



Manual sobre el funcionamiento de la aplicación de seguridad BufferZone para Windows Xp

Bufferzone puede mantener nuestro equipo protegido de acciones externas creando un entorno seguro de ejecución de aplicaciones vinculadas con Internet.

INTRODUCCION

BufferZone es un software creado por Trustware, que mantiene nuestro equipo a salvo de agresiones externas mediante la creación de un **entorno aislado** en el que operan los programas que requieren conexión a internet, protegiendo de esta forma los archivos de nuestro disco duro, además de ofrecernos otras opciones útiles para mantener la seguridad de nuestro PC.

Para descargar el software debemos visitar la página: www.trustware.com y pulsar sobre el botón que inicia la descarga, al hacerlo dispondremos de la versión completa de BufferZone de manera totalmente gratuita, ya que se trata de free-ware, cabe resaltar que la versión que descargamos y de la que vamos a hablar en este manual, es la versión completa del programa, que antes era de pago y ahora está a disposición de cualquier usuario que la quiera descargar gratuitamente.

Funciona sobre Windows XP (aun no se ha desarrollado una versión compatible con Windows 7), requiriendo como mínimo un Pentium 3 a 400 MHz y 128 Mb de RAM. La instalación es muy sencilla, solo hay que dejar los valores por defecto y aceptar el contrato de licencia

FUNCIONAMIENTO

Al utilizar BufferZone en nuestro equipo, todos los programas y archivos que entran en contacto con nuestro equipo a través de internet son re-dirigidos a una zona virtual creada por el programa en nuestro disco duro (C:/Virtual), donde dichos programas y archivos quedan aislados del resto de nuestro equipo mientras se ejecutan, para evitar que cualquier software malintencionado entre en contacto con nuestro sistema operativo y con los archivos guardados en nuestro equipo.

Cualquier modificación, archivo o sitio web sospechoso se ejecutara únicamente dentro de la zona virtual, facilitando de esta manera su posterior eliminación. Esto mantiene nuestro equipo limpio y a salvo, y permite navegar por internet, realizar descargas, o utilizar chats, con toda tranquilidad.

Cualquier virus o spyware que se ejecute dentro de la zona virtual, nunca podrá dañar, manipular, ni obtener información de carpetas privadas, ya que BufferZone protege las carpetas susceptibles de ser espiadas, como por ejemplo "Mis Documentos", estas carpetas se señalan con un candado encima del icono de la carpeta en cuestión. De esta forma nuestras carpetas privadas siempre estarán a salvo, ya que aunque un virus llegue a entrar en la zona virtual, no podrá entrar en contacto con las mismas.

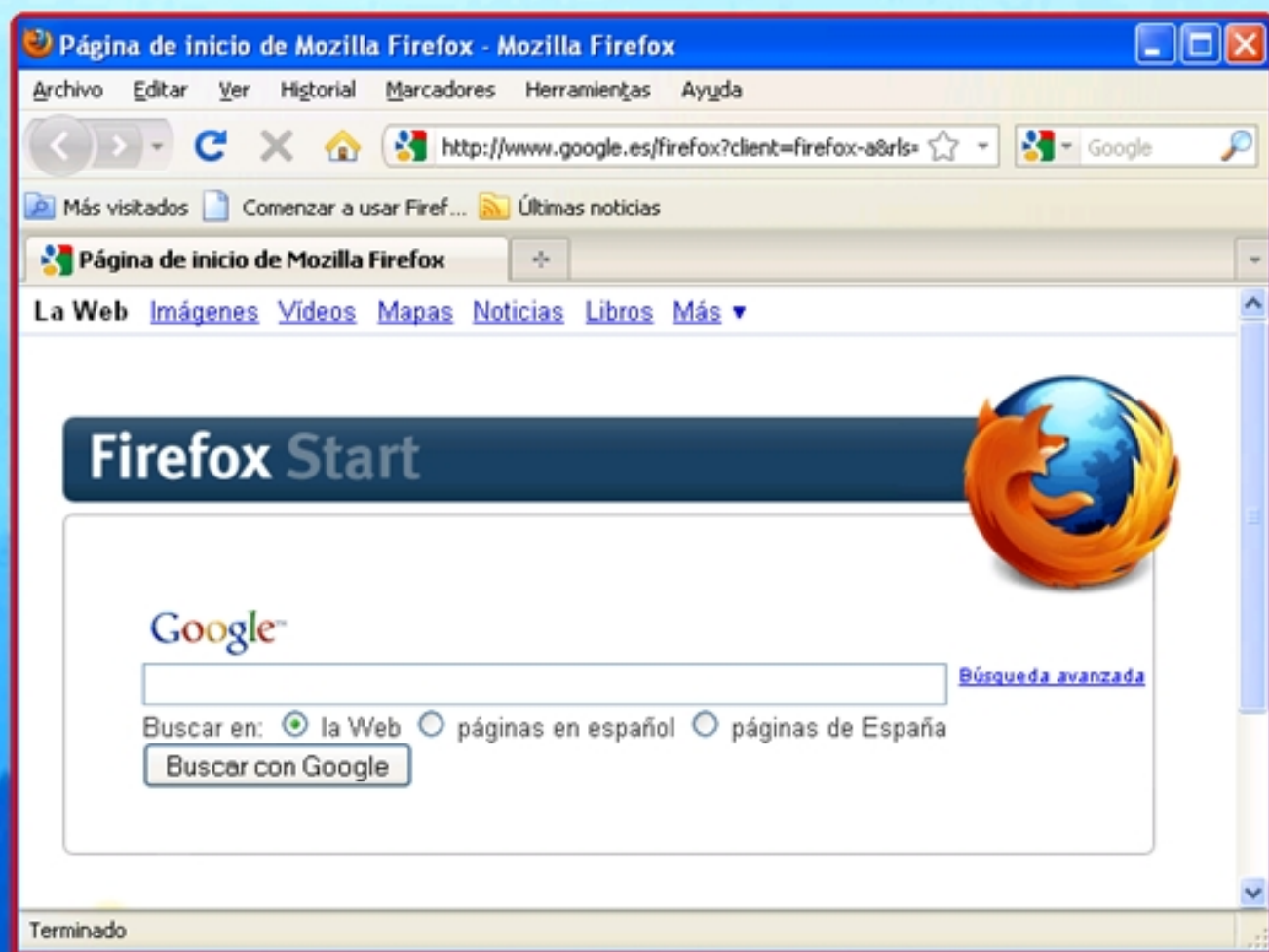
 Mis documentos



Manual Bufferzone

Escrito por Daniel Ortega Carrasco
Miércoles, 25 de Mayo de 2011 00:00

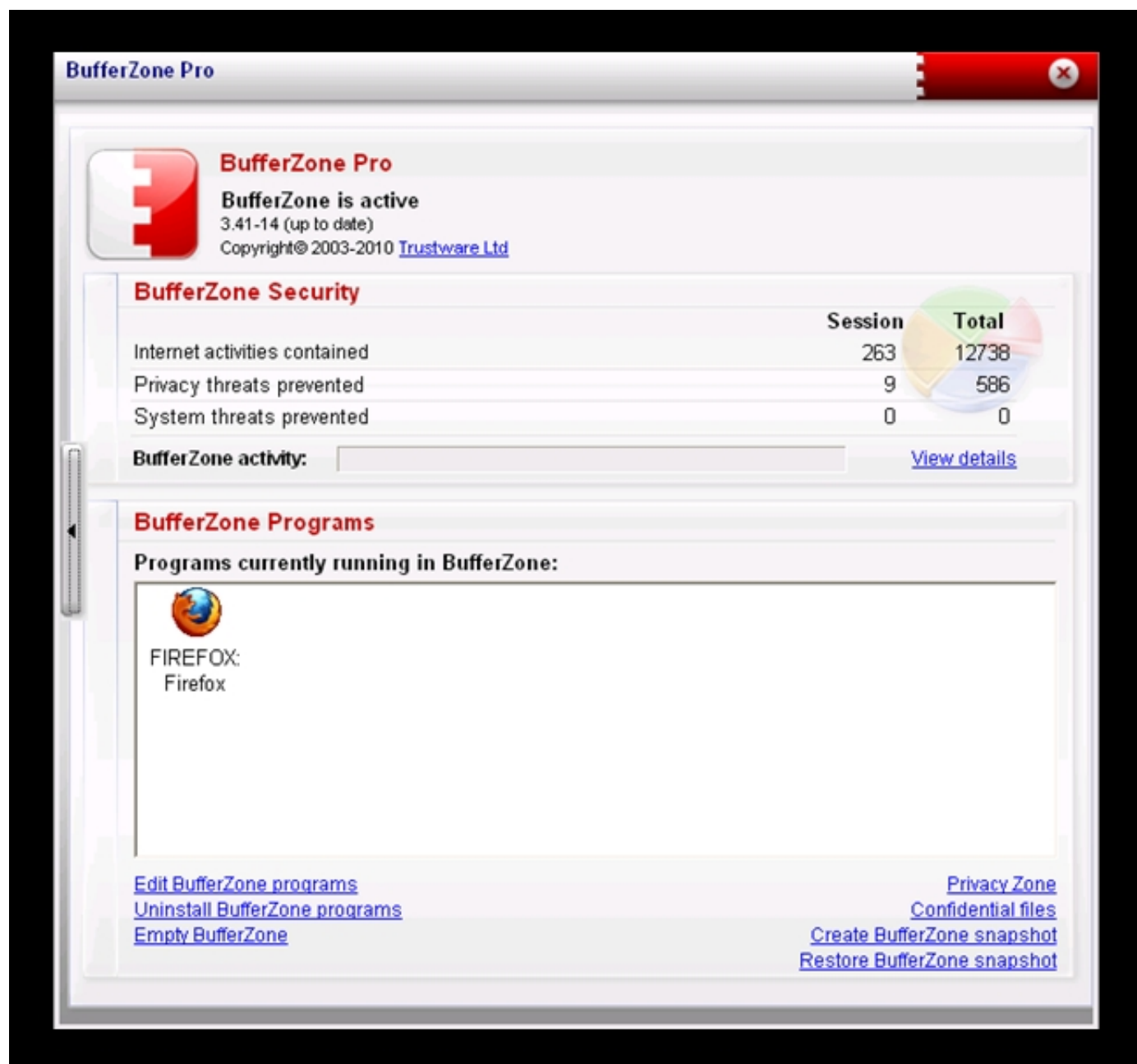
BufferZone mantiene la actividad en internet aislada en la zona virtual, esta zona queda representada sobre el icono de los programas protegidos por BufferZone, y por un borde rojo alrededor de la ventana del navegador, así sabremos en todo momento si estamos operando dentro de la zona segura, o no.



Esto incluye chats, descargas, archivos adjuntos de correo electrónico, operaciones con bancos, y compras online

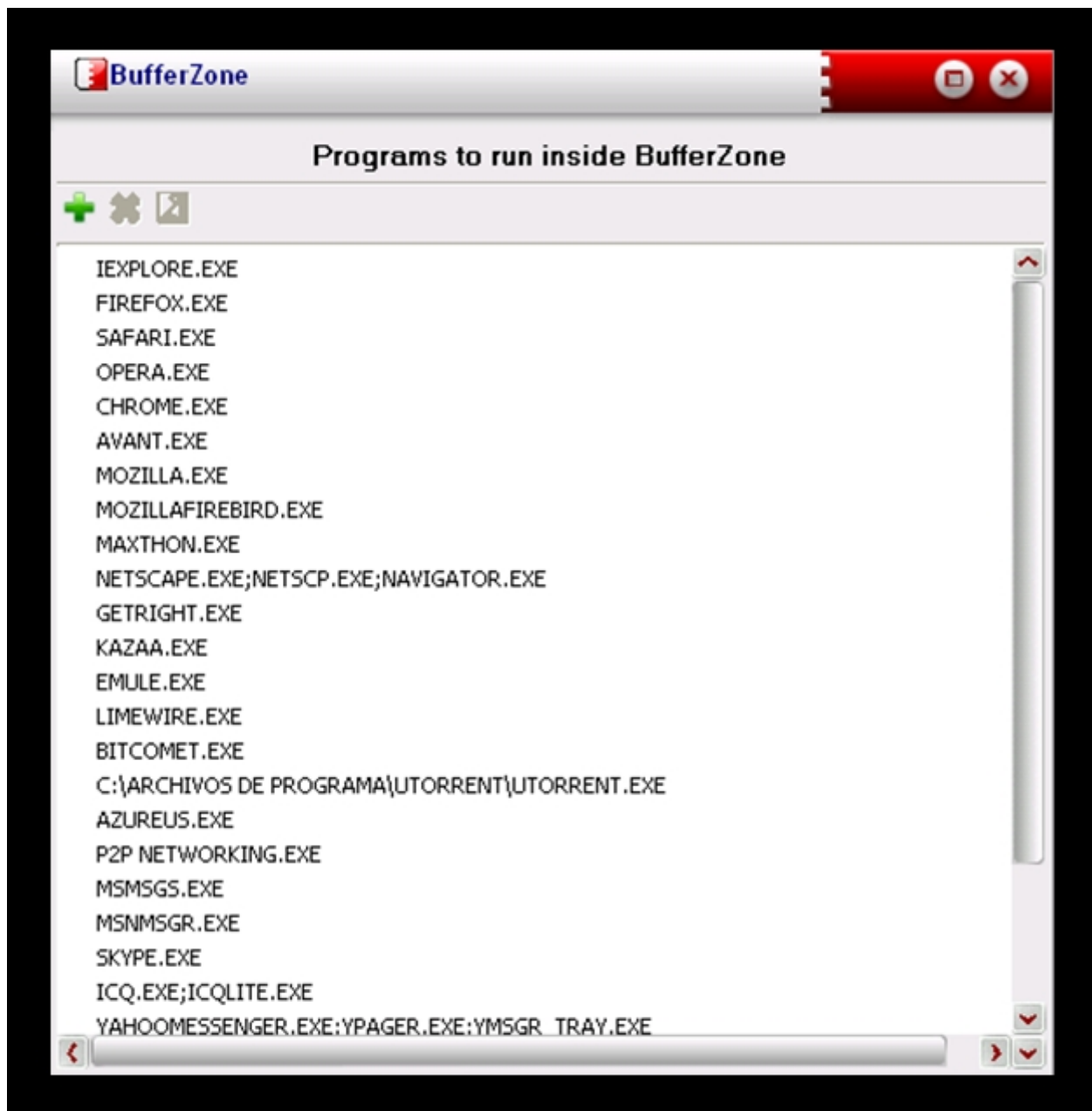
1. INICIO

A continuación se muestra la pantalla de inicio de BufferZone:

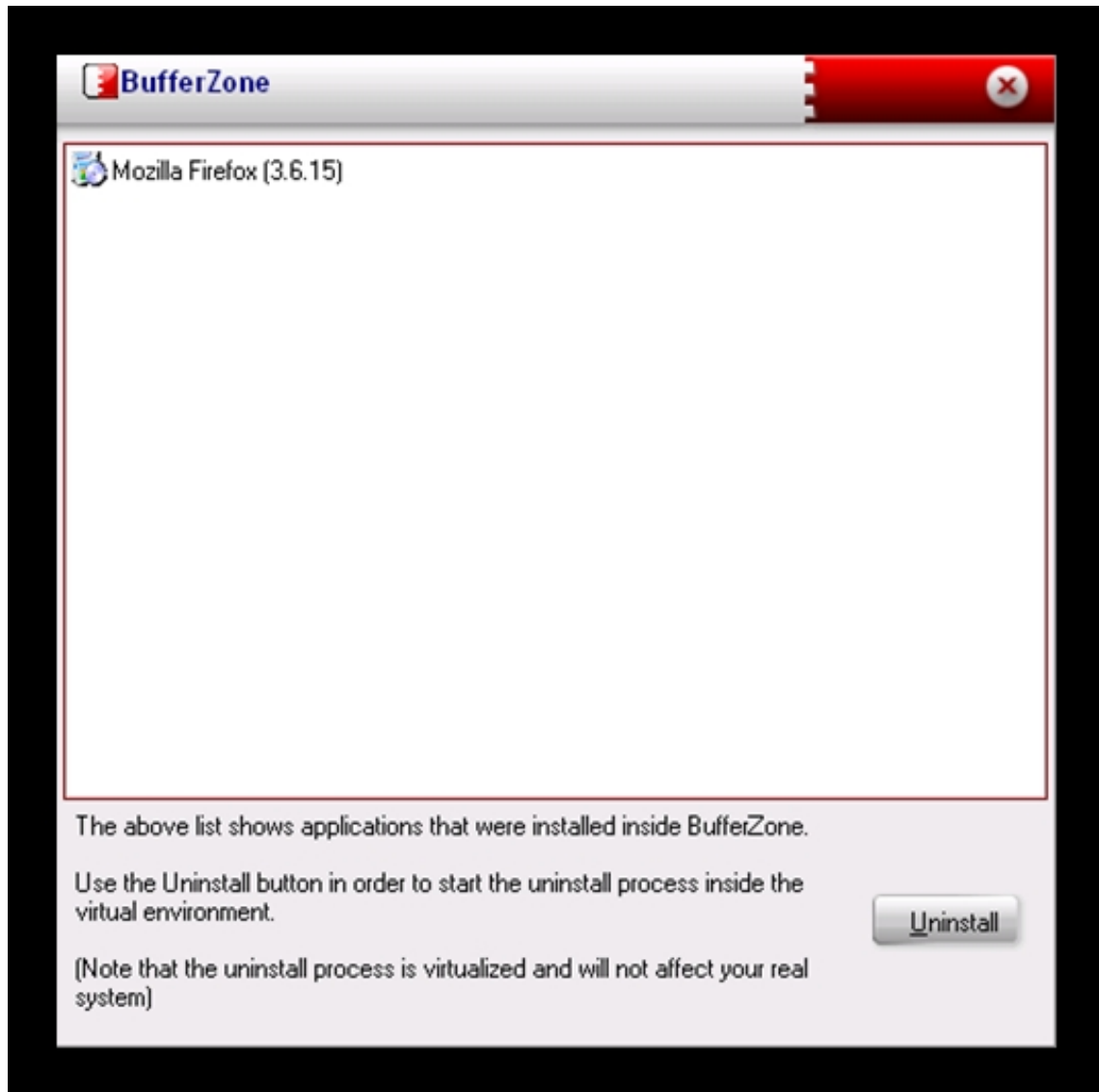


En ella aparece la versión del programa que estamos ejecutando, si esta actualizada o no, el nivel de actividad de la aplicación, los programas que se están ejecutando bajo su protección, y una serie de opciones a modo de hipervínculos:

- Edit BufferZone programs: Edita la lista de programas protegidos por BufferZone. Aquí podremos añadir programas de los que nos queramos proteger, o por el contrario quitar de la lista programa que sepamos que son seguros y no necesiten protección.

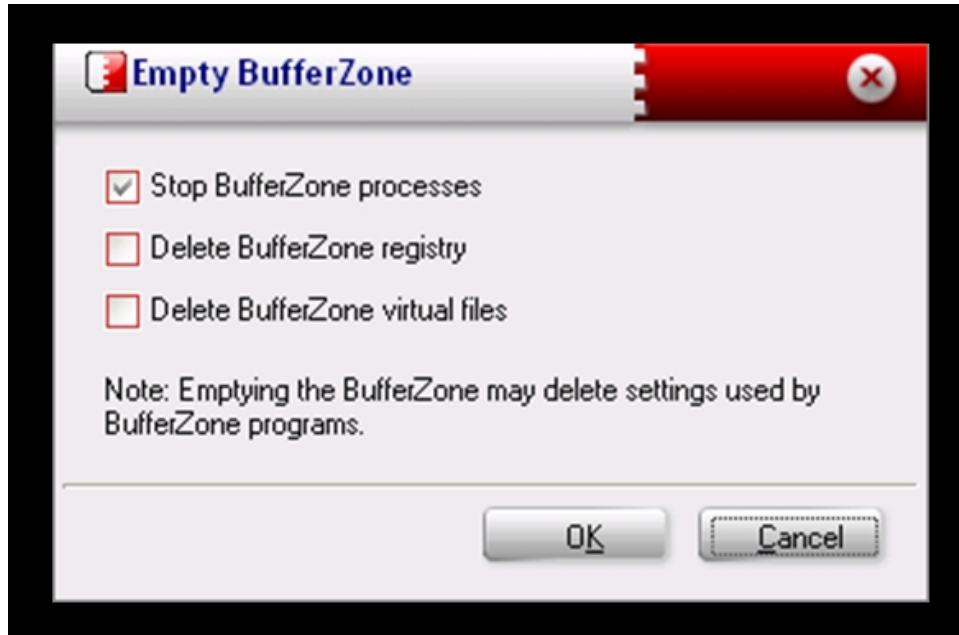


- **Uninstall BufferZone programs:** Sirve para desinstalar aplicaciones instaladas dentro de la zona virtual, sin afectar al funcionamiento del equipo, si una aplicación está instalada fuera de la zona virtual no se desinstalará.



- **Empty BufferZone:** Esta opción elimina la información instalada o copiada en la zona virtual, y consta de las siguientes opciones:
 - **Stop BufferZone processes:** Detiene todos los procesos que se estén ejecutando en la zona virtual, sin borrar nada.
 - **Delete BufferZone registry:** Elimina todo el registro virtual creado dentro de BufferZone.

- Delete BufferZone virtual files: Borra todo el contenido de la carpeta virtual. Cualquier contenido descargado o movido a la carpeta virtual será borrado, así que conviene asegurarse antes de utilizar esta opción.



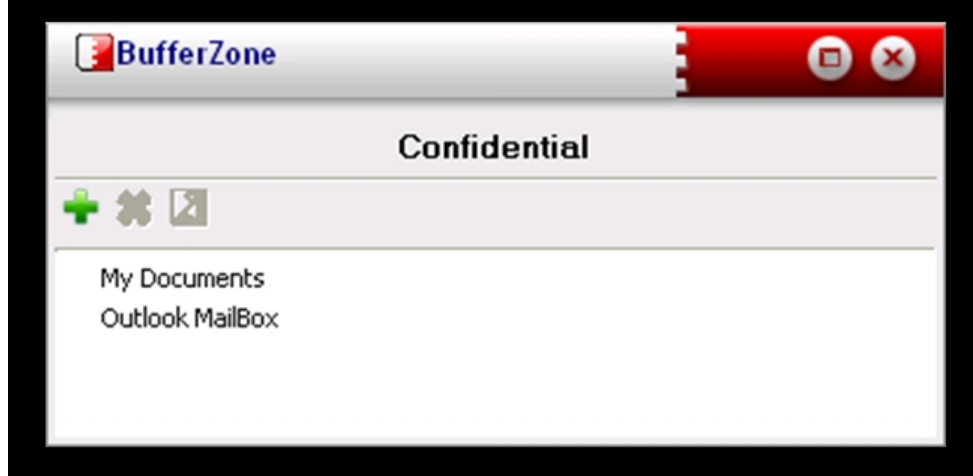
- Privacy Zone: Esta opción nos permite añadir sitios web que consideremos seguros y que se ejecutaran fuera de la zona de seguridad.

Manual BufferZone

Escrito por Daniel Ortega Carrasco
Miércoles, 25 de Mayo de 2011 00:00



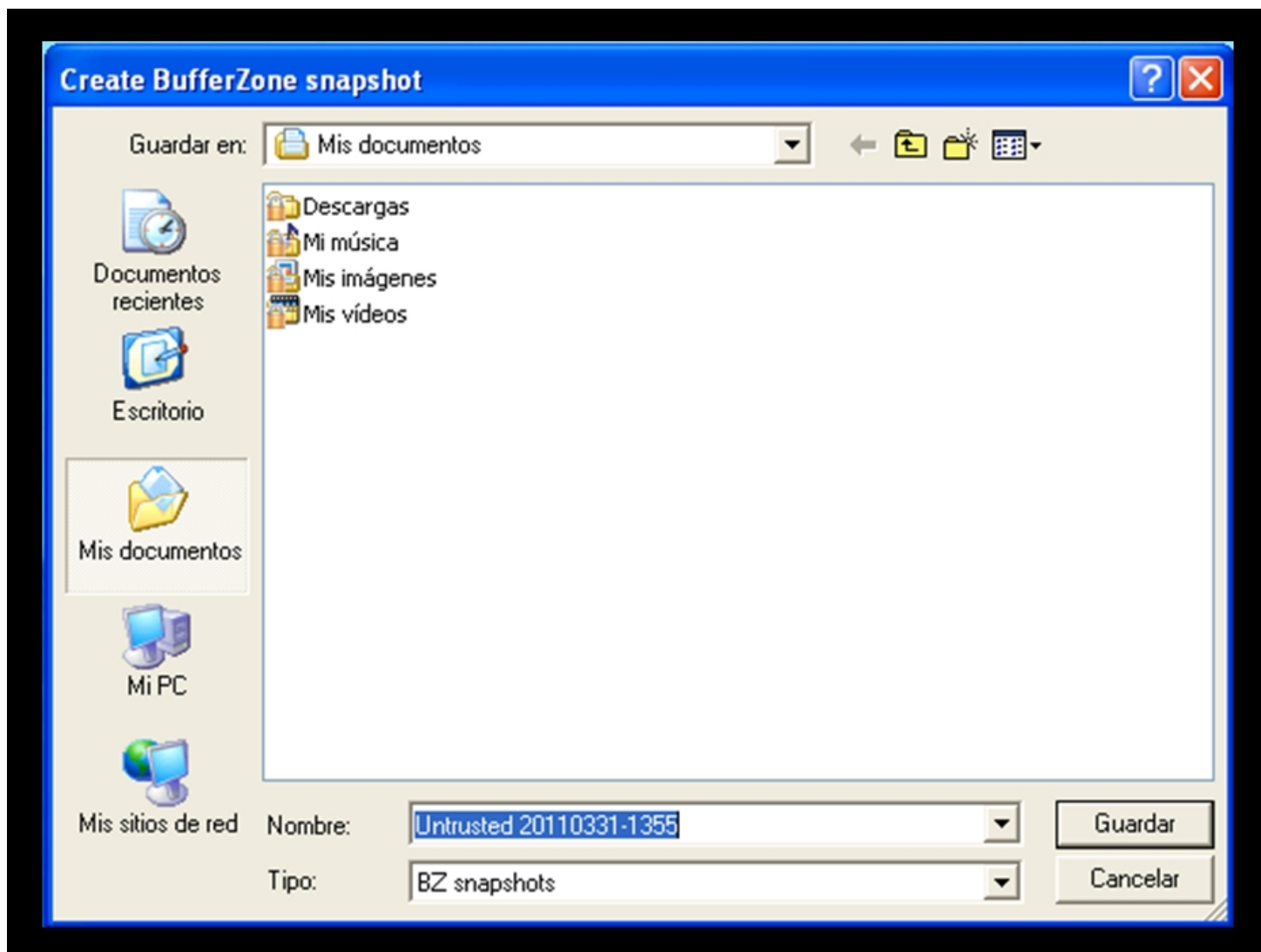
Multiplataforma



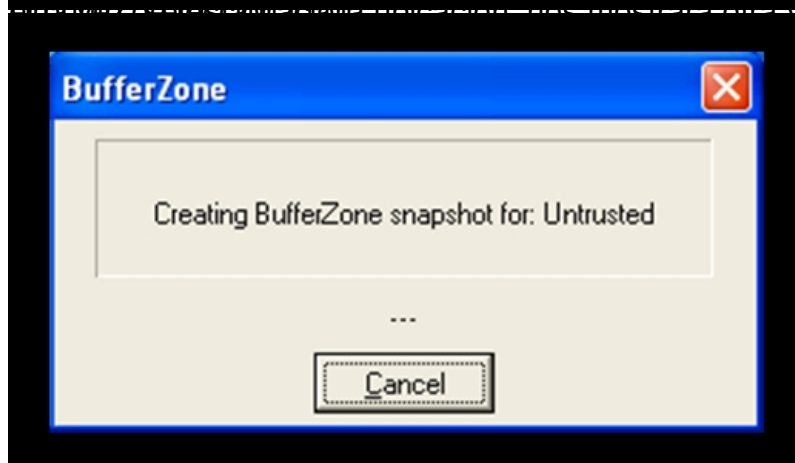
personal (e-mail, calendar, etc.) and confidential data, such as e-mail, calendar, etc.

Manual Bufferzone

Escrito por Daniel Ortega Carrasco
Miércoles, 25 de Mayo de 2011 00:00



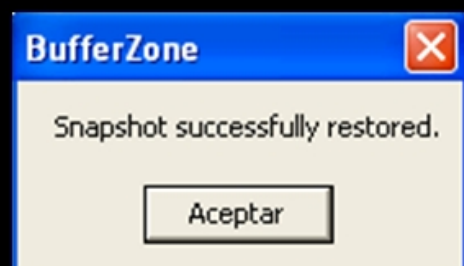
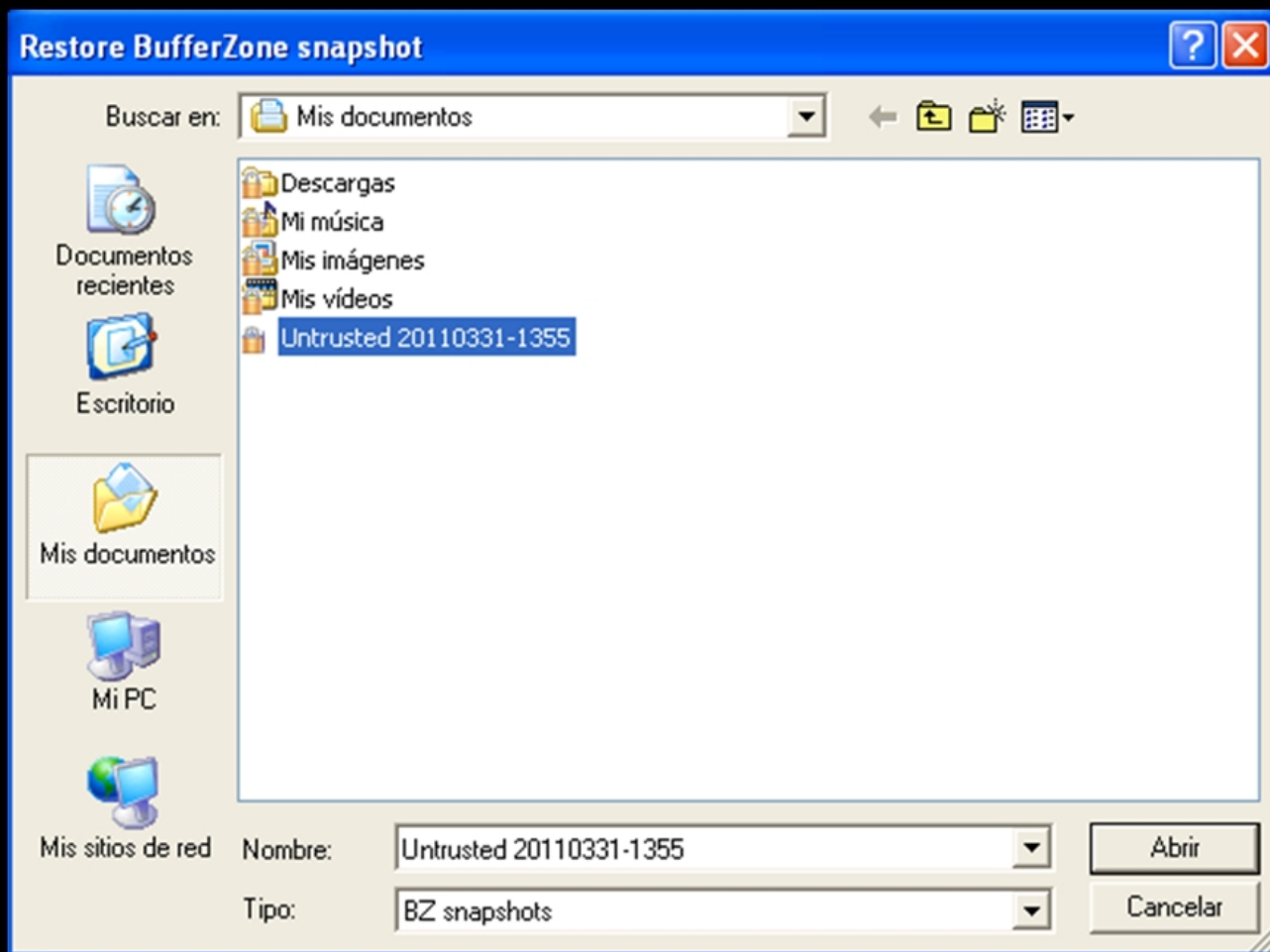
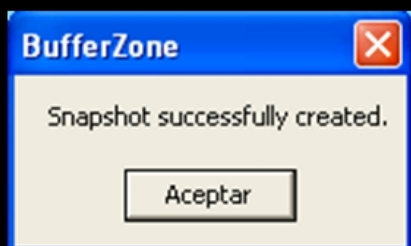
La siguiente ventana que indica que se está creando



La siguiente ventana indica que el punto de restauración se ha creado con éxito:

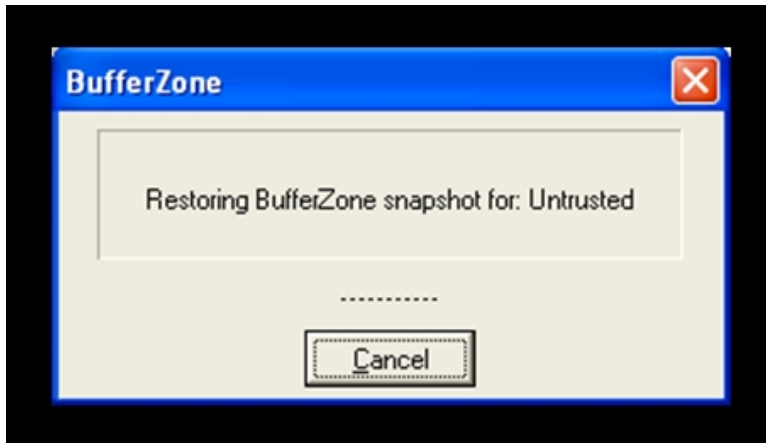
Manual Bufferzone

Escrito por Daniel Ortega Carrasco
Miércoles, 25 de Mayo de 2011 00:00

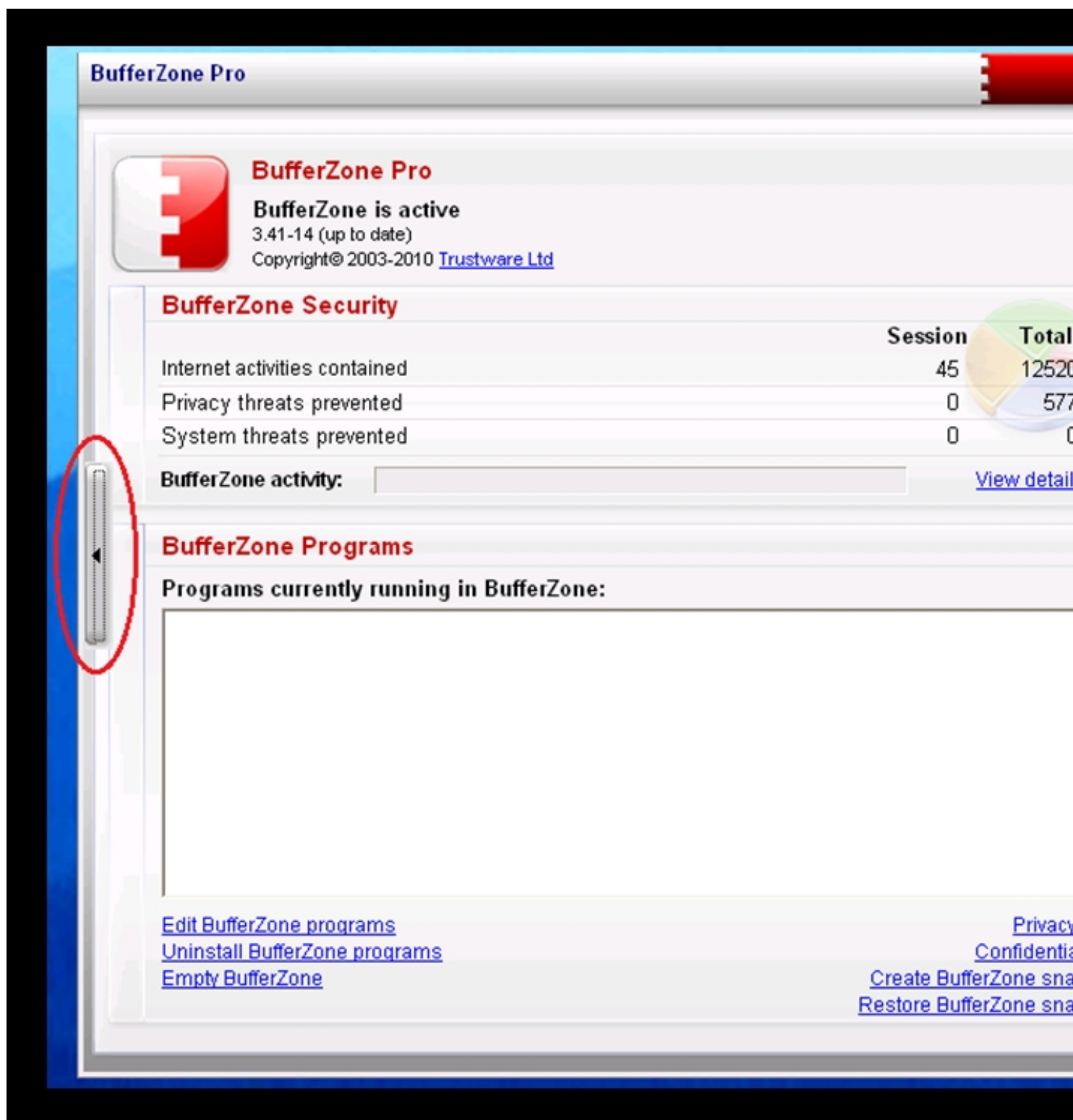


Manual Bufferzone

Escrito por Daniel Ortega Carrasco
Miércoles, 25 de Mayo de 2011 00:00



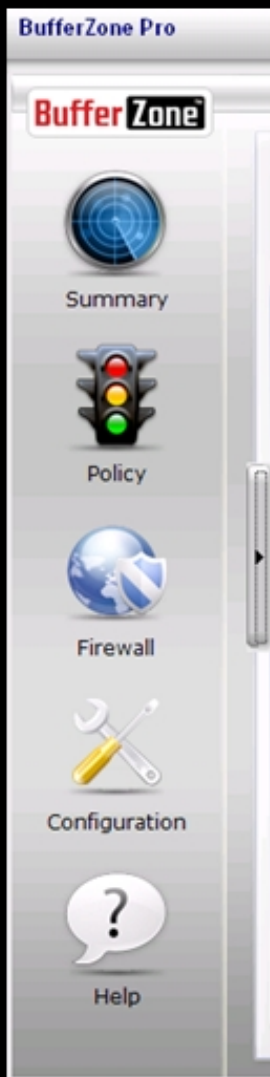
que al aso pedimos que podemos de avance, para aceptar de los de los debemos pulsar la pestaña



Al activarla aparecen las siguientes opciones.

Manual Bufferzone

Escrito por Daniel Ortega Carrasco
Miércoles, 25 de Mayo de 2011 00:00



Installers and Updates Inside BufferZone

Files downloaded from the Internet or residing inside BufferZone

Maximum



No protection



Maximum Protection

All programs will automatically be installed inside BufferZone
BufferZone will not prompt for confirmation

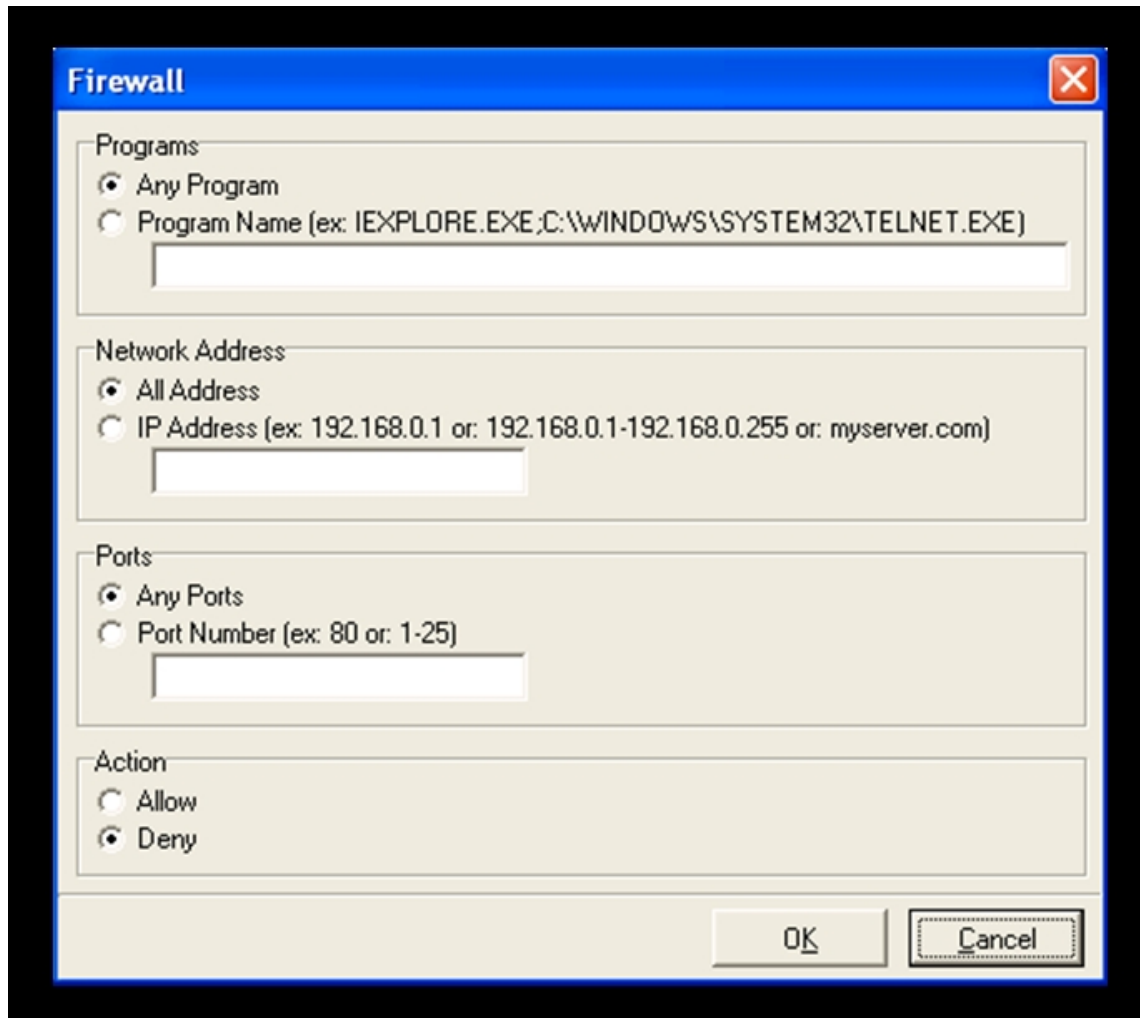


Recommended only when most strict protection is required

de BufferZone Pro, los programas que se instalan dentro de BufferZone se ejecutaran dentro de BufferZone y no en el sistema operativo. Esto significa que los programas que se instalan dentro de BufferZone no podran acceder a los recursos del sistema operativo, como el disco duro, la memoria RAM, etc. Esto es lo que se llama "proteccion en zona".

2. FIREWALL

Controla el tráfico de la red dentro de BufferZone. Las normas del Firewall se configuran únicamente para las aplicaciones que se ejecutan dentro de BufferZone.



Se puede establecer el firewall para cualquier programa (Any program) o para algún programa en concreto escribiendo el nombre del programa y su extensión en la caja de texto. También se puede establecer de la misma manera para cualquier dirección IP o para alguna en

concreto, para cualquier puerto o para un puerto determinado. Y por último se establece que queremos que haga, denegar el acceso o permitirlo.

3. CONFIGURACION

En este apartado podremos modificar opciones que afectan a partes muy diversas del programa como contraseñas, interfaz de usuario... Al pulsar sobre **configuration**, aparece la siguiente ventana con la pestaña

settings

marcada:

Manual Bufferzone

Escrito por Daniel Ortega Carrasco
Miércoles, 25 de Mayo de 2011 00:00

Settings Misc Advanced Policy

Password

☐ Administrator's password:

Confirm password:

☒ Memorize password for (seconds): default: "admin"

☐ Basic maintenance password:

BufferZone

☒ Draw a red border around BufferZone programs (reboot required)

☒ Notify me about new versions

☒ Show me protection pop-up messages

Virtual repository drive (reboot required): ▼

When a trusted program opens an unknown script/macro: ▼

Advanced

[Forbidden Programs](#) Prevent opening and execution of certain files

[Advanced Rules](#) Define BufferZone exceptions

[Event Log](#) Displays events recorded by BufferZone

BufferZone

☒ Draw a red border around BufferZone programs (reboot required)

☒ Notify me about new versions

☒ Show me protection pop-up messages

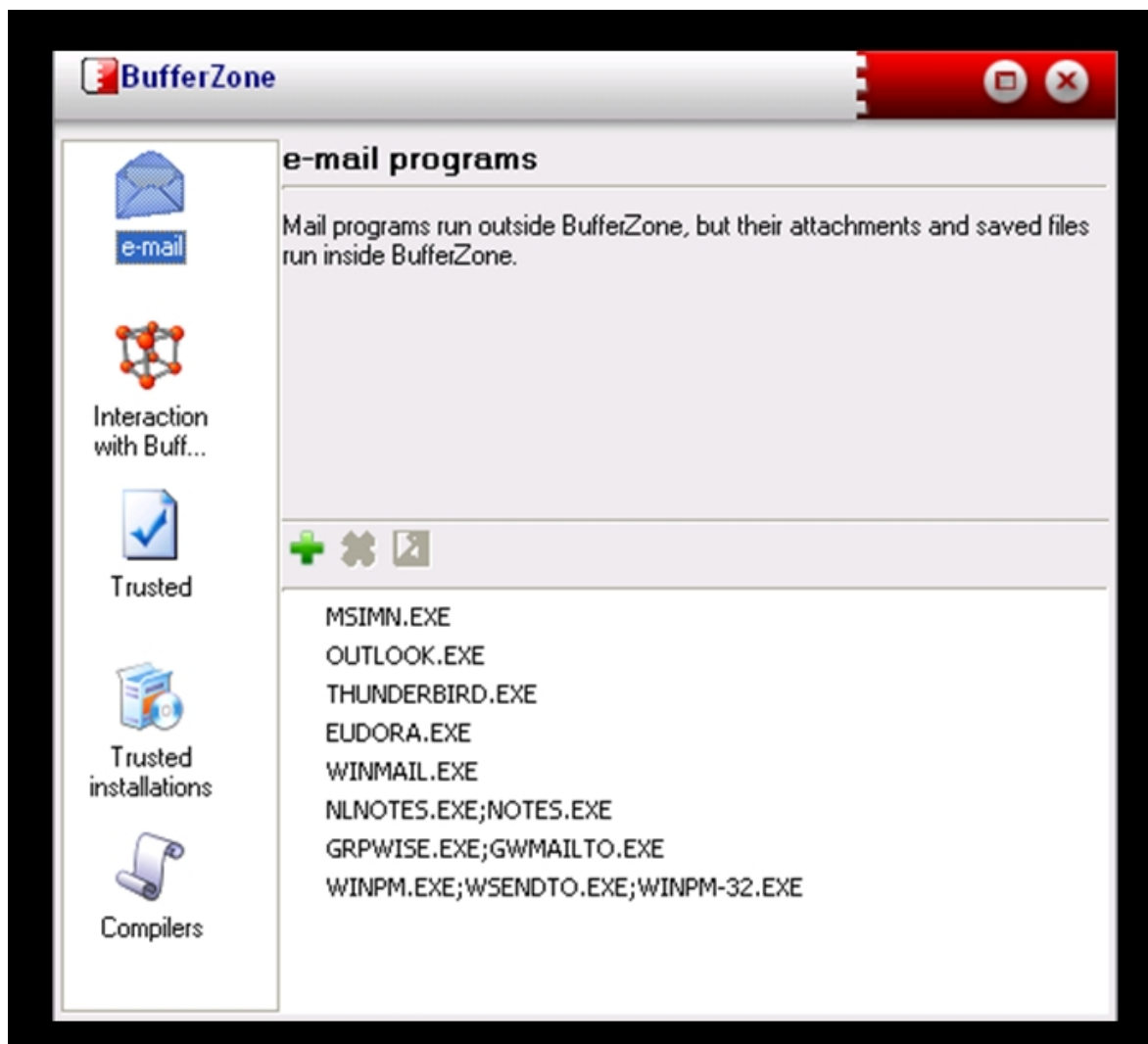
Virtual repository drive (reboot required): ▼

When a trusted program opens an unknown script/macro: ▼

Advanced

[Forbidden Programs](#) Prevent opening and execution of certain files

Prompt user
Open inside BufferZone
Deny opening
Allow



BufferZone is a security application that runs in the background and monitors the system for suspicious activity. It can be configured to block or allow specific programs and files. The BufferZone interface is shown in the screenshot above.

Settings Misc **Advanced Policy**

BufferZone Maintenance

☐ Automatically empty BufferZone

☒ Once every 30 days

☐ Once every (week days) Sunday

☐ Every first Sunday of the month

Hour: 1:00

☒ Delete BufferZone registry

☐ Delete BufferZone virtual files

Application Control

 Application Control is a strict policy mode which tracks all new executable files and scripts created on your hard disk, and ensures they run inside BufferZone.

☐ Activate Application Control (reboot required)

When an Unknown program is executed: Run inside BufferZone

Close Apply

BufferZone Maintenance

☒ Automatically empty BufferZone

☒ Once every 30 days

☐ Once every (week days) Sunday

☐ Every first Sunday of the month

Hour: 1:00

☒ Delete BufferZone registry

☐ Delete BufferZone virtual files

Manual Bufferzone

Escrito por Daniel Ortega Carrasco
Miércoles, 25 de Mayo de 2011 00:00

Application Control



Application Control is a strict policy mode which tracks all new executable files and scripts created on your hard disk, and ensures they run inside BufferZone.

☒ Activate Application Control (reboot required)

When an Unknown program is executed:

[Unknown programs](#)

Run inside BufferZone

Run inside BufferZone

Prompt user

Deny execution

Open outside BufferZone

Installers and Updates Inside BufferZone



Files downloaded from the Internet or residing inside BufferZone

Installer Authenticode signature	Action
Signed Installer	Prompt
Unsigned Installer	Prompt In BufferZone Outside BufferZone

Prohibe BufferZone por defecto que se haga con el archivo que se ejecute.

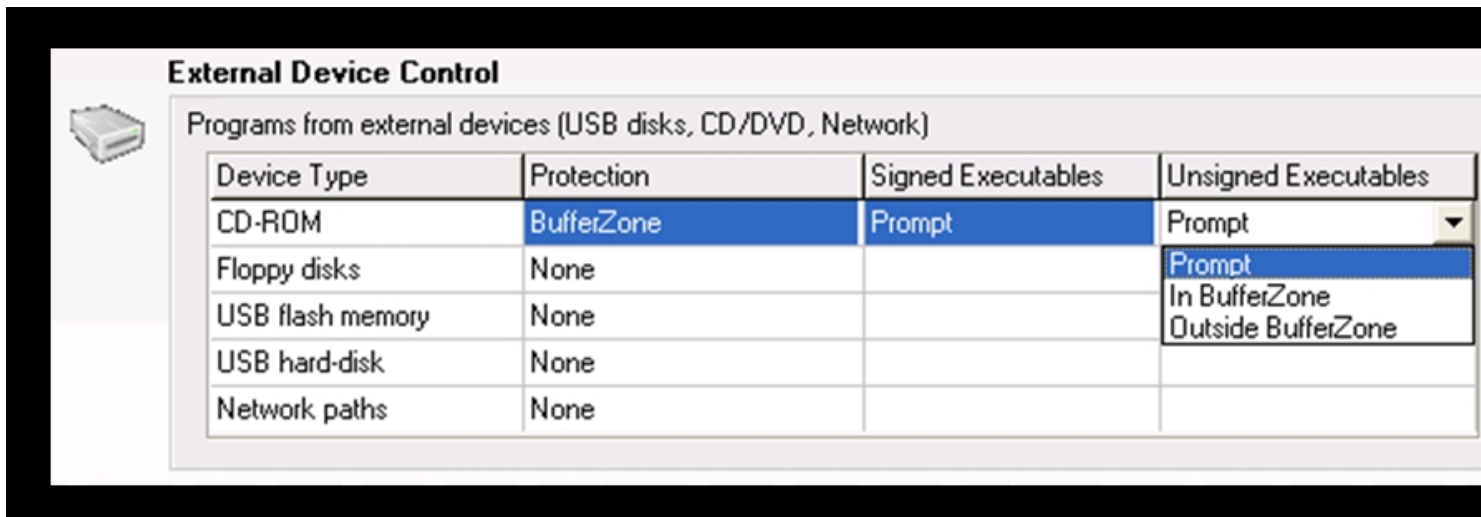
External Device Control



Programs from external devices (USB disks, CD/DVD, Network)

Device Type	Protection	Signed Executables	Unsigned Executables
CD-ROM	None		
Floppy disks	None		
USB flash memory	BufferZone		
USB hard-disk	Forbidden		
Network paths	Confidential		

selecciona una directiva de seguridad al medio de almacenamiento que se va a utilizar para ejecutar programas.



selección **Prompt**: Preguntará que hacer con el archivo que se ejecute desde el medio externo. Ejecutará el archivo en nuestro equipo fuera de la zona segura.
- **Outside BufferZone**: Ejecutará el archivo en nuestro equipo fuera de la zona segura.
- **Forbidden**: Prohibe la ejecución de cualquier archivo contenido en un medio externo.
- **In BufferZone**: Ejecutará el archivo en la zona segura de BufferZone. Para ejecutarlo, el usuario deberá estar en la zona segura de BufferZone.
- **Outside BufferZone**: Ejecutará el archivo en nuestro equipo fuera de la zona segura.
Enlaces de interés:

- <http://www.trustware.com> - Pagina web oficial del equipo desarrollador de BufferZone
- <http://www.trustware.com/support.php> - Pagina donde se da soporte técnico en todo lo referente al funcionamiento de la aplicación mediante los foros de la comunidad de usuarios de Bufferzone.
- [Tutorial](#) - Pequeño tutorial con diapositivas a modo de Powerpoint, de las opciones más básicas del programa.