

Manual de Usuario de CRAT-TOOL

Tabla de Contenidos

Introducción	3
¿Qué es?	3
¿Que características posee?	3
Instalación	5
Requisitos del Sistema	5
Servidor	5
Cliente	5
Guía De Uso	6
Conectar con la Red	6
Acciones	6
Información del Sistema	7
Software	7
Procesos	8
Ventanas	8
Servicios	9
Acciones de Apagado	10
Acciones de Bloqueo	10
Acceso Remoto	10
Escritorio Remoto	11
Consola Remota	11
Envío	12
Message Box	13
Pagina Web	13

Introducción

¿Qué es?

CRat es una herramienta cuya finalidad consiste en habilitar a un administrador a manejar/interactuar de forma cómoda y rápida los equipos de la red en la que se encuentra o de forma totalmente remota a través de internet, permitiéndole obtener información o ejecutar acciones concretas en los equipos. Ha sido desarrollada como proyecto de fin de curso del ciclo DAM

¿Que características posee?

Las principales **características** que posee **CRat** son:

- Los equipos clientes los que se conecten al equipo **Administrador** automáticamente siempre que les sea posible y no al revés, de forma que el administrador pueda seguir recibiendo conexiones aun **sin saber la dirección de los equipos clientes** y así tener controlada la red.
- El administrador puede **Enviar mensajes** de aviso (información, alerta, error) al equipo que desee.
- Posibilidad de **recopilar información del sistema** del cliente que desee (**Software, Ventanas, Procesos, Servicios...**).
- Posibilidad de **realizar acciones sobre las ventanas** que se encuentran abiertas en el equipo que desee, pudiendo minimizarlas, bloquearlas permanentemente,desbloquearlas, cambiarle el título(Joke).
- Posibilidad de **Iniciar o Matar Procesos** en los clientes que desee.
- Posibilidad de **abrir páginas** de forma remota en los equipos que desee, lanzando el navegador con la web solicitada automáticamente.
- Posibilidad **Apagar, Reiniciar , Suspender y Cerrar sesión** en los equipos.
- Posibilidad de **ejecutar comandos de consola** (cmd) de forma remota y visualizar su respuesta.
- Podrá iniciar **escritorio remoto** con el equipo deseado, tanto en modo visualización como manejable.
- Crea un **historial con todas las acciones** que ha realizado el administrador y las respuestas de los respectivos clientes (almacenado en DB).
- Permite la personalización de la aplicación servidora mediante temas que se pueden cambiar en tiempo de ejecución.
- Permite la elección del idioma de la aplicación (Español/Ingles).
- **Genera informes** en base a la información anterior en los formatos **PDF, Word, Excel, txt, HTML**, con una presentación limpia para impresión y manejando de forma eficiente la información de la base de datos para generar gráficas sobre el uso de la aplicación (Por cliente,fecha,en función de acciones...).

Asimismo, la aplicación cliente también dispone de algunas características propias que el administrador podrá definir de formar fácil antes de distribuirla:

- Permite **definir la dirección** a la que el cliente intentará conectarse [IP : Puerto].
- Permite la **ejecución** del cliente en **modo consola** (debug) o en forma de **proceso oculto** (recomendable).
- Permite **proteger el cliente con una contraseña**, de forma que ningún administrador con la aplicación servidora podrá manejar ese cliente sin autenticarse con posterioridad.
- Permite definir **los tiempos de re-conexión** del cliente.
- Permite definir una contraseña adicional para la conexión de escritorio remoto, así como el puerto que usará para establecerla.

Instalación

Requisitos del Sistema

Los requisitos del sistema son:

- **Sistema Operativo:** Windows XP, Windows Vista, Windows 7, Windows 8.
- **Procesador:** 1GHz.
- **RAM:** 512MB.
- **Microsoft .NetFramework:** 2.0 / 3.5 / 4.0
- **Red:** Red Local o Internet para conectar con los diferentes clientes.

Servidor

Para **instalar** la aplicación **Servidor**, debemos instalar los siguientes componentes en el siguiente orden:

- **Microsoft .Net Framework 2.0**
- **Microsoft .Net Framework 4.0**
- **Servidor CRat (Instalador distribuido con la aplicación).**
- **Instalar Base de datos Mysql.**
- **Ejecutar el script de creación de la DB que almacenará la información.**

!En el caso de windows 7 o superior solo es necesario el Framework .Net 4.0

Una vez instalados los componentes, ya podrá empezar a hacer uso de la aplicación Servidor de CRat.

Cliente

Para hacer funcionar la aplicación **Cliente**, no se necesita ningún tipo de preparación adicional a excepción del framework .NET

- **Microsoft .Net Framework 2.0**
- **Microsoft .Net Framework 4.0**

***En el caso de windows 7 o superior solo es necesario el Framework .Net 4.0**

Una vez instalados los componentes, ya podrá ejecutar la aplicación **cliente** en el equipo servidor.

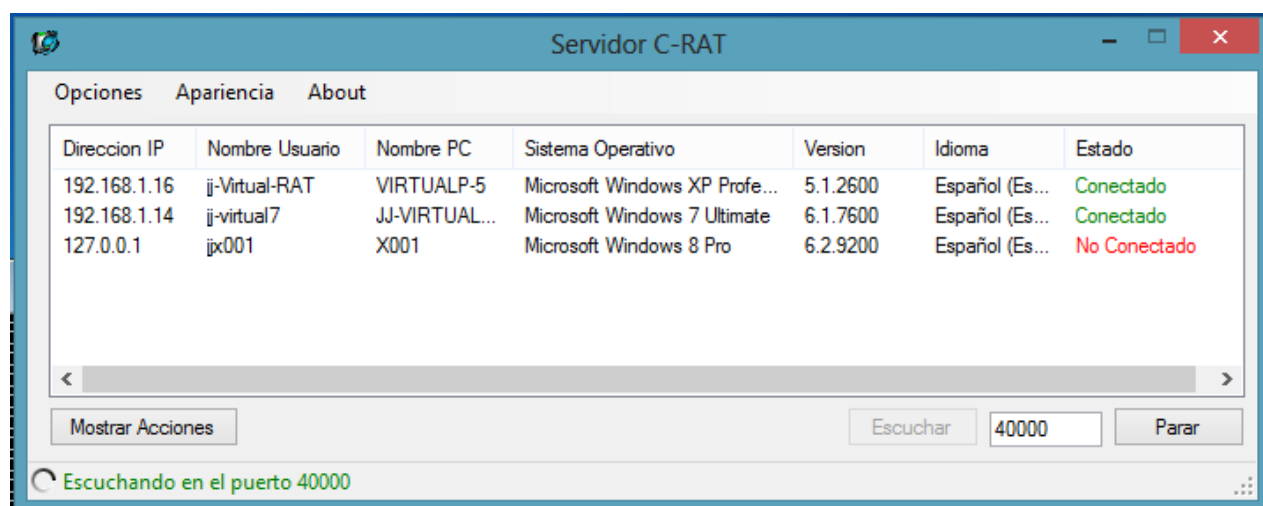
Conectar con la Red

Empezar a administrar una red con **C-RAT** es muy sencillo.

C-RAT se trata de una herramienta de conexión inversa es decir, realmente son los servidores los que se distribuyen y actúan como clientes realizando las ordenes que nosotros les enviamos desde nuestra aplicación cliente (que realmente es el servidor que escucha las conexiones).

Gracias a esta estructura de conexión cliente-servidor inversa, obtenemos la posibilidad de manejar todos los equipos de una red o incluso equipos fuera de ella, **sin conocer la dirección IP** de la maquina que queremos manejar, tan solo necesitamos distribuir el ejecutable de cliente a los equipos que queremos administrar y ellos mismos se encargarán de conectarse a nosotros.

Para empezar a escuchar las conexiones de los equipos de la red en los cuales se ha ejecutado nuestra aplicación cliente, tan solo debemos hacer click en el botón '**Escuchar**' y indicar el puerto sobre el que queremos hacerlo.



En este momento nuestro equipo ya está listo para escuchar empezar a administrar a los equipos que se conecten.

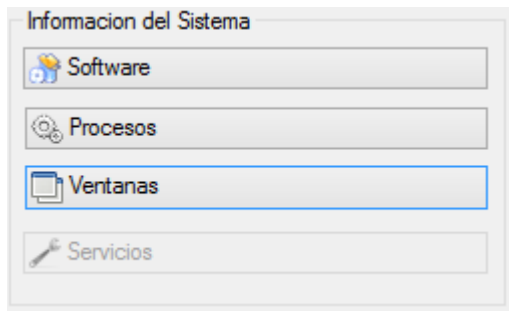
Acciones

Información del Sistema

Las acciones de **Información del Sistema**, son aquellas que nos permiten conocer sobre la información que posee ese sistema del cliente en concreto.

Podemos conocer y realizar acciones acerca de:

- [Software](#)
- [Procesos](#)
- [Ventanas](#)
- [Servicios](#)



Software

La acción '**Ver Software**' nos permite conocer todo tipo de software instalado en el equipo del cliente conectado.

De cada aplicación instalada nos ofrece la siguiente información:

- **Nombre:** Nombre del software.
- **Autor:** Compañía / Persona que lo desarrolló.
- **Url:** Web de la compañía que lo desarrolló.
- **Fecha De Instalación:** Fecha en la que se instaló el software en equipo.

Información del Sistema: Software Instalado [127.0.0.1]						Acciones
	Nombre	Version	Autor	Url	Fecha Instalacion	
▶	HelpNDoc 3.9...	3.9.0.595 Pers...	IBE Software	http://www.ib...	11/05/2013	
	Pro Evolution S...	1.10.0000	Nombre de su o...	http://www.ko...	14/03/2013	
	Call of Duty(R) ...	1.7	Activision	www.activision...	18/03/2013	
	Left 4 Dead 2	Repack por ald...	www.identi.li	http://www.id...	13/03/2013	
	tools-freebsd	9.2.3.1031769	VMware, Inc.		03/05/2013	
	Microsoft Visual...	10.0.30319	Microsoft Corpo...		07/04/2013	
	JetBrains ReSh...	7.1.2000	JetBrains Inc	http://www.jet...	07/04/2013	
	Microsoft SQL ...	10.1.2531.0	Microsoft Corpo...		03/04/2013	
	Microsoft ASP....	2.0.50217.0	Microsoft Corpo...		07/04/2013	
	tools-netware	9.2.3.1031769	VMware, Inc.		03/05/2013	
	MySQL Connec...	6.6.5	Oracle	http://www.my...	15/05/2013	
	Microsoft Visual...	9.0.30729.4148	Microsoft Corpo...		03/05/2013	
	Java 7 Update ...	7.0.210	Oracle	http://java.com	11/03/2013	
	LG United Mobi...	3.8.1	LG Electronics	http://www.L...	03/05/2013	
	Microsoft SQL ...	3.5.8080.0	Microsoft Corpo...		03/04/2013	
	Prototype 2 (rep...	1.0	Radical Entertai...	http://www.tar...	18/03/2013	
	Microsoft ASP....	2.0.50217.0	Microsoft Corpo...		07/04/2013	
	Dotfuscator Sof...	5.0.2300.0	PreEmptive Sol...		07/04/2013	
	Microsoft SQL ...	10.50.1447.4	Microsoft Corpo...		03/04/2013	
	Java Auto Upd...	2.1.9.5	Sun Microsyste...		28/04/2013	
	Skype™ 6.3	6.3.107	Skype Technol...	http://www.sk...	11/06/2013	
	Microsoft ASP....	2.0.50414.0	Microsoft Corpo...		07/04/2013	
	Objetos de adm...	10.50.1447.4	Microsoft Corpo...		03/04/2013	
	Microsoft Visual...	10.0.30319	Microsoft Corpo...		07/04/2013	
	Microsoft SQL ...	10.50.1447.4	Microsoft Corpo...		07/04/2013	
	Microsoft Visual...	9.0.30729	Microsoft Corpo...		07/04/2013	
	Microsoft Visual...	8.0.56336	Microsoft Corpo...		11/03/2013	
Consultar Info						
Se recibieron 97 registros						

Procesos

La acción '**Ver Procesos**' nos permite conocer los procesos que se están ejecutando en el sistema cliente.

De cada proceso nos indica:

- **Handle:** Es el manejador interno del proceso, a través del cual se puede hacer referencia a él. Muy útil si queremos realizar acciones externas sobre el proceso.
- **Nombre:** Nombre del proceso.
- **Ventana Asociada:** Nos indica si el proceso dispone de alguna ventana asociada a él.

Además podemos realizar las siguientes acciones sobre los procesos:

- **Ejecutar Nuevo:** Permite ejecutar un nuevo proceso en el sistema del cliente, indicándole el nombre. Por ejemplo: '*cmd*' abriría una consola en el cliente.
- **Matar Proceso:** Finaliza la ejecución del proceso/s seleccionado/s en el equipo del cliente. Utilizar con cuidado ya que puede causar la inestabilidad del sistema operativo del cliente al finalizar algún proceso crítico.

The screenshot shows a window titled 'Información del Sistema: Procesos En Ejecución [127.0.0.1]'. It contains a table of running processes and a panel of actions on the right.

Id	Nombre	VentanaAsociada
0	Idle	
1008	dwm	
1164	svchost	
1212	Skype	Skype™ - xkrossx2
124	svchost	
1320	hamachi-2	
1392	spoolsv	
1420	svchost	
1572	daemonu	
1584	amsvc	
1632	dasHost	
1692	devenv	Servidor - Microsoft Visual St...
1720	splwow64	
1728	mdm	
1752	hnd3	HelpNDoc
1812	MsMpEng	
1828	PnkBstrA	
1880	sqlservr	
1888	svchost	
1896	Cliente.Servicio	Cliente.Servicio.exe - Acces...
1916	vmnat	
2184	vmnetdhcp	
2216	vmware-usbarbitrator64	
2236	chrome	
2284	vmware-authd	
2412	ComUpdates	
2488	RatServer.vshost	

On the right, the 'Acciones' panel contains two buttons: 'Iniciar Proceso' and 'Matar Proceso'.

At the bottom left, there is a 'Consultar Info' button and a status bar that reads 'Se recibieron 83 registros'.

Ventanas

La acción '**Ver ventanas**' nos permite conocer las ventanas visibles (las que el usuario que está en el PC puede ver) en el equipo del cliente conectado.

De cada ventana visible nos ofrece la siguiente información:

- **Handle:** Manejador interno de la ventana, a través del cual podemos hacer referencia a ella desde el exterior.
- **Título:** Título visible de la ventana. El que aparece en el marco superior.
- **Habilitada:** Nos indica si la ventana se encuentra habilitada para el usuario. Una ventana no habilitada es aquella que el sistema operativo se está encargando de bloquear, por alguna razón para que el usuario no pueda interactuar con ella, por ejemplo las ventanas que tiene una ventana modal delante.

Además, en la ventana de '**Ver Ventanas**' seleccionando las ventanas sobre las que queremos actuar, podemos realizar

algunas acciones directamente sobre las ventanas del cliente.

Las acciones actualmente disponibles son:

- **Cambiar Nombre:** Cambia el título de la ventana seleccionada por el que nosotros le indiquemos.
- **Minimizar Ventana:** Minimiza la ventana seleccionada.
- **Bloquear Ventana:** Inhabilita totalmente el uso de la ventana. La ventana quedará bloqueada hasta que el administrador la desbloquee. El usuario del equipo no podrá hacer nada con ella.
- **Desbloquear Ventana:** Desbloquea las ventanas seleccionadas si estas están bloqueadas.

Información del Sistema: Ventanas Visibles [127.0.0.1]

Handle	Título	Habilitada
724186	Información del Sistema: Vent...	SI
1182446	Servidor C-RAT	NO
1114656	Recortes	SI
722768	manualDeUsuario.hnd - Help...	SI
528070	HelpNDoc	SI
525690	Cliente.Servicio.exe - Acceso ...	SI
918980	Servidor - Microsoft Visual Stu...	SI
591832	Servidor	SI
524900	Skype™ - xkrossx2	SI
132094	crystal - Resultados de la bús...	SI
656196	Documentos	SI
263026	Debug	SI
329214	imagenes	SI
984446	7.Otra Documentacion	SI
462524	Windows 7 ServerCrat - VMw...	SI
65768	Program Manager	SI

Acciones

- Cambiar Título
- Minimizar
- Bloquear
- Desbloquear

Recorte de ventana

Consultar Info

Se recibieron 16 registros

Servicios

La acción '**Ver Servicios**' nos permite conocer los servicios del sistema cliente.

De cada proceso nos indica:

Ademas podemos realizar las siguientes acciones sobre los procesos:

- **Iniciar Servicio:** Inicia el servicio seleccionado en el sistema del cliente.
- **Parar Servicio:** Para el servicio seleccionado en el sistema del cliente.

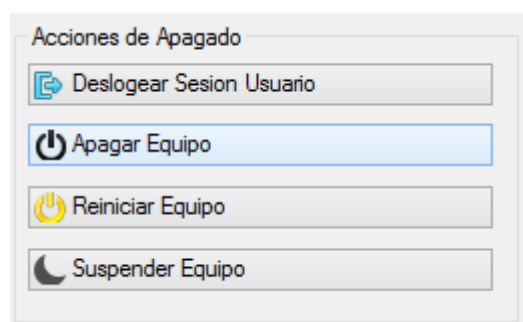
Acciones de Apagado

Las **acciones de apagado** nos ofrecen la posibilidad de realizar las siguientes opciones sobre el sistema cliente que tengamos seleccionado.

*Una vez usada alguna de estás opciones, perderemos la conexión con el equipo, ya que nuestro cliente dejará de ser accesible.

Las acciones de Apagado que nos ofrece C-RAT son:

- **Apagar Equipo.**
- **Reiniciar Equipo.**
- **Suspender Equipo.**
- **Cerrar sesión / Desloguear Usuario.**



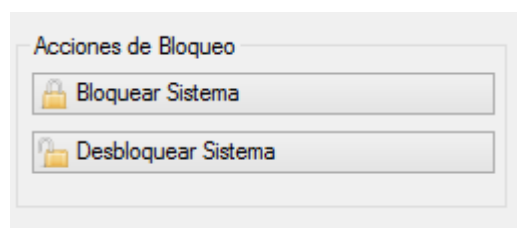
Acciones de Bloqueo

Las acciones de bloqueo, inhabilitan totalmente al usuario, dejándole bloqueada todo tipo de dispositivo de entrada al ordenador (principalmente teclado y Ratón).

Las acciones que tenemos disponibles son:

- **Bloquear sistema.**
- **Desbloquear sistema.**

Utilízalas con cuidado, ya que si bloqueas el equipo quedara totalmente "Congelado" hacia el exterior y tu serás la única persona que puedas desbloquearlo.

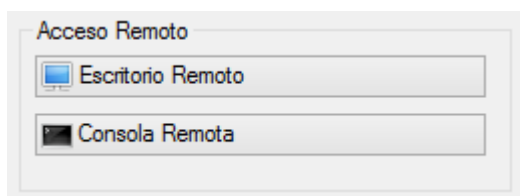


Acceso Remoto

Las acciones de **Acceso Remoto** son las acciones que nos permiten interactuar con el equipo, de forma similar a como si nos encontrásemos físicamente en él.

Existen dos tipos de acceso remoto en C-RAT:

- [Escritorio Remoto](#)
- [Consola Remota](#)



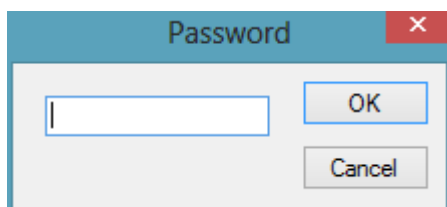
Escritorio Remoto

El acceso de **Escritorio Remoto** nos permite obtener el control del equipo como si nos encontrásemos físicamente en él, visualizando en nuestra ventana lo que veríamos si nos encontrásemos ante el monitor del equipo que controlamos.

Podemos elegir Habilitar/Deshabilitar dos opciones:

- **Modo Solo Lectura:** Habilita el modo Escritorio Remoto de forma que solo podemos ver lo que el otro usuario hace en su maquina, sin opción a manejarla. (Deshabilitado por defecto.)
- **Modo Escalable:** Nos permite escalar la pantalla al tamaño de nuestra ventana y evitar así tener que hacer scroll para ver la pantalla entera, perdiendo resolución. (Habilitado por defecto.)
-

El cliente solicitará contraseña en caso de estar protegido.

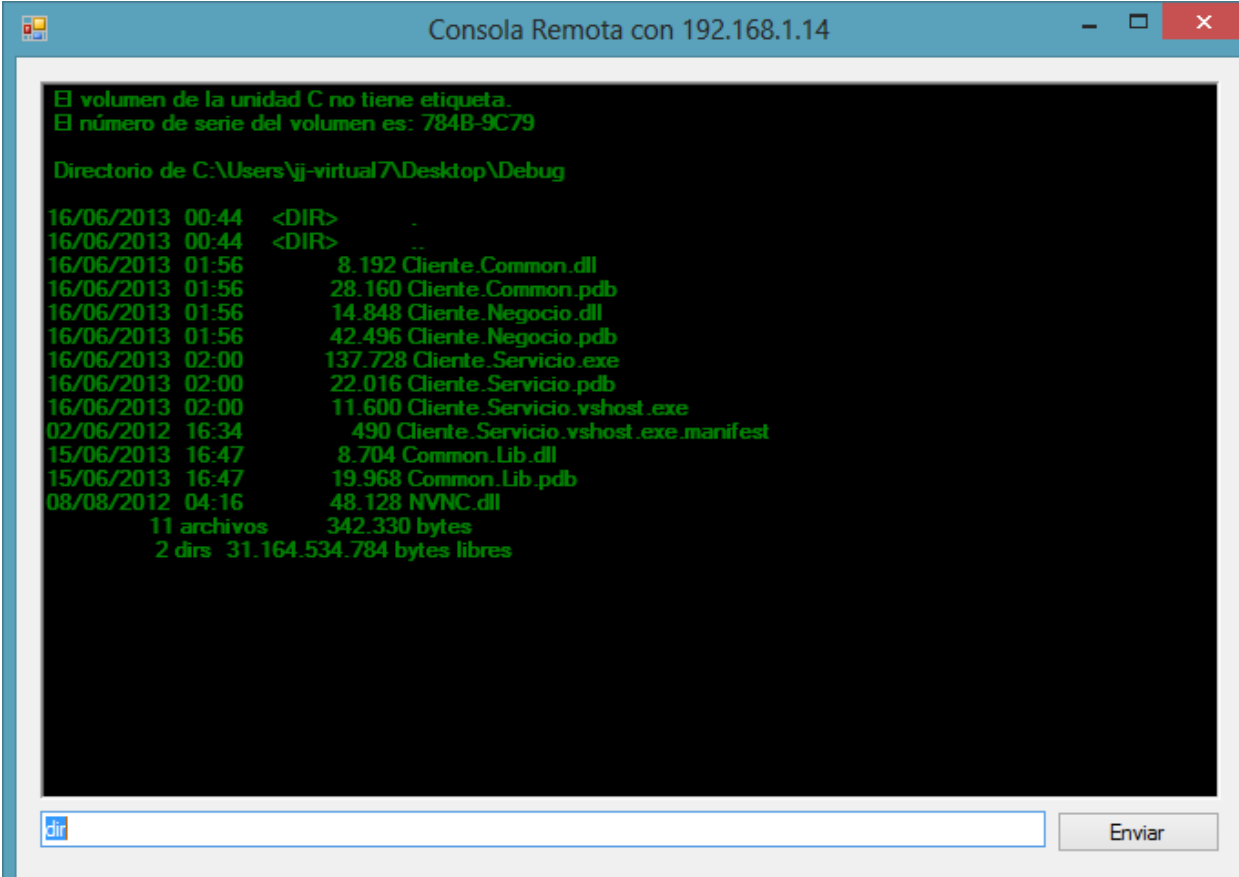


Si la contraseña especificada es la correcta, obtendremos acceso remoto en una nueva ventana al cliente solicitado.



Consola Remota

La **conexión de consola** remota nos permitirá la **ejecución de cualquier comando** que podamos ejecutar en una consola en local (cmd), pero de forma totalmente **remota** obteniendo la respuesta del cliente a nuestra acción.



```
Consola Remota con 192.168.1.14

El volumen de la unidad C no tiene etiqueta.
El número de serie del volumen es: 784B-9C79

Directorio de C:\Users\jj-virtual\A\Desktop\Debug

16/06/2013 00:44 <DIR>      .
16/06/2013 00:44 <DIR>      ..
16/06/2013 01:56          8.192 Cliente.Common.dll
16/06/2013 01:56        28.160 Cliente.Common.pdb
16/06/2013 01:56        14.848 Cliente.Negocio.dll
16/06/2013 01:56        42.496 Cliente.Negocio.pdb
16/06/2013 02:00       137.728 Cliente.Servicio.exe
16/06/2013 02:00        22.016 Cliente.Servicio.pdb
16/06/2013 02:00       11.600 Cliente.Servicio.vshost.exe
02/06/2012 16:34          490 Cliente.Servicio.vshost.exe.manifest
15/06/2013 16:47          8.704 Common.Lib.dll
15/06/2013 16:47        19.968 Common.Lib.pdb
08/08/2012 04:16        48.128 NVNC.dll
          11 archivos      342.330 bytes
          2 dirs 31.164.534.784 bytes libres

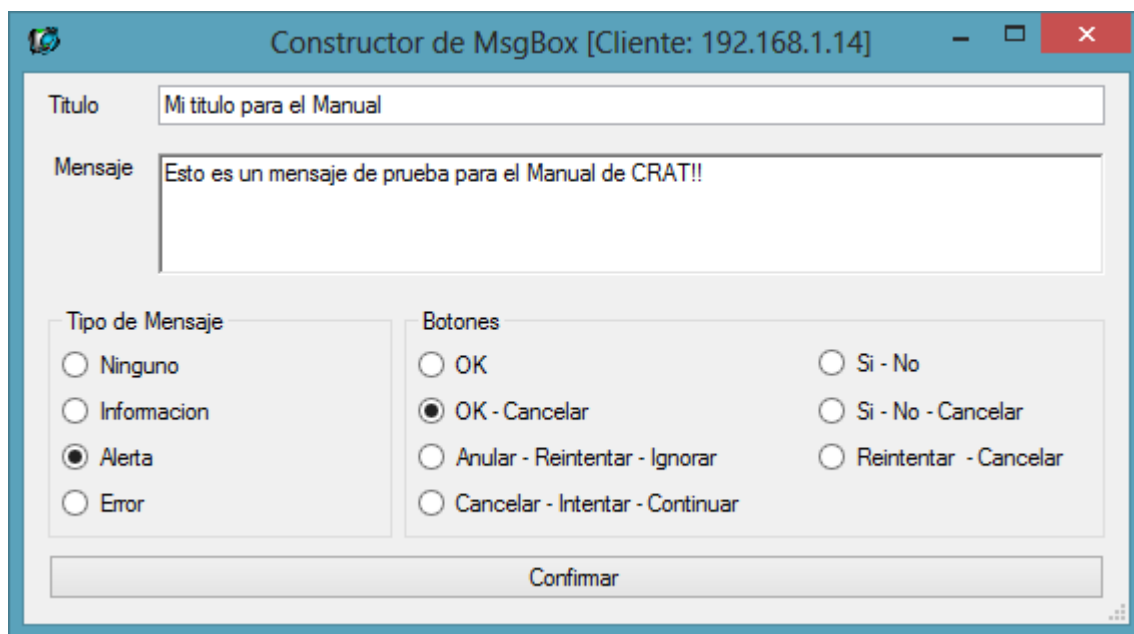
dir
Enviar
```

Envio

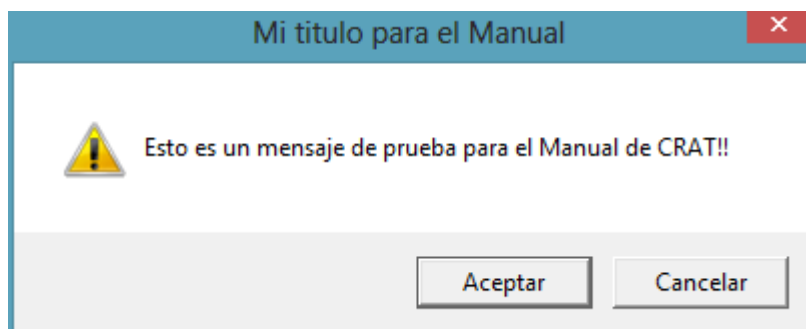
Message Box

El envío de **MessageBox**, es una funcionalidad que nos permite enviar mensajes de aviso de Windows al cliente.

Puedes elegir entre Diferentes tipos de Mensaje, con titulo y texto personalizado de forma muy simple mediante nuestra interfaz **MessageBox Builder**.



Al hacer click en confirmar, se le enviará al cliente que hallamos seleccionado, un mensaje del siguiente estilo. (En el caso de la imagen superior.)



Pagina Web

El envío de **Paginas Web**, es una funcionalidad que nos permite enviar al usuario directamente la web indicada.

El formato de la pagina web debe ser el correcto, por ejemplo ' <http://www.google.es> ', de lo contrario recibirá un error y será imposible enviarla.

Una vez enviada la pagina web, se abrirá en el equipo cliente al que se la enviamos en su **navegador predeterminado**.