PCADMIN®

Ver. 2022

Manual de Referencia

TECNOLOGÍA DE HARDWARE Y SOFTWARE PCTECHSOFT S.A.S.

www.pctechsoft.com

I. INSTALACION DE CONSOLA PCADMIN

Inserte el CD de instalación y abra la aplicación INSTALAR PCADMIN.exe que se encuentra en la carpeta PCadmin.

Siga los pasos, aceptando y pulsando el botón Siguiente. Al terminar, reinicie el equipo.

PCadmin quedará instalado en la carpeta **C:\PCSECURE** y creará otra carpeta **C:\DATA** en la cual se recibirán todos los informes y estadísticas que se soliciten a los PCs con PCsecure instalado. Igualmente se creará **c:\inetpub\wwwroot\downloads** en la cual se podrán guardar archivos, programas e imágenes para transferir vía HTTP hacia los PCs, usando el WEBSERVER embebido de PCadmin, que se carga automáticamente con la consola. NOTA: Si aparece mensaje de Error - NetBind ó Puerto en uso, Ud. Debe deshabilitar algún otro Webserver que esté usando el puerto 80 (apache,ISS (Microsoft), Skype, etc.), o de lo contrario no podrá efectuar descargas desde su consola hacia los PCs pero si tendrá todas las demás opciones de control de la consola disponibles.

(IMPORTANTE: ESTAS 3 CARPETAS DEBEN TENER PERMISOS DE LECTURA – ESCRITURA ACCESO TOTAL PARA TODOS LOS USUARIOS LOCALES)

II. OPERACIÓN DE LA CONSOLA

La consola PCadmin se activa a través del icono en el Menú Inicio - Programas- PCadmin, o a través del icono en el escritorio. Aparecerá la ventana de clave de acceso que permite entrar a utilizar la interfase de trabajo de la consola. Digite el Usuario y Contraseña y pulse el botón "ACEPTAR"

Enseguida se habilitarán las acciones de la interface principal de la pantalla de PCadmin. Con el botón desbloquear / bloquear que aparece en la parte superior derecha de la interface, también se puede bloquear o volver a entrar a hacer uso de la interface de consola.

Descripción de las áreas de trabajo de la interfase de la consola PCadmin

(ver imagen Anexo 1)

(1) Área de herramientas principales para acciones rápidas o llamada a otras utilidades de la consola PCadmin.

Aparecen en su orden de izquierda a derecha los botones para dar acceso al visor de logs, al inventario de hardware y software, al controlo monitoreo remoto, al controlo monitoreo vía http - web, al módulo de chat para conversar con el usuario remoto, a los analizadores de estadísticas web y uso de software y finalmente a la presentación del último informe cuando se han solicitado datos en línea.

(2) Selección de modo de contacto a equipos con las opciones de búsqueda por nombre o búsqueda por dirección IP. Para equipos cercanos (red Microsoft local), se puede hacer por nombre, para otras redes o equipos remotos se sugiere usar la dirección IP.

(3) Área de selección de comandos. Aquí se seleccionan los comandos que se quieren aplicar al equipo o equipos que se han escogido previamente en el árbol de selección del lado derecho de los comandos. Existen tres tipos de comandos: a) simples, sin parámetro adicional. b) con parámetro opcional entre las palabras SI/NO. c) con parámetro obligatorio que varía dependiendo el comando y se escribe en la caja de texto en la parte inferior de la interfase.

(4) Área de entrada / selección de parámetros

(5) Área de equipos reportados a la consola. Aquí se organizan y relacionan todos los computadores que tienen instalado PCsecure y que se han reportado a la consola a través de la red, por lo menos en una ocasión, momento en el cual, si no existe se crea automáticamente el grupo al cual pertenezcan y se incluye en el mismo el nombre del equipo con su dirección IP respectiva. En esta área se puede seleccionar un solo PC, un grupo, o equipos individuales pulsando la tecla CTRL.

Si se pulsa clic derecho en esta área aparecerá un menú contextual, dependiendo si se hace sobre un grupo o sobre un PC, lo cual permitirá efectuar comandos directos de uso común sobre el objeto seleccionado (un PC o un grupo), tales como del inventario de hardware, cargar o quitar un perfil de seguridad, ordenar los grupos de equipos reportados, etc.

Al lado derecho de la interfase se presentan cuatro áreas horizontales en las cuales se muestran mensajes recibidos desde los PC remotos o mensajes informativos cuando el administrador ejecuta comandos sobre los mismos.

(6) En el área superior aparecen en color **rojo** los mensajes de **alertas de seguridad crítica** tales como los de equipos que no tienen control de software o intentos de acceder a carpetas del sistema por parte del usuario.

(7) En la siguiente área aparecen en color **azul,** todos los **reportes de bloqueos** tanto de ejecución autorizada como de intentos de modificar parámetros del equipo o del sistema operaciona l.

(8) Enseguida aparecen en color **verde** los **mensajes informativos de respuesta comandos** o cuando los equipos remotos inician la sesión de trabajo mostrándose el equipo, la dirección IP, la versión del sistema operacional la fecha y la hora. Al lado derecho de estos mensajes en el área con fondo amarillo se muestra cuando un equipo remoto ha recibido una orden de parte del administrador de la consola, lo cual permite fácilmente determinar a cuales equipos les llegó el comando y a cuáles no.

(9) Los equipos a los que no llega el comando porque están pagados, por ejemplo, aparecerán en la última franja inferior en color rojo, indicando que la consola no pudo contactar a ese PC. En esta misma

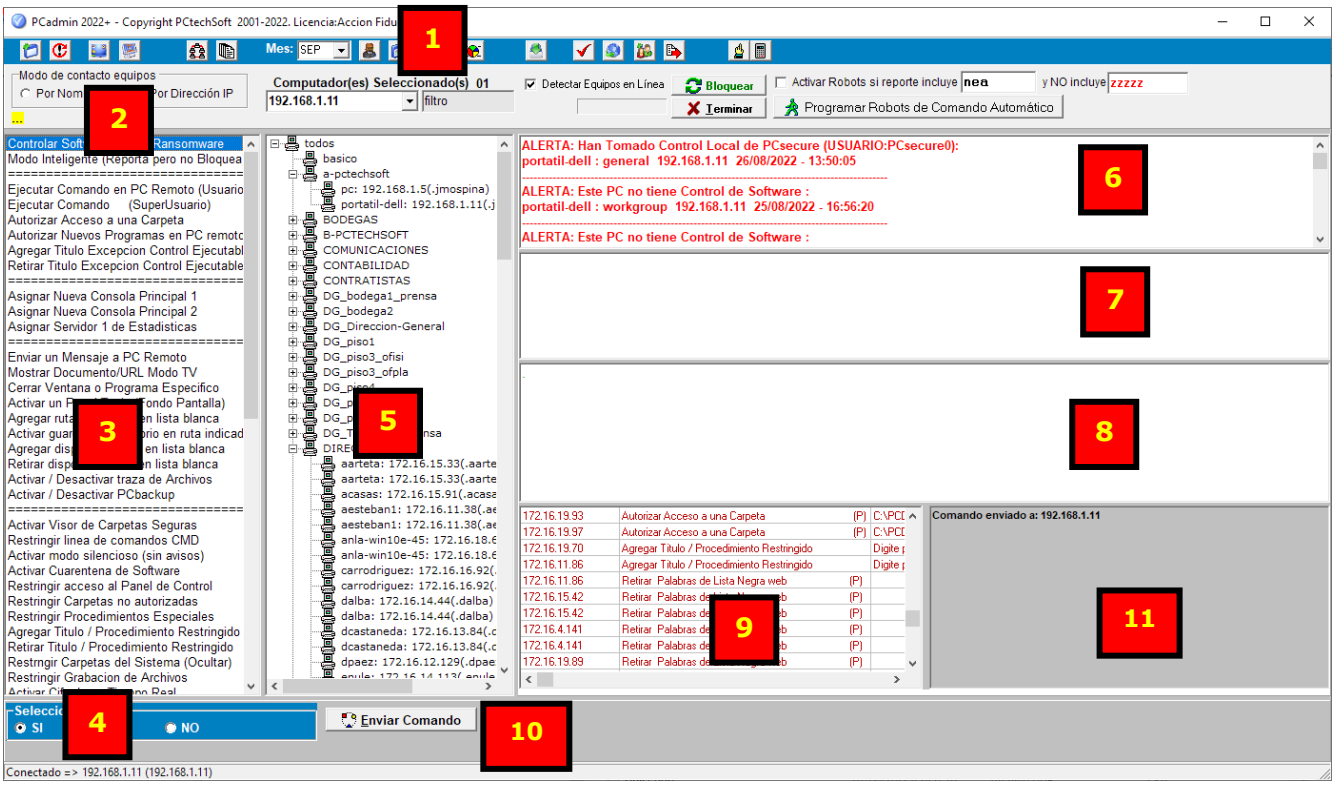
en color rojo periódicamente aparece la activación del socket de comunicaciones, dependiendo del número de mensajes recibidos por la consola.

Todos estos mensajes quedan guardados en los registros de Logs locales, los cuales se pueden analizar con el respectivo botón de la barra superior de herramientas.

(10) En la parte inferior aparecen los botones de envío y cancelación de comandos con los cuales se inicia la ejecución de un comando en el equipo remoto o la cancelación de un comando enviado previamente a un grupo de equipos.

(11) Área de reporte de comando enviado. Cuando se envían comandos, aparecerá allí la lista de equipos que recibieron el comando correctamente.

ANEXO 1 - AREAS DE INTERFASE DE LA CONSOLA PCADMIN



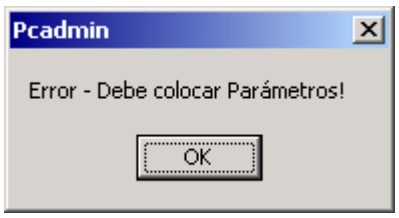
Los pasos a seguir para el envío de comandos hacia un PC remoto son:

1° Seleccione el equipo o equipos a los cuales les desea aplicar el comando, marcando los que la sección 5. También puede escribir la dirección IP por nombre del equipo en la casilla destinada para este fin ubicada sobre el área de selección de equipos.

2° Seleccione el comando que desea ejecutar de la lista de comandos en el área de la izquierda (sección 3). Es posible que en este momento aparezca en la parte inferior la opción para seleccionar un parámetro si/no lo cual significa activar o desactivar esa función en el equipo remoto, o una caja de texto para escribir el parámetro respectivo que requiera el comando (4).
3° Haga clic en el botón "**enviar comando**" ubicado en la parte inferior (10), con lo cual se iniciará el proceso de envío del comando hacia el equipo o equipos seleccionados, y a la velocidad que se haya

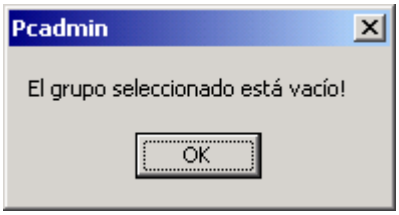
indicado con el control de velocidad de envío (11).

Inmediatamente los equipos que reciban la orden aparecerán en la sección 8 a la derecha (fondo amarillo). Dependiendo de la velocidad de envío de comando, los equipos que reciben el mismo, responderán y la respuesta aparecerá en la sección 8 en color verde. Aquellos que estén apagados o no hayan sido contactados serán reportados en color rojo en la sección 9. Aparecerá el botón "abortar comando" en la parte inferior, que permite cancelar la ejecución de un comando remoto (generalmente se usa cuando no responde el PC o el *Time Out* es demasiado y no se ha obtenido respuesta). Es importante verificar cuales equipos no recibieron el comando para ejecutarlo posteriormente cuando se reporten a la consola.
En caso de error, pueden presentarse estos tipos de mensajes:



Significa que el comando escogido requiere un parámetro que Ud. no indicó. Escríbalo en la casilla de **PARÁMETROS.**

Significa que falta la Dirección o Nombre en la casilla **PC DESTINO**. Seleccione un grupo o PC o digite una IP en la casilla



Significa que el GRUPO escogido no tiene PCs asignados. Seleccione otro grupo o PC o digite una IP en la dirección **PC DESTINO.**

Significa que el comando escogido, no se puede aplicar a más de un PC a la vez. Seleccione un solo PC o digite una IP en la dirección **PC DESTINO.**

Referencia rápida de los comandos de la consola PCadmin

Controlar Software, Spyware, Scripts, Virus

Activa / Desactiva el control de ejecutables en el PC remoto.

Si este queda desactivado, se enviará periódicamente, un reporte de Alerta Crítico a la Consola, indicando que no tiene control de software.

Ejecutar un Comando en PC Remoto / Ejecutar un Comando en PC Remoto (Super usuario)

Permite lanzar un programa en el PC remoto. SE pueden usar rutas locales a ese PC o de red, con parámetros adicionales (se sugiere incluir entre comillas dobles aquellos parámetros con espacios intermedios, dado que Windows usa el espacio como separador de parámetros). Permite instalaciones masivas y desatendidas, tanto de software comercial, como parches, actualizaciones de productos y scripts del sistema.

Ejemplos (parámetro):

:\windows\notepad.exe	Lanza el notepad local del PC remoto
Explorer http://www.google.com	Lanza la exploración del sitio Google
\\server1\quitavirus\borrablaster.exe	Lanza el programa borrablaster.exe de \\server1
command.com /C copy *.doc f:\	Ejecuta un único comando (copy) de *.doc en F:\

Explorer "c:\mis documentos',"
Abre Mis documentos en el (los) pes remoto(s)

Autorizar Acceso a una Carpeta

Permite agregar una carpeta en la lista de directorios autorizados para "explorar" (si se quiere recursivo, agregue un asterisco * al final)

Ejemplos (parámetro):

c:\actas	Autoriza la exploración de c: \actas
c:\actas*	Autoriza la exploración de c.xactas y sus sub-carpetas

Autorizar Nuevos Programas en PC remoto

Permite agregar ejecutables a la base de datos de programas autorizados. Se debe indicar la RUTA donde se encuentra(n) el (los) ejecutables. Este se usa por ejemplo para cuando se ha instalado nuevo software en el PC. (ATENCION: la autorización es recursiva desde el directorio que se indique)

Ejemplos (parámetro):

C:\archivos de programa\games	Autoriza los programas en C:\archivos de programa\games
\\server1\utiles	Autoriza todos los programas en \\serverl \utiles
f:\	Autoriza todos los programas en F:\

Enviar un Mensaje a PC Remoto

Muestra un mensaje en pantalla completa en el PC remoto, hasta que el usuario haga click con el mouse.

Ejemplos (parámetro):

Se informa que hoy habrá corte de energía a las 3:00 pm. Recuerde guardar sus archivos y apagar su PC

unos minutos antes. Dirección de Mantenimiento.

Muestra el mensaje citado en la pantalla del PC remoto.

Cerrar Ventana o Programa Especifico

Cierra en el PC remoto la ventana o ventanas indicadas (por título completo o parte del mismo) ó por nombre de ejecutable.

Ejemplos (parámetro):

Calcula Cierra todas las ventanas (y programas) que incluyan la subcadena calcula En su título.
Notepad.exe Cierra todas instancias del programa y ventanas asociadas al ejecutable notepad.exe

Activar un Papel Tapiz (Fondo Pantalla)

Establece una imagen como fondo de escritorio en los PCs remotos. Debe ser un Bitmap. Se activará al siguiente reinicio del PC o sesión de usuario. Se puede dar en el parámetro la palabra "Ninguno" se se quiere que no haya fondo de pantallas. NOTA: El bitmap asignado debe ser "reducido" a un tamaño menor a 800 Kb con algún utilitario gráfico (para evitar tráfico alto en su red).

Ejemplos (parámetro):

\\server2\pelicula. bmp
Establece como fondo (papel tapiz) la imagen pelicula.bmp ubicada en \\server2\

Asignar Nueva Consola Administradora (1 y 2)

Asigna a uno o más PCs un nuevo PC administrador / Sub administrador

Ejemplos (parámetro):

172.16.10.130
Asigna la consola IP 172.16.10.130 como nuevo administrador del PC o PCs remotos.

Asignar Nuevo Servidor de Estadísticas (1 y 2)

Asigna a uno o más PCs un nuevo Servidor a donde deben reportar inventarios y estadísticas

Ejemplos (parámetro):

172.16.10.130
Asigna el servidor con dirección IP 172.16.10.130 como nuevo receptor de LOGs e Inventarios para el PC o PCs remotos.

Asignar Nueva Clave de PCsecure

Cambia la clave de administrador para acceder PCsecure localmente en los PCs indicados

Ejemplos (parámetro):

ADMIN2010
Establece la nueva clave de administrador como ADMIN2010

Agregar Palabras Autorizadas en Web

Adiciona palabras nuevas a la lista de sitios autorizados para navegar. Si la página visitada NO cumple con tener en el URL o título una de las palabras autorizadas, PCsecure cerrará el navegador y

redireccionará al sitio asignado. Si se pone en el parámetro más de una palabra, deben ir separadas con coma. NOTA: Al agregar al menos una palabra autorizada, se cambia la modalidad de filtroweb: pasa de navegar en todo excepto lo que contenga oo. a No navegar en ninguna pagina, excepto si contiene oo.

Ejemplos (parámetro):

salud, gov, futbol
Agrega estas 3 palabras a la lista de web autorizada en los PCs

Borrar todas Palabras Autoriz. Web

Elimina todas las palabras Web autorizadas. De inmediato pasa a la modalidad de filtro: navegar en todas os excepto en oo.

Agregar Palabras Restringidas en Web

Adiciona palabras nuevas a la lista de restricciones para cuando el usuario navega en internet. Si la página visitada cumple con tener en el URL o título una de las palabras restringidas, PCsecure cerrará el navegador y redireccionará al sitio asignado. Si se pone en el parámetro más de una palabra, deben ir separadas con coma.

Ejemplos (parámetro):

games, hacker, ossama
Agrega estas 3 palabras a la lista de web restringido en los PCs

---

A continuación se presenta otro grupo de comandos en los cuales se usa el parámetro (SI/NO), con el cual se activan o desactivan las características individuales de Configuración en el PCsecure del PC remoto. Esto modifica guarda y aplica como perfil.

Simplemente se selecciona SI o NO, para Activar o Desactivar la Opción.

Ejemplos (OPCION):

Restringir Horas de Navegación
Si se escoge "SI" para el Ejemplo: Resultado => Se podrá navegar a cualquier hora / dia.

Activar modo silencioso (sin avisos para el usuario)

Deshabilita / habilita que cuando el usuario intenta una acción contralada por PCsecure, se visual icen o no, las pantallas con mensajes indicando que esa acción no está permitida.

Activar Cuarentena de Software

Deshabilita / habilita que si el usuario intenta ejecutar un programa, software, script, juego, instalador, etc, y este no está autorizado, será borrado (enviado a la carpeta C:\TRASH) .

Restringir acceso al Panel de Control

Restringe o activa el acceso a los ítems del Panel de Control.

Restringir Carpetas no autorizadas

Restringe o activa el acceso para explorar carpetas de los discos locales. Por default, todas la unidades de red, CDs, memorias USB, y dispositivos removibles están autorizados para explorar libremente.

Restringir USB de Almacenamiento masivo (Bloqueo total, Modo lectura ó Acceso total)

Restringe o activa el acceso para configurar y utilizar unidades de almacenamiento masivo, tales como memorias USB, Palms, Flash Memory, Discos externos, etc. evitando así fuga masiva de información e introducción de datos, mp3, videos, etc, hacia los discos locales.

Permitir Navegación en Internet

Restringe o activa el acceso para navegar en la web. El proceso cambia parámetros en la sección de los Proxy y puerto, para que el PC no "salga" de la red interna.

Restringir Sitios de Internet indicados

Restringe o activa el acceso a sitios de Internet, que contengan palabras o urls, restringidas, de acuerdo a la lista asignada. Opcional mente, el usuario será redireccionado a la página que se haya indicado en PCsecure.

Restringir Horas de Navegación

Restringe o activa la restricción de horario que se haya asignado en PCsecure. Si no se marcaron horas restringidas, no se afecta el servicio. Si se quieren cambiar las horas restringidas en los PCs remotos, se debe generar un perfil, exportarlo y luego aplicarlo a todos los equipos que se requiera.

Restringir Multi-Sesión Internet

Restringe o activa la restricción de número de sesiones simultáneas del navegador, para optimizar el recurso del ancho de banda y de la carga de la máquina. Si se quiere cambiar el topo máximo de sesiones simultáneas en los PCs remotos, se debe generar un perfil, exportarlo y luego aplicarlo a todos los equipos que se requiera.

Restringir Tecla Print Screen

Restringe o activa la opción de capturar la pantalla (screenshot) cuya imagen queda en el portapapeles de Windows

Restringir Acceso a diskette

Restringe o activa la opción de usar la unidad de discos flexibles.

Restringir Acceso a Registry

Restringe o activa la opción de modificar el registro de Windows y el uso de herramientas del sistema para este fin.

Restringir Impresiones en papel

Restringe o activa la opción de imprimir un documento en papel (suprime diálogo de impresoras).

Activar USB de datos (acceso total)

Activa las unidades de USB de datos en modo normal (se podrá grabar, borrar y editar en ellas)

Restringir USB de datos (solo lectura)

Activa las unidades de USB de datos en modo lectura (no se podrá grabar ni borrar ó editar en ellas)

Restringir USB de datos (completamente)

Desactiva el uso de unidades de USB de datos. Si se configura una unidad de almacenamiento, se bloqueará temporalmente el PC hasta su desconexión.

Cancelar toda la Seguridad (queda predet)

Cancela toda la seguridad y guarda como predeterminado este perfil en el PC remoto. NOTA: se debe aplicar un perfil predeterminado, importado o manualmente restaurar las opciones de cada Panel de seguridad, cuando se quiera restablecer el nivel de restricciones. Si el PC queda sin seguridad, enviará un reporte de Alerta Crítico a la Consola, indicando que no tiene control de software.

Cargar Perfil Estandar (queda Predet)

Carga el perfil de seguridad que se instaló inicialmente con PCsecure. Si se hicieron cambios a ese perfil, estos no serán activados y se deben modificar uno a uno, en caso necesario.

Traer Bitácora de Eventos de Seguridad

Envía orden de reportar Bitácora de seguridad al PC remoto. Será enviada al directorio de trabajo C:\DATA en el PC de la consola PCadmin. El nombre del archivo será:
NombrePC.SEG (posteriormente se pueden analizar con PCadmin)

Traer Estadísticas de uso del PC remoto

Envía orden de reportar Bitácora de Ejecución al PC remoto. Será enviada al directorio de trabajo C:\DATA en el PC de la consola. El nombre del archivo será:
NombrePC.USO (posteriormente se pueden analizar con PCadmin)

Traer Inventario de Hardware y Software

Envía orden de reportar Listado de Software Instalado en el PC remoto. Será enviado al directorio de trabajo C:\DATA en el PC de la consola. El nombre de los archivos será:
NombrePC.HAR = > Todos los programas "formalmente" instalados (reportados por el registro de Windows). (posteriormente se pueden analizar con PCadmin)

Verificar Inventarios de Hardware y Software

Envía orden para que se efectúe un "refresco" del inventario actual del pe. Este será enviado automática mente al server de estadísticas asignado y se consolidará con la herramienta PCinventory instalada en el mismo.

Apagar Computador Remoto

Envía orden de apagarse al PC remoto

Reiniciar Computador Remoto

Envía orden de reiniciar al PC remoto

Cerrar sesión en Computador Remoto

Cierra todos los programas y efectúa un "LOGOFF".

Exportar Eventos Programados

Envía orden reportar la lista de eventos programados que tenga el PC remoto. Posteriormente el administrador los editará y guardará en disco. Se pueden luego exportar y aplicar a uno o más PCs de la Red

Bloquear PC remoto

Envía orden para que el PC remoto quede "bloqueado" con una pantalla de PCsecure. Si el Usuario reinicia el PC, de nuevo continuará bloqueado. El administrador lo puede desbloquear, desde la consola
b.
o localmente, digitando la clave de PCsecure que tenga asignado el pe. Este mismo bloqueo aparece si PCsecure fue "atacado", caso en el cual se debe usar el desinstalador o un Upgrade de PCsecure, para "revivirlo".

Desbloquear PC remoto

Envía orden para que el PC remoto quede "desbloqueado".

Borrar archivos de Cuarentena (Trash)

Efectúa una limpieza de la carpeta de cuarentena (normalmente c:\trash) en los PCs remotos. Allí quedan los ejecutables que se hayan eliminado por intentos no autorizados de ejecución.

Encender Remotamente PCs Seleccionados

Permite enviar la orden de encendido a PCs remotos con tecnología ATX y Wake on LAN en su tarjeta de red. Funcionará, siempre y cuando se tenga el inventario de hardware del PC remoto en la consola PCadmin (se usa la MAC para el encendido).

MÓDULO DE MONITOREO Y CONTROL REMOTO

Este Botón permite ejecutar una solicitud de monitoreo o control remoto hacia un PC específico.

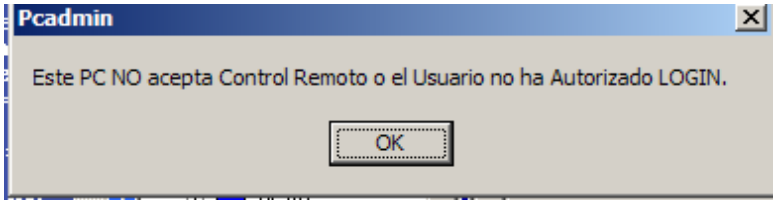
Hay tres opciones para la toma de control remoto (en PCsecure – Panel *Varios*) así:

a. El PC permite tomar control remoto en cualquier momento y sin autorización
b. El PC permite control remoto autorizado por el usuario remoto
c. El PC no permite toma de control remoto bajo ningún parámetro

Dependiendo de los *flags* indicadores que estén configurados en el PC remoto, PCadmin podrá o no, monitorear y tomar control remoto del PC solicitado.

A continuación se muestran las diferentes resultados del comando, según la citada configuración:

Cuando el PC no permite control remoto o el usuario remoto lo niega, aparece lo siguiente:



En cualquiera de los casos de esta opción (b.), aparecerá la siguiente ventana de interface para configurar el tipo de control remoto hacia el PC que ha autorizado:

- En **TIPO DE ACCESO** se define si se quiere tomar control de teclado y mouse o simplemente visualizar el PC remoto.

- En **MODO DE VIDEO**, se define la calidad de la imagen a transmitir. (bits es adecuado y más rápido para la mayoría de aplicaciones, pero en algunos casos se requiere color real (Full color), que puede ser un poco más lento.

- En **MODO DE CONEXIÓN,** se escoge entre privado o compartido. En modo compartido, varios PCadmin (varios administradores), pueden visualizar la misma pantalla simultáneamente, mientras que en modo privado, el administrador que entre de último es quien toma el control de la conexión.

- En **MODO DE VISOR**, se escoge si se quiere el acceso en una ventana o en pantalla completa (en este ultimo caso saldrá el siguiente aviso, recordando que con las combinaciones de teclas Ctrl. + Esc y Alt + Tab tendremos acceso al PC local (PC administrador) y a comandos adicionales del menú emergente de ***Pcvisor.***

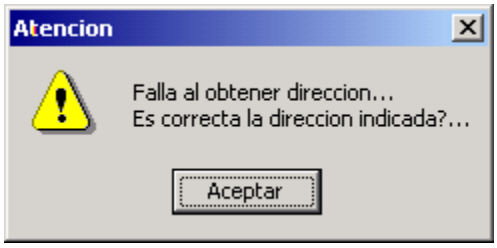
Estos comandos se acceden directamente, haciendo clic con el botón derecho del mouse sobre el programa en la barra de tareas (modo ventana) u oprimiendo Ctrl Esc (para llamar el escritorio local) y luego si seleccionar con botón derecho un comando del Pcvisor. (En Windows Vista y 7 pulse SHIFT antes de hacer clic para que aparezca el menú de opciones)

Se pueden tener múltiples conexiones simultáneas a distintos PCs y bajo diferentes configuraciones (monitoreo, control, pantalla completa, etc.)

Por último, si se marca la casilla **TRANSFERENCIA DE ARCHIVOS,** se lanzará interfase similar al Explorador de Windows al momento de hacer la conexión con el cual se pueden intercambiar archivos entre los PCS.

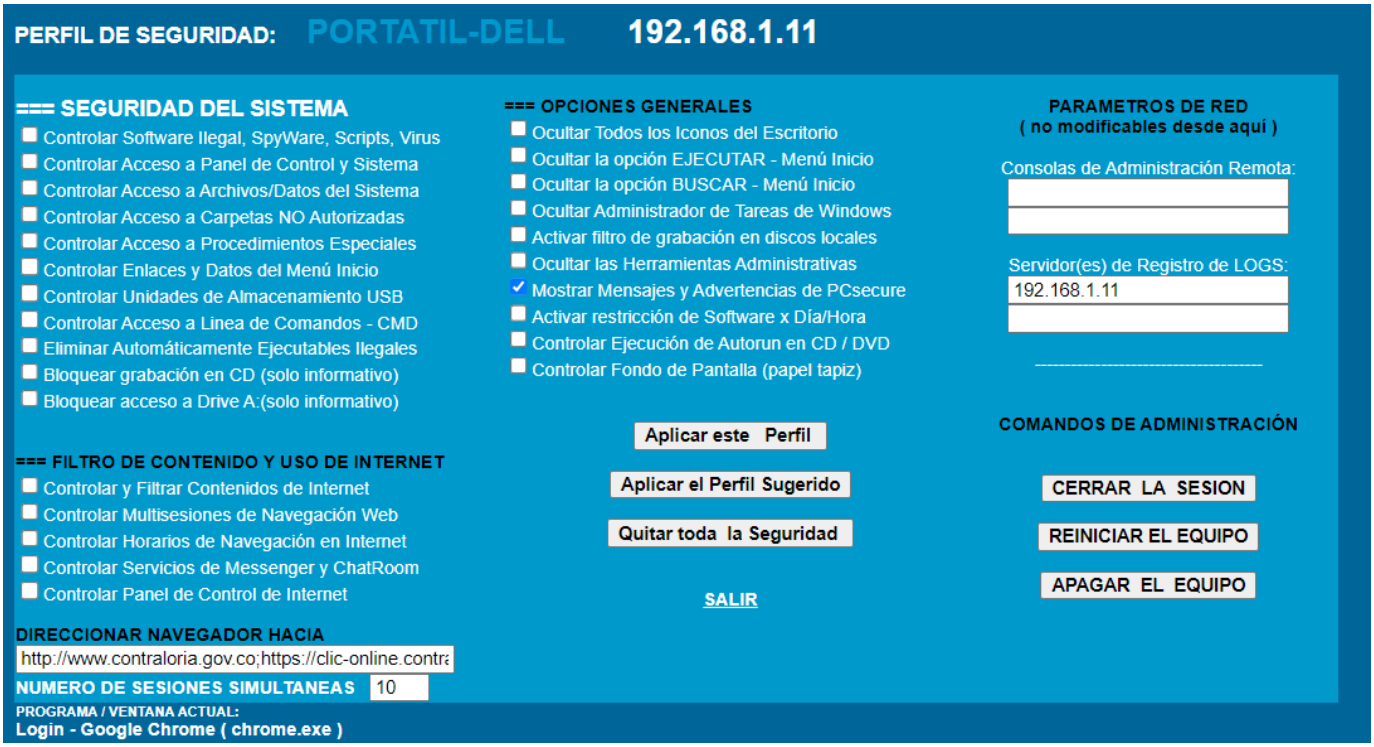
El Clipboard (porta papeles) se comparte entre el PC administrador y el PC que está siendo controlado, pero únicamente para cadenas de texto.

NOTAS: Al tomar control remoto, el usuario remoto aún puede usar su teclado y mouse. Se puede cancelar los mismos con la opción Bloquear "inputs" - entradas en PC remoto de este menú. Si al momento de intentar la conexión aparece alguno de los siguientes mensajes, posiblemente el PC remoto está reiniciando o apagando en el momento de autorizar la conexión:

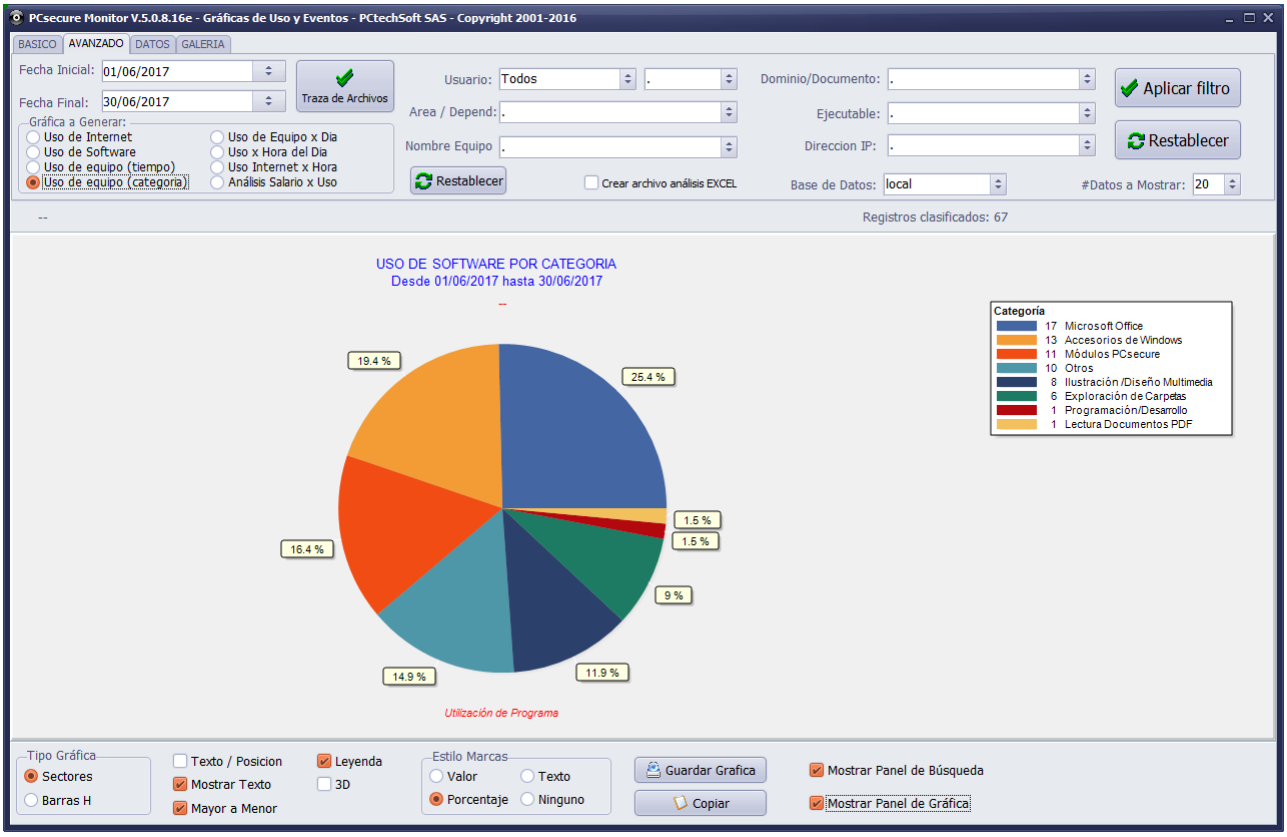


ADMINISTRACIÓN HTTP

Permite, con los mismos requisitos de autorización, conectarse al PC remoto usando el Internet Explorer. No se requiere conexión o servidor Web para la Intranet. En caso de conexión remota, requiere acceso vía RAS a la red interna de la empresa. Este módulo, más que tomar control remoto, ejecuta *administración remota*, sencilla sobre el PC. Se conecta por el puerto 82 bajo protocolo http. Las opciones disponibles son las siguientes:

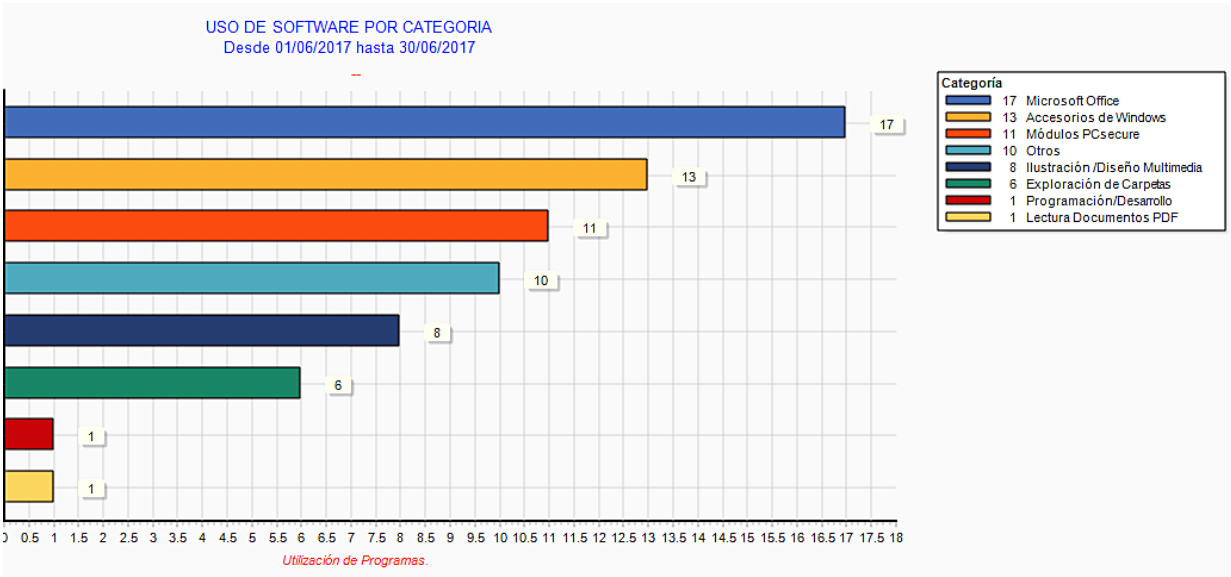


GRAFICACIÓN Y ANÁLISIS DE ESTADISTICAS



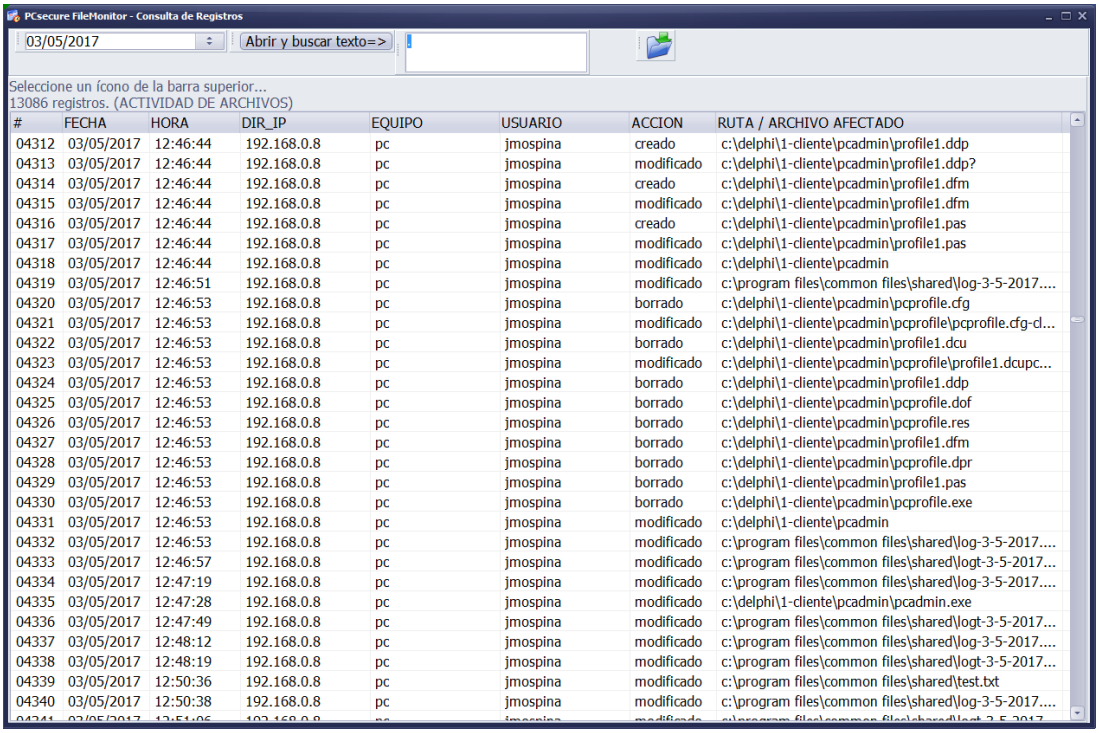
Este módulo permite seleccionar, analizar y graficar las estadísticas de uso y operación del sistema. Adicionalmente, se puede ver **ESTADISTICAS DETALLADAS,** que permite analizar paso a paso el uso de PC (forense), ver eventos de seguridad, clasificar el uso del PC por aplicación, analizar carpetas exploradas, ejecución de software, navegación web, etc.

Modelo de Graficación de Datos



TRAZABILIDAD DE ARCHIVOS

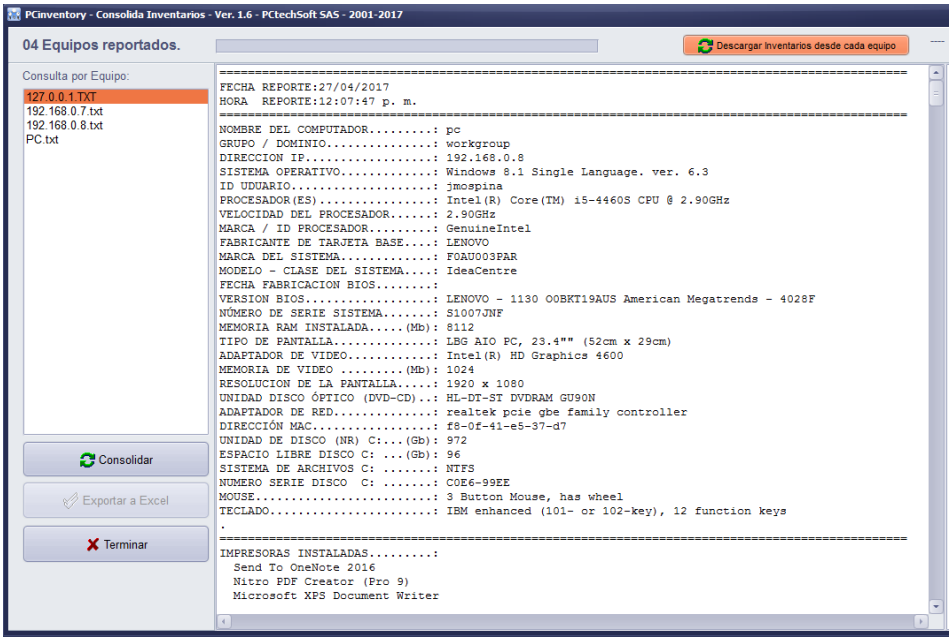
Este módulo permite seleccionar, analizar la actividad de archivos en los discos locales o ruta de red específicamente indicada. Se verán los archivos creados, modificados y eliminados por parte de los usuarios.



#	FECHA	HORA	DIR_IP	EQUIPO	USUARIO	ACCION	RUTA / ARCHIVO AFECTADO
04312	03/05/2017	12:46:44	192.168.0.8	pc	jmospina	creado	c:\delphi\1-cliente\pcadmin\profile1.ddp
04313	03/05/2017	12:46:44	192.168.0.8	pc	jmospina	modificado	c:\delphi\1-cliente\pcadmin\profile1.ddp?
04314	03/05/2017	12:46:44	192.168.0.8	pc	jmospina	creado	c:\delphi\1-cliente\pcadmin\profile1.dfm
04315	03/05/2017	12:46:44	192.168.0.8	pc	jmospina	modificado	c:\delphi\1-cliente\pcadmin\profile1.dfm
04316	03/05/2017	12:46:44	192.168.0.8	pc	jmospina	creado	c:\delphi\1-cliente\pcadmin\profile1.pas
04317	03/05/2017	12:46:44	192.168.0.8	pc	jmospina	modificado	c:\delphi\1-cliente\pcadmin\profile1.pas
04318	03/05/2017	12:46:44	192.168.0.8	pc	jmospina	modificado	c:\delphi\1-cliente\pcadmin
04319	03/05/2017	12:46:51	192.168.0.8	pc	jmospina	modificado	c:\program files\common files\shared\log-3-5-2017....
04320	03/05/2017	12:46:53	192.168.0.8	pc	jmospina	borrado	c:\delphi\1-cliente\pcadmin\pcprofile.cfg
04321	03/05/2017	12:46:53	192.168.0.8	pc	jmospina	modificado	c:\delphi\1-cliente\pcadmin\pcprofile\pcprofile.cfg-cl...
04322	03/05/2017	12:46:53	192.168.0.8	pc	jmospina	borrado	c:\delphi\1-cliente\pcadmin\profile1.dcu
04323	03/05/2017	12:46:53	192.168.0.8	pc	jmospina	modificado	c:\delphi\1-cliente\pcadmin\pcprofile\profile1.dcupc...
04324	03/05/2017	12:46:53	192.168.0.8	pc	jmospina	borrado	c:\delphi\1-cliente\pcadmin\profile1.ddp
04325	03/05/2017	12:46:53	192.168.0.8	pc	jmospina	borrado	c:\delphi\1-cliente\pcadmin\pcprofile.dof
04326	03/05/2017	12:46:53	192.168.0.8	pc	jmospina	borrado	c:\delphi\1-cliente\pcadmin\pcprofile.res
04327	03/05/2017	12:46:53	192.168.0.8	pc	jmospina	borrado	c:\delphi\1-cliente\pcadmin\profile1.dfm
04328	03/05/2017	12:46:53	192.168.0.8	pc	jmospina	borrado	c:\delphi\1-cliente\pcadmin\pcprofile.dpr
04329	03/05/2017	12:46:53	192.168.0.8	pc	jmospina	borrado	c:\delphi\1-cliente\pcadmin\profile1.pas
04330	03/05/2017	12:46:53	192.168.0.8	pc	jmospina	borrado	c:\delphi\1-cliente\pcadmin\pcprofile.exe
04331	03/05/2017	12:46:53	192.168.0.8	pc	jmospina	modificado	c:\delphi\1-cliente\pcadmin
04332	03/05/2017	12:46:53	192.168.0.8	pc	jmospina	modificado	c:\program files\common files\shared\log-3-5-2017....
04333	03/05/2017	12:46:57	192.168.0.8	pc	jmospina	modificado	c:\program files\common files\shared\logt-3-5-2017...
04334	03/05/2017	12:47:19	192.168.0.8	pc	jmospina	modificado	c:\program files\common files\shared\log-3-5-2017....
04335	03/05/2017	12:47:28	192.168.0.8	pc	jmospina	modificado	c:\delphi\1-cliente\pcadmin\pcadmin.exe
04336	03/05/2017	12:47:49	192.168.0.8	pc	jmospina	modificado	c:\program files\common files\shared\logt-3-5-2017...
04337	03/05/2017	12:48:12	192.168.0.8	pc	jmospina	modificado	c:\program files\common files\shared\log-3-5-2017....
04338	03/05/2017	12:48:19	192.168.0.8	pc	jmospina	modificado	c:\program files\common files\shared\logt-3-5-2017...
04339	03/05/2017	12:50:36	192.168.0.8	pc	jmospina	modificado	c:\program files\common files\shared\test.txt
04340	03/05/2017	12:50:38	192.168.0.8	pc	jmospina	modificado	c:\program files\common files\shared\log-3-5-2017....

CONSOLIDACION y CONSULTA DE INVENTARIOS DE HARDWARE Y SOFTWARE

En la interface PCINVENTORY (Icono en escritorio del LogServer) se pueden efectuar consultas por IP, Nombre del equipo ó por grupo Windows. Primero se deja abierto al menos 2 días para que consolide inventarios. Se cierra y al abrir se tendrá la información así:



Al consultar el Hardware se tienen además de los campos básicos, otros detalles del equipo relativos a la seguridad. (ver detalle adjunto)

DETALLE DE LA INFORMACIÓN OBTENIDA EN UNA CONSULTA x PC:

```
================================================================================================
FECHA REPORTE:05/01/2011
HORA  REPORTE:11:04:05 a.m.
================================================================================================
```

Consulta de Hardware por NOMBRE DEL COMPUTADOR.....: jmo-01

```
GRUPO / DOMINIO.............: inicioms
DIRECCION IP................: 192.168.0.10
SISTEMA OPERATIVO...........: Windows 7 Ultimate. ver. 6.1
ID UDUARIO..................: systems
PROCESADOR(ES)..............: Intel(R) Core(TM)2 Duo CPU     T5870  @ 2.00GHz
VELOCIDAD DEL PROCESADOR....: 2.00GHz
MARCA / ID PROCESADOR.......: GenuineIntel
FABRICANTE DE TARJETA BASE..: Dell Inc.
MARCA DEL SISTEMA...........: Vostro1510
MODELO - CLASE DEL SISTEMA..: Vostro
FECHA FABRICACION BIOS......: 10/09/08
VERSION BIOS................: DELL   - 6040000 Ver 1.00
NÚMERO DE SERIE SISTEMA.....: BSPQWF1
MEMORIA RAM INSTALADA.....(Mb): 3072
TIPO DE PANTALLA............: LPL0000, 15.4"" (33cm x 21cm)
ADAPTADOR DE VIDEO..........: Mobile Intel(R) 965 Express Chipset Family
MEMORIA DE VIDEO .........(Mb): 384
RESOLUCION DE LA PANTALLA...: 1280 x 800
UNIDAD DISCO ÓPTICO (DVD-CD)..: MATSHITA DVD+-RW UJ-875S ATA Device
ADAPTADOR DE RED............: dell wireless 1395 wlan mini-card
DIRECCIÓN MAC...............: 00-24-2b-a5-ad-05
UNIDAD DE DISCO (NR) C:...(Gb): 157
ESPACIO LIBRE DISCO C: ...(Gb): 67
SISTEMA DE ARCHIVOS C: .....: NTFS
NUMERO SERIE DISCO  C: .....: 7C94-C8B1
UNIDAD DE DISCO (NR) D:...(Gb): 2
ESPACIO LIBRE DISCO D: ...(Gb): 1
SISTEMA DE ARCHIVOS D: .....: NTFS
NUMERO SERIE DISCO  D: .....: DC5E-64BE
MOUSE.......................: 3 Button Mouse, has wheel
TECLADO.....................: Japanese, 12 function keys
 ==============================================================================================
IMPRESORAS INSTALADAS.........:
  Microsoft XPS Document Writer
  Microsoft Office Document Image Writer
  MagicPDF
  LexmarkX543-RED
  Fax
  CIB pdf brewer
================================================================================================
RECURSOS COMPARTIDOS..........:
  ipc$                                      ipc remota
  print$       c:\windows\system32\spool\drivers
                                            controladores de impresora
  e$           e:\                          recurso compartido predet.
  lexmark x543 xps
               192.168.0.205          en cola  lexmarkx543-red
================================================================================================
USUARIOS REGISTRADOS..........:
  administrador
  administrator
  guest
  usuario
================================================================================================
```

CONSULTA DE SOFTWARE INSTALADO (Alfabetico y versión)

2007 Microsoft Office Suite Service Pack 2
5.0.8 c:\pcdata\bde\
Adobe Flash Player 10 ActiveX (10.1.102.64)
Adobe Shockwave Player 11.5 (11.5.6.606)
Advertising Center (0.0.0.2)
Apple Application Support (1.1.0)
Ask Toolbar (1.9.1.0)
AutoIt v3.3.4.0
Avira AntiVir Personal - Free Antivirus (10.0.0.42)
AviSynth 2.5
AVStoDVD 2.3.2 (2.3.2)
BDE
Borland Delphi 6 (6.0)
BroadCam Video Streaming Server
Camtasia Studio 5 (5.0.1)
CIB pdf brewer 2.5.29 (2.5.29)
Consulta LOGs 1.3 C:\data\
Consulta LOGs 1.4 C:\data\
Consulta LOGs 1.5 C:\data\
Consulta LOGs 1.6 C:\data\
ConsultaMSN c:\LOGs_Mess\
CorelDRAW Graphics Suite X3 (13.1)
Cryptext
Database Engine Full Install
Debut Video Capture Software
Delphi 7 Second Edition C:\Program Files\Delphi7SE\
EurekaLog 6.0.24 Trial C:\Program Files\EurekaLog 6\
FontNav (5.0)
Form Extractor
Foxit Reader (4.3.0.1110)
Free Studio version 4.9.13 C:\Program Files\DVDVideoSoft\Free Studio\
Google Chrome (7.0.517.44)
Google Earth (5.2.1.1588)
Google Update Helper (1.2.183.39)
Haali Media Splitter
Hauppauge MCE XP/Vista Software Encoder (2.0.25149)
Herramienta de carga de Windows Live (14.0.8014.1029)
HSDPA USB MODEM version 4.099 C:\Program Files\HSDPA USB MODEM\
HyperMedia Software C:\Program Files\KWorld Multimedia\HyperMedia\
HyperMediaCenter 3.6 C:\Program Files\KWorld Multimedia\HyperMedia\
ImgBurn (2.5.2.0)
Inno Setup versión 5.2.0 (5.2.0)
Intel (8.15.10.1930)
IrfanView
IsoBuster 2.8.5 (2.8.5)
Java (6.0.210)
Java Auto Updater (2.0.2.1)
K-Lite Codec Pack 5.7.0 (5.7.0)
KWorld EM_USB Device Utilities (3.0.0.0)
KWorld PVR-TV BDA Drivers C:\Program Files\KWorld MultiMedia\Driver\
LanSpy C:\Program Files\LanTricks\LanSpy\
Laptop Integrated Webcam Driver
Lernout & Hauspie TruVoice American English TTS Engine
MagicPDF 2.01 C:\Program Files\MagicPDF\
ManyCam 2.5.48 (2.5.48)
MCE Software Encoder 1.1 (1.1.0.1108)
Media Player Codec Pack 3.9.5
Microsoft Application Error Reporting (12.0.6012.5000)
Microsoft Choice Guard (2.0.48.0)
Microsoft Document Explorer 2008 C:\Program Files\Common Files\Microsoft Shared\Help 9\
Microsoft Office Access MUI (12.0.6425.1000)

```
Microsoft Office Enterprise 2007    (12.0.6425.1000)
Microsoft Office Excel MUI    (12.0.6425.1000)
Microsoft Office FrontPage 2003    (11.0.5614.0)
Microsoft Office Groove MUI    (12.0.6425.1000)
Microsoft Office InfoPath MUI    (12.0.6425.1000)
Microsoft Office OneNote MUI    (12.0.6425.1000)
Microsoft Office Outlook MUI    (12.0.6425.1000)
Microsoft Office PowerPoint MUI    (12.0.6425.1000)
Microsoft Office Proof    (12.0.6425.1000)
Microsoft Office Proofing    (12.0.4518.1014)
Microsoft Office Publisher MUI    (12.0.6425.1000)
Microsoft Office Shared MUI    (12.0.6425.1000)
Microsoft Office Word MUI    (12.0.6425.1000)
Microsoft Visual C++ 2005 ATL Update kb973923 - x86 8.0.50727.4053    (8.0.50727.4053)
Microsoft Visual C++ 2005 Redistributable    (8.0.56336)
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.4148    (9.0.30729.4148)
Microsoft Visual J# 2.0 Redistributable Package C:\Windows\Microsoft.NET\Framework\v2.0.50727\
MiniTool Partition Wizard Home Edition 5.2 C:\Program Files\MiniTool Partition Wizard Home Edition 5.2\
Mozilla Firefox    (3.6.13 (es-ES))
MSNcontrol 2.1 c:\archivos de programa\pcmsn\
MSVCRT    (14.0.1468.721)
MSXML 4.0 SP2 Parser and SDK    (4.20.9818.0)
MySQL Connector/ODBC 5.1    (5.1.8)
MySQL Server 5.1    (5.1.54)
NCH Toolbox
Nero 9 Lite C:\Program Files\Nero\Nero ControlCenter 4
Nero ControlCenter    (9.0.0.1)
Nero Installer    (4.4.9.0)
Nero Online Upgrade    (1.3.0.0)
Nero StartSmart    (9.4.31.100)
neroxml    (1.0.0)
Nokia Connectivity Cable Driver    (6.80.5.1)
NS Remote Port Scanner 1.32
O2Micro Flash Memory Card Reader Driver    (3.27)
O2Micro Flash Memory Card Windows Driver    (2.0.09)
Panda USB Vaccine 1.0.1.4 C:\Program Files\Panda USB Vaccine\
PandoraRecovery
Partition Wizard Home Edition 5.0 C:\Program Files\Partition Wizard Home Edition 5.0\
PCadmin 5.0 C:\PCsecure\
PCMessServer 1.6 c:\logs_mess\
PCnetServer 1.6 c:\PCdata\
PhotoFiltre
Picasa 3    (3.1)
PowerDVD    (7.30.0000)
SUPER © Version 2010.bld.37    (Version 2010.bld.37 (Jan 2, 2010))
TouchChip USB Driver 2.19    (2.19.0.0173)
TVUPlayer 2.5.3.1    (2.5.3.1)
Uninstall 1.0.0.1 C:\Program Files\Common Files\DVDVideoSoft\
Unlocker 1.9.0    (1.9.0)
Update for 2007 Microsoft Office System
Update Manager    (4.60)
VBA    (6.2)
VideoPad Video Editor
VMware Player    (2.5.2.7026)
WD SmartWare    (1.4.2.5)
Windows Live Asistente para el inicio de sesión    (5.000.818.5)
Windows Live Call    (14.0.8064.0206)
Windows Live Communications Platform    (14.0.8098.930)
Windows Live Essentials    (14.0.8089.0726)
Windows Live Messenger    (14.0.8089.0726)
Windows XP Mode    (1.3.7600.16422)
```

Se pueden generar consultas y filtros por los diferentes campos