Si se selecciona esta opción, se indica a VShield que explore los archivos para hallar virus, ofreciendo de esta forma máxima protección.

Si selecciona esta opción, se indica a VShield que explore archivos de programa para hallar virus, ofreciéndole la posibilidad de personalizar VShield para obtener un mejor rendimiento sin que por ello deba sacrificar su seguridad.

Si selecciona esta opción, se indica a VShield que explore los archivos ejecutables que se hallan comprimido utilizando PkLite y LZEXE para hallar virus.

Haga clic aquí para especificar extensiones de archivos de programa.

Utilice este campo para especificar la acción que debe llevarse a cabo al detectar un virus.

Si selecciona esta opción, se indica a VShield que muestre un mensaje personalizado al detectar un virus. Si desea que el mensaje aparezca en pantalla, la opción Acción debe definirse como **Consultar al usuario antes de actuar**.

Escriba el mensaje deseado para que se muestre al detectar un virus.

Si selecciona esta opción, se indica a VShield que registre la información en el archivo de registro especificado.

Escriba el archivo de registro deseado en el cuadro de texto pertinente.

Si selecciona esta opción, se indica a VShield que cree y mantenga un archivo de registro que no exceda un tamaño específico. Si lo que desea es un tamaño de archivo de registro ilimitado, cancele la selección de esta opción.

Escriba el tamaño de archivo de registro deseado en el cuadro de número provisto.

Muestra una lista de extensiones de archivo que VShield puede explorar.

Haga clic aquí para agregar otra extensión de archivo.

Haga clic aquí para eliminar la extensión de archivo seleccionada.

Haga clic para restaurar las extensiones de archivo predeterminadas de VShield.

Escriba la extensión de archivo nuevo aquí.

Haga clic aquí para especificar la ubicación del archivo de registro de VShield.

Si selecciona esta opción, se indica a VShield que cree una entrada de registro con la configuración de VShield para esta sesión.

Si selecciona esta opción, se indica a VShield que cree una entrada de registro que resuma su actividad durante esta sesión.

Si selecciona esta opción, se indica a VShield que explora el área MBR del disquete durante el cierre del sistema.

Si selecciona esta opción, se indica a VShield que incluya el nombre de usuario de Windows cuando se crean entradas de registro.

Escriba la ruta a la carpeta de destino deseado donde se moverán los archivos infectados. Esta carpeta se excluirá automáticamente de las exploraciones de VShield.

Haga clic aquí para hallar la carpeta.

Si selecciona esta opción, se indica a VShield que explore los disquetes en uso para hallar virus.

Si selecciona esta opción, el usuario podrá desactivar la protección que ofrece VShield.

Si selecciona esta opción, se indica a VShield que aparezca como tarea en la barra de tareas.

Si selecciona esta opción, se indica a VShield que cree una entrada de registro cuando se detecte un archivo infectado.

Si selecciona esta opción, se indica a VShield que cree una entrada de registro cuando un archivo infectado se ha limpiado satisfactoriamente.

Si selecciona esta opción, se indica a VShield que cree una entrada de registro cuando se borre un archivo infectado. Si activa esta opción, podrá saber qué archivos debe recuperar de los disquetes originales o de los de respaldo.

Si selecciona esta opción, se indica a VShield que cree una entrada de registro cuando un archivo infectado se ha desplazado a una carpeta de destino.

Si selecciona esta opción, se indica a VShield que incluya la fecha y la hora en cada entrada de registro.

Si selecciona esta opción, se indica a VShield que explore archivos que se arrancaron para hallar virus.

Si selecciona esta opción, se indica a VShield que explore los archivos abiertos para efectuar una copia en el sistema local con el fin de hallar virus.

Si selecciona esta opción, se indica a VShield que explore los archivos creados en el sistema local con el fin de hallar virus.

Si selecciona esta opción, se indica a VShield que explore los archivos que han cambiado de nombre en el sistema local con el fin de hallar virus.

Si selecciona esta opción, se indica a VShield que muestre la opción Limpiar cuando se detectan archivos infectados. Esta opción ofrece al usuario y a VShield una oportunidad para limpiar el archivo infectado. En el caso de que la limpieza no resultara satisfactoria, se ofrecerán opciones adicionales.

Si selecciona esta opción, se indica a VShield que muestre la opción Borrar cuando se detectan archivos infectados. Esta opción ofrece al usuario y a VShield la oportunidad de borrar un archivo infectado.

Si selecciona esta opción, se indica a VShield que muestre la opción Excluir cuando se detecten archivos infectados. Esta opción elimina el archivo de otras exploraciones de la sesión. Si desea una exclusión permanente, la encontrará en la página de propiedades **Exclusiones**.

Si selecciona esta opción, se indica a VShield que muestre la opción Detener cuando se detecten archivos infectados. Esta opción cancelará el acceso al archivo.

Si selecciona esta opción, se indica a VShield que muestre la opción Continuar cuando se detecten virus. Esta opción ignora las advertencias de VShield y permite al usuario seguir accediendo al archivo.

Los objetos, como archivos, carpetas o unidades, definidos en esta lista se excluirán de la detección de virus. Confirme que las adiciones realizadas a la lista no están infectadas.

Haga clic aquí para agregar un objeto de manera que se excluya de la exploración VShield.

Haga clic aquí para eliminar la entrada resaltada de la lista Exclusiones.

Haga clic aquí para editar una entrada resaltada.

Haga clic aquí para cargar automáticamente VShield durante el arranque del sistema.