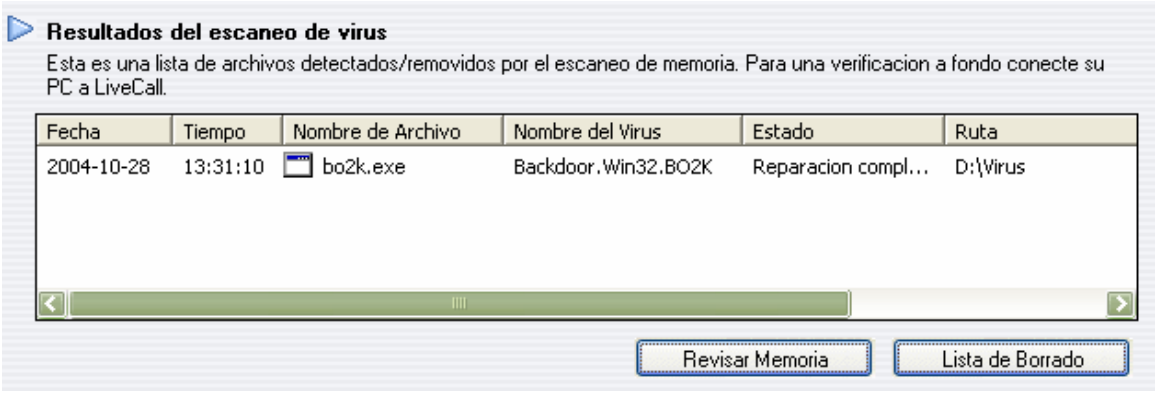
Cuando se hace doble clic sobre el icono LiveCall Suite, se ejecuta la ventana principal. Elija el menú [Escaneo de Virus] después haga clic en [Revisar Memoria].



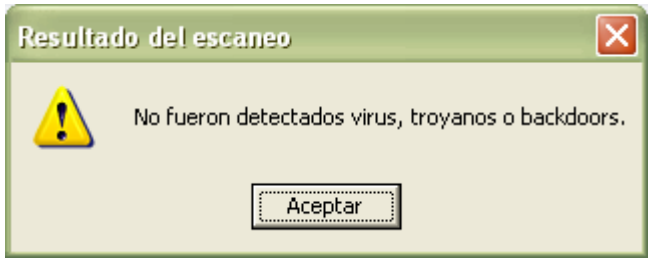
Cuando se detecta una herramienta pirata/virus

Cuando se detecta una herramienta pirata/virus, se despliega el mensaje de advertencia. Si usted elige la opción [Reparado], la herramienta pirata o virus se remueve.

El resultado se despliega como sigue



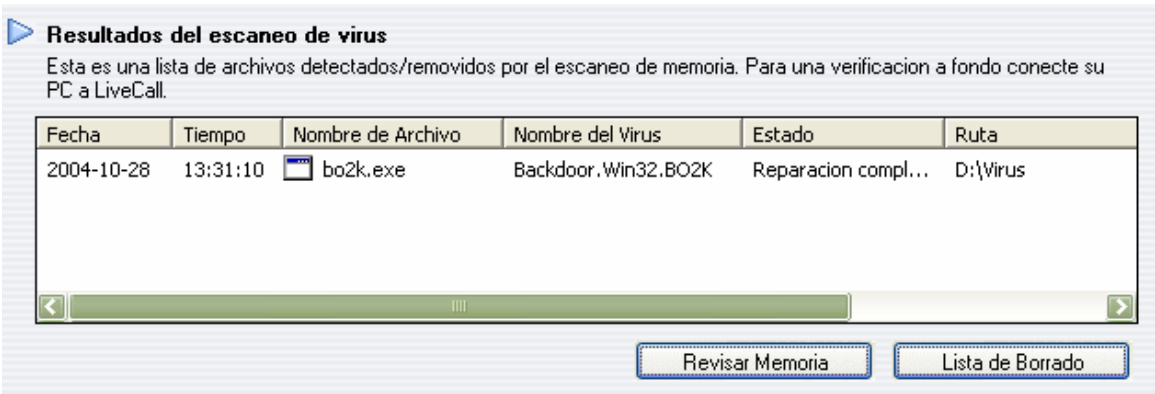
No se detecta virus, troyanos o backdoors.



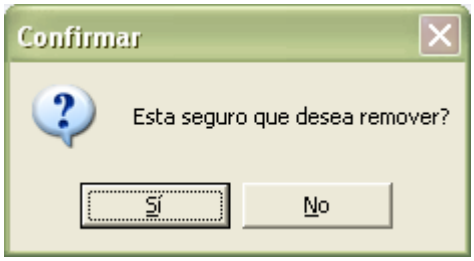
Cuando no se encuentran virus o agente pirata, el siguiente mensaje aparece.

Suprimir la lista

Este es el procedimiento para borrar el expediente en la ventana de detección de virus. Seleccione la lista para remover y haga clic en [Lista de Borrado].



En el cuadro de abajo, el usuario tiene que confirmar su elección



[Si] el resultado se remueve. [No] permanece.

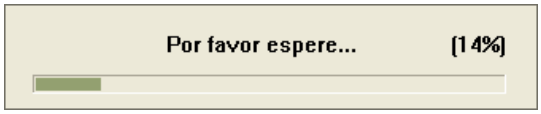
LiveCall Suite está solo indicado para programas actualmente en uso. Para los otros archivos, vaya a la página de inicio del LiveCall Suite http://www.livecall.co.kr para detección y reparación.

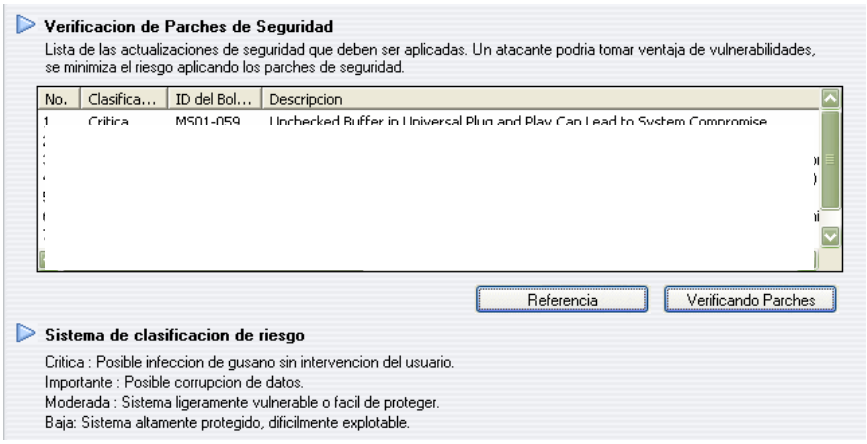
Revisión de los Parches de Seguridad

Los virus y métodos piratas se aprovechan de las vulnerabilidades de seguridad del sistema operativo Microsoft Windows, pudiendo dañar seriamente este sistema.
Los usuarios deben detectarlos y obtener los parches correspondientes.

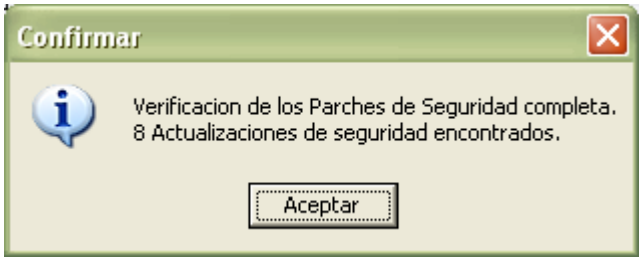
Para Verificar los Parches de Seguridad

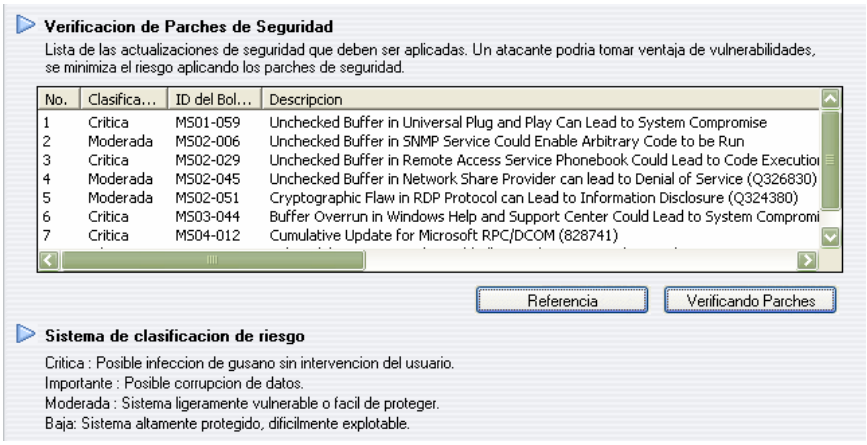
Use el botón [Verificar Parche] y espere un momento. Se comienza a realizar el chequeo de los parches de seguridad





Una vez revisados, se despliega una lista de los parches no instalados.





La información sobre Instalar los parches de seguridad está disponible vía [Referencia] Usted será redirigido al “Boletín de Seguridad de Microsoft”, página de donde puede obtener el parche necesario.

Nivel de Seguridad

Crítica: Un gusano de Internet se puede reproducir sobre un sistema.

Importante: Posible corrupción de datos.

Normal: bajo riesgo, o sistema seguro mediante operaciones básicas.

Bajo: sistema difícilmente explotable.

Si el valor esta en “Crítico” o “Importante” usted deberá descargar el parche para proteger su sistema en contra de infecciones.

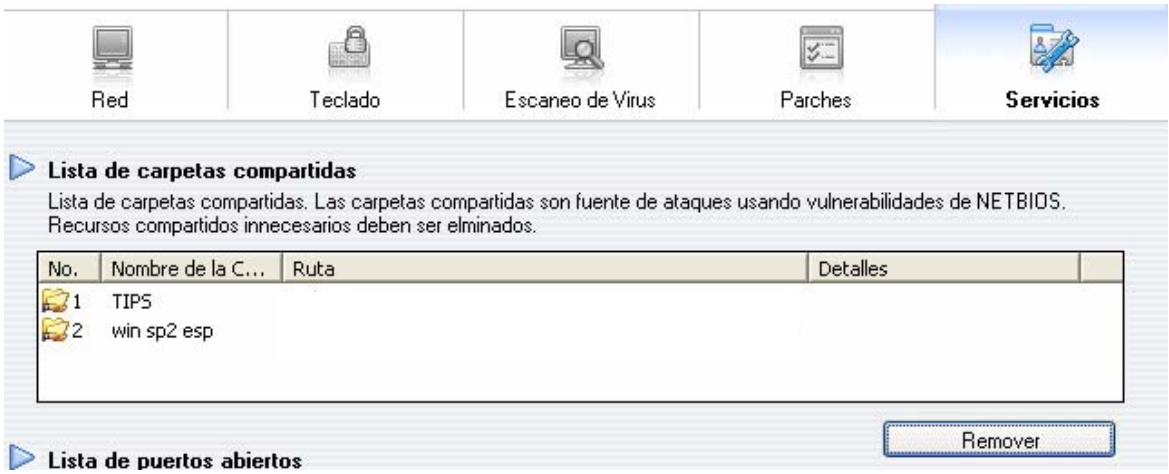
Servicios

Sirve para Entregar información sobre los recursos compartidos que existen dentro del sistema del usuario y chequea (revisa) los puertos actualmente en uso

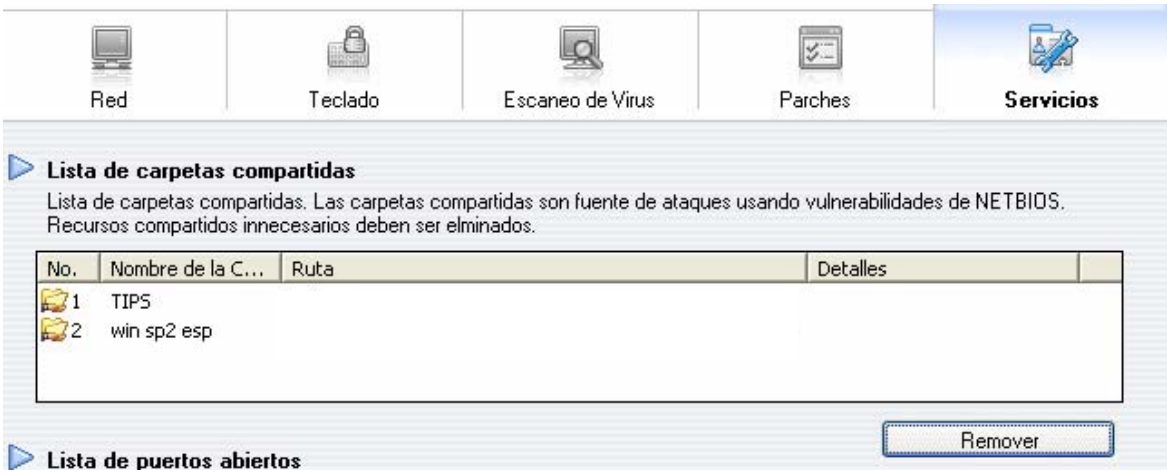
Lista de carpetas compartidos

Las carpetas compartidas pueden compartir información con algún otro sistema remoto. Estas pueden ser la fuente de alguna infección, en donde los usuarios desconocidos puede tener acceso a estos datos. Busque en los recursos compartidos del sistema en uso y deshabilite los que no necesita.

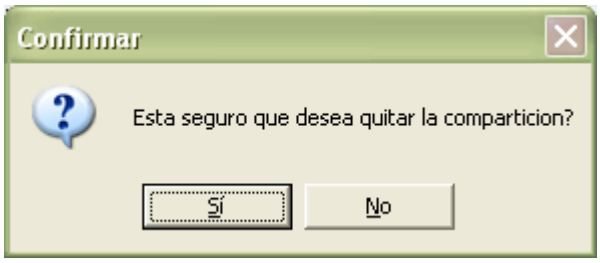
- Usando la opción [Remover] usted elimina la compartición de algunos datos, con terceros, pero la información permanece en el sistema.
- Los recursos compartidos C$, D$, IPC$ no se despliegan.



Liberar una carpeta compartida



Como se ilustra abajo, el usuario debe confirmar su elección:

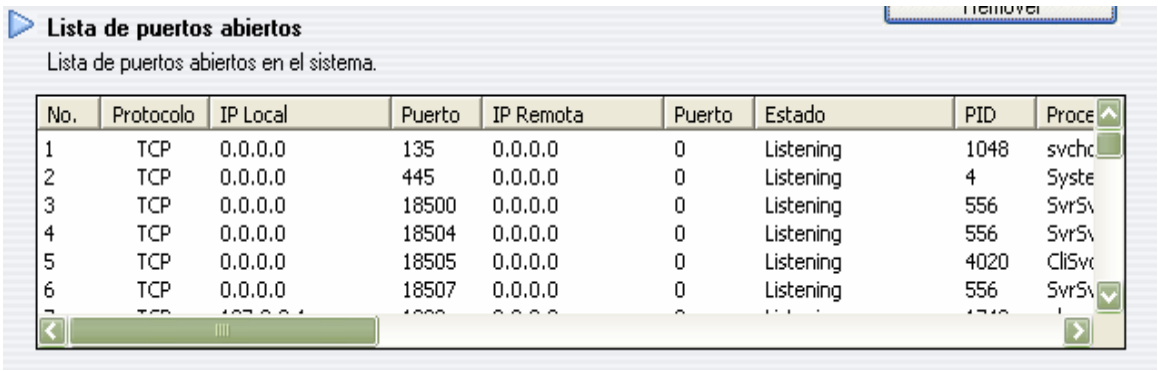


[Si]: la carpeta no es compartido

[No]: la carpeta no cambia

Lista de puertos abiertos

Significa que el puerto esta en uso



Ítem	Descripción
Protocolo	Protocolo en uso para un acceso remoto
Dirección IP Local	Direcciones de Sistemas de Proveedor de Internet
Puerto	Puerto en uso para acceso remoto o enviar datos
Dirección IP Remota	PC externo o dirección de un servidor Proveedor de Internet distante
Puerto	El puerto en uso para que la PC actual pueda enviar información
Estado	Refiérase a la tabla siguiente
Nombre del Puerto	El nombre de los puertos relevantes
Troyano activo y otros Backdoor	Lista de los Troyanos o Backdoors con sus puertos asociados.

Estado	Descripción
LISTEN	El servidor espera una conexión requerida desde un lugar remoto.
SYN-SENT	El servidor espera una respuesta una vez que la conexión y sincronización han sido efectuadas.
SYN-RECEIVED	El servidor espera una nueva petición de conexión.
ESTABLISHED	Se ha establecido una conexión y se usa para intercambiar datos.
FIN-WAIT1	El servidor espera permiso después del término de una conexión.
FIN-WAIT2	El servidor espera permiso después del término de una conexión de alto nivel.
CLOSE-WAIT	La conexión TCP espera el término desde un programa de alto nivel
CLOSING	El servidor espera permiso remoto para el término de la conexión.
LAST-ACK	El servidor espera permiso después que la conexión ha sido terminada desde un lugar remoto.
TIME-WAIT	El servidor se asegura que tiene tiempo suficiente para confirmar el permiso para terminar la conexión, ya enviado desde un lugar remoto.
CLOSED	La conexión entre los dos servidores no existe.