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

Bufferzone puede mantener nuestro equipo protegido de acciones externas creando un entrono seguro de ejecución de aplicaciones vinvuladas 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

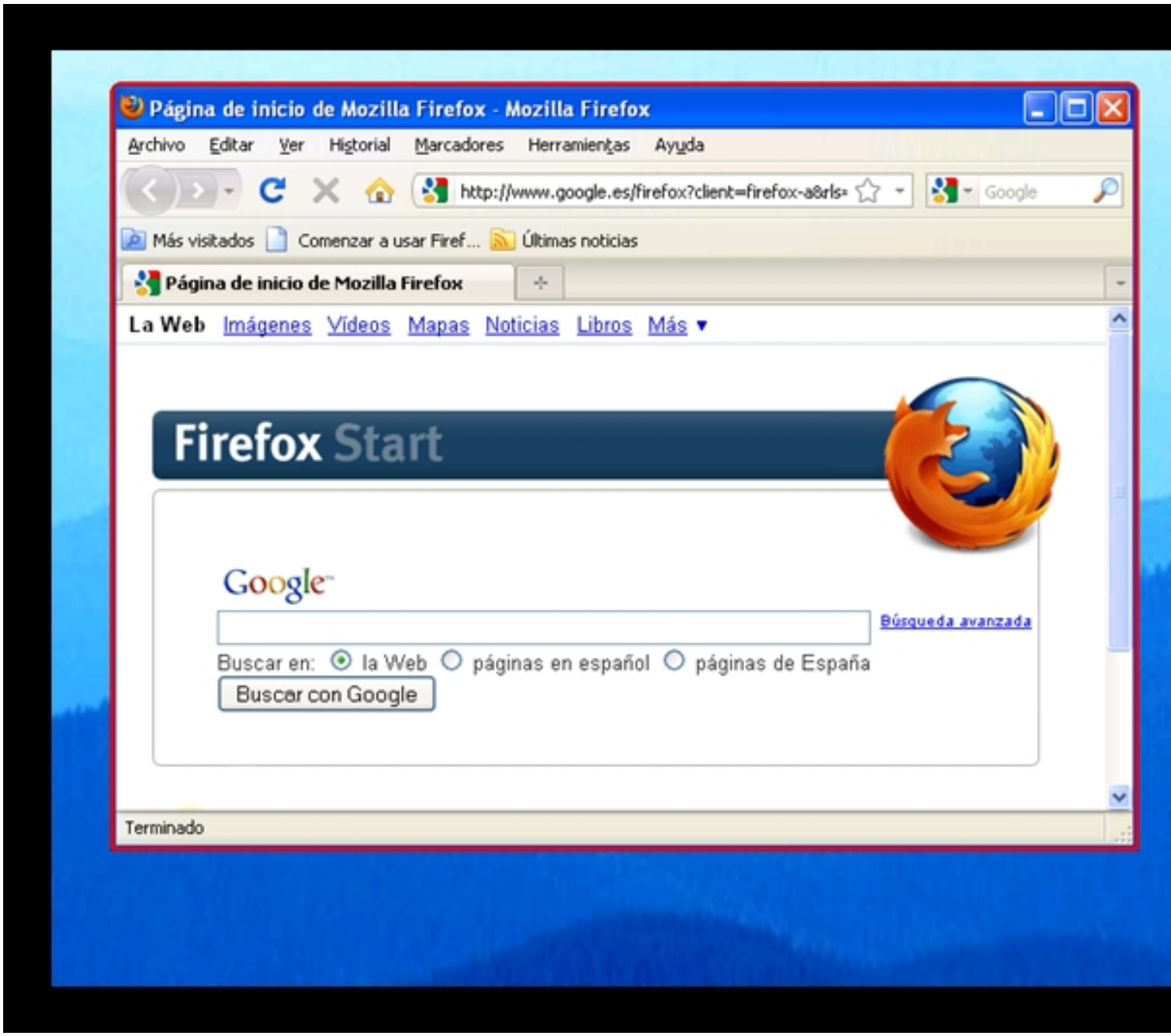
FUNCIONAMIENTO

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.

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.



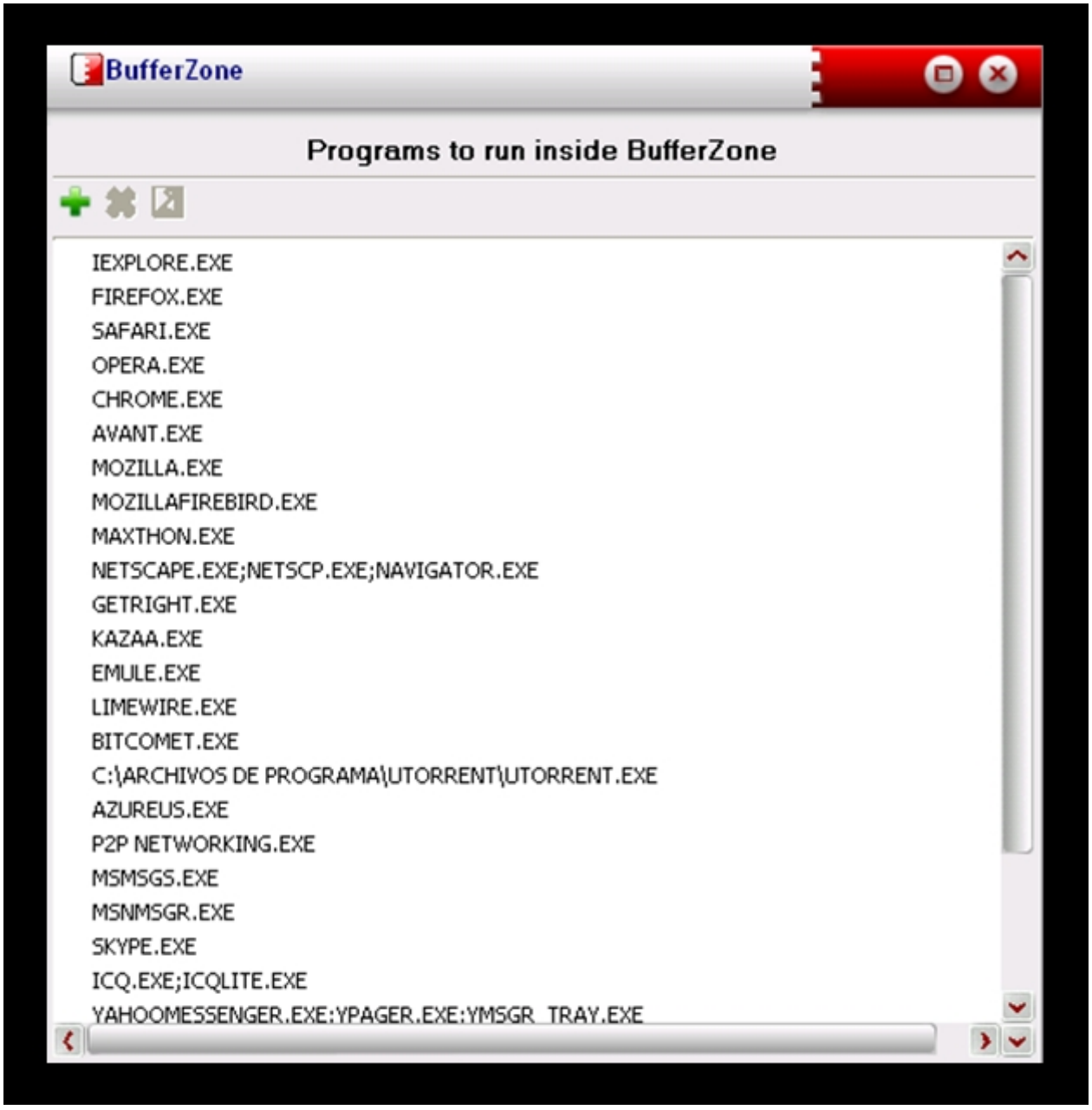
Esto incluye chats, descargas, archivos adjuntos de correo electrónico, operaciones con bancos, y compras online

1. INICIO

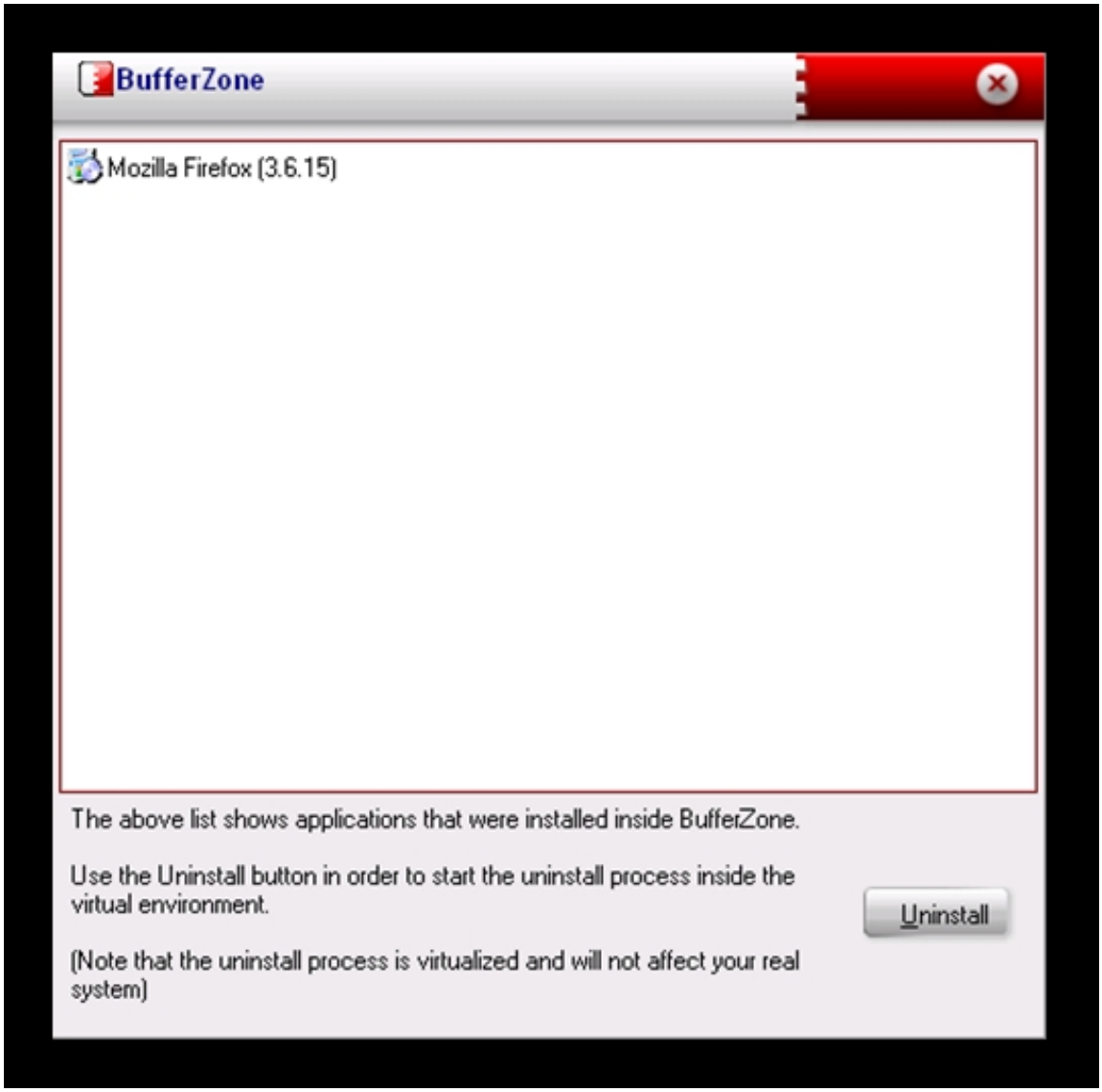
A continuación se muestra la pantalla de inicio de BufferZone:

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.



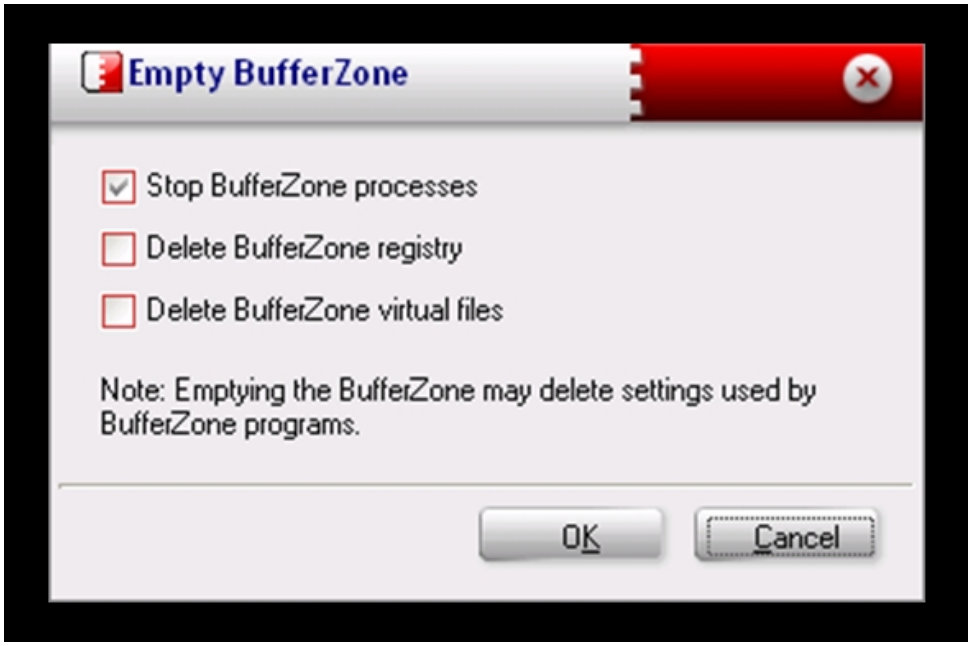
- Uninstall BufferZone programs: Sirve para desinstalar aplicaciones instaladas dentro de la zona virtual, sin afectar al funcionamiento del equipo, si una aplicación está instalada fuera de la zona virtual no se desinstalará.



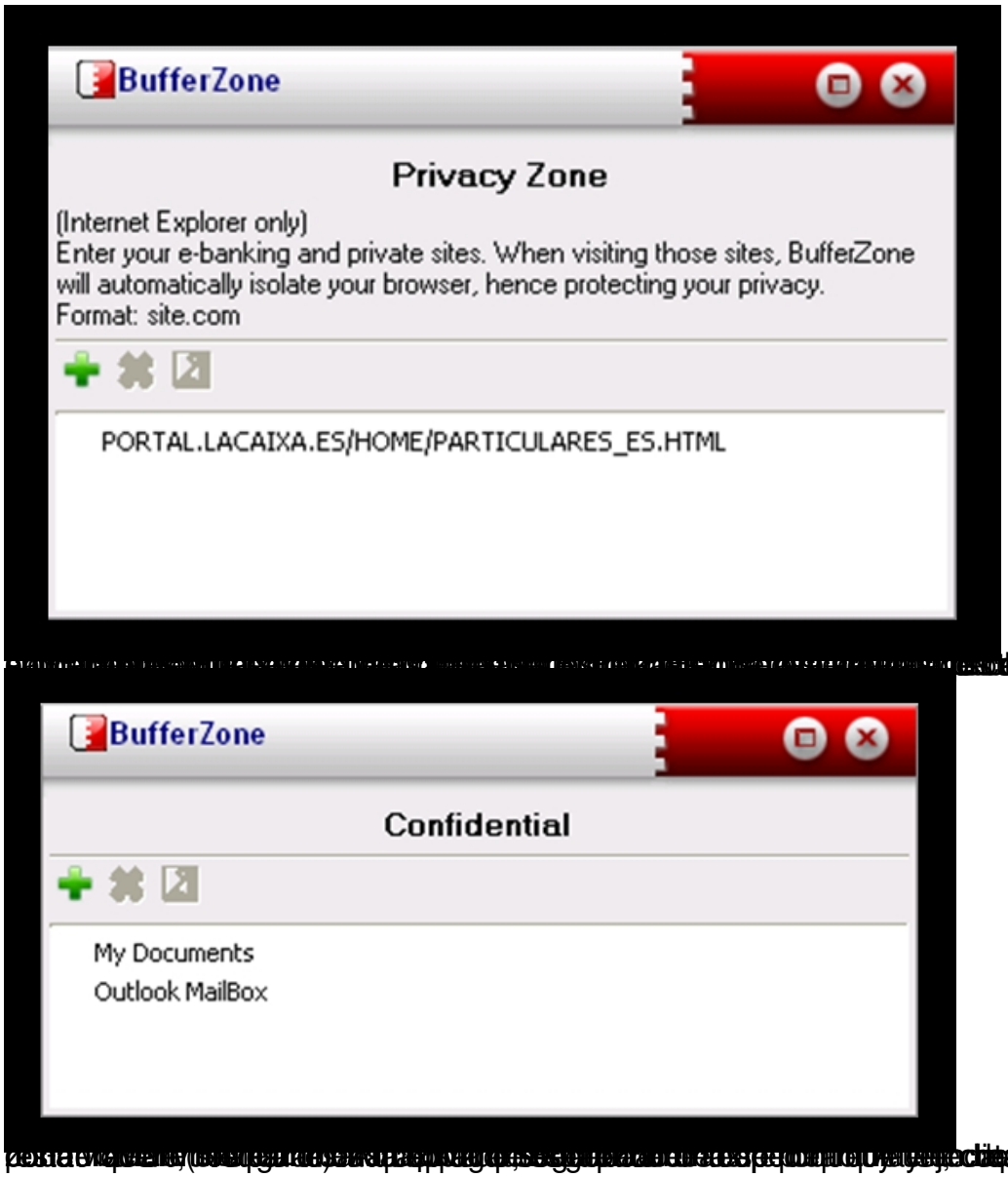
- Empty BufferZone: Esta opción elimina la información instalada o copiada en la zona virtual, y consta de las siguientes opciones:

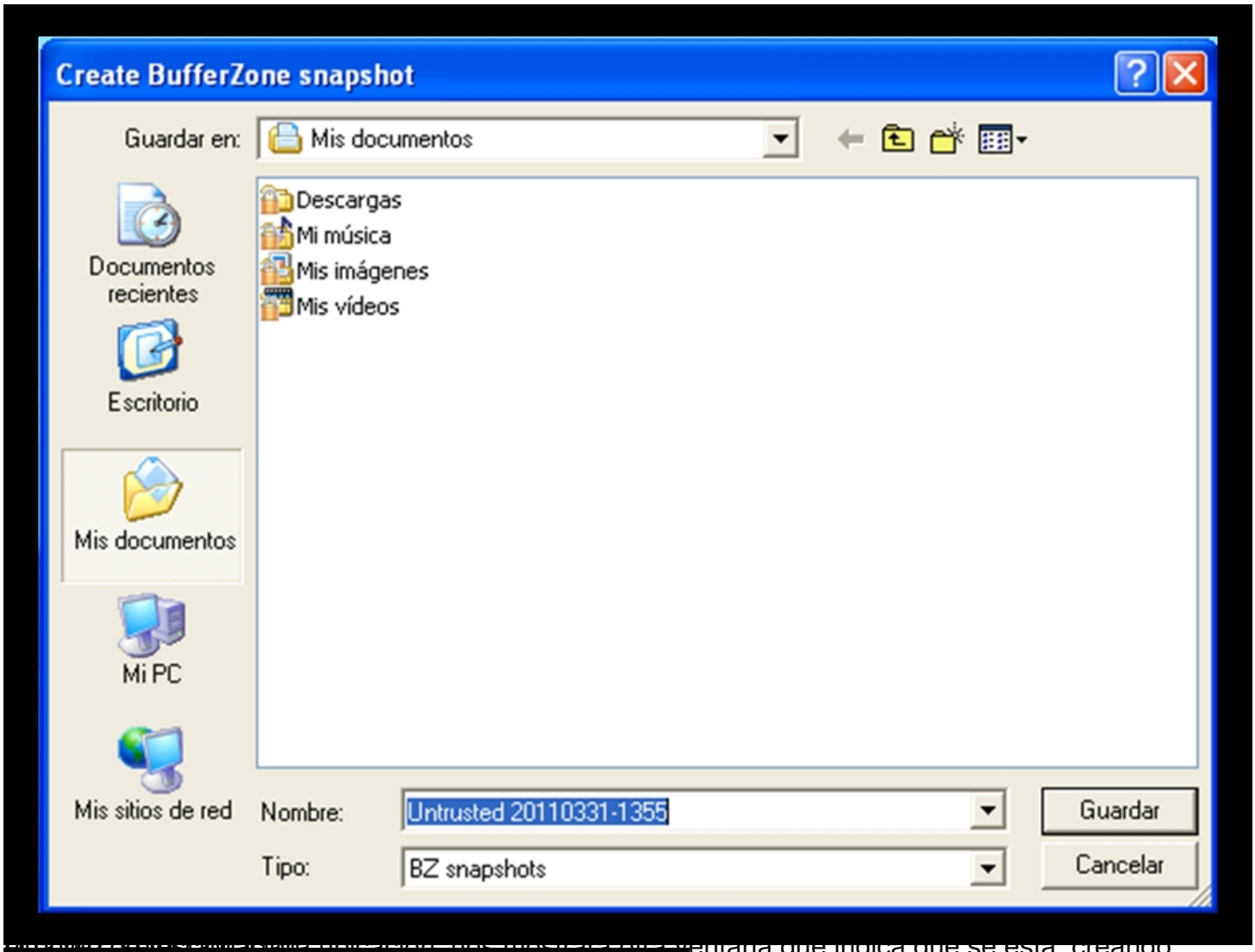
- Stop BufferZone processes: Detiene todos los procesos que se estén ejecutando en la zona virtual, sin borrar nada.
- Delete BufferZone registry: Elimina todo el registro virtual creado dentro de BufferZone.

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

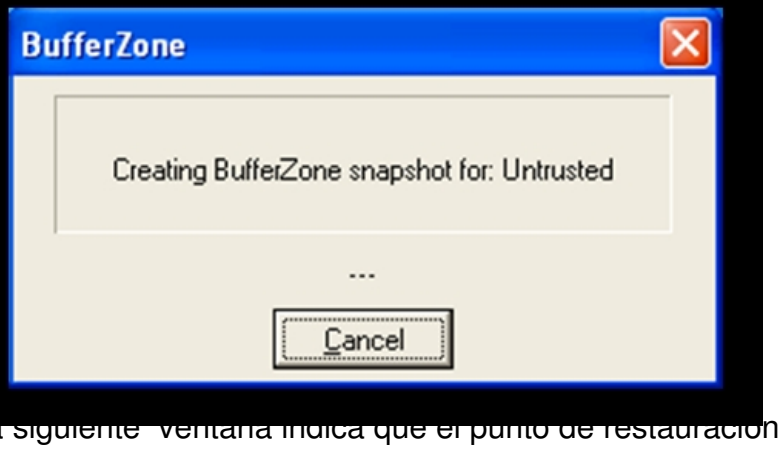


- Privacy Zone: Esta opción nos permite añadir sitios web que consideremos seguros y que se ejecutaran fuera de la zona de seguridad.


BufferZone
Privacy Zone
(Internet Explorer only)
Enter your e-banking and private sites. When visiting those sites, BufferZone will automatically isolate your browser, hence protecting your privacy.
Format: site.com
PORTAL.LACAIXA.ES/HOME/PARTICULARES_ES.HTML
BufferZone
Confidential
My Documents
Outlook MailBox

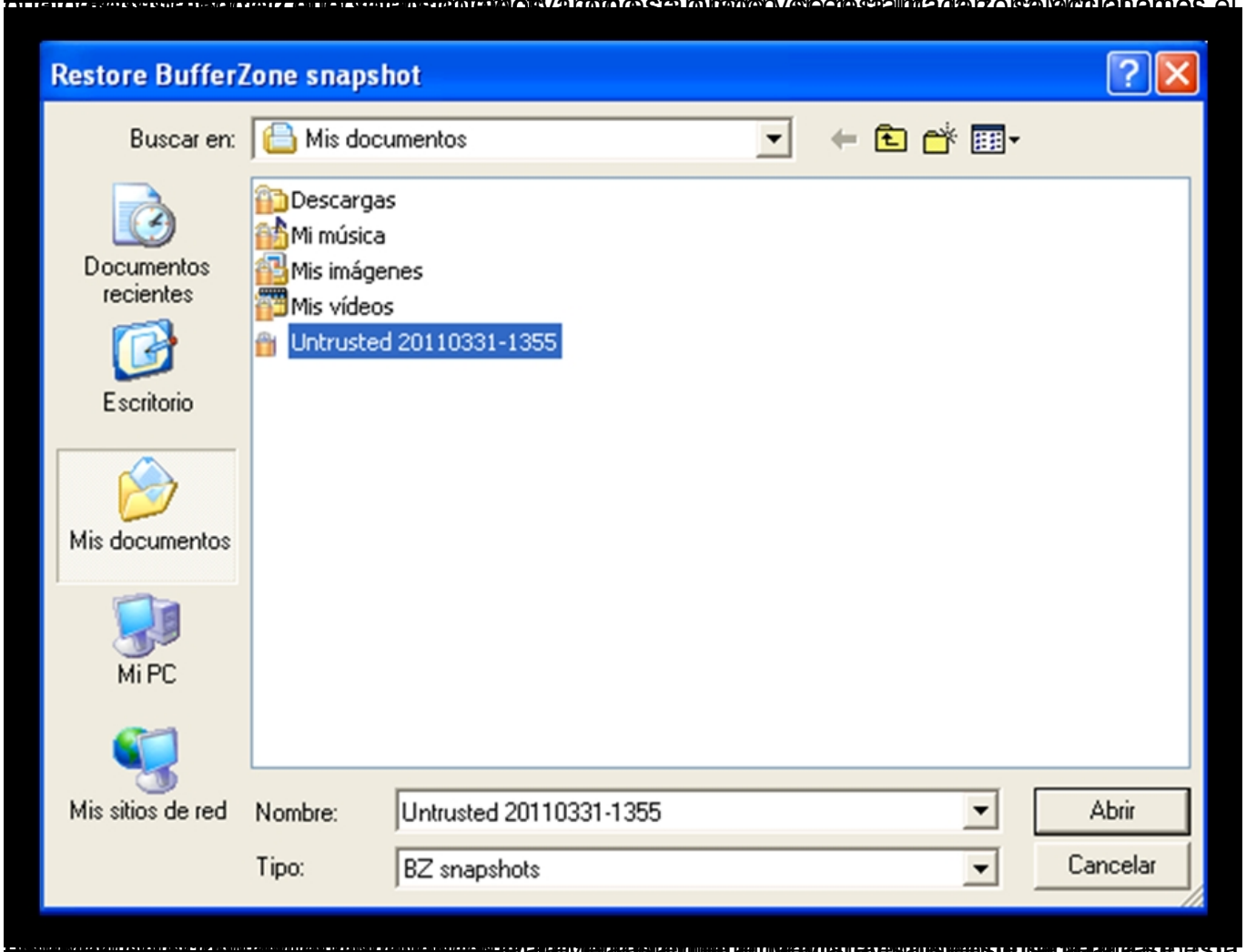


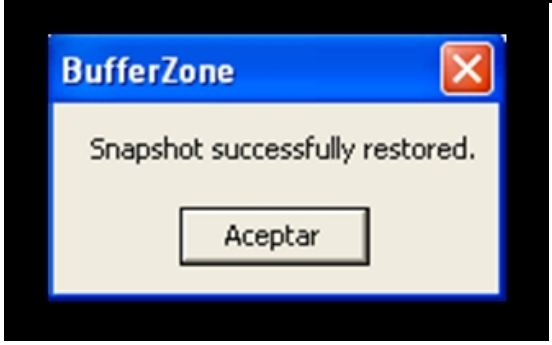
ventana que indica que se está creando

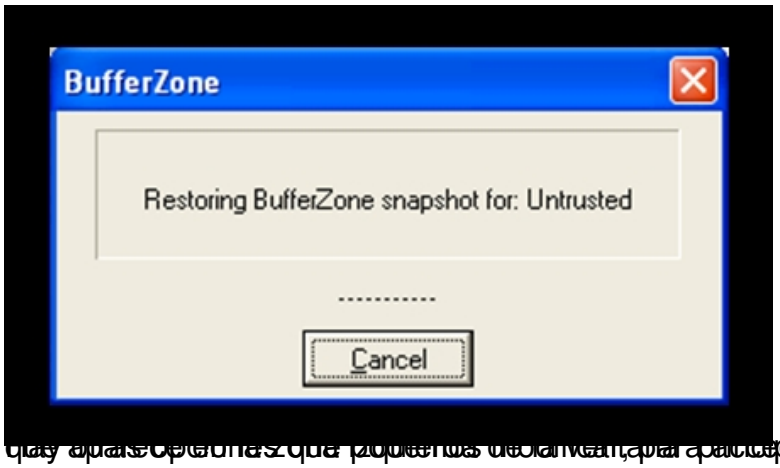


La siguiente ventana indica que el punto de restauración se ha creado con éxito:

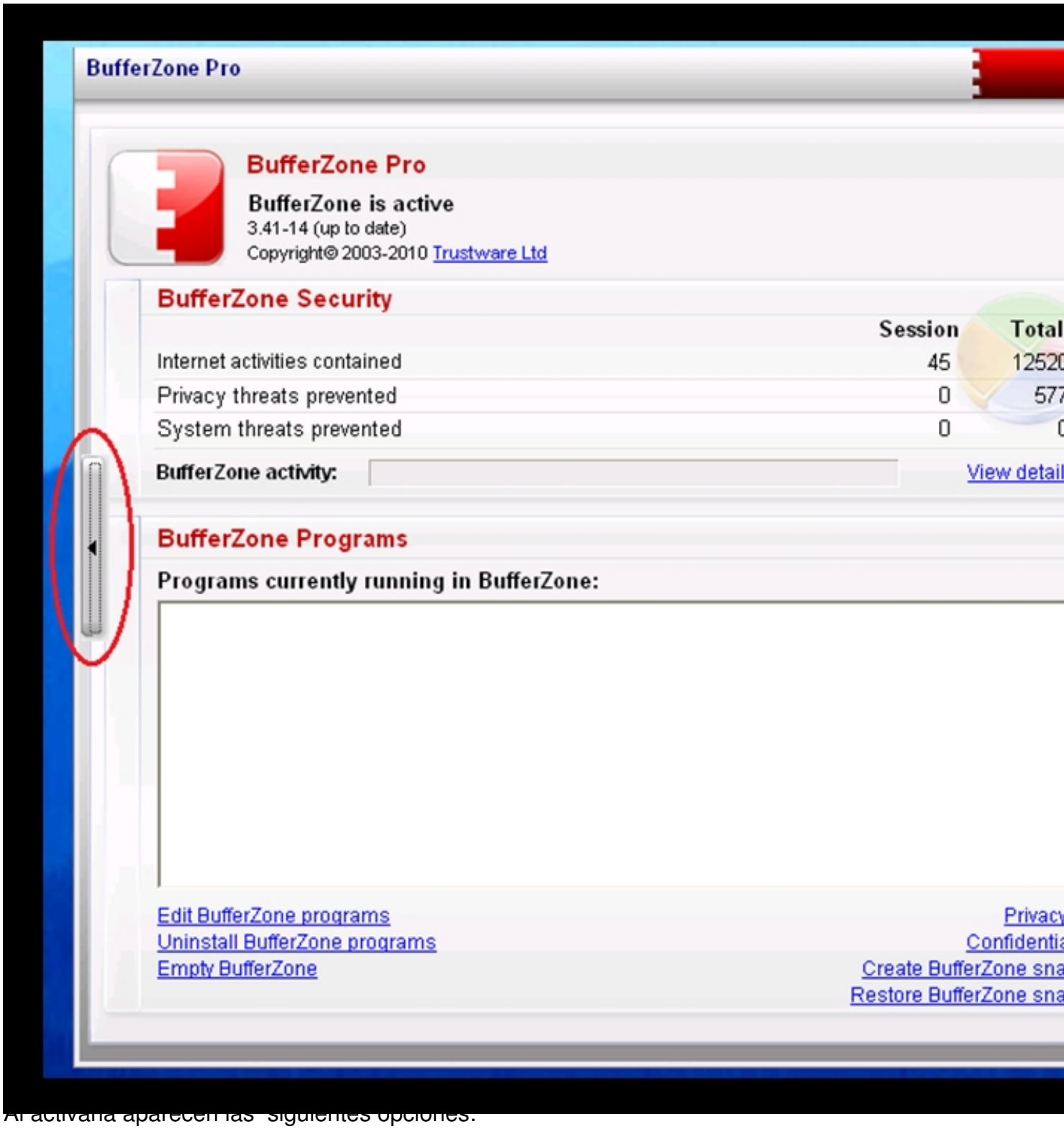
BufferZone
Snapshot successfully created.
Aceptar


Restore BufferZone snapshot
Buscar en:
Mis documentos
Descargas
Mi música
Mis imágenes
Mis vídeos
Untrusted 20110331-1355
Documentos recientes
Escritorio
Mis documentos
Mi PC
Mis sitios de red
Nombre:
Untrusted 20110331-1355
Abrir
Tipo:
BZ snapshots
Cancelar


BufferZone
Snapshot successfully restored.
Aceptar

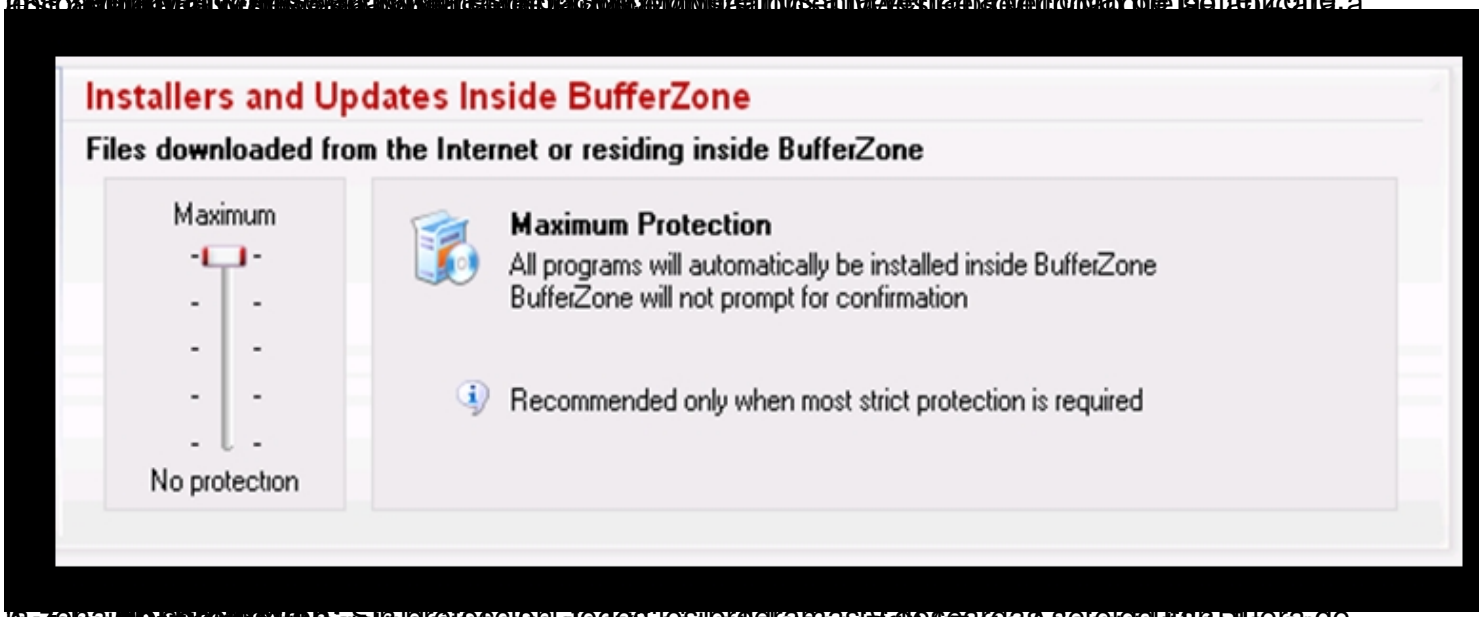


hay algunas opciones que podemos modificar, para acceder a ellas debemos pulsar la pestaña



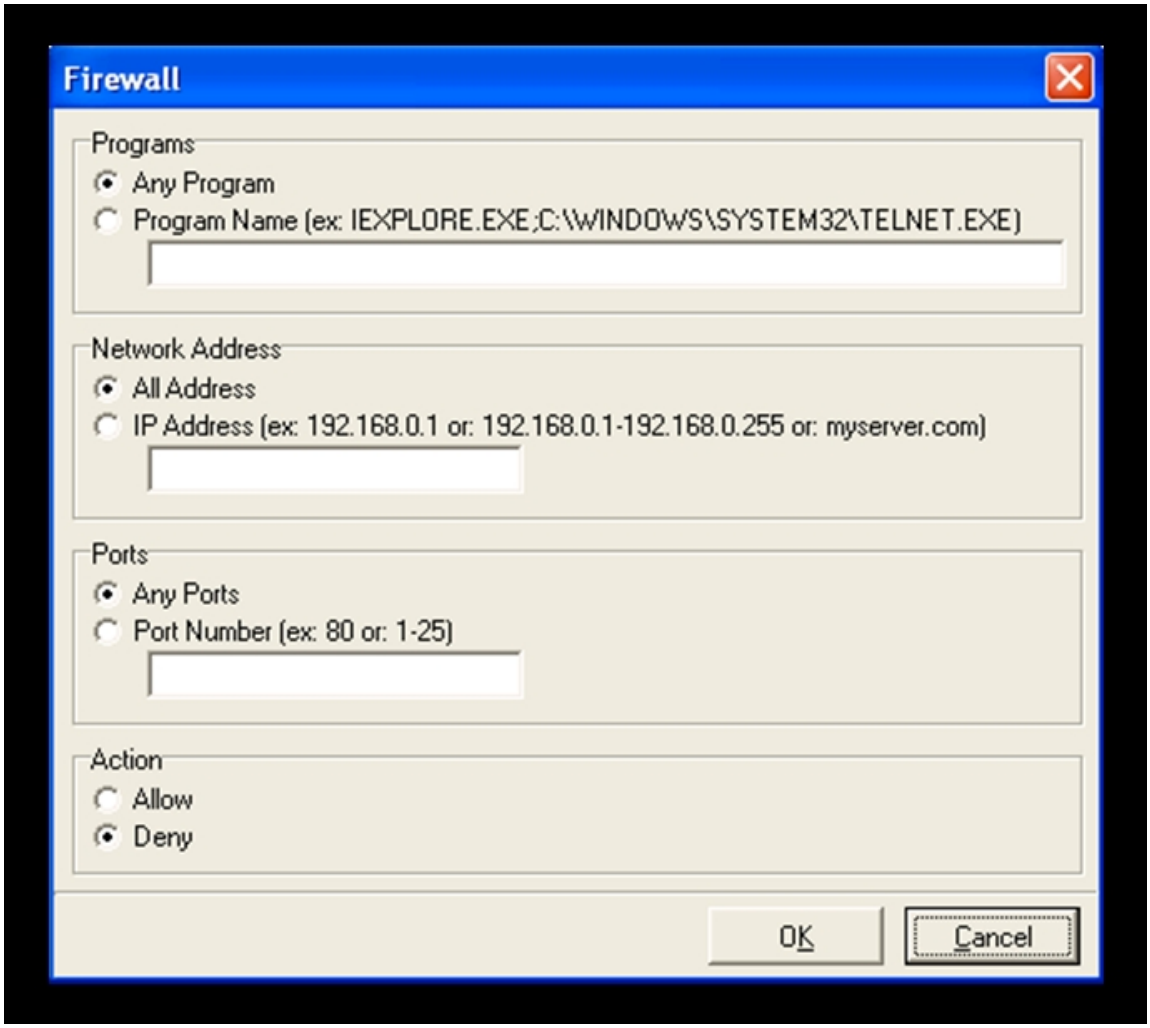
Al activarla aparecen las siguientes opciones:

BufferZone Pro
BufferZone
Summary
Policy
Firewall
Configuration
Help


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

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.

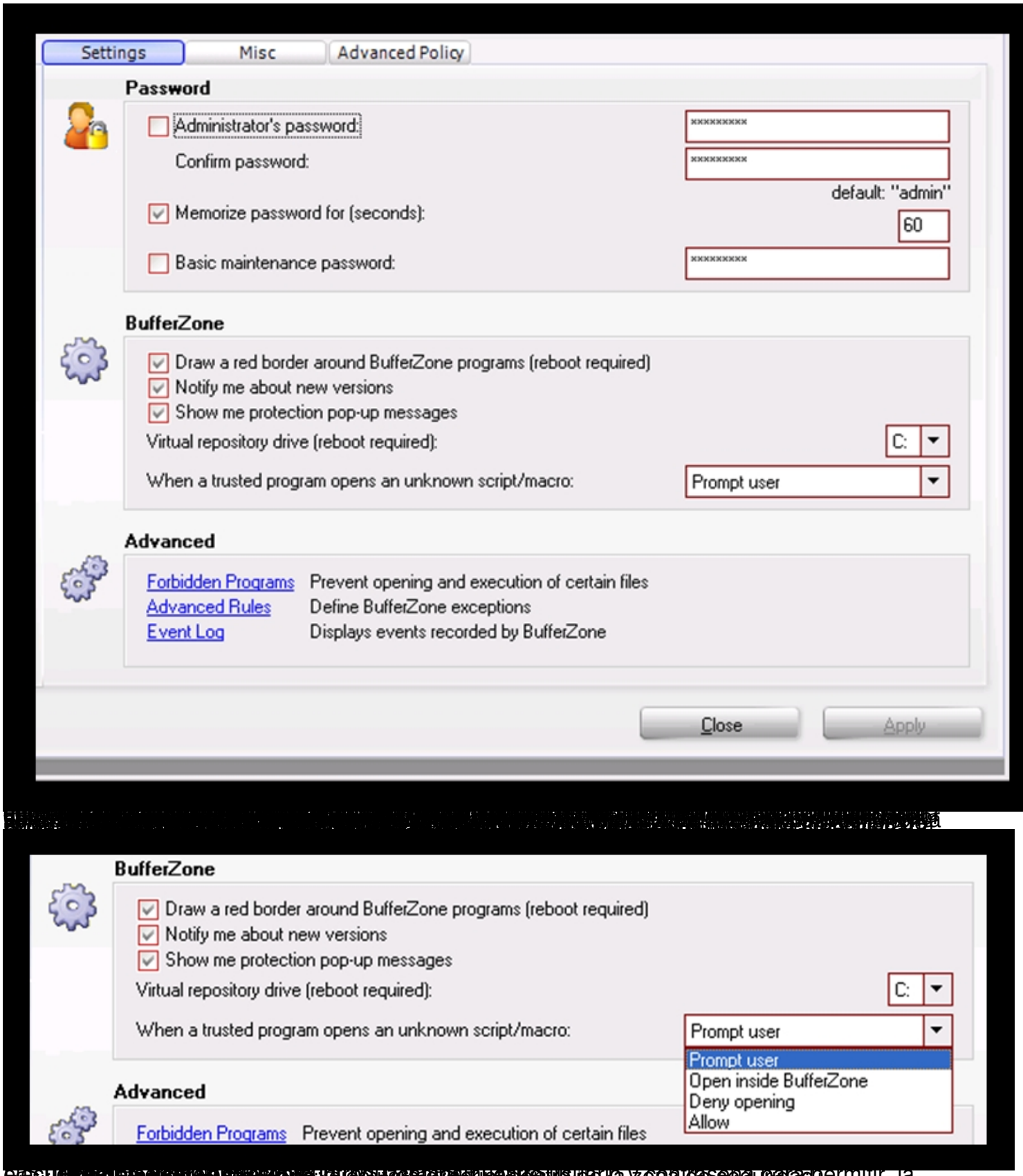


Se puede establecer el firewall para cualquier programa (Any program) o para algún programa en concreto escribiendo el nombre del programa y su extensión en la caja de texto. También se puede establecer de la misma manera para cualquier dirección IP o para alguna en

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

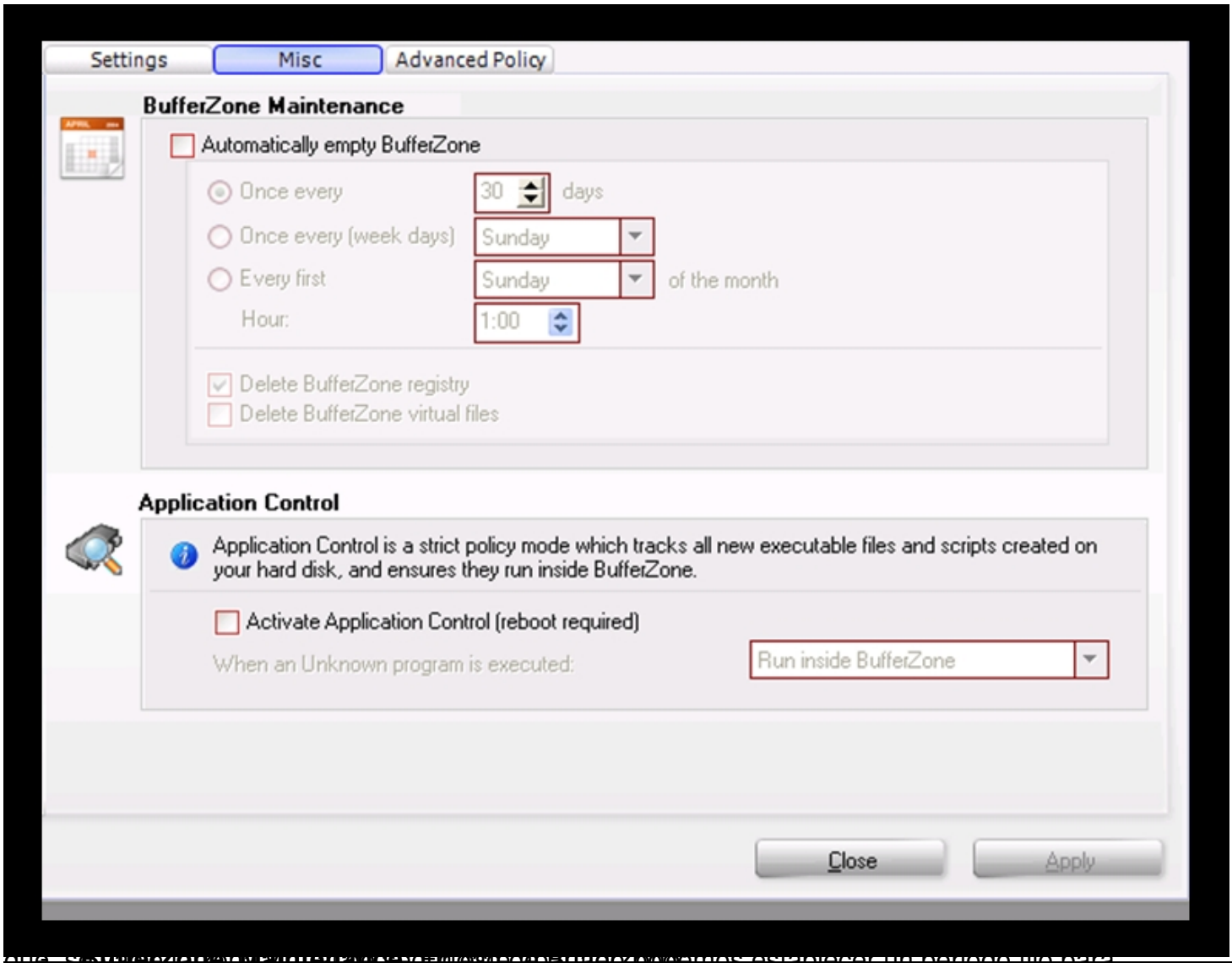
3. CONFIGURACION

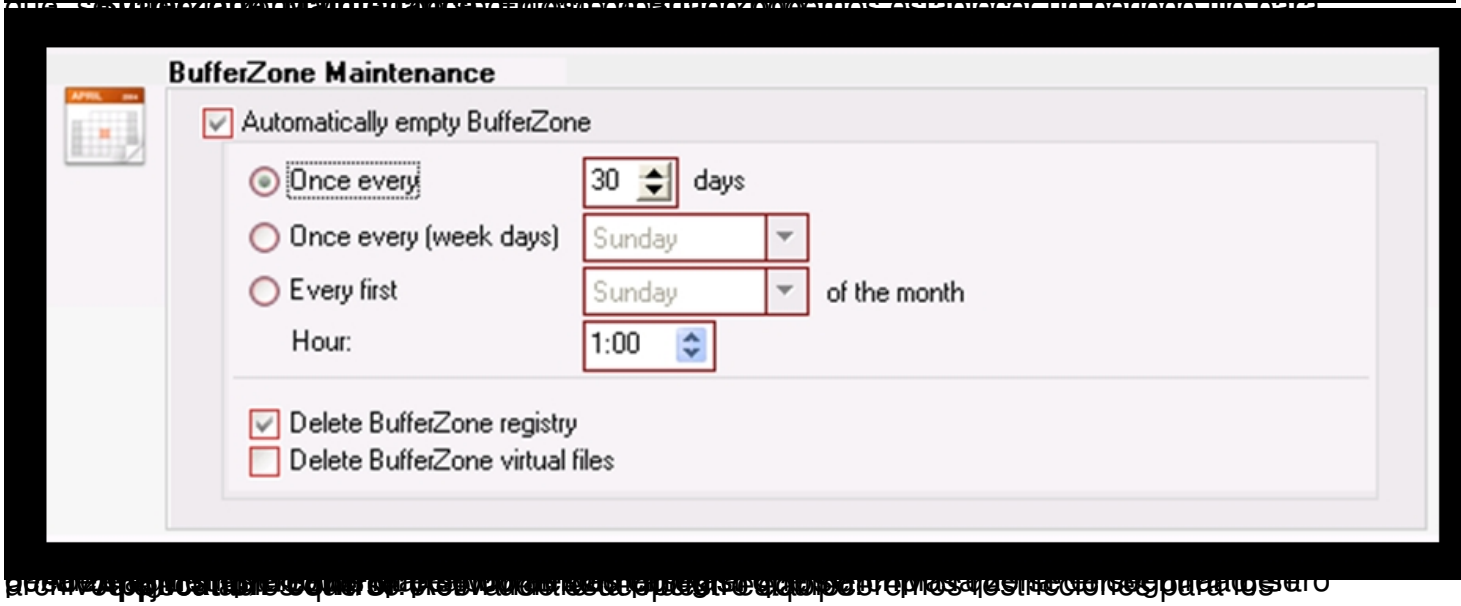
En este apartado podremos modificar opciones que afectan a partes muy diversas del programa como contraseñas, interfaz de usuario… Al pulsar sobre **configuration**, aparece la siguiente ventana con la pestaña
settings
marcada:

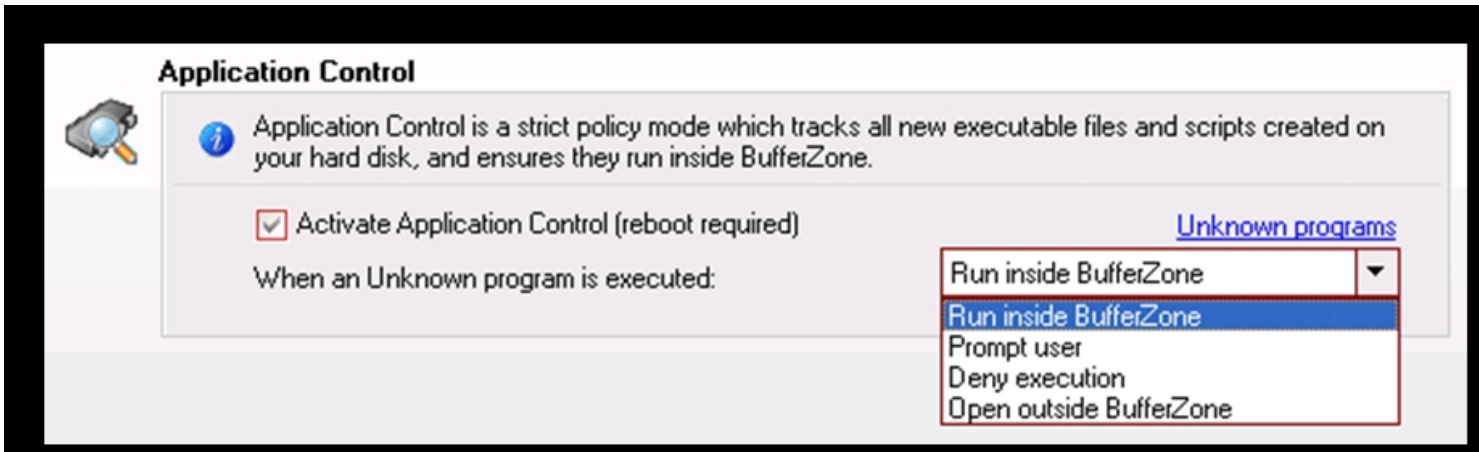

Settings
Misc
Advanced Policy
Password
Administrator's password:
Confirm password:
default: "admin"
Memorize password for (seconds):
60
Basic maintenance password:
BufferZone
Draw a red border around BufferZone programs (reboot required)
Notify me about new versions
Show me protection pop-up messages
Virtual repository drive (reboot required):
C:
When a trusted program opens an unknown script/macro:
Prompt user
Advanced
Forbidden Programs
Prevent opening and execution of certain files
Advanced Rules
Define BufferZone exceptions
Event Log
Displays events recorded by BufferZone
Close
Apply

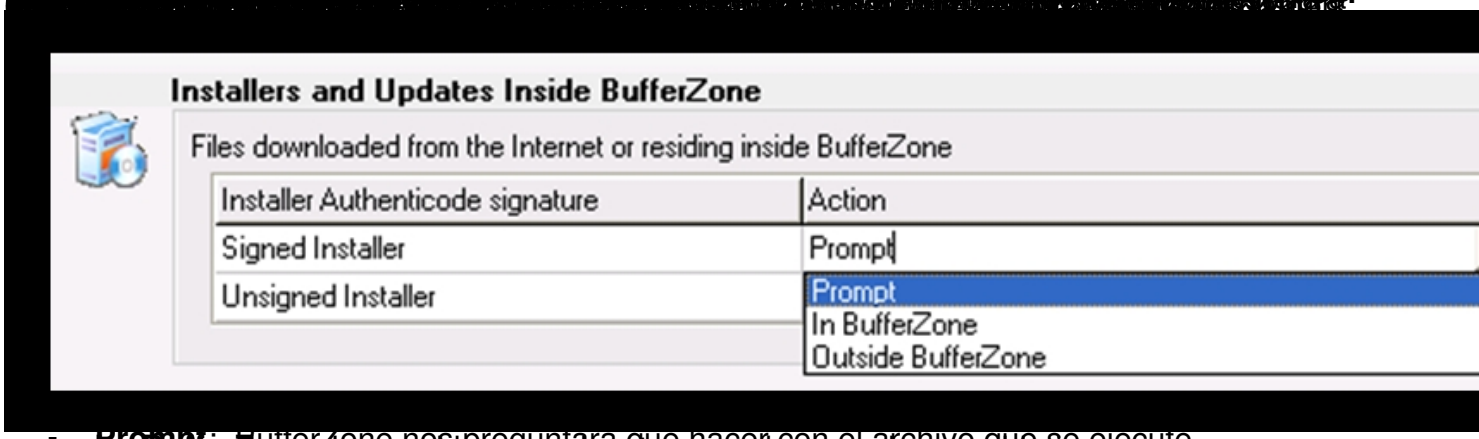
BufferZone
Draw a red border around BufferZone programs (reboot required)
Notify me about new versions
Show me protection pop-up messages
Virtual repository drive (reboot required):
C:
When a trusted program opens an unknown script/macro:
Prompt user
Prompt user
Open inside BufferZone
Deny opening
Allow
Advanced
Forbidden Programs
Prevent opening and execution of certain files

BufferZone
e-mail programs
Mail programs run outside BufferZone, but their attachments and saved files run inside BufferZone.
e-mail
Interaction with Buff...
Trusted
Trusted installations
Compilers
MSIMN.EXE
OUTLOOK.EXE
THUNDERBIRD.EXE
EUDORA.EXE
WINMAIL.EXE
NLNOTES.EXE;NOTES.EXE
GRPWISE.EXE;GWMAILTO.EXE
WINPM.EXE;WSENDTO.EXE;WINPM-32.EXE

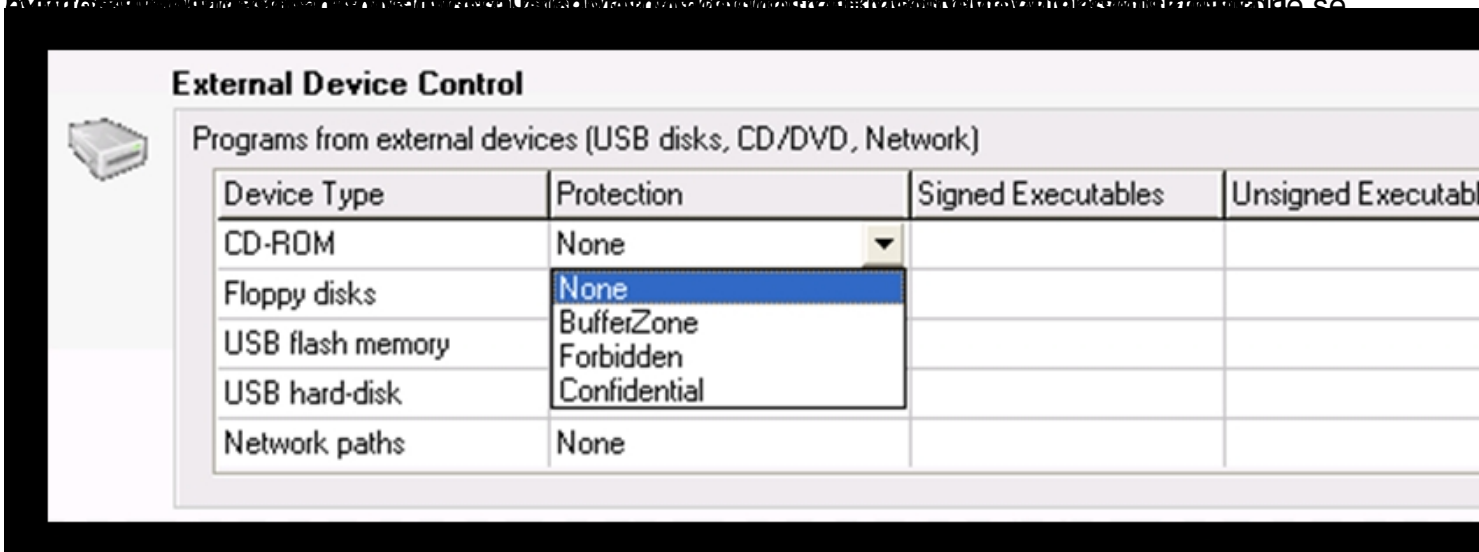

Settings
Misc
Advanced Policy
BufferZone Maintenance
Automatically empty BufferZone
Once every
30
days
Once every (week days)
Sunday
Every first
Sunday
of the month
Hour:
1:00
Delete BufferZone registry
Delete BufferZone virtual files
Application Control
Application Control is a strict policy mode which 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

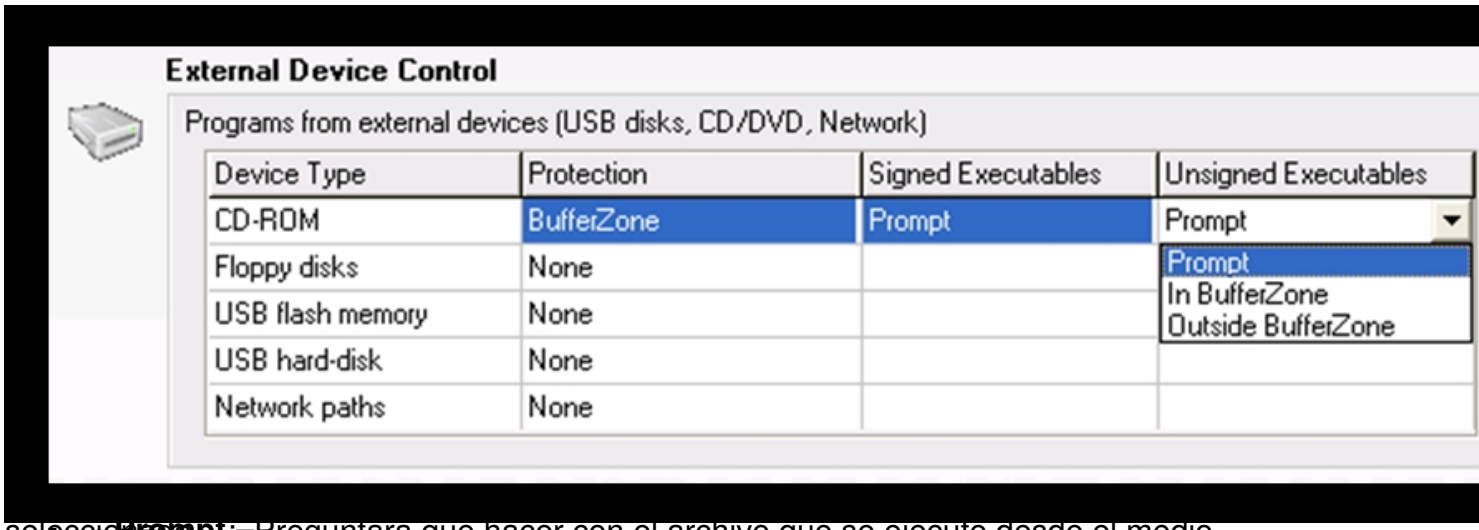

BufferZone Maintenance
Automatically empty BufferZone
Once every
30
days
Once every (week days)
Sunday
Every first
Sunday
of the month
Hour:
1:00
Delete BufferZone registry
Delete BufferZone virtual files





- **Prompt:** BufferZone nos preguntara que hacer con el archivo que se ejecute.





seleccionamos:

- **Prompt**: Preguntara que hacer con el archivo que se ejecute desde el medio
- **Outside BufferZone**: Ejecutara el archivo en nuestro equipo fuera de la zona segura.
- **Forbidden**: Prohibe la ejecucion de cualquier archivo contenido en un medio externo.

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.