Acronis® Internet Security Suite 2010

Guía del Usuario

Acronis Internet Security Suite 2010
Guía del Usuario

publicado 2010.05.25

Advertencia legal

Tabla de contenidos

Prólogo

Esta guía está dirigida a todos los usuarios que han elegido **Acronis Internet Security Suite 2010** como solución de seguridad para sus ordenadores personales. La información presentada en este libro es apta no sólo para expertos en informática, sino para todo aquel capaz de trabajar bajo Windows.

Este manual le describirá su Acronis Internet Security Suite 2010, le guiará durante el proceso de instalación, le mostrará como configurarlo. Descubrirá como utilizar Acronis Internet Security Suite 2010, como actualizar, probar y personalizarlo. Aprenderá como sacarle el mejor partido a Acronis Internet Security Suite 2010.

Le deseamos una útil y placentera lectura.

1. Convenciones utilizadas en este manual

1.1. Convenciones Tipográficas

En este manual se utilizan distintos estilos de texto con el fin de mejorar su lectura. Su aspecto y significado se indica en la tabla que aparece continuación.

Apariencia	Descripción
`sample syntax`	Ejemplos de sintaxis se muestran con letras `monospaced`.
http://www.acronis.es/support/	Los enlaces URL le dirigen a alguna localización externa, en servidores http o ftp.
"Prólogo" (p. ix)	Este es un enlace interno, hacia alguna localización dentro del documento.
`filename`	Los archivos y carpetas se muestran usando una fuente `monoespaciada`.
option	Todas las opciones del producto se muestran usando letra en **negrita**.

1.2. Admoniciones

Las advertencias son notas dentro del texto, marcadas gráficamente, que le facilitan información adicional relacionada con el párrafo que está leyendo.

Nota

La nota es una pequeña observación. Aunque puede omitirla, las notas pueden proporcionar información valiosa, como características específicas o enlaces hacia temas relacionados.

Importante

Este tipo de advertencia requiere su atención y no es recomendable omitirla. Normalmente proporciona información importante, aunque no extremadamente crítica.

Aviso

Se trata de información crítica que debería tratar con extrema cautela. No ocurrirá nada malo si sigue las indicaciones. Debería leer y entender estas notas, porque describen algo extremadamente arriesgado.

2. Estructura del Manual

Esta guía está dividida en varias partes que abordan los temas más importantes: Además, se incluye un glosario para aclarar los términos técnicos utilizados en la guía.

Instalación y eliminación. Instrucciones paso a paso para instalar Acronis Internet Security Suite 2010. Comenzando por los requisitos para una instalación correcta, será guiado a través del proceso de instalación. Finalmente, el proceso de desinstalación se describe en caso de que necesite desinstalar Acronis Internet Security Suite 2010.

Iniciando. Contiene toda la información que necesita para iniciarse con Acronis Internet Security Suite 2010. Se presenta con una interfaz de Acronis Internet Security Suite 2010 y cómo reparar incidencias, configurar los ajustes básicos y registrar su producto.

Modo Intermedio. Presenta la interfaz de Modo Intermedio de Acronis Internet Security Suite 2010.

Modo Avanzado. Una presentación detallada de la interfaz de Acronis Internet Security Suite 2010 en Modo Avanzado. Se le ha enseñado a configurar y utilizar todos los módulos de Acronis Internet Security Suite 2010 para proteger a su equipo eficazmente contra toda clase de amenazas (malware, spam, hackers, contenido inapropiado y otros).

Integrado en Windows y software de terceros. Muestra como usar las opciones de Acronis Internet Security Suite 2010 en el menú de Windows y la barra de herramientas de Acronis integrada en programas compatibles de terceros.

Cómo. Proporciona procedimientos para realizar rápidamente las tareas más comunes de Acronis Internet Security Suite 2010.

Solución de Problemas y Ayuda. Dónde consultar y dónde pedir ayuda si se produce una situación inesperada.

Glosario. El Glosario trata de explicar algunos términos técnicos y poco comunes que encontrará en las páginas de este documento.

Instalación y eliminación

1. Requisitos del Sistema

Sólo podrá instalar Acronis Internet Security Suite 2010 en aquellos equipos que dispongan de los siguientes sistemas operativos:

- Windows XP (32/64 bit) con Service Pack 2 o superior
- Windows Vista (32/64 bit) o Windows Vista con Service Pack 1
- Windows 7 (32/64 bit)

Antes de instalar el producto, compruebe que el equipo reúne los siguientes requisitos del sistema:

Nota

Para averiguar el sistema operativo que utiliza su equipo e información sobre el hardware, haga clic derecho sobre el icono **Mi PC** del Escritorio y seleccione la opción **Propiedades** en el menú.

1.1. Requisitos Mínimos del Sistema

- 450 MB disponibles de espacio libre en disco
- 800 MHz procesador
- Memoria RAM:
  - ▶ 512 MB para Windows XP
  - ▶ 1 GB para Windows Vista y Windows 7
- Internet Explorer 6.0
- .NET Framework 1.1 (disponible en el paquete de instalación)

1.2. Requisitos de Sistema Recomendado

- 600 MB disponibles de espacio libre en disco
- Intel CORE Duo (1.66 GHz) o procesador equivalente
- Memoria RAM:
  - ▶ 1 GB para Windows XP y Windows 7
  - ▶ 1.5 GB para Windows Vista
- Internet Explorer 7 (o superior)
- .NET Framework 1.1 (disponible en el paquete de instalación)

1.3. Software Soportado

Protección Antiphishing disponible sólo para:

- Internet Explorer 6.0 o superior
- Mozilla Firefox 2.5 o superior
- Yahoo Messenger 8.5 o superior
- Windows Live Messenger 8 o superior

Cifrado de Mensajería Instantánea (IM) disponible sólo para:

- Yahoo Messenger 8.5 o superior
- Windows Live Messenger 8 o superior

Protección Antispam disponible para todos los clientes de correo POP3/SMTP. La barra de herramientas Antispam de Acronis Internet Security Suite 2010 sólo está integrada en:

- Microsoft Outlook 2000 / 2003 / 2007
- Microsoft Outlook Express
- Microsoft Windows Mail
- Thunderbird 2.0.0.17

2. Preparándose para la Instalación

Antes de instalar Acronis Internet Security Suite 2010, complete estos preparativos para garantizar la instalación sin problemas:

- Asegúrese que el equipo donde va a instalar Acronis Internet Security Suite 2010 cumple los requisitos mínimos de sistema. Si el equipo no cumple todos los requisitos mínimos del sistema, Acronis Internet Security Suite 2010 no se instalará o, si es instalado, no funcionará correctamente y provocará que el sistema se ralentice y sea inestable. Para una lista completa de los requisitos de sistema, por favor diríjase a "*Requisitos del Sistema*" (p. 2).
- Inicie sesión en el equipo utilizando una cuenta de Administrador.
- Desinstalar otro software de seguridad de su equipo. La ejecución de dos programas de seguridad simultáneamente puede afectar al funcionamiento y causar mayores problemas con el sistema. Windows Defender ha de estar desactivado por defecto antes de que inicie la instalación.
- Desactive o elimine cualquier programa cortafuego que puede estar ejecutándose en el equipo. La ejecución de dos programas de cortafuego simultáneamente puede afectar al funcionamiento y causar mayores problemas con el sistema. El Cortafuego de Windows será desactivado por defecto antes de que se inicie la instalación.

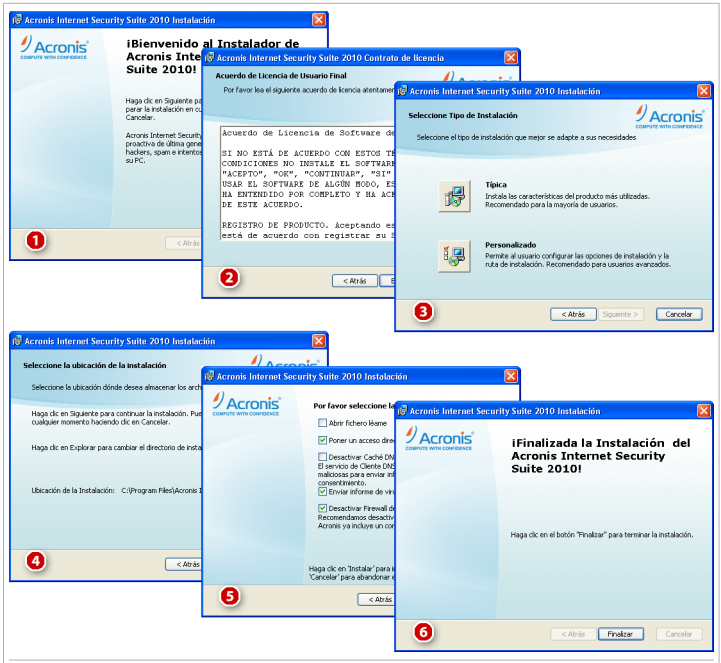
3. Instalando Acronis Internet Security Suite 2010

Usted puede adquirir y descargar el archivo de instalación desde el sitio web de Acronis Inc.:

http://www.acronis.es/homecomputing/

Para instalar Acronis Internet Security Suite 2010, localice el archivo de instalación en su equipo y haga doble clic en el. Este iniciará un asistente, el cual le guiará a través del proceso de instalación.

El instalador comprobará primero su equipo para validar la instalación. Si la instalación es validada, aparecerá el asistente de instalación. La siguiente imagen muestra los pasos del asistente de instalación.



Pasos de la Instalación

Siga estos pasos para instalar Acronis Internet Security Suite 2010:

1. Haga clic en **Siguiente**. Puede cancelar la instalación en cualquier momento que desee haciendo clic en **Cancelar**.

   Acronis Internet Security Suite 2010 le alertará si tiene otros productos antivirus instalados en su ordenador. Haga clic en **Desinstalar** para eliminar el producto

correspondiente. Si desea continuar sin desinstalar los productos detectados, haga clic en **Siguiente**.

Aviso

Se recomienda encarecidamente desinstalar los productos antivirus detectados antes de iniciar la instalación de Acronis Internet Security Suite 2010. Ejecutar dos antivirus a la vez puede provocar inestabilidad en el sistema.

2. Por favor, lea los términos del Contrato de Licencia y si está de acuerdo con las condiciones previstas, haga clic en **Acepto**.

Importante

Si no está de acuerdo con la condiciones, haga clic en **Cancelar**. Abandonará el proceso de instalación y saldrá del asistente.

3. Seleccione el tipo de instalación a realizar.
   - **Típica** - para instalar el programa inmediatamente, utilizando las opciones de instalación por defecto. Si selecciona esta opción, vaya al Paso 6.
   - **Personalizada** - para configurar las opciones de instalación, y a continuación, instalar el programa. Esta opción le permite cambiar la ruta de instalación.
4. Por defecto, Acronis Internet Security Suite 2010 se instalará en `C:\Archivos de Programa\Acronis Internet Security Suite\Acronis Internet Security Suite 2010`. Si desea cambiar la ruta de instalación, haga clic en **Explorar** y seleccione la carpeta donde desea instalar Acronis Internet Security Suite 2010.

   Haga clic en **Siguiente**.
5. Seleccione las opciones relativas al proceso de instalación. Las opciones recomendadas son seleccionadas por defecto:
   - **Abrir fichero léame** - para abrir el fichero léame al final de la instalación.
   - **Crear acceso directo en el Escritorio** - para situar un acceso directo de Acronis Internet Security Suite 2010 en el Escritorio al finalizar la instalación.
   - **Desactivar la caché DNS** - para desactivar la caché DNS (Nombre de Dominio de Sistema). El servicio de Cliente DNS puede ser utilizado por aplicaciones maliciosas para enviar información por la red sin su consentimiento.
   - **Enviar Informe de Virus** - enviar los informes de virus a Acronis Lab para su análisis. Los informes no tendrán datos confidenciales, tales como nombre, dirección IP u otra información, ni serán utilizados con fines comerciales.
   - **Desactivar el cortafuego de Windows** - para desactivar el Firewall de Windows.

Importante

Le recomendamos desactivar el Firewall de Windows puesto que Acronis Internet Security Suite 2010 ya incluye un cortafuego avanzado. Ejecutar dos cortafuegos en el mismo ordenador puede causar problemas.

- **Desactivar Windows Defender** - para desactivar Windows Defender; esta opción sólo aparece en Windows Vista.

Haga clic en **Instalar** para iniciar la instalación del programa. En caso de no disponer de .NET Framework 1.1, Acronis Internet Security Suite 2010 empezará con la instalación de este componente.

6. Espere hasta que la instalación acabe y entonces haga clic en **Finalizar**. Es posible que sea necesario reiniciar el sistema para que se complete el proceso de instalación. Recomendamos realizarlo lo antes posible.

4. Activando el producto

Cuando reinicie el equipo después de la instalación, el programa funcionará en modo de prueba durante 30 días. Durante el periodo, el producto debe ser activado. Si no ha activado el producto en ese plazo, dejará de funcionar.

Cuando usted compra el producto, usted recibe un número de serie de 16 caracteres, ya sea con la caja o por e-mail. El número de serie de 64 caracteres para activar el producto será enviado a su dirección de e-mail después de introducir el número de serie de 16 caracteres en la página web de registro.

Tenga en cuenta que su suscripción al producto durante 1 año comienza en el momento en que se envía el número de serie de 64 caracteres. Tras finalizar su periodo de suscripción, su licencia expirará y usted no podrá utilizar el producto. Para desbloquear el producto, usted necesita comprar una nueva licencia. Un nuevo número de serie de 16 caracteres le será enviado a su e-mail y tendrás que realizar el proceso de activación una vez más.

Activación paso a paso

Cuando inicie el programa por primera vez, le preguntará si usted tiene el número de serie de 64 caracteres.

Caso 1 - Si usted tiene el número de serie de 64 caracteres:

1. Haga click en el botón **Si, tengo**.
2. En la siguiente página, pegue el número de serie correspondiente en la casilla (mediante la combinación CTRL+V).
3. Haga click en el botón **Activar**.

Caso 2 - Si usted no tiene el número de serie de 64 caracteres, pero tiene el número de serie de 16 caracteres:

1. Haga click en el botón **Obtener número de serie**.
2. En el sitio web, introduzca su información de cuenta de Acronis, su número de serie de 16 caracteres y su dirección de e-mail. Se le enviará un mensaje con el número de serie de 64 caracteres a la dirección e-mail que ha especificado.

   Si aún no tiene una cuenta de Acronis, será creada mediante el uso de la información personal que usted facilitó cuando registró el producto.
3. Abra el e-mail recibido y copie el número de serie.
4. Vuelva al programa y haga click en el botón **Si, tengo**.
5. En la siguiente página, pegue el número de serie correspondiente en la casilla (mediante la combinación CTRL+V).
6. Haga click en el botón **Activar**.

Caso 3 - Si usted no tiene ni el número de serie de 16 caracteres ni el de 64 caracteres:

1. Haga click en el enlace **Compra online**.
2. Compre el producto. Se le enviará por e-mail el número de serie de 16 caracteres.
3. Realice todos los pasos del caso 2.

Caso 4 - Si usted no tiene ningún número de serie y quiere probar el producto primero:

1. Haga click en el botón **Más tarde**. El producto completamente funcional estará disponible para usted durante el periodo de prueba.
2. Si usted decide comprar el producto, realice todos los pasos del caso 3.

5. Reparando o Desinstalando Acronis Internet Security Suite 2010

Si desea reparar o desinstalar Acronis Internet Security Suite 2010, siga la ruta desde el menú de Inicio de Windows: **Inicio → Programas → Acronis → Acronis Internet Security Suite 2010 → Reparar o Desinstalar**.

Luego se le pedirá confirmar su elección pulsando **Siguiente**. Se le mostrará una ventana en la que podrá seleccionar:

- **Reparar** - para reinstalar todos los componentes del programa instalados anteriormente.

  Si elige reparar Acronis Internet Security Suite 2010, aparecerá una nueva ventana. Haga clic en **Reparar** para iniciar el proceso de reparación.

  Reinicie el equipo cuando se le indique y, a continuación, haga clic en **Instalar** para reinstalar Acronis Internet Security Suite 2010.

  Al finalizar el proceso de instalación, aparecerá una nueva ventana. Haga clic en **Finalizar**.

- **Eliminar** - para quitar todos los componentes instalados.

  Nota

  Recomendamos elegir la opción **Desinstalar** para realizar una re-instalación limpia.

  Si elije desinstalar Acronis Internet Security Suite 2010, aparecerá una ventana nueva.

  Importante

  Al desinstalar Acronis Internet Security Suite 2010, no estará protegido contra las amenazas de malware, como virus, spyware, o hackers. Si desea activar el Firewall de Windows y Windows Defender (sólo en Windows Vista) al finalizar la desinstalación de Acronis Internet Security Suite 2010, seleccione la casilla correspondiente.

  Haga clic en **Desinstalar** para iniciar la desinstalación de Acronis Internet Security Suite 2010 de su equipo.

  Al finalizar el proceso, aparecerá una nueva ventana. Haga clic en **Finalizar**.

  Nota

  Al finalizar el proceso de desinstalación, recomendamos eliminar la carpeta `Acronis Internet Security Suite` ubicada dentro de `Archivos de Programa`.

Iniciando

6. Vista general

Una vez tenga Acronis Internet Security Suite 2010 instalado, su equipo estará protegido.

6.1. Abriendo Acronis Internet Security Suite 2010

Para acceder a la interfaz principal de Acronis Internet Security Suite 2010, utilice el menú de Inicio de Windows, siguiendo la ruta **Inicio → Programas → Acronis → Acronis Internet Security Suite 2010 → Acronis Internet Security Suite 2010** o, rápidamente, doble clic en el icono Acronis en la barra de tareas.

6.2. Modos de Vista de la Interfaz de Usuario

Acronis Internet Security Suite 2010 satisface las necesidades tanto de los usuarios más técnicos como de los usuarios principiantes. Esta interfaz de usuario gráfica esta diseñada para satisfacer todas y cada una de las categorías de usuario.

Puede seleccionar la vista de la interfaz de usuario mediante tres modos, dependiendo de sus conocimientos y su experiencia con Acronis.

Modo	Descripción
Modo Básico	Adecuado para gente principiante que desea que Acronis Internet Security Suite 2010 proteja su equipo y sus datos sin ser molestado. Este modo es simple de utilizar y requiere una mínima interacción por su parte. Todo lo que tiene que hacer es reparar todas las incidencias que existan cuando se lo indique Acronis Internet Security Suite 2010. Un asistente intuitivo le guiará paso a paso para reparar estas incidencias. Además, puede realizar tareas comunes, como una actualización de firmas de virus de Acronis Internet Security Suite 2010 y archivos de producto o análisis del equipo.
Modo Intermedio	Dirigido a usuarios con conocimientos medios, este modo extiende lo que puede hacer en el Modo Básico. Puede reparar incidencias por separado y seleccionar que incidencias van a ser monitorizadas. Además, puede administrar remotamente los productos de Acronis instalados en los equipos de su red.
Modo Avanzado	Diseñado para usuarios más técnicos, este modo permite configurar completamente cada función de

Modo	Descripción
	Acronis Internet Security Suite 2010. Puede utilizar todas las tareas proporcionadas para proteger su equipo y sus datos.

Por defecto, la interfaz de usuario se muestra en modo intermedio. Para cambiar a un modo de interfaz de usuario diferente, siga estos pasos:

1. Abrir Acronis Internet Security Suite 2010.
2. Haga clic en el botón **Ajustes** en la esquina superior derecha de la ventana.
3. En la categoria de ajustes de Interfaz de Usuario, haga clic en la flecha del botón y seleccione el modo deseado desde el menú.
4. Haga clic en **Ok** para guardar y aplicar los cambios.

6.2.1. Modo Básico

Si es un principiante en el pc, mostrando la interfaz de usuario en Modo Básico puede ser la elección más adecuada para usted. Este modo es sencillo de utilizar y requiere mínima interacción por su parte.

Modo Básico

La ventana está organizada en cuatro secciones principales:

- **Estado** - Le alerta en caso de que haya incidencias que afecten a su equipo y le ayuda a repararlas. Haciendo Clic en **Reparar Todas Incidencias**, un asistente le ayudará a eliminar fácilmente cualquier amenaza a su equipo y datos de

seguridad. Para más información, por favor, consulte el capítulo "*Reparar Incidencias*" (p. 34).

- **Proteja su PC**es donde puede encontrar las tareas necesarias para proteger su equipo y sus datos. Las tareas disponibles que se puede realizar son diferentes dependiendo del perfil de uso seleccionado.
  - ▶ El botón **Analizar** inicia un análisis estándar de su sistema en busca de virus, spyware y otro malware. El Asistente de Análisis Antivirus aparecerá y le guiara por todo el proceso de análisis. Para información detallada acerca de este asistente, por favor consulte "*Asistente del análisis Antivirus*" (p. 45).
  - ▶ El botón **Actualizar** le ayuda a actualizar las firmas de virus y archivos del producto de Acronis Internet Security Suite 2010. Aparecerá una nueva ventana dónde podrá ver el estado de la actualización. Si se detectan actualizaciones, estas son automáticamente descargadas e instaladas en su equipo.
  - ▶ Cuando el perfil seleccionado es **Tipico**, el botón **Comprobar Vulnerabilidades** inicia un asistente que le ayuda a encontrar y reparar vulnerabilidades del sistema, como software obsoleto o actualizaciones perdidas de Windows. Para información detallada, diríjase a la sección "*Asistente de Análisis de Vulnerabilidad*" (p. 57).
  - ▶ Cuando el perfil **Padre** está seleccionado, el botón **Control Parental** le permite configurar el Control Parental. El Control Parental restringe el equipo y las actividades online de sus hijos basados en las reglas que usted ha definido. Las restricciones deben incluir el bloqueo de páginas web inapropiadas, así como la limitación de juego y acceso a Internet de acuerdo con la planificación especificada. Para más información sobre como configurar el Control Parental, por favor diríjase a "*Control Parental* " (p. 174).
  - ▶ Cuando se selecciona el perfil **Jugador** el botón **Activar/Desactivar Modo Juego** le permite activar/desactivar Modo Juego. El Modo Juego modifica temporalmente las opciones de seguridad para minimizar su impacto sobre el rendimiento del sistema.
- **Proteja su PC** es donde puede encontrar tareas adicionales para proteger su equipo y sus datos.
  - ▶ **Añadir Archivo al Blindaje** inicia el asistente que le permite guardar sus archivos/documentos privados importantes cifrándolos en unidades especiales blindadas.
  - ▶ **Análisis en profundidad** inicia un análasis completo de su sistema en busca de todo tipo de malware.
  - ▶ **Analizar Mis Documentos** analiza en busca de virus y otro malware en sus carpetas mas utilizadas: `Mis Documentos` y `Escritorio`. De este modo se garantizará la seguridad de sus documentos, un espacio de trabajo seguro y limpio y aplicaciones que se ejecutan en el inicio.

- **Perfil de Uso** indica el perfil de uso que está seleccionado actualmente. El perfil de uso refleja las principales actividades realizadas en el el equipo. Dependiendo del perfil de uso, la interfaz de producto se organiza para permitir el acceso fácilmente a sus tarea preferidas.

  Si desea cambiar a un perfil diferente o editar el que esta utilizando, haga clic en el perfil y siga el Asistente de Configuración.

En la esquina superior derecha de la venta, puede ver el botón de **Configuración**. Se abre una ventana donde puede cambiar el modo de interfaz de usuario y activar y desactivar los ajustes principales de Acronis Internet Security Suite 2010. Para más información, por favor, consulte el apartado *"Configurando los Ajustes Básicos" (p. 37)*.

En la esquina inferior derecha de la ventana, puede encontrar varios enlaces útiles.

Enlace	Descripción
Comprar/Renovar	Abra una página web donde puede comprar una licencia para su producto Acronis Internet Security Suite 2010.
Soporte	Le permite ponerse en contacto con el equipo de soporte de Acronis.
Ayuda	Le da acceso a un fichero de ayuda que le enseña como utilizar Acronis Internet Security Suite 2010.
Logs	Le permite ver un historial detallado sobre las tareas que Acronis Internet Security Suite 2010 ha realizado en su sistema.

6.2.2. Modo Intermedio

Dirigido a usuarios con conocimientos medios, el Modo Intermedio es una interfaz simple que le da acceso a todos los módulos en un nivel básico. Tendrá que hacer un seguimiento de las advertencias, las alertas criticas y la solución de incidencias no deseadas.

Modo Intermedio

La venta del Modo Intermedio consiste en cinco pestañas. La siguiente tabla describe brevemente cada pestaña. Para más información, por favor, consulte el capitulo “Modo Intermedio” (p. 83) de esta guía de usuario.

Pestaña	Descripción
Visualizador	Muestra el estado de seguridad de su sistema y permite ajustar el perfil de uso.
Seguridad	Muestra el estado de los módulos de seguridad (antivirus, antiphishing, cortafuego, antispam, cifrado de IM, privacidad, comprobación de vulnerabilidades y actualización) junto con enlaces a tareas antivirus, actualización y comprobación de vulnerabilidades.
Parental	Muestra el estado del módulo Control Parental. El Control Parental le permite restringir el acceso de sus hijos a Internet y a aplicaciones específicas.
Blindaje de Archivo	Muestra el estado de los módulos blindaje de archivos, así como enlaces a tareas de relacionadas con éste.
Red	Muestra la estructura de la red doméstica de Acronis. Desde aquí puede realizar varias acciones para configurar y administrar los productos Acronis instalados en su red. De

Pestaña	Descripción
	esta manera, puede administrar la seguridad de su red desde un solo ordenador.

En la esquina superior derecha de la venta, puede ver el botón de **Configuración**. Se abre una ventana donde puede cambiar el modo de interfaz de usuario y activar y desactivar los ajustes principales de Acronis Internet Security Suite 2010. Para más información, por favor, consulte el apartado *"Configurando los Ajustes Básicos" (p. 37)*.

En la esquina inferior derecha de la ventana, puede encontrar varios enlaces útiles.

Enlace	Descripción
Comprar/Renovar	Abra una página web donde puede comprar una licencia para su producto Acronis Internet Security Suite 2010.
Registro	Le permite introducir su número de serie y ver el estado de registro.
Soporte	Le permite ponerse en contacto con el equipo de soporte de Acronis.
Ayuda	Le da acceso a un fichero de ayuda que le enseña como utilizar Acronis Internet Security Suite 2010.
Logs	Le permite ver un historial detallado sobre las tareas que Acronis Internet Security Suite 2010 ha realizado en su sistema.

6.2.3. Modo Avanzado

El Modo Avanzado le da acceso a cada componente específico de Acronis Internet Security Suite 2010. Aquí es donde puede configurar Acronis Internet Security Suite 2010 al detalle.

Nota
El Modo Avanzado es adecuado para usuarios que estén por encima de la media, que conocen el tipo de amenazas a las que se expone un equipo y como trabajan los programas de seguridad.

Modo Avanzado

En la parte izquierda de la ventana hay un menú que contiene todos los módulos de seguridad. Cada módulo tiene una o más pestañas donde puede configurar los correspondientes ajustes de seguridad, ejecutar seguridad o tareas administrativas. La siguiente tabla describe brevemente cada módulo. Para más información, por favor, consulte el capítulo “Modo Avanzado” (p. 104) de esta guía de usuario.

Módulo	Descripción
General	Le permite acceder a la configuración general o ver el visualizador e información del sistema.
Antivirus	Le permite configurar la protección antivirus en tiempo real y operaciones de análisis, establecer excepciones y configurar el módulo cuarentena.
Antispam	Le permite mantener su bandeja de entrada libre de SPAM y configurar las opciones de antispam en detalle.
Control Parental	Le permite impedir el acceso a contenido inapropiado a través de reglas de acceso personalizadas.

Módulo	Descripción
Control de Privacidad	Le ayuda a impedir el robo de datos de su equipo y protege su privacidad mientras está conectado a Internet.
Cortafuego	Le permite proteger su sistema frente a los intentos de conexión externos o internos no autorizados. Algo parecido a tener un guardia en su puerta – vigilará su conexión a Internet y monitorizará todas las conexiones que decida autorizar o bloquear.
Vulnerabilidad	Le permite tener actualizado el software crucial de su PC.
Cifrado	Le permite cifrar las conversaciones de Yahoo y Windows Live (MSN) Messenger, así como cifrar sus archivos, carpetas o particiones críticos.
Modo Juego/Portátil	Le permite posponer tareas planificadas de Acronis cuando su portátil funcione con batería y desactivar todas las alertas mientras juega.
Red	Le permite configurar y administrar los equipos de una pequeña red de usuarios.
Actualización	Le permite obtener información sobre las últimas actualizaciones, actualizar el producto y configurar el proceso de actualización en detalle.

En la esquina superior derecha de la venta, puede ver el botón de **Configuración**. Se abre una ventana donde puede cambiar el modo de interfaz de usuario y activar y desactivar los ajustes principales de Acronis Internet Security Suite 2010. Para más información, por favor, consulte el apartado "*Configurando los Ajustes Básicos*" (p. 37).

En la esquina inferior derecha de la ventana, puede encontrar varios enlaces útiles.

Enlace	Descripción
Comprar/Renovar	Abra una página web donde puede comprar una licencia para su producto Acronis Internet Security Suite 2010.
Registro	Le permite introducir su número de serie y ver el estado de registro.
Soporte	Le permite ponerse en contacto con el equipo de soporte de Acronis.
Ayuda	Le da acceso a un fichero de ayuda que le enseña como utilizar Acronis Internet Security Suite 2010.

Enlace	Descripción
Logs	Le permite ver un historial detallado sobre las tareas que Acronis Internet Security Suite 2010 ha realizado en su sistema.

6.3. Configurando Acronis Internet Security Suite 2010

Acronis Internet Security Suite 2010 le permite configurar fácilmente su configuración principal y la interfaz de usuario configurando un perfil de uso. El perfil de uso refleja las principales actividades realizadas en el el equipo. Dependiendo del perfil de uso, la interfaz de producto se organiza para permitir el acceso fácilmente a sus tarea preferidas.

Por defecto, el perfil **Típico** se aplica después de que se instale Acronis Internet Security Suite 2010. Este perfil es adecuado para los equipos que se utilizan principalmente para navegar y actividades multimedia.

Para reconfigurar el perfil de uso, siga estos pasos:

1. Abrir Acronis Internet Security Suite 2010.
2. Haga clic en el botón **Ajustes** en la esquina superior derecha de la ventana.
3. En la categoría de configuración de interfaz de usuario, haga click en **Reconfigurar perfil**.
4. Siga el asistente de configuración.

6.3.1. Paso 1 - Seleccione el Perfil de Uso

Perfil de Uso

Haga clic en el botón que mejor describe las actividades realizadas en este equipo (el perfil de uso)

Opción	Descripción
Típica	Haga clic aquí si este PC es utilizado principalmente para navegar y actividades multimedia.
Padre	Haga clic aquí si este PC es utilizado por niños y desea controlarle el acceso a Internet utilizando el módulo de Control Parental.
Jugador	Haga clic aquí si este PC se utiliza principalmente para juegos.
Personalizado	Haga clic aquí si desea configurar todas las configuraciones principales de Acronis Internet Security Suite 2010.

Puede reiniciar más tarde el perfil de uso desde la interfaz de producto.

6.3.2. Paso 2 - Descripción del Equipo

Descripción del equipo

Seleccionar las opciones a aplicar a su equipo:

- **Este equipo esta en una red.** Seleccione esta opción si desea administrar remotamente (desde otro equipo) el producto de Acronis instalado en este equipo. Un asistente adicional le permitirá configurar el módulo de Administración de Red.
- **Este equipo es un portátil.** Seleccione esta opción si desea tener activado el Modo Portátil por defecto. Mientras este en Modo Portátil, las tareas de análisis planificadas no se ejecutarán, una de ellas requiere más recursos del sistema, implícitamente e incremento de energía.

Haga clic en **Siguiente** para continuar.

6.3.3. Paso 3 - Seleccione la Interfaz de Usuario

Modos de Vista de la Interfaz de Usuario

Haga clic en el botón que mejor describe su conocimiento de equipo para seleccionar la interfaz de usuario apropiada. Puede seleccionar la vista de la interfaz de usuario mediante tres modos, dependiendo de sus conocimientos y su experiencia con Acronis Internet Security Suite 2010.

Modo	Descripción
Modo Básico	Adecuado para gente principiante que desea que Acronis Internet Security Suite 2010 proteja su equipo y sus datos sin ser molestado. Este modo es simple de utilizar y requiere una mínima interacción por su parte. Todo lo que tiene que hacer es reparar todas las incidencias que existan cuando se lo indique Acronis Internet Security Suite 2010. Un asistente intuitivo le guiará paso a paso para reparar estas incidencias. Además, puede realizar tareas comunes, como una actualización de firmas de virus de Acronis Internet Security Suite 2010 y archivos de producto o análisis del equipo.
Modo Intermedio	Dirigido a usuarios con conocimientos medios, este modo extiende lo que puede hacer en el Modo Básico.

Modo	Descripción
	Puede reparar incidencias por separado y seleccionar que incidencias van a ser monitorizadas. Además, puede administrar remotamente los productos de Acronis instalados en los equipos de su red.
Modo Avanzado	Diseñado para usuarios más técnicos, este modo permite configurar completamente cada función de Acronis Internet Security Suite 2010. Puede utilizar todas las tareas proporcionadas para proteger su equipo y sus datos.

6.3.4. Paso 4 - Configurar el Control Parental

Nota

Este paso aparece sólo si ha seleccionado la opción **Personalizar** en el Paso 1.

Configuración del Control Parental

El Control Parental de le permite controlar el acceso a Internet y a determinadas aplicaciones para cada una de las cuentas de usuario del sistema.

Si desea usar el Control Parental, siga estos pasos:

1. Seleccionar **Activar Control Parental**.

2. Si su cuenta de usuario de Windows es compartida con su hijo, seleccione la casilla correspondiente y escriba una contraseña en el campo correspondiente para proteger la configuración del Control Parental. Cualquiera que intente cambiar la configuración del Control Parental, debe introducir la contraseña que ha configurado.

Haga clic en **Siguiente** para continuar.

6.3.5. Paso 5 - Configurar Red Acronis

Nota
Este paso aparece sólo si tiene especificado que el equipo está conectado a una red en el Paso 2.

Configuración de red Acronis

Acronis Internet Security Suite 2010 le permite crear una red virtual de equipo en su casa y administrar los productos Acronis compatibles instalados en esta red.

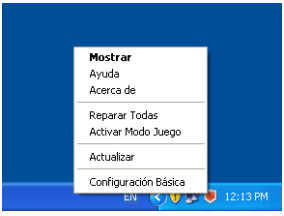
Si desea que este equipo forme parte de la Red de Administración de Acronis, siga estos pasos:

1. Seleccionar **Activar Red**.
2. Introduzca la misma contraseña de administración en cada uno de los campos editables. Esta contraseña permite que un usuario administrador gestione el producto Acronis desde otro equipo.

Haga clic en **Finalizar**.

6.4. Icono Barra de Tareas

Para administrar todo el producto más fácilmente, puede usar el icono Acronis en la barra de tareas. Si hace doble clic en este icono, se abrirá Acronis Internet Security Suite 2010. Además, haciendo clic derecho en el icono, un menú le permitirá administrar rápidamente Acronis Internet Security Suite 2010.



Icono Barra

- **Mostrar** - abre la interfaz principal de Acronis Internet Security Suite 2010.
- **Ayuda** - abre el fichero de ayuda, que explica en detalle como configurar y utilizar Acronis Internet Security Suite 2010.
- **Acerca de** - abre la ventana dónde puede verse información sobre Acronis Internet Security Suite 2010 y dónde encontrar ayuda en caso necesario.
- **Reparar Todas** - ayuda a eliminar las actuales vulnerabilidades de seguridad. Si esta opción no está disponible, no hay ninguna incidencia para reparar. Para más información, por favor, consulte el capítulo "*Reparar Incidencias*" (p. 34).
- **Activar / Desactivar Modo Juego** - activa / desactiva Modo Juego.
- **Actualizar** - realiza una actualización inmediata. Aparecerá una nueva ventana dónde podrá ver el estado de la actualización.
- **Ajuste Básicos** - abre una ventana donde puede cambiar la interfaz de modo de usuario y activar o desactivar los ajustes del producto principal. Para más información, por favor, consulte el apartado "*Configurando los Ajustes Básicos*" (p. 37).

El icono de Acronis en la barra de tareas le informa cuando una incidencia afecta a su equipo o como funciona el producto, mostrando un símbolo especial, como el siguiente:

Icono rojo con un signo de admiración: Incidencias crítica afectan a la seguridad de su sistema. Requieren su atención inmediata y deben ser reparadas lo antes posible.
Letra G: El producto funciona en Modo Juego.

Si Acronis Internet Security Suite 2010 no funciona, el icono de la barra de tareas aparecerá en gris. Esto sucede normalmente cuando la licencia caduca. También puede ocurrir cuando los servicios de Acronis Internet Suite 2010 no responden o cuando otros errores afectar al funcionamiento normal de Acronis Internet Security Suite 2010.

6.5. Barra de Actividad del Análisis

La **barra de análisis de la actividad** es una vista gráfica de la actividad de análisis de su sistema. Esta pequeña ventana esta disponible por defecto sólo en Modo Avanzado.

Las barras grises (**Archivos**) representan el número de archivos analizados por segundo, en una escala de 0 a 50. Las barras narajas mostradas en la zona **Internet** representan el número de KBytes transferidos (enviados y recibidos por Internet) por segundo, en una escala de 0 a 100.

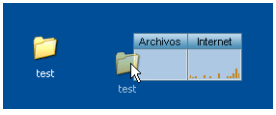
Barra de Actividad del Análisis

Nota
La Barra de Actividad del Análisis le avisará si la protección en tiempo real o el Cortafuego están desactivados, mostrando una cruz roja en la zona correspondiente (**Archivos** o **Internet**).

6.5.1. Analizar Ficheros y Carpetas

Puede utilizar la Barra de Actividad del Análisis para analizar rápidamente ficheros y carpetas. Arrastre el archivo o la carpeta que desea analizar y suéltelo sobre la **Barra de Actividad del Análisis**, tal y como se puede ver en las siguientes imágenes.

Arrastrar Archivo



Soltar Archivo

El Asistente de Análisis Antivirus aparecerá y le guiara por todo el proceso de análisis. Para información detallada acerca de este asistente, por favor consulte "*Asistente del análisis Antivirus*" (p. 45).

Configurar las opciones del análisis. Las opciones de análisis están preconfiguradas para mejores resultados de detección. Si se detectan ficheros

infectados, Acronis Internet Security Suite 2010 intentará desinfectarlos (eliminar el código malicioso). Si la desinfección falla, el Asistente de Análisis Antivirus le permitirá especificar otras acciones a realizar con los ficheros infectados. Las opciones de análisis son estándar y no las puede modificar.

6.5.2. Desactivar/Restaurar Barra de Actividad del Análisis

Para ocultar la barra de actividad haga clic derecho encima y seleccione **Ocultar**. Para restaurar la Barra de Actividad del Análisis, siga estos pasos:

1. Abrir Acronis Internet Security Suite 2010.
2. Haga clic en el botón **Ajustes** en la esquina superior derecha de la ventana.
3. En la categoría de Ajustes Generales, seleccione la casilla correspondiente para la **Barra de actividad de Análisis**.
4. Haga clic en **Ok** para guardar y aplicar los cambios.

6.6. Análisis manual de Acronis

El Análisis Manual de Acronis le premite analizar una carpeta específica o una partición del disco duro sin tener que crear una tarea de análisis. Esta característica ha sido diseñada para ser utilizada cuando Windows se ejecuta en Modo Seguro. Si su sistema está infectado con un virus residente, puede intentar eliminarlo iniciando Windows en Modo Seguro y analizando cada partición de su disco duro utilizando el Análisis Manual de Acronis.

Para acceder al Análisis Manual de Acronis, usa el menú de Inicio de Windows, siguiendo la ruta **Inicio → Programas → Acronis → Acronis Internet Security Suite 2010 → Acronis Análisis Manual** Aparecerá la siguiente pantalla:

Análisis manual de Acronis

Haga clic en **Añadir Carpeta**, seleccione la ubicación que desea analizar y haga clic en **Aceptar**. Si desea analizar múltiples carpetas, repita esta acción para cada ubicación adicional.

Las rutas de las ubicaciones seleccionadas aparecerán en la columna **Ruta**. Si cambia de idea y desea eliminar alguno de los elementos seleccionados, simplemente haga clic en el botón **Quitar** situado junto a este elemento. Haga clic en el botón **Eliminar todas las Rutas** para eliminar todas las ubicaciones que están en la lista.

Cuando ha seleccionado las ubicaciones, haga clic en **Continuar**. El Asistente de Análisis Antivirus aparecerá y le guiara por todo el proceso de análisis. Para información detallada acerca de este asistente, por favor consulte "*Asistente del análisis Antivirus*" (p. 45).

Configurar las opciones del análisis. Las opciones de análisis están preconfiguradas para mejores resultados de detección. Si se detectan ficheros infectados, Acronis Internet Security Suite 2010 intentará desinfectarlos (eliminar el código malicioso). Si la desinfección falla, el Asistente de Análisis Antivirus le permitirá especificar otras acciones a realizar con los ficheros infectados. Las opciones de análisis son estándar y no las puede modificar.

¿Qué es el Modo Seguro?
El Modo Seguro es una manera especial de iniciar Windows, utilizado normalmente para solucionar incidencias que afectan el funcionamiento normal de Windows.

Estos problemas pueden ser desde drivers conflictivos hasta virus que impidan el inicio normal de Windows. En Modo Seguro, Windows inicia sólo un mínimo de componentes y drivers básicos. Sólo algunas aplicaciones funcionan en Modo Seguro. Por esta razón los virus están inactivos en Modo Seguro y pueden ser eliminados fácilmente.
Para iniciar Windows en Modo Seguro, reinicie el equipo y presione la tecla F8 hasta que aparezca el Menú de Opciones Avanzadas de Windows. Puede elegir varias opciones para iniciar Windows en Modo Seguro. Puede seleccionar **Modo Seguro con Funciones de Red** con tal de tener acceso a Internet.

Nota

Para más información acerca del Modo Seguro, puede dirigirse a la Ayuda de Windows y Centro de Soporte (el menú Inicio, haga click en **Ayuda y Soporte**). También puede encontrar información de utilidad buscando en Internet.

6.7. Modo Juego y Modo Portátil

Algunas de las actividades del equipo, como juegos o presentaciones, requieren una mayor respuesta e incremento del sistema, y no interrupciones. Cuando el portátil está funcionando con la batería, es mejor que las operaciones innecesarias, que consumen más energía, se aplacen hasta que el portátil está conectado de nuevo a la corriente.

Para adaptarse a estas situaciones particulares, Acronis Internet Security Suite 2010 incluye dos modos de trabajar:

- Modo Juego
- Modo Portátil

6.7.1. Modo Juego

El Modo Juego modifica temporalmente las opciones de seguridad para minimizar su impacto sobre el rendimiento del sistema. Cuando activa el Modo Juego, se aplica la siguiente configuración:

- Minimiza el consumo de procesador y memoria
- Pospone las tareas de análisis y actualización
- Elimina todas las alertas y ventanas emergentes
- Analiza sólo los archivos más importantes

Mientras en Modo Juego, puede ver la letra G sobre el icono Acronis.

Usando el Modo Juego

Por defecto, Acronis Internet Security Suite 2010 automáticamente entra en Modo Juego cuando inicia un juego desde la lista de juegos conocidos o cuando una

aplicación va a pantalla completa. Acronis Internet Security Suite 2010 volverá automáticamente al modo de operación normal cuando cierre el juego o cuando se detecte que se ha salido de una aplicación en pantalla completa.

Si desea activar manualmente el Modo Juego, utilice uno de los siguientes métodos:

- Clic derecho en el icono de Acronis de la Bandeja del Sistema y seleccione **Activar Modo Juego**.
- Pulse `Ctrl+Shift+Alt+G` (el atajo de teclado predeterminado).

Importante

No olvide desactivar el Modo Juego una vez haya terminado. Para desactivarlo puede seguir los mismos pasos que ha utilizado para activarlo.

Cambiando el Atajo de Teclado del Modo Juego

Si desea cambiar el atajo de teclado, siga estos pasos:

1. Abra Acronis Internet Security Suite 2010 y cambie la interfaz de usuario al Modo Avanzado.
2. Haga click en **Modo Juego / Portátil** en el menú de la izquierda.
3. Haga clic en la pestaña **Modo Juego**.
4. Haga clic en el botón **Opciones Avanzadas**.
5. Debajo de la opción **Usar Atajos de Teclado**, configure la combinación de teclas deseada:
   - Elija las teclas que desea utilizar seleccionado alguna de las siguientes: Control (`Ctrl`), Shift (`Shift`) o Alternate (`Alt`).
   - En el campo editable, escriba la tecla que desea utilizar en combinación con la tecla indicada en el paso anterior.

   Por ejemplo, si desea utilizar la combinación de teclas `Ctrl+Alt+D`, marque sólo `Ctrl` y `Alt`, y a continuación escriba la tecla `D`.

   Nota

   Si desmarca la casilla correspondiente a **Usar Atajos de Teclado**, desactivará la combinación de teclas.

6. Haga clic en **Aceptar** para guardar los cambios.

6.7.2. Modo Portátil

El Modo Portátil está especialmente para usuarios de portátiles. Su objetivo es minimizar el impacto de Acronis Internet Security Suite 2010 en el consumo de energía cuando estos dispositivos funcionan con batería. Mientras este en Modo

Portátil, las tareas de análisis planificadas no se ejecutarán, una de ellas requiere más recursos del sistema, implícitamente e incremento de energía.

Acronis Internet Security Suite 2010 detecta cuando su portátil hace uso de la batería y activa automáticamente el Modo Portátil. Asimismo, Acronis Internet Security Suite 2010 desactivará automáticamente el Modo Portátil cuando detecte que el portátil ha dejado de funcionar con batería.

Para activar el Modo Portátil en Acronis Internet Security Suite 2010, siga estos pasos:

1. Abrir Acronis Internet Security Suite 2010.
2. Haga clic en el botón **Ajustes** en la esquina superior derecha de la ventana.
3. En la categoría de Ajustes Generales, seleccione la casilla correspondiente para la **Detección de Modo Portátil**.
4. Haga clic en **Ok** para guardar y aplicar los cambios.

6.8. Detección Automática de dispositivos.

Acronis Internet Security Suite 2010 detecta automáticamente al conectar un dispositivo de almacenamiento extraíble a su equipo y ofrece un análisis antes de acceder a los archivos. Le recomendamos con el fin de evitar virus y otro malware que infecten a su equipo.

La detección de dispositivos se dividen en una de estas categorías:

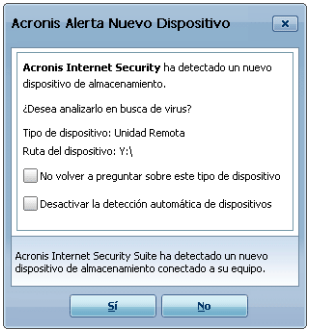
- Cds/DVDs
- Dispositivos de almacenamiento USB, como lápices flash y discos duros externos.
- Unidades de red (remotas) mapeadas.

Cuando un dispositivo es detectado, se visualizará una ventana de alerta.

Para analizar el dispositivo de almacenamiento, haga clic **Si**. El Asistente de Análisis Antivirus aparecerá y le guiara por todo el proceso de análisis. Para información detallada acerca de este asistente, por favor consulte "*Asistente del análisis Antivirus*" (p. 45).

Si no desea analizar un dispositivo, debe hacer clic en **No**. En este caso, puede encontrar una de estas opciones útiles:

- **No volver a preguntar acerca de este tipo de dispositivo** - Acronis Internet Security Suite 2010 no volverá a analizar estos tipos de dispositivos de almacenamiento cuando estén conectados a su equipo.



Detección de Dispositivos

- **Desactivar la detección automática de dispositivo** - No se le pedirá analizar nuevos dispositivos de almacenamiento cuando estén conectados a su equipo.

Si accidentalmente desactiva la detección automática de dispositivos y desea activarlo, o si desea configurar ajustes, siga estos pasos:

1. Abra Acronis Internet Security Suite 2010 y cambie la interfaz de usuario al Modo Avanzado.
2. Vaya a **Antivirus>Análisis de Virus**.
3. En la lista de tareas de análisis, localice la tarea de **Análisis de detección de dispositivos**.
4. Haga clic derecho sobre la tarea y seleccione **Abrir**. Aparecerá una nueva ventana.
5. En la pestaña **Descripción General**, configure las opciones de análisis que necesite. Para más información, por favor, consulte el capítulo "*Configurando las Opciones de Análisis*" (p. 128).
6. En la pestaña **Detección**, elija que tipos de dispositivos de almacenamiento serán detectados.
7. Haga clic en **Ok** para guardar y aplicar los cambios.

7. Reparar Incidencias

Acronis Internet Security Suite 2010 utiliza un sistema de seguimiento de incidencias para detectar e informarle acerca de las incidencias que pueden afectar a la seguridad de su equipo y datos. Por defecto, monitorizará sólo una serie de incidencias que están consideradas como muy importantes. Sin embargo, puede configurar según su necesidad, seleccionando que incidencias específicas desea que se le notifique.

Así es como se notifican las incidencias pendientes:

- Un símbolo especial se mostrará sobre el icono de Acronis en la barra de herramientas para indicarle las incidencias pendientes.

  Icono rojo con un signo de admiración: Incidencias crítica afectan a la seguridad de su sistema. Requieren su atención inmediata y deben ser reparadas lo antes posible.

  Además, si mueve el cursor del ratón encima del icono, una ventana emergente le confirmará la existencia de incidencias pendientes.

- Cuando abre Acronis Internet Security Suite 2010, el área de Estado de Seguridad le indicará el número de incidencias que afectan a su sistema.

  ▶ En el Modo Intermedio, el estado de seguridad se muestra en la pestaña de **Panel de Control**.

  ▶ En Modo Avanzado, vaya a **General>Panel de Control** para comprobar el estado de seguridad.

7.1. Asistente para Reparar Todas las Incidencias

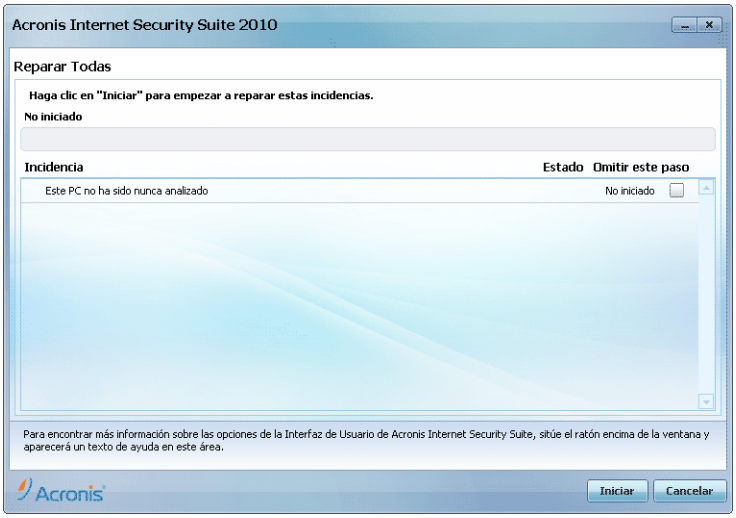
La forma más fácil de reparar las incidencias existentes es siguiendo paso a paso el asistente **Reparar Todas**. El asistente ayuda a eliminar fácilmente amenazas en su equipo y seguridad de los datos. Para abrir el asistente, realice lo siguiente:

- Haga clic derecho en el icono Acronis en la barra de tareas y seleccione **Reparar Todas**.
- Abrir Acronis Internet Security Suite 2010. Dependiendo del modo de interfaz de usuario, proceda de la siguiente manera:

  ▶ En Modo Básico, haga clic en **Reparar Todas**.

  ▶ En Modo Intermedio, vaya a la pestaña **Visor Estado** y haga clic **Reparar Todas**.

  ▶ En Modo Avanzado, vaya a **General>Visor Estado** y haga clic en **Reparar Todas**.



Asistente para Reparar Todas las Incidencias

El asistente muestra la lista de las vulnerabilidad de seguridad existente en su equipo.

Todas las incidencias actuales que están seleccionadas se repararan. Si esta es una incidencia que no desea reparar, sólo seleccione la casilla correspondiente. Si lo hace, el estado cambiará a **Omitir**.

Nota

Si no desea que se le notifique acerca de incidencias especificas, debe configurar la monitorización del sistema en consecuencia, como se describe en la siguiente sección.

Para reparar las incidencias seleccionadas, haga clic en **Iniciar**. Algunas incidencias se reparan inmediatamente. Para otras, un asistente le ayuda a repararlas.

Las incidencias que este asistente le ayuda a reparar pueden ser agrupadas dentro de estas principales categorías:

- **Desactivar configuración de seguridad.** Estas incidencias se reparan inmediatamente, al permitir la configuración de seguridad respectiva.
- **Tareas preventivas de seguridad que necesita realizar.** Un ejemplo de como una tarea analiza su equipo. Recomendamos que analice su equipo una vez a la semana. Acronis Internet Security Suite 2010 hará esto automáticamente por usted en la mayoría de casos. Además, si ha cambiado la planificación del análisis o si la planificación no está completada, se le notificará sobre esta incidencia.

Cuando repara estas incidencias, un asistente le ayuda a completar la tarea con éxito.

- **Vulnerabilidades del Sistema.** Acronis Internet Security Suite 2010 comprueba automáticamente las vulnerabilidades de su sistema y le avisa sobre ellas. Las vulnerabilidades del sistema son las siguientes:

  ▶ contraseñas inseguras de cuentas de usuario de Windows.

  ▶ software obsoleto en su equipo.

  ▶ Actualizaciones de Windows que faltan.

  ▶ Las Actualizaciones Automáticas de Windows están desactivadas.

  Cuando estas incidencias están para reparar, el asistente de análisis de vulnerabilidad se inicia. Este asistente le ayuda a reparar las vulnerabilidades del sistema detectadas. Para información detallada, diríjase a la sección "*Asistente de Análisis de Vulnerabilidad*" (p. 57).

7.2. Configurando Seguimiento de Incidencias

El sistema de seguimiento de incidencias está pre-configurado para monitorizar y alertarle acerca de los problemas más importantes que pueden afectar a la seguridad y los datos de su equipo. El resto de problemas, serán monitorizados en base a su elección en el Asistente de configuración (cuando usted configura su perfil de uso). Además de las incidencias monitorizadas por defecto, hay otras incidencias que le pueden informar acerca de estas.

Puede configurar el sistema de seguimiento para un mejor servicio para la seguridad que necesita escogiendo que incidencias especificas serán informadas. Puede hacerlo en Modo Intermedio o en Modo Avanzado.

- En Modo Intermedio, el sistema de seguimiento puede ser configurado desde ubicaciones separadas. Siga estos pasos:
  1. Diríjase a **Seguridad**, **Parental** o la pestaña **Cifrado**.
  2. Haga click en **Configurar alertas de estado**.
  3. Seleccione la casilla correspondiente a las incidencias que desea que sean monitorizadas.

  Para más información, por favor, consulte el capitulo "Modo Intermedio" (p. 83) de esta guía de usuario.

- En Modo Avanzado, el seguimiento de sistema puede ser configurado desde una ubicación central. Siga estos pasos:
  1. Vaya a **General>Cuadro de mandos**.
  2. Haga click en **Configurar alertas de estado**.
  3. Seleccione la casilla correspondiente a las incidencias que desea que sean monitorizadas.

  Para información detallada, por favor diríjase al apartado "*Visor Estado*" (p. 105).

8. Configurando los Ajustes Básicos

Puede configurar los ajustes principales del producto (incluyendo el cambio del modo de vista de la interfaz de usuario) de la ventana de ajustes básicos. Para abrirlo, realice cualquiera de los siguientes:

- Abra Acronis Internet Security Suite 2010 y haga clic en el botón **Configuración** en la esquina superior derecha de la ventana.
- Haga clic derecho en el icono Acronis y seleccione en la barra de tareas y seleccione **Configuración Básica**.

Nota

Para configurar el producto en detalle, utilice la interfaz de Modo Avanzado. Para más información, por favor, consulte el capítulo "Modo Avanzado" (p. 104) de esta guía de usuario.

Configuración Básica

Los ajustes se organizan en tres categorías:

- Ajustes de Interfaz de Usuario
- Ajustes de Seguridad
- Configuración General

Para aplicar y guardar los cambios que ha realizado, haga clic en **Aceptar**. Para cerrar la ventana sin guardar los cambios, haga clic en **Cancelar**.

8.1. Configuraciones de Interfaz de Usuario

En esta área, puede cambiar la vista de la interfaz de usuario y restaurar el perfil de usabilidad.

Cambiar la vista de la interfaz de usuario. Cómo se describe en la sección "*Modos de Vista de la Interfaz de Usuario*" (p. 12), estos son tres modos de ver la interfaz de usuario. Cada modo de interfaz de usuario está diseñada para un categoría de usuario especifica, basada en los conocimientos de cada uno de ellos. De esta manera, la interfaz de usuario se adapta a todas las clases de usuario, desde usuarios principiantes a muy técnicos

El primer botón muestra la actual vista de la interfaz de usuario. Cambiar la interfaz de usuario, haga clic en la flecha del botón y seleccione el modo deseado desde el menú.

Modo	Descripción
Modo Básico	Adecuado para gente principiante que desea que Acronis Internet Security Suite 2010 proteja su equipo y sus datos sin ser molestado. Este modo es simple de utilizar y requiere una mínima interacción por su parte. Todo lo que tiene que hacer es reparar todas las incidencias que existan cuando se lo indique Acronis Internet Security Suite 2010. Un asistente intuitivo le guiará paso a paso para reparar estas incidencias. Además, puede realizar tareas comunes, como una actualización de firmas de virus de Acronis Internet Security Suite 2010 y archivos de producto o análisis del equipo.
Modo Intermedio	Dirigido a usuarios con conocimientos medios, este modo extiende lo que puede hacer en el Modo Básico. Puede reparar incidencias por separado y seleccionar que incidencias van a ser monitorizadas. Además, puede administrar remotamente los productos de Acronis instalados en los equipos de su red.
Modo Avanzado	Diseñado para usuarios más técnicos, este modo permite configurar completamente cada función de Acronis Internet Security Suite 2010. Puede utilizar todas las tareas proporcionadas para proteger su equipo y sus datos.

Reconfigurando el perfil de uso. El perfil de uso refleja las principales actividades realizadas en el el equipo. Dependiendo del perfil de uso, la interfaz de producto se organiza para permitir el acceso fácilmente a sus tarea preferidas.

Para reconfigurar el perfil de uso, haga click en **Reconfigurar perfil** y siga el asistente de configuración.

8.2. Ajustes de Seguridad

En esta área, puede activar o desactivar los ajustes del producto que cubren varios aspectos de la seguridad de datos y del equipo. El actual estado de una configuración está indicado mediante uno de estos iconos:

Círculo Verde con una marca de verificación: La configuración está activada.
Circulo Rojo con un marca de exclamación: La configuración está desactivada.

Para activar/desactivar una configuración, marcar/desmarcar la correspondiente casilla de **Activar**.

Aviso

Preste especial atención a la hora de desactivar la protección en tiempo real antivirus, el cortafuego o la actualización automática. Desactivar estas opciones puede afectar a la seguridad de su equipo. Si realmente necesita desactivarlas, recuerde reactivarlas lo antes posible.

Toda la lista de configuraciones y su descripción se muestra en la siguiente tabla:

Configuración	Descripción
Antivirus	La protección en Tiempo Real asegura que todos los archivos que son analizados son accesibles por usted o por una aplicación en ejecución en su sistema.
Actualización Automática	La Actualización Automática asegura que los productos y firmas de archivos de Acronis Internet Security Suite 2010 más recientes se descargan e instalan automáticamente de forma regular.
Análisis de Vulnerabilidad	La Comprobación Automática de Vulnerabilidades comprueba si el software crucial de su PC está actualizado.
Antispam	Los filtros Antispam de los correos que recibe, marca el correo no deseado y el correo basura como SPAM.
Antiphishing	La Protección Antiphishing Web en Tiempo Real detecta y le alerta si una página web está configurada para robar información personal.

Configuración	Descripción
Control de Identidad	El Control de Identidad le ayuda a preservar que sus datos personales no se envíen por Internet sin su consentimiento. Bloquea cualquier mensaje instantáneo, correo o formularios web que trasmitan datos definidos como privados a receptores no autorizados (direcciones).
Cifrado de IM	El cifrado IM (Mensajeria Instantanea) asegura sus conversaciones a través de Yahoo! Messenger y Windows Live Messenger, siempre que sus contactos de IM utilicen un producto de Acronis y software IM compatible .
Control Parental	El Control Parental restringe el equipo y las actividades online de sus hijos basados en las reglas que usted ha definido. Las restricciones deben incluir el bloqueo de páginas web inapropiadas, así como la limitación de juego y acceso a Internet de acuerdo con la planificación especificada.
Cortafuego	El Cortafuego protege su equipo frente a hackers y ataques externos.
Cifrado de Archivo	El cifrado de Archivo mantiene sus documentos confidenciales cifrados en unidades blindadas especiales. Si desactiva el Cifrado de Archivo, se bloquearán todos los blindajes existentes y no podrá acceder a los archivos que contienen.

El estado de algunos de estos ajustes pueden ser monitorizados por el sistema de seguimiento de incidencias de Acronis Internet Security Suite 2010. Si desactiva una configuración monitorizada, Acronis Internet Security Suite 2010 le indicará que está es una incidencia que necesita repararse.

Si no desea que se monitoricen las configuraciones que están desactivadas que se muestran como incidencias, puede configurar el sistema de seguimiento de acuerdo con la incidencia. Puede hacerlo tanto en Modo Intermedio como en Modo Avanzado.

- En Modo Intermedio, el sistema de seguimiento puede ser configurado desde ubicaciones separadas, dependiendo de la configuración de las categorías. Para más información, por favor, consulte el capitulo “Modo Intermedio” (p. 83) de esta guía de usuario.
- En Modo Avanzado, el seguimiento de sistema puede ser configurado desde una ubicación central. Siga estos pasos:
  1. Vaya a **General>Cuadro de mandos**.

2. Haga click en **Configurar alertas de estado**.
3. Desmarcar la casilla correspondiente en el elemento que no desea ser monitorizado.

Para información detallada, por favor diríjase al apartado "*Visor Estado*" (p. 105).

8.3. Configuración General

En esta área, puede activar o desactivar la configuración que afecta al comportamiento del producto y la experiencia del usuario. Para activar/desactivar una configuración, marcar/desmarcar la correspondiente casilla de **Activar**.

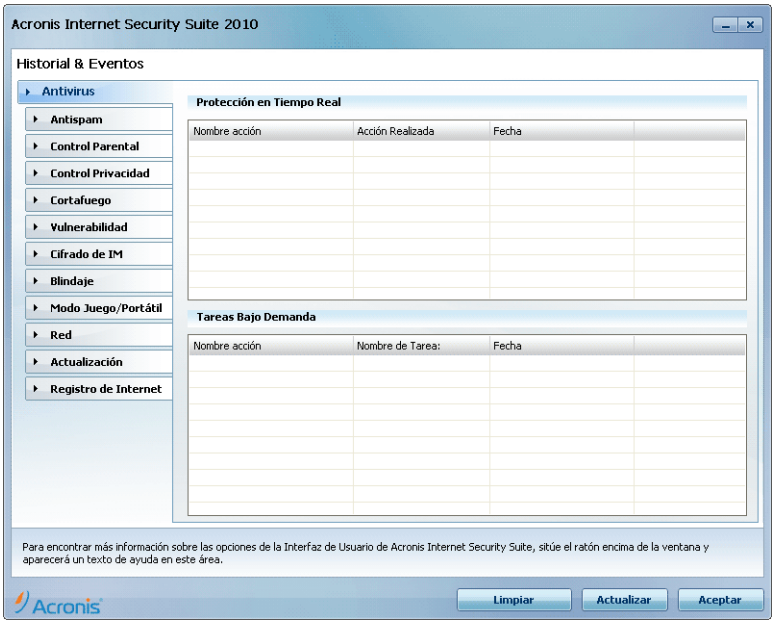
Toda la lista de configuraciones y su descripción se muestra en la siguiente tabla:

Configuración	Descripción
Modo Juego	El Modo Juego modifica temporalmente las opciones de seguridad para minimizar su impacto y sacar el máximo rendimiento a su experiencia de juego.
Detección Modo Portátil	El Modo Portátil modifica temporalmente las opciones de seguridad para modificar su impacto y prolongar la duración de su batería.
Contraseña de la Configuración	Al activar esta opción, protegerá la configuración de Acronis Internet Security Suite 2010 de modo que sólo pueda modificarla la persona que conozca la contraseña. Cuando active esta opción, se le pedirá configurar una contraseña. Escriba la contraseña deseada en ambos campos y haga clic en **Aceptar** para establecer la contraseña.
Notícias de Acronis Internet Security Suite	Active esta opción si desea recibir noticias importantes sobre Acronis, las actualizaciones del producto y las nuevas amenazas de seguridad.
Alertas de Notificación del Producto	Al activar esta opción, recibirá alertas de información sobre la actividad del producto.
Barra de Actividad del Análisis	La Barra de Actividad del Análisis es una ventana pequeña y transparente que indica el progreso de la actividad de análisis de Acronis Internet Security Suite 2010. Para más información, por favor, consulte el capítulo "*Barra de Actividad del Análisis*" (p. 27).
Enviar Informes de Virus	Al activar esta opción, enviará informes de análisis virus a los Laboratorios Acronis para su análisis. Los informes no contienen datos confidenciales, como su

Configuración	Descripción
	nombre, dirección IP u otros datos, ni se usarán con fines comerciales.
Detección de Epidemias	Al activar esta opción, enviará informes sobre amenazas potenciales a los Laboratorios Acronis para su análisis. Los informes no contienen datos confidenciales, como su nombre, dirección IP u otros datos, ni se usarán con fines comerciales.

9. Historial y Eventos

El enlace **Logs** en la parte superior de la ventana principal de Acronis Internet Security Suite 2010 abre otra ventana con el historial & eventos de Acronis Internet Security Suite 2010. Esta ventana le ofrece una vista precia de los eventos relacionados con la seguridad. Por ejemplo, puede comprobar fácilmente si la actualización se ha realizado con éxito, si se ha encontrado malware en su equipo, etc.



Eventos

Para ayudarle a filtrar el historial y eventos de Acronis Internet Security Suite 2010, se muestran las siguientes categorías en la parte izquierda:

- **Antivirus**
- **Antispam**
- **Control Parental**
- **Control de Privacidad**
- **Cortafuego**
- **Vulnerabilidad**
- **Cifrado de IM**
- **Cifrado de Archivo**

- **Modo Juego/Portátil**
- **Red**
- **Actualización**
- **Registro de Internet**

Dispone de una lista de eventos para cada categoría. Cada evento incluye la siguiente información: un descripción breve, la acción realizada por Acronis Internet Security Suite 2010, su resultado, y la fecha y hora en que se ha producido. Si desea más información sobre un evento en particular, haga clic encima del mismo.

Haga clic en **Limpiar Log** si desea eliminar los registros antiguos, o en **Actualizar** para asegurarse que se visualizan los últimos registros.

10. Asistentes

Con el fin de que Acronis Internet Security Suite 2010 sea muy fácil de usar, varios asistentes le ayudan a llevar acabo tareas especificas de seguridad o configurar los ajustes de productos más complejos. En este capítulo se describen los asistentes que le pueden aparecer cuando repara incidencias o realiza tareas específicas con Acronis Internet Security Suite 2010. Otros asistentes de configuración se describen separadamente en la "Modo Avanzado" (p. 104) parte.

10.1. Asistente del análisis Antivirus

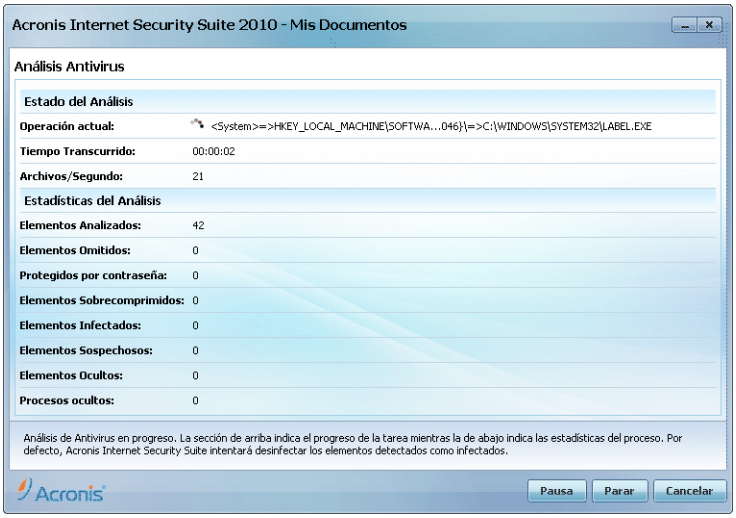
Siempre que inicie un análisis bajo demanda (por ejemplo, botón derecho sobre una carpeta y seleccionar **Analizar con Acronis Internet Security Suite**), aparecerá el asistente de Análisis Antivirus. Siga el proceso guiado de tres pasos para completar el proceso de análisis.

Nota

Si el asistente de análisis no aparece, puede que el análisis esté configurado para ejecutarse en modo silencioso, en segundo plano. Busque en el icono de progreso de análisis en la barra de tareas. Puede hacer clic en este icono para abrir la ventana de análisis y ver el progreso del análisis.

10.1.1. Paso 1/3 – Analizando

Acronis Internet Security Suite 2010 comenzará el análisis de los objetos seleccionados.



Analizando

Puede ver el estado y las estadísticas del análisis (velocidad de análisis, número de archivos analizados / infectados / sospechosos / objetos ocultos y otros).

Espere a que Acronis Internet Security Suite 2010 finalice el análisis.

Nota

El análisis puede llevar un tiempo, dependiendo de la compejidad del análisis.

Archivos protegidos por contraseña. Si Acronis Internet Security Suite 2010 detecta un archivo protegido por contraseña durante el análisis y la acción por defecto es **Solicitar contraseña**, se le pedirá introducir la contraseña. Los archivos comprimidos protegidos con contraseña no pueden ser analizados, a no ser que introduzca la contraseña. Tiene las siguientes opciones a su disposición:

- **Deseo introducir la contraseña para este objeto.** Si desea que Acronis Internet Security Suite 2010 analice el archivo, seleccione esta opción e introduzca la contraseña. Si no conoce la contraseña, elija una de las otras opciones.
- **No deseo introducir la contraseña para este objeto.** Marque esta opción para omitir el análisis de este archivo.
- **No deseo introducir la contraseña para ningún objeto (omitir todos los objetos protegidos por contraseña).** Seleccione esta opción si no desea que se le pregunte acerca de archivos protegidos por contraseña. Acronis Internet

Security Suite 2010 no podrá analizarlos, pero se guardará información acerca de ellos en el informe de análisis.

Haga clic en **Aceptar** para continuar el análisis.

Detener o pausar el análisis. Puede detener el análisis en cualquier momento, haciendo clic en botón **Parar**. Irá directamente al último paso del asistente. Para detener temporalmente el proceso de análisis, haga clic en **Pausa**. Para seguir con el análisis haga clic en **Reanudar**.

10.1.2. Paso 2/3 – Seleccionar Acciones

Cuando el análisis haya finalizado, aparecerá una nueva ventana donde podrá ver los resultados del análisis.

Acciones

Puede ver el número de incidencias que afectan a su sistema.

Los objetos infectados se muestran agrupados a partir del malware que los ha infectado. Haga clic en el enlace correspondiente a una amenaza para obtener más información sobre los objetos infectados.

Puede elegir una opción global que se aplicará a todas las incidencias, o bien elegir una opción por separado para cada una de las incidencias.

Una o varias de las siguientes opciones pueden aparecer en el menú:

Acción	Descripción
Ninguna Acción	No se realizará ninguna acción sobre los archivos detectados. Al finalizar el proceso de análisis, puede abrir el informe para ver información sobre estos archivos.
Desinfectar	Elimina el código de malware de los archivos infectados.
Eliminar	Elimina los archivos detectados.
Mover a Cuarentena	Traslada los archivos detectados a la cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado.
Renombrar ficheros	Renombra los ficheros ocultos añadiendo `.bd.ren` a su nombre. Como resultado, podrá buscar y encontrar estos ficheros en su equipo, en caso de que existan. Por favor tenga en cuenta que estos ficheros ocultos no son ficheros que usted ocultó de Windows. Son fichero ocultados por programas especiales, conocidos como rootkits. Los rootkits no son maliciosos por naturaleza. De todas maneras, son utilizados normalmente para hacer que los virus o spyware no sean detectados por programas normales antivirus.

Haga clic en **Continuar** para aplicar las acciones indicadas.

10.1.3. Paso 3/3 – Ver Resultados

Una vez Acronis Internet Security Suite 2010 ha finalizado la reparación de los problemas, aparecerán los resultados del análisis en una nueva ventana.

Sumario

Puede ver el resumen de los resultados. Si desea obtener información completa sobre el proceso de análisis, haga clic en **Mostrar Informe** para ver el informe de análisis.

Importante

En caso necesario, por favor, reinicie su equipo para completar el proceso de desinfección.

Haga clic en **Cerrar** para cerrar la ventana.

Acronis Internet Security Suite 2010 No Pudo Resolver Algunas Incidencias

En la mayoría de casos, Acronis Internet Security Suite 2010 desinfecta los archivos infectados detectados o aísla estos archivos en la Cuarentena. Sin embargo, algunas incidencias no pueden repararse.

En estos casos, le recomendamos que contacte con el equipo de soporte de Acronis en http://www.acronis.es/support/?ow=1. Nuestro equipo de representantes le ayudará a resolver las incidencias que experimente.

Acronis Internet Security Suite 2010 Detectó Archivos Sospechosos

Los archivos sospechosos son archivos detectados por el análisis heurístico como potencialmente infectados con malware, aunque su firma de virus todavía no se ha realizado.

Si durante el análisis se detectan archivos sospechosos, se le solicitará enviarlos a los Laboratorios de Acronis. Haga clic en **Aceptar** para enviar estos archivos al Laboratorio de Acronis para su posterior análisis.

10.2. Personalizar el Asistente de Análisis

El Asistente Personalizado de Análisis le ayuda a crear y ejecutar un tarea de análisis personalizada y opcionalmente guardar esta como una Tarea Rápida cuando utiliza Acronis Internet Security Suite 2010 en el Modo Intermedio.

Para ejecutar una tarea de análisis personalizada utilizando el Asistente de Personalización de Análisis debe seguir estos pasos:

1. En Modo Intermedio, diríjase a la pestaña **Seguridad**.
2. En el área Tareas Rápidas, haga clic en **Asistente de Análisis**.
3. Siga el proceso guiado para completar el proceso de análisis.

10.2.1. Paso 1/6 - Ventana de bienvenida

Esta es una ventana de bienvenida.

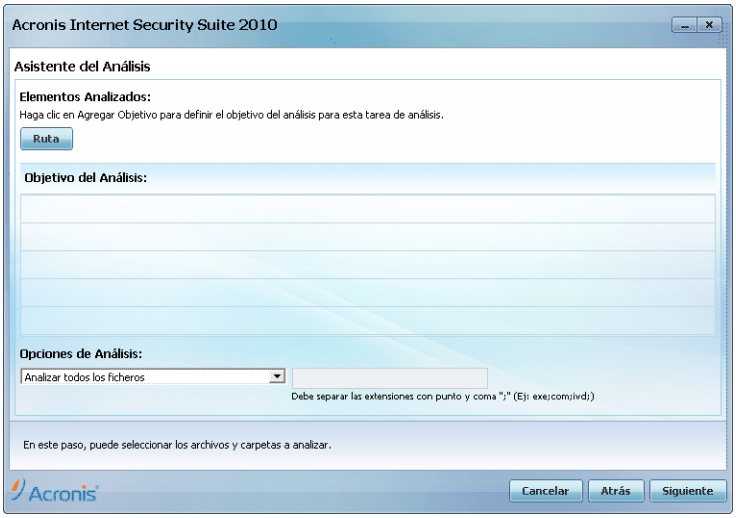
Ventana de Bienvenida

Si desea omitir esta ventana cuando ejecuta este asistente en el futuro, seleccione la casilla **No mostrar este paso la próxima vez que se ejecute este asistente**.

Haga clic en **Siguiente**.

10.2.2. Paso 2/6 - Seleccionar Ruta

Aquí puede especificar los archivos o carpetas que serán analizas así como las opciones de análisis.



Seleccionar Objetivo

Haga clic en **Añadir Ruta**, seleccione los archivos o carpetas que desea analizar y haga clic en **Aceptar**. Las rutas seleccionadas aparecerán en la columna **Ruta de Análisis**. Si cambia de idea y desea eliminar alguno de los elementos seleccionados, simplemente haga clic en el botón **Quitar** situado junto a este elemento. Haga clic en el botón **Eliminar Todas** para eliminar todas las ubicaciones que están en la lista.

Cuando termine de seleccionar las ubicaciones, ajuste las **Opciones de analisis**. Los siguiente están disponibles:

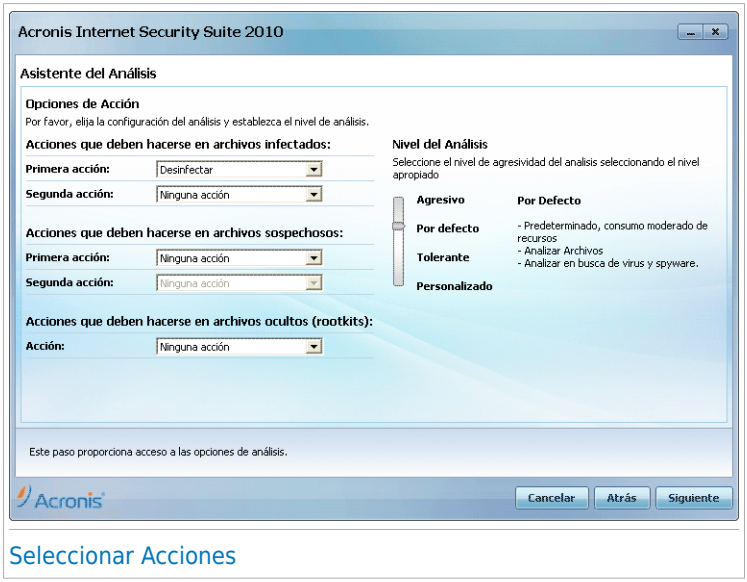
Opción	Descripción
Analizar todos los archivos	Seleccione esta opción para analizar todos los archivos de las carpetas seleccionadas.
Analizar sólo extensiones de aplicaciones	Únicamente se analizarán los archivos con las siguientes extensiones: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`;

Opción	Descripción
	.vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml y .nws.
Analizar sólo extensiones definidas por el usuario	Para analizar sólo los ficheros que tienen las extensiones especificadas por el usuario. Dichas extensiones deben estar separadas por ";".

Haga clic en **Siguiente**.

10.2.3. Paso 3/6 – Seleccionar Acciones

Aquí puede especificar la configuración del análisis y el nivel.



Seleccionar Acciones

- Seleccionar las acciones a realizar cuando se detecten archivos infectados y sospechosos. Tiene las siguientes opciones a su disposición:

Acción	Descripción
Ninguna Acción	No se realizará ninguna acción con los ficheros infectados. Estos ficheros aparecerán en el informe de análisis.

Acción	Descripción
Desinfectar archivos	Elimina el código de malware de los archivos infectados detectados.
Eliminar archivos	Elimina los archivos infectados inmediatamente y sin previa advertencia.
Mover a la Cuarentena	Para trasladar los archivos infectados a la cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado.

- Seleccione la acción a realizar en archivos ocultos (rootkits). Tiene las siguientes opciones a su disposición:

Acción	Descripción
Ninguna Acción	No se realizará ninguna acción con los archivos ocultos. Estos archivos aparecerán en el informe de análisis.
Renombrar	Renombra los ficheros ocultos añadiendo `.bd.ren` a su nombre. Como resultado, podrá buscar y encontrar estos ficheros en su equipo, en caso de que existan.

- Configurar agresividad del análisis. Existen 3 niveles para seleccionar. Arrastre el deslizador para fijar el nivel de protección apropiado:

Nivel del Análisis	Descripción
Tolerante	Solo archivos de aplicaciones serán analizados por virus. El nivel consumo de recursos es bajo.
Por Defecto	El nivel de consumo de recursos es moderado. Todos los archivos se analizan en busca de virus y spyware.
Agresivo	Todos las carpetas (incluso archivos) son analizadas en busca de virus y spyware. Los archivos ocultos y procesos son incluidos en el analisis, el nivel de consumo de recursos es alto.

Los usuarios avanzados pueden aprovecharse de las ventajas de configuración de análisis que ofrece Acronis Internet Security Suite 2010. El analisis puede ser ejecutado sólo en busca de amenazas específicas de malware. Esto puede reducir

mucho el tiempo de análisis y mejorar la respuesta de su equipo durante un análisis.

Mueva el control deslizante para seleccionar **Personalizar** y haga clic en el botón **Personalizar Nivel**. Aparecerá una ventana. Especifique el tipo de malware que desea que Acronis Internet Security Suite 2010 analice para seleccionar las opciones apropiadas:

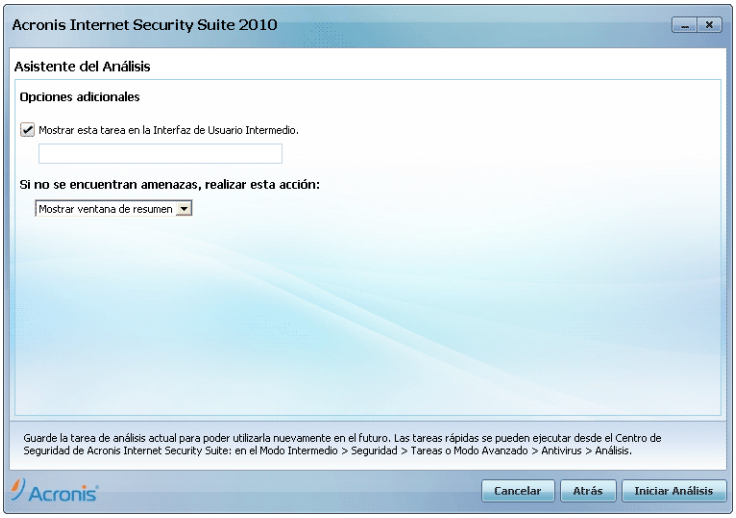
Opción	Descripción
Analizar en busca de virus	Analizar en busca de virus conocidos. Acronis Internet Security Suite 2010 detecta también cuerpos de virus incompletos, eliminando así cualquier posible amenaza que pueda afectar la seguridad de su sistema.
Analizar en busca de adware	Analiza en busca de adware. Estos archivos se tratarán como si fuesen archivos infectados. El software que incluya componentes adware puede dejar de funcionar si esta opción está activada.
Analizar en busca de spyware	Analiza en busca de spyware. Estos archivos se tratarán como si fuesen archivos infectados.
Analizar aplicaciones	Analiza en busca de aplicaciones legítimas que pueden utilizarse como herramientas de espionaje, para ocultar aplicaciones maliciosas u otros fines maliciosos.
Analizar en busca de dialers	Analiza en busca de dialers de números de alta tarificación. Estos ficheros se tratarán como fuesen si ficheros infectados. El software que incluya componentes dialer puede dejar de funcionar si esta opción está activada.
Analizar en busca de Rootkits	Analizar en busca de objetos ocultos (archivos y procesos), generalmente denominados rootkits.
Analizar en busca de keyloggers	Analiza en busca de aplicaciones maliciosas que graben las teclas pulsadas.

Haga clic en **Aceptar** para cerrar la ventana.

Haga clic en **Siguiente**.

10.2.4. Paso 4/6 - Configuraciones Adicionales

Antes de empezar el análisis, están disponibles estas opciones:



Configuraciones Adicionales

- Para guardar la tarea personalizada que ha creado para usarla en un futuro seleccione **Mostrar esta tarea en la Interfaz de Usuario Intermedio** marque la casilla e introduzca un nombre para la tarea en la casilla editable.

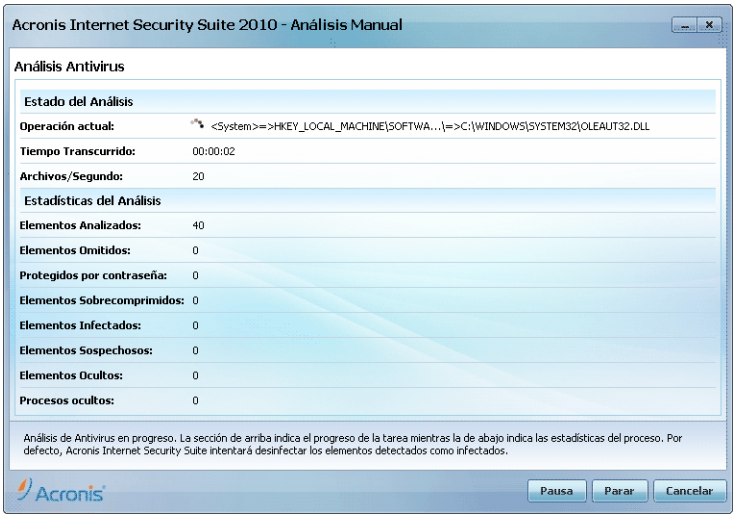
  La tarea será añadida a la lista de Tareas Rápidas ya disponible en la pestaña de Seguridad y aparecerá en **Modo Avanzado > Antivirus > Análisis**.

- Desde el menú correspondiente, seleccione una acción a realizar si no se detectan amenazas.

Haga clic en **Ejecutar Análisis**.

10.2.5. Paso 5/6 - Analizar

Acronis Internet Security Suite 2010 comenzará el análisis de los objetos seleccionados:



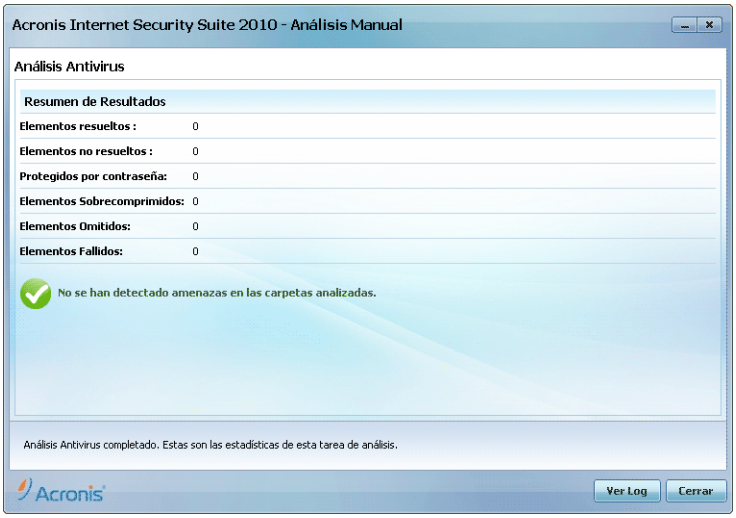
Analizando

Nota

El análisis puede llevar un tiempo, dependiendo de la compejidad del análisis. Puede hacer clic en el icono de progreso de análisis en la barra de tareas para abrir la ventana de análisis y ver el progreso del análisis.

10.2.6. Paso 6/6 – Ver Resultados

Cuando Acronis Internet Security Suite 2010 complete el análisis, los resultados del análisis aparecerán en una nueva ventana:



Sumario

Puede ver el resumen de los resultados. Si desea información completa sobre los resultados del análisis, haga clic en **Mostrar Informe** para ver el informe del análisis.

Importante
En caso necesario, por favor, reinicie su equipo para completar el proceso de desinfección.

Haga clic en **Cerrar** para cerrar la ventana.

10.3. Asistente de Análisis de Vulnerabilidad

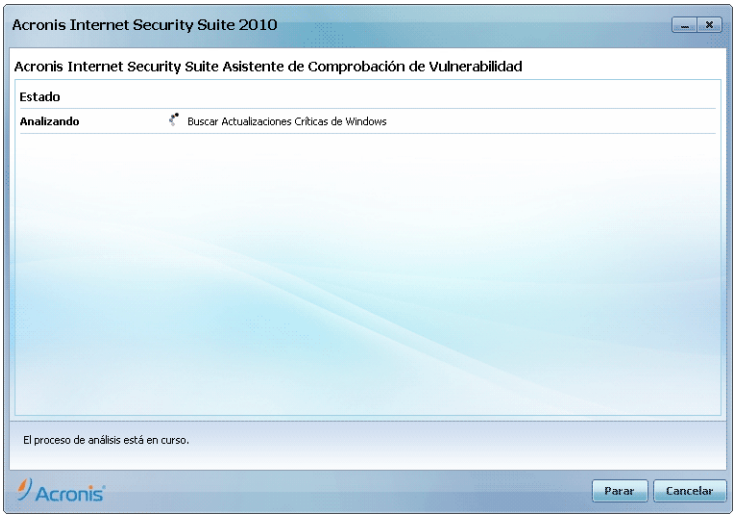
Este asistente comprueba las vulnerabilidades del sistema y le ayuda a repararlas.

10.3.1. Paso 1/6 – Seleccione las Vulnerabilidades a Comprobar

Vulnerabilidades

Haga clic en **Siguiente** para analizar su sistema en busca de las vulnerabilidades seleccionadas.

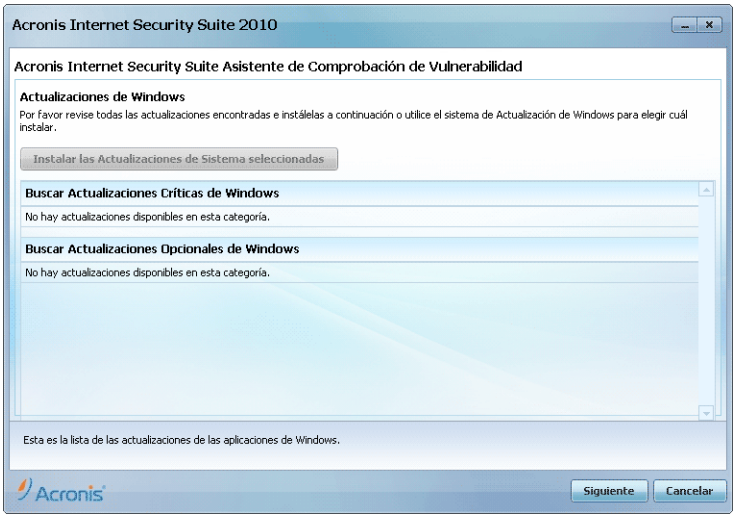
10.3.2. Paso 2/6 - Comprobando Vulnerabilidades



Comprobación de Vulnerabilidades

Espere hasta que Acronis Internet Security Suite 2010 finalice la comprobación de vulnerabilidades.

10.3.3. Paso 3/6 - Actualizar Windows



Actualizaciones de Windows

Puede ver la lista de las actualizaciones críticas y no-críticas que actualmente no están instaladas en su equipo. Haga clic en **Instalar Todas las Actualizaciones del Sistema** para instalar todas las actualizaciones disponibles.

Haga clic en **Siguiente**.

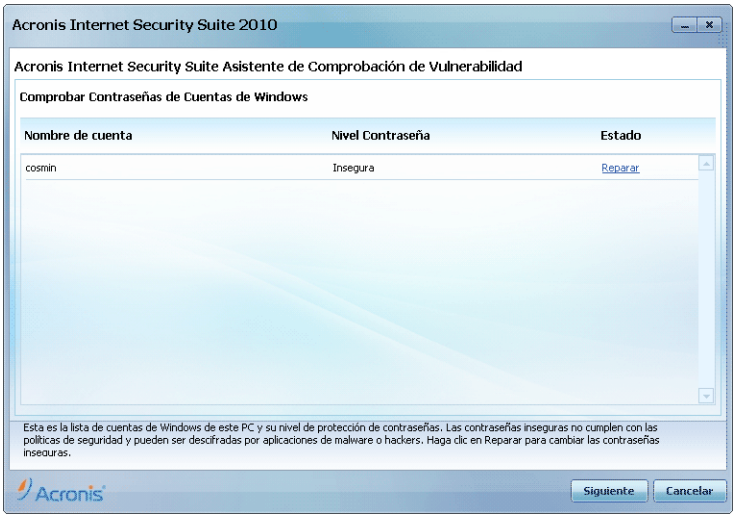
10.3.4. Paso 4/6 – Actualizar Aplicaciones

Aplicaciones

Puede ver la lista de todas las aplicaciones comprobadas por Acronis Internet Security Suite 2010 y su estado de actualización. Si una aplicación no está actualizada, haga clic en el enlace indicado para descargar la nueva versión.

Haga clic en **Siguiente**.

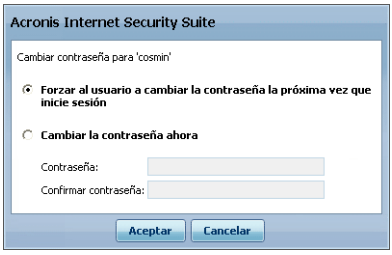
10.3.5. Paso 5/6 - Cambiar contraseñas déblies



Contraseñas de los Usuarios

Puede ver la lista de las cuentas de usuario de Windows configuraras en su equipo y el nivel de protección de sus contraseñas. Una contraseña puede ser **segura** (difícil de adivinar) o **insegura** (fácil de adivinar por personas maliciosas con software especializado).

Haga clic en **Reparar** para modificar las contraseñas inseguras. Aparecerá una nueva ventana.



Cambiar Contraseña

Seleccione el método de reparación de esta incidencia:

- **Forzar al usuario a cambiar la contraseña la próxima vez que inicie sesión.** Acronis Internet Security Suite 2010 solicitará al usuario que cambie su contraseña la próxima vez que este usuario inicie sesión en Windows.
- **Cambiar contraseña del usuario.** Debe introducir la nueva contraseña en los campos de texto. Asegúrese de informar al usuario acerca del cambio de contraseña.

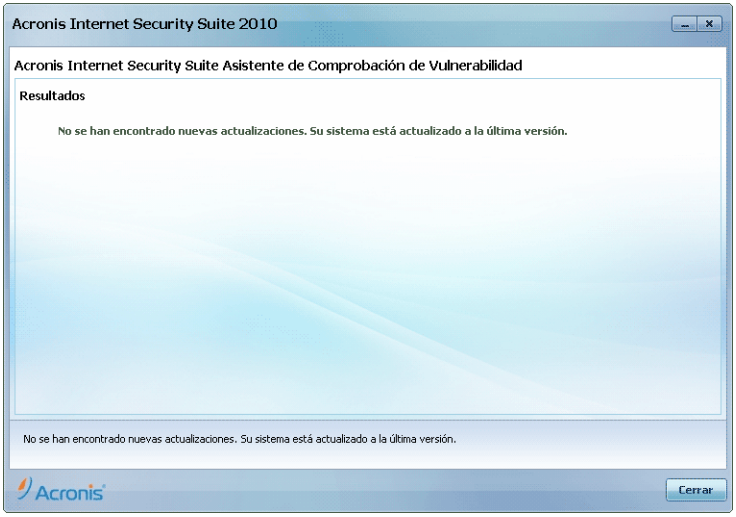
Nota

Para conseguir una contraseña segura, utilice una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (como #, $ o @). Para más información y consejos sobre cómo crear contraseñas seguras puede buscar en Internet.

Haga clic en **Aceptar** para cambiar la contraseña.

Haga clic en **Siguiente**.

10.3.6. Paso 6/6 – Ver Resultados



Resultados

Haga clic en **Cerrar**.

10.4. Asistente de Blindaje de Archivo

El asistente de Blindaje de Archivo le ayuda a crear y administrar blindajes de archivos en Acronis Internet Security Suite 2010. Un blindaje de archivo es un espacio de almacenamiento cifrado en su equipo don puede almacenar con seguridad archivos importantes, documentos e incluso carpetas enteras.

Estos asistentes no aparecen cuando repara incidencias, porque los blindajes de archivo son un método de protección opcional de sus datos. Sólo puede ser iniciado desde la interfaz en Modo Intermedio de Acronis Internet Security Suite 2010, la pestaña **Almacenamiento**, como sigue:

- **Blindar Archivo** - inicia un asistente que le permite almacenar sus archivos / documentos de forma privada cifrándolos en unidades especiales blindadas.
- **Desblindar Archivos** - inicia un asistente que le permite eliminar sus datos del blindaje.
- **Ver Blindaje** -Inicia el asistente que le permite ver el contenido de sus blindajes.
- **Bloquear Blindaje** - inicia el asistente le permite bloquear un blindaje abierto y proteger su contenido.

10.4.1. Blindar Archivos

Este asistente le ayuda a crear un blindaje y añadir archivos a este con el fin de guardarlos seguros en su equipo.

Paso 1/6 - Seleccione el Objetivo

Aquí puede especificar los archivos y carpetas que se añadirán al blindaje.

Objetivo

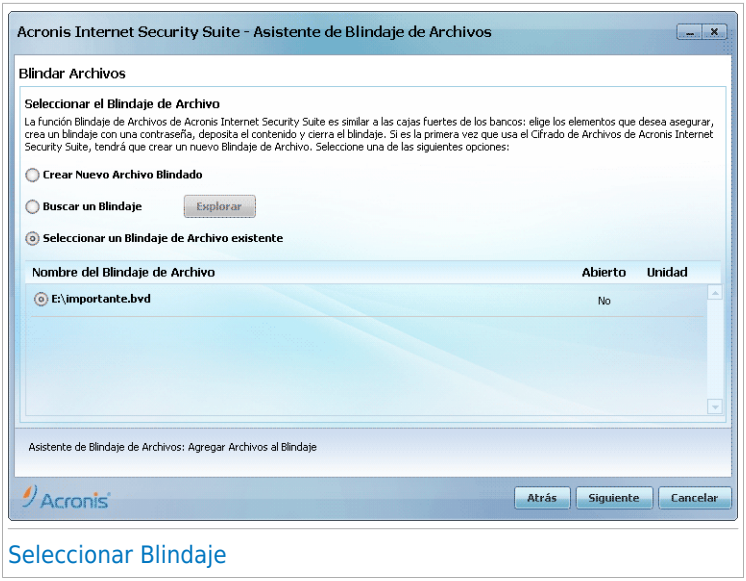
Haga clic en **Ruta**, seleccione el archivo o carpeta que desea añadir y haga clic en **Aceptar**. La rutas de los elementos seleccionados aparecerá en la columna **Ruta**. Si cambia de idea y desea eliminar alguno de los elementos seleccionados, simplemente haga clic en el botón **Quitar** situado junto a este elemento.

Nota
Puede seleccionar una o varias ubicaciones.

Haga clic en **Siguiente**.

Paso 2/6 - Seleccione el Blindaje

Desde aquí puede crear un nuevo blindaje o seleccionar un blindaje existente.



Seleccionar Blindaje

Si selecciona **Buscar un Archivo de Blindaje**, deberá hacer clic en **Explorar** y seleccionar el archivo de blindaje. Se le dirigirá al paso 5 si el blindaje seleccionado está abierto (montado) o al paso 4 si el blindaje está bloqueado (desmontado).

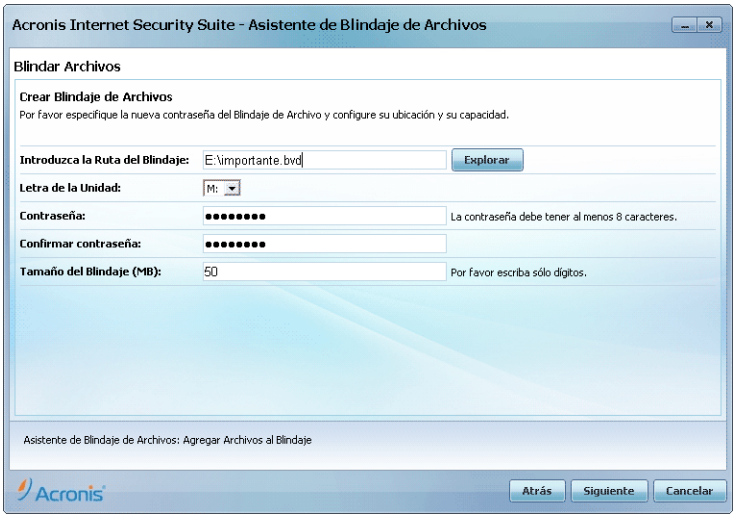
Si hace clic en **Seleccionar un Archivo de Blindaje existente**, deberá hacer clic en el nombre del blindaje deseado de la lista. Se le dirigirá al paso 5 si el blindaje seleccionado está abierto (montado) o al paso 4 si el blindaje está bloqueado (desmontado).

Seleccione **Crear Nuevo Blindaje de Archivos** si ninguno de los blindajes existentes se ajusta a sus necesidades. Se le dirigirá al paso 3.

Haga clic en **Siguiente**.

Paso 3/6 – Crear un Blindaje

Aquí puede especificar la información del nuevo Blindaje.



Crear Blindaje

Para completar la información relacionada con el blindaje, siga estos pasos:

1. Haga clic en **Explorar** e indique la ubicación del archivo bvd.

   Nota
   Recuerde que el archivo de blindaje es un archivo cifrado ubicado en si equipo con extensión bvd.

2. Seleccione la letra de la unidad del nuevo blindaje en el correspondiente menú desplegable.

   Nota
   Recuerde que cuando monta un archivo bvd, aparecerá una nueva partición lógica (una nueva unidad).

3. Introduzca una contraseña para el blindaje en el campo correspondiente.

   Nota
   La contraseña debe tener como mínimo 8 caracteres.

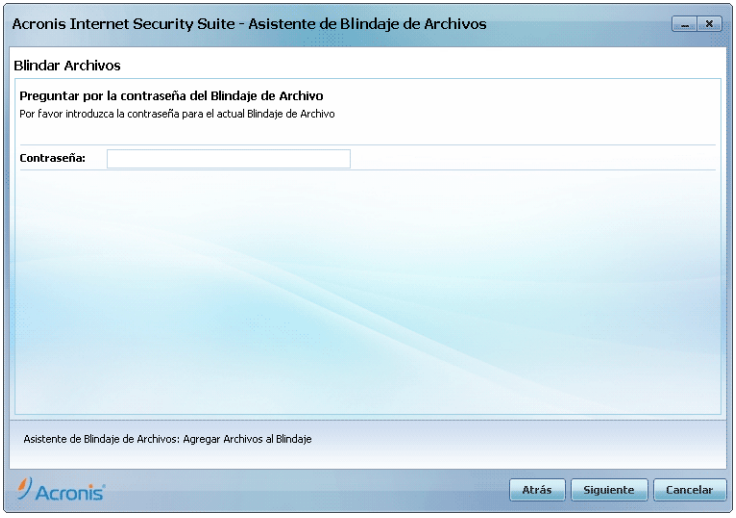
4. Vuelva a introducir la contraseña.
5. Defina el tamaño del blindaje (en MB) introduciendo un número en el campo correspondiente.

Haga clic en **Siguiente**.

Se le dirigirá al paso 5.

Paso 4/6 - Contraseña

Aquí es donde debe introducir la contraseña del blindaje seleccionado.

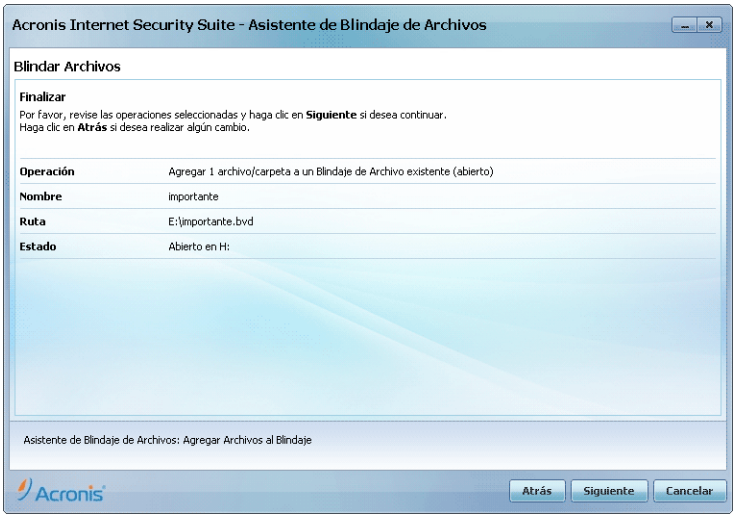


Confirmar contraseña

Introduzca la contraseña en el campo correspondiente y haga clic en **Siguiente**.

Paso 5/6 - Resumen

Desde aquí puede revisar las operaciones seleccionadas en los pasos del asistente.

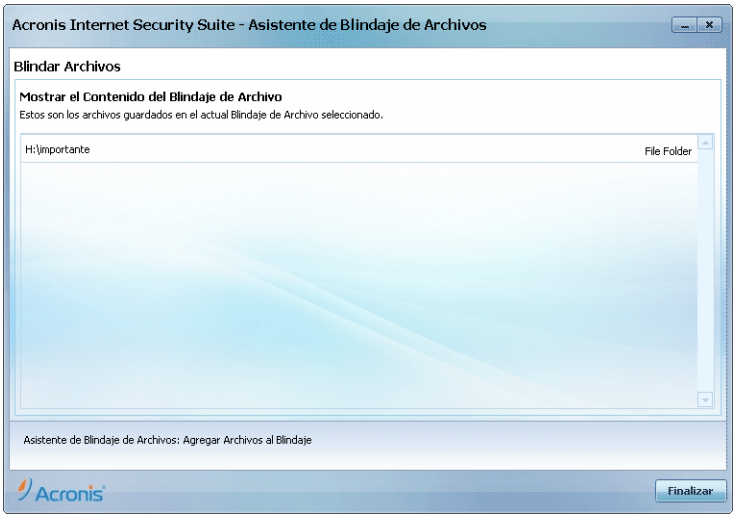


Sumario

Haga clic en **Siguiente**.

Paso 6/6 – Resultados

Aquí puede ver el contenido del blindaje.



Resultados

Haga clic en **Finalizar**.

10.4.2. Desblindar Archivos

Este asistente le ayuda a eliminar archivos de un blindaje específico.

Paso 1/5 - Seleccione un Blindaje

Aquí puede indicar el blindaje del que desea quitar los archivos.

Seleccionar Blindaje

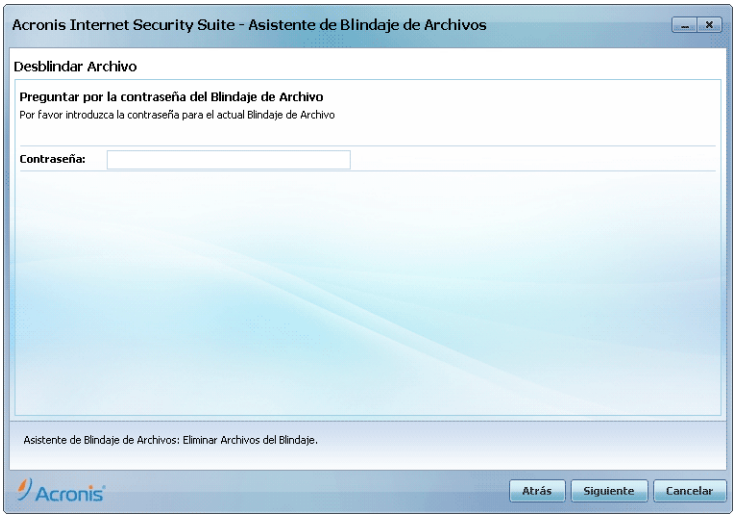
Si selecciona **Buscar un Archivo de Blindaje**, deberá hacer clic en **Explorar** y seleccionar el archivo de blindaje. Se le dirigirá al paso 3 si el blindaje seleccionado está abierto (montado) o al paso 2 si el blindaje está bloqueado (desmontado).

Si hace clic en **Seleccionar un Archivo de Blindaje existente**, deberá hacer clic en el nombre del blindaje deseado de la lista. Se le dirigirá al paso 3 si el blindaje seleccionado está abierto (montado) o al paso 2 si el blindaje está bloqueado (desmontado).

Haga clic en **Siguiente**.

Paso 2/5 - Contraseña

Aquí es donde debe introducir la contraseña del blindaje seleccionado.

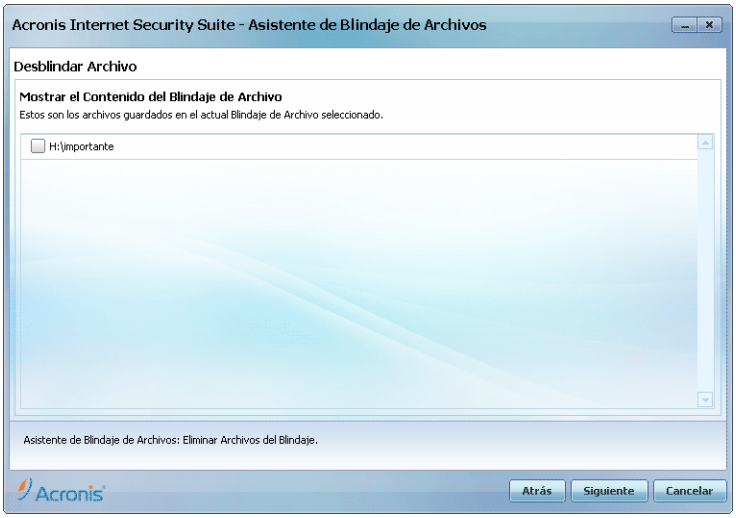


Confirmar contraseña

Introduzca la contraseña en el campo correspondiente y haga clic en **Siguiente**.

Paso 3/5 – Seleccione los Archivos

Aquí puede ver la lista de archivos que contiene el blindaje previamente seleccionado.

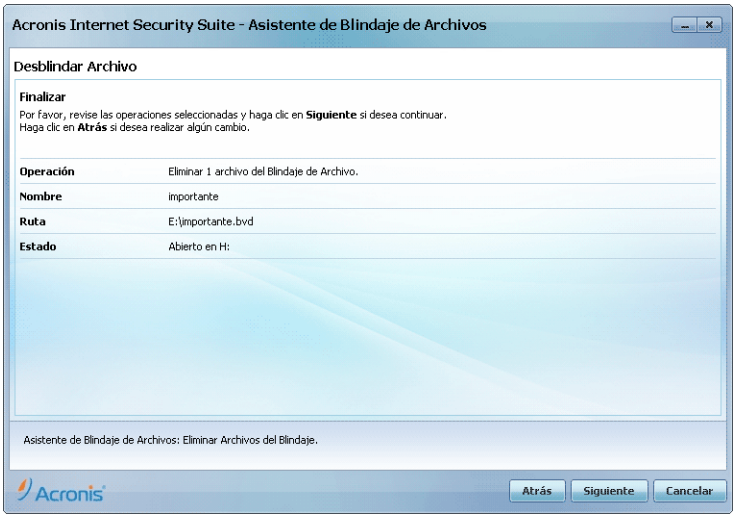


Selección de los archivos

Seleccione los archivos a eliminar y haga clic en **Siguiente**.

Paso 4/5 - Resumen

Desde aquí puede revisar las operaciones seleccionadas en los pasos del asistente.

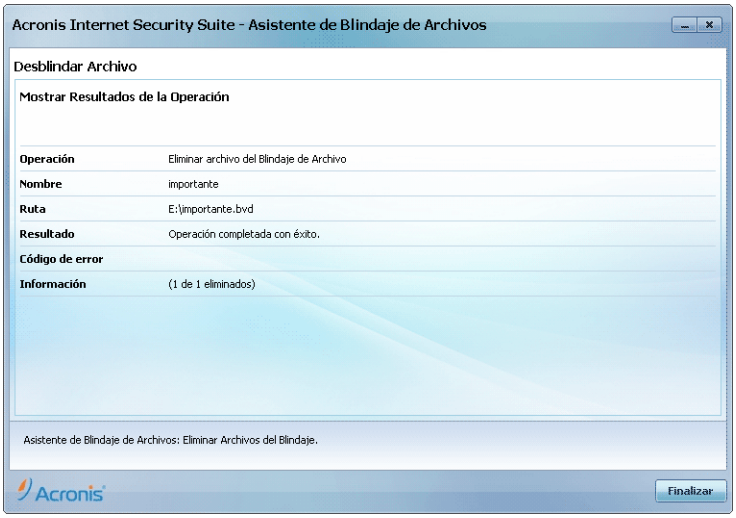


Sumario

Haga clic en **Siguiente**.

Paso 5/5 – Resultados

Aquí puede ver los resultados de la operación.



Resultados

Haga clic en **Finalizar**.

10.4.3. Ver Blindaje

Este asistente le ayuda a abrir un blindaje específico y ver los archivos que contiene.

Paso 1/4 - Seleccione el Blindaje

Aquí puede especificar el blindaje cuyo contenido desea visualizar.

Seleccionar Blindaje

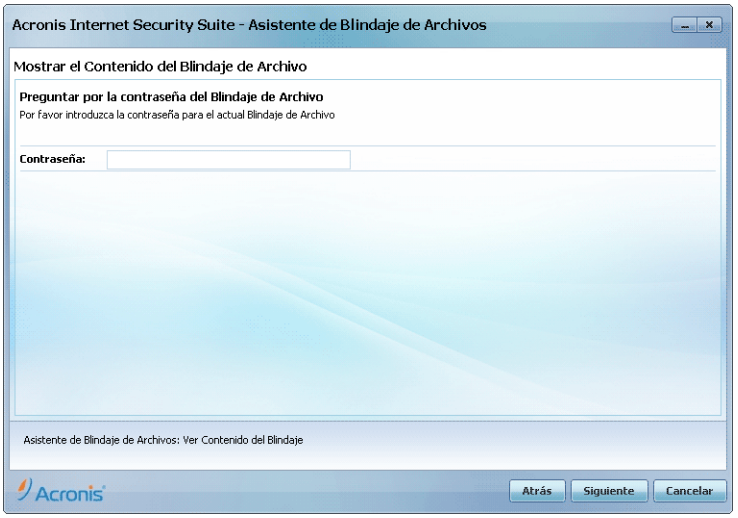
Si selecciona **Buscar un Archivo de Blindaje**, deberá hacer clic en **Explorar** y seleccionar el archivo de blindaje. Se le dirigirá al paso 3 si el blindaje seleccionado está abierto (montado) o al paso 2 si el blindaje está bloqueado (desmontado).

Si hace clic en **Seleccionar un Archivo de Blindaje existente**, deberá hacer clic en el nombre del blindaje deseado de la lista. Se le dirigirá al paso 3 si el blindaje seleccionado está abierto (montado) o al paso 2 si el blindaje está bloqueado (desmontado).

Haga clic en **Siguiente**.

Paso 2/4 - Contraseña

Aquí es donde debe introducir la contraseña del blindaje seleccionado.

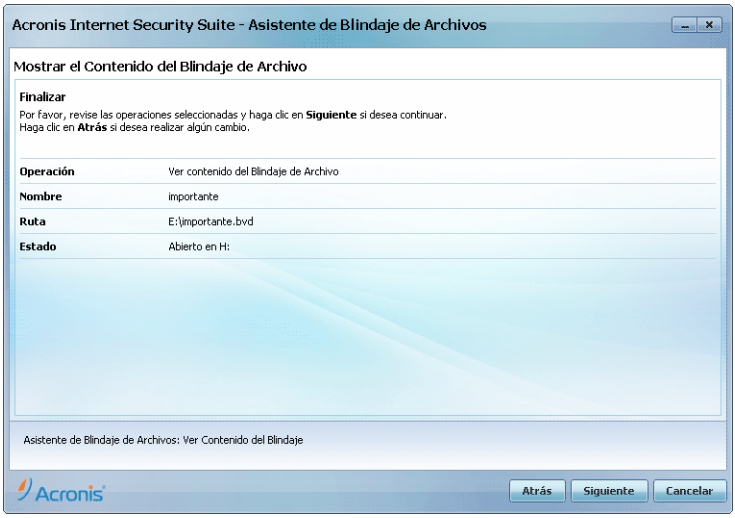


Confirmar contraseña

Introduzca la contraseña en el campo correspondiente y haga clic en **Siguiente**.

Paso 3/4 - Resumen

Desde aquí puede revisar las operaciones seleccionadas en los pasos del asistente.



Sumario

Haga clic en **Siguiente**.

Paso 4/4 – Resultados

Desde aquí puede ver los archivos que contiene el blindaje.

Resultados

Haga clic en **Finalizar**.

10.4.4. Bloquear Blindaje

Este asistente le ayuda a bloquear un blindaje específico con el fin de proteger este contenido.

Paso 1/3 - Seleccione el Blindaje

Aquí puede indicar el blindaje que desea bloquear.

Seleccionar Blindaje

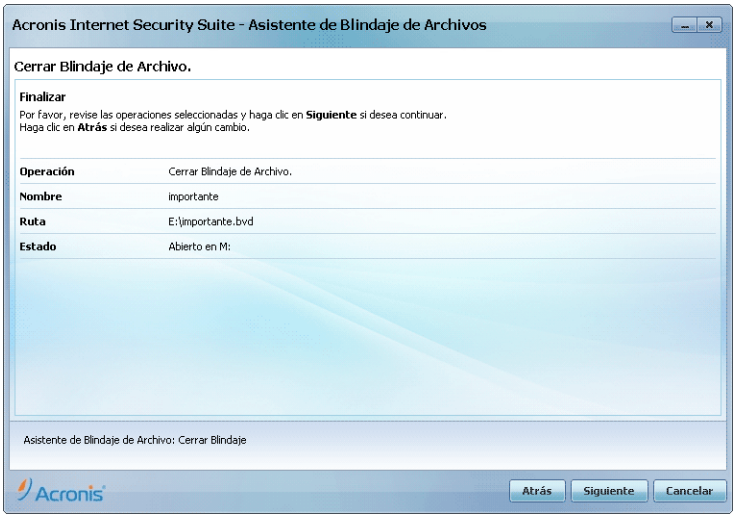
Si selecciona **Buscar un Archivo de Blindaje**, deberá hacer clic en **Explorar** y seleccionar el archivo de blindaje.

Si hace clic en **Seleccionar un Archivo de Blindaje existente**, deberá hacer clic en el nombre del blindaje deseado de la lista.

Haga clic en **Siguiente**.

Paso 2/3 - Resumen

Desde aquí puede revisar las operaciones seleccionadas en los pasos del asistente.



Sumario

Haga clic en **Siguiente**.

Paso 3/3 – Resultados

Aquí puede ver los resultados de la operación.

Resultados

Haga clic en **Finalizar**.

Modo Intermedio

11. Visor Estado

El Visor Estado proporciona información en cuanto a la seguridad de su equipo y permite reparar todas las incidencias pendientes.

Visor Estado

El panel de control consiste en los siguientes apartados:

- **Estado** - Indica el número de incidencias que afectan a su equipo y le ayuda a repararlas. Si existen alguna incidencia pendiente, las verá una **marca en circulo rojo con una exclamación** y el botón **Reparar Todas**. Haga clic en el botón para iniciar el asistente Reparar Todas.
- **Estado** - Indica el estado de cada módulo utilizando frases explícitas y uno de los siguientes iconos:

  Círculo Verde con una marca de verificación: Ninguna incidencia afecta al estado de seguridad. Su equipo y sus datos están protegidos.

  Circulo gris con una marca de exclamación: La actividad de los componentes de este modulo no están monitorizadas. Por lo tanto, no hay información disponible respecto al estado de seguridad. Pueden haber incidencias especificas relacionadas con este módulo.

  Circulo Rojo con un marca de exclamación: Existen incidencias que afectan a la seguridad de su sistema. Incidencias críticas requieren su atención inmediata. Incidencias no criticas también deberían abordarse lo antes posible.

Haga click en el nombre del módulo para ver más detalles acerda del estado y para configurar las alertas de estado para sus componentes.

- **Perfil de Uso**- Indica el perfil de uso que esta actualmente seleccionado y ofrece un enlace a tareas relevantes para este perfil:
  - ▶ Cuando el perfil **Típico** es seleccionado, el botón **Analizar Ahora** permite configurar un Análisis de Sistema utilizando el Asistente de Análisis de Antivirus. Se analizará por completo el sistema, excepto para archivos. En la configuración predeterminada, analiza todos los tipos de malware otros rootkits.
  - ▶ Cuando el perfil **Padre** está seleccionado, el botón **Control Parental** le permite configurar el Control Parental. Para más información sobre como configurar el Control Parental, por favor diríjase a *"Control Parental "* (p. 174).
  - ▶ Cuando se selecciona el perfil **Jugador** el botón **Activar/Desactivar Modo Juego** le permite activar/desactivar Modo Juego. El Modo Juego modifica temporalmente las opciones de seguridad para minimizar su impacto sobre el rendimiento del sistema.
  - ▶ Cuando selecciona **Personalizar** perfil, botón **Actualizar Ahora** inicia inmediatamente una actualización. Aparecerá una nueva ventana dónde podrá ver el estado de la actualización.

  Si desea cambiar a un perfil diferente o editar el que esta utilizando, haga clic en el perfil y siga el Asistente de Configuración.

12. Seguridad

Acronis Internet Security Suite 2010 incluye un módulo de Seguridad que le ayuda a mantener su Acronis Internet Security Suite 2010 actualizado y su equipo libre de virus. Para entrar en el módulo de Seguridad, haga clic en la pestaña **Seguridad**.

Seguridad

El módulo Seguridad consta de dos apartados:

- **Estado** - Muestra el estado actual de todos los componentes de seguridad monitorizados y le permite elegir que componente debe ser monitorizado.
- **Tareas Rápidas** - Desde aquí puede encontrar enlaces a las tareas de seguridad más importantes: actualizar, análisis de sistema, analizar Mis Documentos, análisis en profundidad, analisis de vulnerabilidades.

12.1. Área de Estado

En el visor de estado puede ver la lista completa de los componentes de seguridad monitorizados y su actual estado. Para monitorizar cada módulo de seguridad, Acronis Internet Security Suite 2010 le permitirá conocer no solo cuando modifica la configuración que podría afectar a la seguridad de su equipo, pero también cuando se olvida de realizar tareas importantes.

El estado actual de un componente se indica utilizando frases explícitas y uno de los siguientes iconos:

Círculo Verde con una marca de verificación: Ninguna incidencia afecta al componente.

Circulo Rojo con un marca de exclamación: Incidencias afectan al componente.

Las frases que describen las incidencias están escritas en rojo. Sólo haga clic en el botón **Reparar** correspondiente a la frase para reparar la incidencia. Si una incidencia no se repara en el momento, siga el asistente para repararla.

12.1.1. Configurando las Alertas de Estado

Para seleccionar los componente de Acronis Internet Security Suite 2010 debe monitorizarlos, haga clic en **Configurar Alertas** y seleccione la casilla **Activar alertas** correspondiente a las características que desea que se monitoricen.

Importante

Necesita activar el seguimiento de estado de alerta para un componente si desea que se le notifique cuando una incidencia afecta a la seguridad de este componente. Para asegurarse que su sistema está totalmente protegido, active monitorizar todos los componentes y repare todas las incidencias mostradas.

El estado de los siguientes componentes de seguridad pueden ser monitorizados por Acronis Internet Security Suite 2010:

- **Antivirus** - Acronis Internet Security Suite 2010 monitoriza el estado de dos componentes del Antivirus: Protección en Tiempo Real y análisis bajo demanda. El problema más común de una incidencia para este componente se muestra en la siguiente tabla.

Incidencia	Descripción
Protección en Tiempo Real desactivada	Los archivos no son analizados, ya que esta accediendo usted o bien una aplicación que se esta ejecutando en el sistema.
Nunca ha analizado su equipo en busca de malware	Nunca se ha realizado un análisis de sistema bajo demanda para comprobar si los archivos guardados en su equipo están libre de malware.
El último análisis de sistema iniciado fue abortado antes de finalizar	Un análisis completo de sistema fué iniciado pero no se completó.
El Antivirus está en un estado crítico	La protección en Tiempo Real esta desactivada y un análisis de sistema se ha retrasado.

- **Actualizar** - Acronis Internet Security Suite 2010 monitoriza si están las firmas de malware al día. El problema más común de una incidencia para este componente se muestra en la siguiente tabla.

Incidencia	Descripción
Actualizaciones Automáticas están desactivadas	Las firmas de malware en su producto Acronis Internet Security Suite 2010 no están siendo actualizadas automáticamente de forma periódica.
No se ha realizado ninguna actualización en los últimos x días	Las firmas de malware de su producto Acronis Internet Security Suite 2010 están obsoletas.

- **Cortafuego** - Acronis Internet Security Suite 2010 monitoriza el estado del Cortafuego. Si este no está activado, la incidencia **Cortafuego desactivado** se mostrará.
- **Antispam** - Acronis Internet Security Suite 2010 monitoriza el estado del Antispam. Si este no está activado, la incidencia **Antispam está desactivado** se mostrará.
- **Antiphishing** - Acronis Internet Security Suite 2010 monitoriza el estado de la función del Antiphishing. Si no esta activada para todas las aplicaciones soportados, la incidencia **Antiphishing esta desactivada** será informada.
- **Comprobación de Vulnerabilidades** - Acronis Internet Security Suite 2010 mantiene la monitorización de la función de Comprobación de Vulnerabilidad. La comprobación de Vulnerabilidad le permite conocer si necesita instalar alguna actualización de Windows, actualizaciones de aplicaciones o si necesita fortalecer cualquier contraseña.

  El problema más común de una incidencia para este componente se muestra en la siguiente tabla.

Estado	Descripción
Comprobación de Vulnerabilidades desactivada	Acronis Internet Security Suite 2010 no comprueba las vulnerabilidades potenciales con respecto a actualizaciones de windows ausentes, actualizaciones de aplicaciones o contraseñas inseguras.
Se han detectado múltiples vulnerabilidades	Acronis Internet Security Suite 2010 encontró actualizaciones que faltan de aplicaciones/Windows y/o contraseñas inseguras.

Estado	Descripción
Actualizaciones Críticas de Microsoft	Actualizaciones Criticas de Microsoft están disponibles pero no instaladas.
Otras actualizaciones de Microsoft	Actualizaciones no criticas de Microsoft están disponibles pero no instaladas.
Actualizaciones Automáticas de Windows están desactivadas	Actualizaciones de seguridad de Windows no serán instaladas automáticamente tan pronto como estén disponibles.
Aplicación (obsoleta)	Una nueva versión de la Aplicación está disponible pero no instalada.
Usuario (Contraseña insegura)	Una contraseña de usuario es fácil de descubrir por delincuentes con software especializado.

12.2. Tareas Rápidas

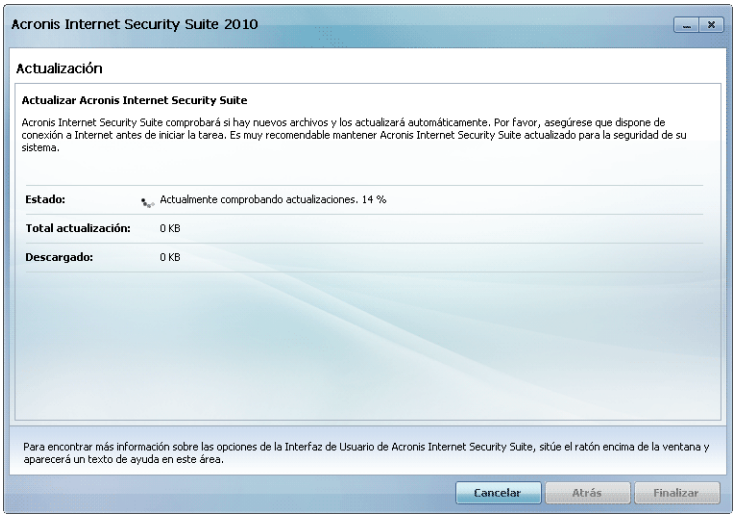
Aquí encontrará un enlace a las tareas de seguridad más importantes:

- **Actualizar** - realiza una actualización inmediata.
- **Análisis de sistema** - Inicia un análisis estándar en su equipo (excepto fichero comprimidos). Para tareas de análisis bajo demanda adicionales, haga clic en la flecha en este botón y seleccione una tarea de análisis diferente: Analizar Mis Documentos o Análisis en profundidad.
- **Análisis Personalizado** - Inicia un asistente que le permite crear y ejecutar una tarea de análisis personalizada.
- **Vulnerabilidades** - inicia un asistente que comprueba las vulnerabilidades del sistema y le ayuda a resolverlas.

12.2.1. Actualizando Acronis Internet Security Suite 2010

Cada día se encuentran nuevas amenazas de malware. Por esta razón es muy importante mantener Acronis Internet Security Suite 2010 actualizado con las últimas firmas de malware.

Por defecto, Acronis Internet Security Suite 2010 comprueba si hay nuevas actualizaciones cuando enciende su equipo y **cada hora** a partir de ese momento. Sin embargo, puede actualizar Acronis Internet Security Suite 2010 en cualquier momento haciendo clic en **Actualizar**. Se iniciará el proceso de actualización e inmediatamente aparecerá la siguiente ventana:



Actualizando Acronis Internet Security Suite 2010

En esta ventana podrá ver el estado del proceso de actualización.

El proceso de actualización se realiza al instante, actualizando o reemplazando los archivos antiguos progresivamente. De este modo, el proceso de actualización no afectará al rendimiento del producto a la vez que se evita cualquier riesgo.

Si desea cerrar esta ventana, haga clic en **Cancelar**. En cualquier caso, al cerrar la ventana no se detiene el proceso de actualización.

Nota
Si está conectado a Internet a través de una conexión por módem analógico, es recomendable actualizar Acronis Internet Security Suite 2010 manualmente.

Reinicie el equipo si así se le solicita. Cuando se produzca una actualización importante, se le solicitará reiniciar el equipo. Haga clic en **Reiniciar** para reiniciar el equipo inmediatamente.

Si desea reiniciar el equipo más tarde, haga clic en **Aceptar**. Recomendamos reiniciar el equipo tan pronto como sea posible.

12.2.2. Analizando con Acronis Internet Security Suite 2010

Para analizar su equipo en busca de malware, ejecute una tarea de análisis haciendo clic el botón correspondiente o seleccionándolo desde el menú desplegable. La siguiente tabla presenta las tareas de análisis disponibles, junto con su descripción:

Tarea	Descripción
Análisis de sistema	Analiza todo el sistema, excepto los archivos comprimidos. En la configuración predeterminada, busca todos los tipos de malware distintos a rootkits.
Analizar Mis Documentos	Utilice esta tarea para analizar las carpetas del usuario en uso: `Mis Documentos`, `Escritorio` e `Inicio`. Así asegurará el contenido de sus documentos, conseguirá un espacio de trabajo seguro y que las aplicaciones iniciadas al cargar el sistema están limpias.
Análisis en Profundidad	Analiza el sistema por completo. En la configuración predeterminada, analiza en busca de cualquier tipo de malware que pueda amenazar a su sistema, como virus, spyware, adware, rootkits y otros.
Análisis Personalizado	Use esta tarea para analizar archivos y carpetas concretos.

Nota

A través de las tareas **Análisis en Profundidad** y **Análisis Completo** puede analizar el sistema por completo, pero el proceso requerirá bastante tiempo. Por ello, recomendamos ejecutar estas tareas con baja prioridad, o preferiblemente, cuando no utilice el equipo.

Cuando inicia un Análisis de Sistema, Análisis en Profundidad o Análisis de Mis Documentos, aparecerá el asistente de Análisis de Antivirus. Siga el proceso guiado de tres pasos para completar el proceso de análisis. Para información detallada acerca de este asistente, por favor consulte "*Asistente del análisis Antivirus*" (p. 45).

Cuando inicia un Análisis Personalizado, el asistente de Análisis Personalizado le guiará por el proceso de análisis. Siga los seis pasos guiados para proceder a analizar archivos o carpetas específicos. Para información detallada acerca de este asistente, por favor diríjase a "*Personalizar el Asistente de Análisis*" (p. 50).

12.2.3. Buscando Vulnerabilidades

El Análisis de Vulnerabilidad comprueba las actualizaciones de Microsoft Windows, Microsoft Windows Office y las contraseñas de sus cuentas de Windows para asegurarse que su sistema está actualizado y sus contraseñas no son vulnerables.

Para comprobar las vulnerabilidades de su equipo, haga clic en **Vulnerabilidades** y siga los seis pasos del asistente. Para más información, por favor diríjase a "*Reparar Vulnerabilidades*" (p. 232).

13. Parental

Acronis Internet Security Suite 2010 incluye un módulo de Control Parental. El Control Parental le permite restringir el acceso de sus hijos a Internet y a aplicaciones específicas. Para comprobar el estado del Control Parental, haga clic en la pestaña **Control Parental**.

Parental

El módulo Parental consta de dos apartados:

- **Estado** - Le permite ver si el Control Parental esta configurado y activar/desactivar la monitorización de este módulo.
- **Tareas Rápidas** - Desde aquí puede encontrar enlaces a las tareas de seguridad más importantes: Análisis de sistema, Análisis en profundidad, actualizar ahora.

13.1. Área de Estado

El actual estado del módulo de Control Parental se indica utilizando frases explícitas y uno de los siguientes iconos:

Círculo Verde con una marca de verificación: Ninguna incidencia afecta al componente.

Circulo Rojo con un marca de exclamación: Incidencias afectan al componente.

Las frases que describen las incidencias están escritas en rojo. Sólo haga clic en el botón **Reparar** correspondiente a la frase para reparar la incidencia. El problema más común de incidencias para este módulo es **Control Parental no configurado**.

Si desea que Acronis Internet Security Suite 2010 monitorice el módulo de Control Parental, haga clic en **Configurar Alertas** y seleccione la casilla **Activar alertas** para este módulo.

13.2. Tareas Rápidas

Para configurar el Control Parental, haga clic en **Control Parental** en el área Tareas Rápidas. Aparecerá una nueva ventana.

Configurar Control Parental

Aquí puede ver el estado del Control Parental para cada cuenta de usuario de Windows y puede configurar las reglas del Control Parental. Esta ventana de configuración es similar a la pestaña de Control Parental en Modo Avanzado. Para más información, por favor, consulte el capítulo “*Control Parental* ” (p. 174).

14. Blindaje

Acronis Internet Security Suite 2010 viene con un módulo de Blindaje de Archivo que no solo le ayuda a mantener sus datos a salvo, sino también a mantener su confidencialidad. Para conseguirlo, utilice el cifrado de archivo.

Para acceder al módulo Blindaje de Archivos, haga clic en la pestaña **Blindaje de Archivos**.

Blindaje

El módulo Blindaje de Archivos consta de dos apartados:

- **Estado** - Le permite ver la lista completa de los componentes monitorizados. Puede elegir qué componentes se monitorizarán. Se recomienda activar la opción de monitorización para todos ellos.
- **Tareas** - Desde aquí puede encontrar enlaces a las tareas de seguridad más importantes: añadir, ver, bloquear y eliminar blindajes de archivo.

14.1. Área de Estado

El estado actual de un componente se indica utilizando frases explícitas y uno de los siguientes iconos:

Círculo Verde con una marca de verificación: Ninguna incidencia afecta al componente.

Circulo Rojo con un marca de exclamación: Incidencias afectan al componente.

Las frases que describen las incidencias están escritas en rojo. Sólo haga clic en el botón **Reparar** correspondiente a la frase para reparar la incidencia. Si una incidencia no se repara en el momento, siga el asistente para repararla.

El estado en en la pestaña de Blindaje de Archivo ofrece información respecto al estado del módulo de **Cifrado**.

Si desea que Acronis Internet Security Suite 2010 monitorice el Cifrado de Archivo, haga clic en **Configurar las Alertas de Estado** y seleccionar la casilla **Activar alertas**.

14.2. Tareas Rápidas

Dispone de los siguientes botones:

- **Blindar Archivo** - inicia un asistente que le permite almacenar sus archivos / documentos de forma privada cifrándolos en unidades especiales blindadas. Para más información, por favor diríjase a "*Blindar Archivos*" (p. 64).
- **Desblindar Archivos** - inicia un asistente que le permite eliminar sus datos del blindaje. Para más información, por favor diríjase a "*Desblindar Archivos*" (p. 70).
- **Ver Blindaje** -Inicia el asistente que le permite ver el contenido de sus blindajes. Para más información, por favor diríjase a "*Ver Blindaje*" (p. 75).
- **Bloquear Blindaje** - Inicia el asistente que le permite bloquear su blindaje y proteger su contenido. Para más información, por favor diríjase a "*Bloquear Blindaje*" (p. 79).

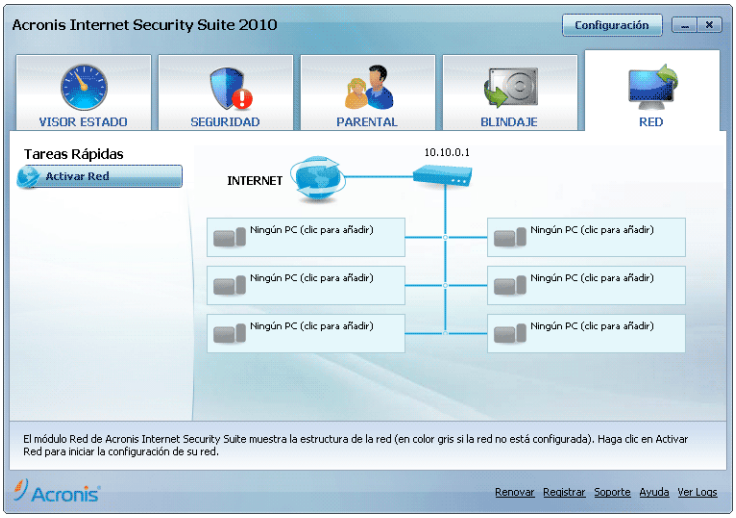
15. Red

El módulo Red le permite administrar los productos Acronis instalados en los equipos de una pequeña red desde un único equipo. Para acceder al módulo Red, haga clic en la pestaña **Red**.

Importante

Usted solamente puede gestionar los siguientes productos de seguridad Acronis:

- Acronis AntiVirus 2010
- Acronis Internet Security Suite 2010
- Acronis Backup and Security 2010



Red

Para poder administrar los productos Acronis de los otros equipos de la pequeña red, debe seguir estos pasos:

1. Únase a la red de administración de Acronis desde su equipo. Unirse a una red consiste en establecer una contraseña de administración para gestionar la red de administración.
2. Diríjase a cada unos de los equipos que desee administrar remotamente y únalos a la red (defina una contraseña).
3. Vuelva a su equipo y añada los equipos que desee administrar.

15.1. Tareas Rápidas

Inicialmente, sólo habrá un botón disponible.

- **Activar Red** - Permite establecer una contraseña de red, así como crear y unirse a la red.

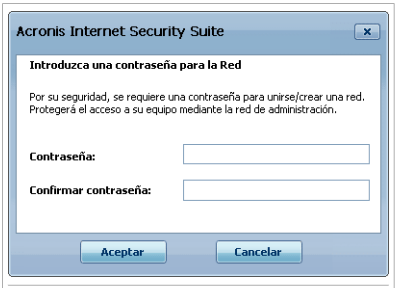
Una vez se haya unido a la red, aparecerán varios botones.

- **Desactivar Red** - Le permite salir de la red.
- **Añadir Equipo** - Le permite añadir equipos a su red.
- **Analizar Todos** - le permite analizar todos los equipos administrados a la vez.
- **Actualizar Todos** - le permite actualizar todos los equipos administrados a la vez.

15.1.1. Uniéndose a la red de Acronis

Para unirse a la red de administración de Acronis, siga estos pasos:

1. Haga clic en **Activar Red**. Se le solicitará configurar la contraseña de administración de red.



Configurar Contraseña

2. Introduzca la misma contraseña en cada uno de los campos de texto.
3. Haga clic en **Aceptar**.

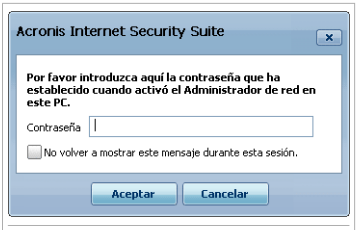
Podrá ver como el nombre del equipo aparece en el mapa de la red.

15.1.2. Añadiendo Equipos a la Red de Acronis

Antes de que usted pueda añadir un equipo a la red de Acronis, usted debe configurar la contraseña de gestión doméstica de Acronis en el equipo correspondiente.

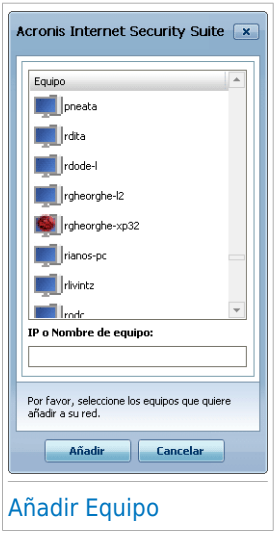
Para añadir un equipo a la red de administración de Acronis, siga estos pasos:

1. Haga clic en **Agregar Equipo**. Se le solicitará introducir la contraseña de administración de red local.



Introducir Contraseña

2. Introduzca la contraseña de administración de red y haga clic en el botón **Aceptar**. Aparecerá una nueva ventana.



Añadir Equipo

Podrá ver la lista de los equipos de la red. A continuación se explica el significado de los iconos:

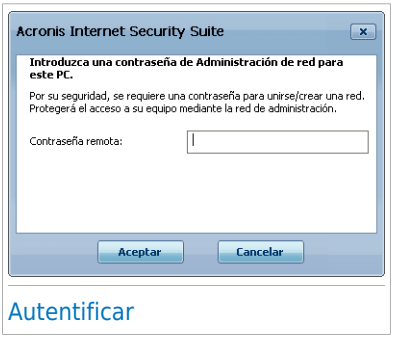
Indica un equipo conectado con ningún producto gestionable Acronis instalado.

Indica un equipo conectado con productos gestionables Acronis instalados.

Indica un equipo no conectado con un producto gestionable Acronis instalado.

3. Realice una de estas acciones:
   - Seleccione un equipo de la lista para añadirlo.
   - Introduzca la dirección IP o el nombre del equipo a añadir en el campo editable correspondiente.

4. Haga clic en **Añadir**. Se le solicitará la contraseña de administración de red del equipo correspondiente.



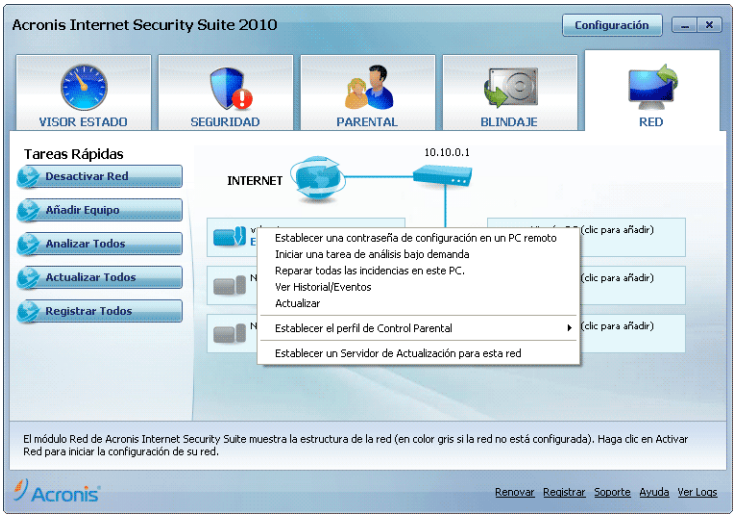
Autentificar

5. Introduzca la contraseña de administración de red configurada en el equipo correspondiente.
6. Haga clic en **Aceptar**. Si ha introducido la contraseña correcta, el nombre del equipo seleccionado aparecerá en el mapa de la red.

Nota
Puede añadir hasta cinco equipos en el mapa de la red.

15.1.3. Gestionando la red de Acronis

Un vez haya creado con éxito un red doméstica de Acronis, usted puede gestionar todos los productos Acronis desde un único equipo.



Mapa de la Red

Si situa el cursor del ratón encima de un equipo del mapa de red, podrá ver información sobre el (nombre, dirección IP, número de incidencias que afectan a la seguridad del sistema).

Si hace clic derecho en el nombre de un equipo del mapa de la red, podrá ver todas las tareas de administración que puede ejecutar remotamente.

- **Quitar Pc de la red**

  Permite eliminar un PC de la red.

- **Establecer contraseña de configuración en un PC remoto**

  Permite crear una contraseña para restringir el acceso a la configuración de Acronis en este PC.

- **Ejecutar una tarea de Análisis bajo demanda**

  Permite ejecutar un análisis bajo demanda en un equipo remoto. Puede realizar cualquiera de las siguiente tareas de análisis: Analizar Mis Documentos, Análisis de sistema o Análisis en Profundidad.

- **Reparar todas las incidencias en este PC**

  Le permite reparar todas las incidencias que están afectando a la seguridad de este equipo siguiendo el asistente Reparar Todas.

- **Historial**

Le permite acceder al módulo **Historial&Eventos** en el producto instalado de Acronis en este equipo.

- **Actualizar ahora**

  Inicia el proceso de actualización para el producto Acronis instalado en este equipo.

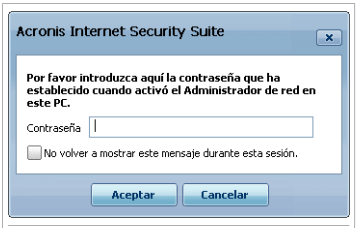
- **Establecer Perfil de Control Parental**

  Le permite establecer la categoría de edad que será utilizada por el filtro web del Control Parental en este equipo: niños, adolescentes o adultos.

- **Establecer un Servidor de Actualizaciones para esta Red**

  Permite establecer este equipo como servidor de actualización para todos los productos Acronis instalados en los equipos de esta red. Utilice esta opción para reducir el tráfico de Internet, porque sólo se conectará un equipo de esta red a Internet para descargar las actualizaciones.

Antes de ejecutar una tarea en un equipo determinado, se le solicitará la contraseña de administración de red local.



Introducir Contraseña

Introduzca la contraseña de administración de red y haga clic en el botón **Aceptar**.

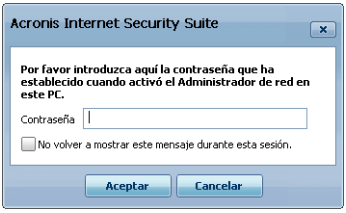
Nota

Si tiene previsto ejecutar varias tareas, puede interesarle la opción **No mostrar este mensaje durante esa sesión**. Al seleccionar esta opción, no se le volverá a solicitar esta contraseña durante la actual sesión.

15.1.4. Analizando Todos los Equipos

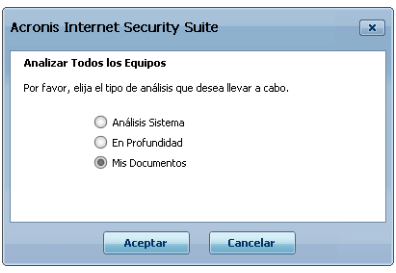
Para analizar todos los equipos administrados, siga estos pasos:

1. Haga clic en **Analizar Todos**. Se le solicitará introducir la contraseña de administración de red local.



Introducir Contraseña

2. Seleccione un tipo de análisis.
   - **Análisis de Sistema** - Inicia un análisis completo de su equipo (archivos comprimidos excluidos).
   - **Análisis en Profundidad** - inicia un análisis completo de su equipo (archivos comprimidos incluidos).
   - **Analizar Mis Documentos** - inicia un análisis rápido de sus documentos.



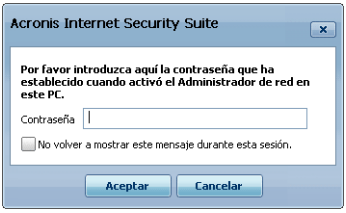
Selección del Tipo de Análisis

3. Haga clic en **Aceptar**.

15.1.5. Actualizando Todos los Equipos

Para actualizar todos los equipos administrados, siga estos pasos:

1. Haga clic en **Actualizar Todos**. Se le solicitará introducir la contraseña de administración de red local.



Introducir Contraseña

2. Haga clic en **Aceptar**.

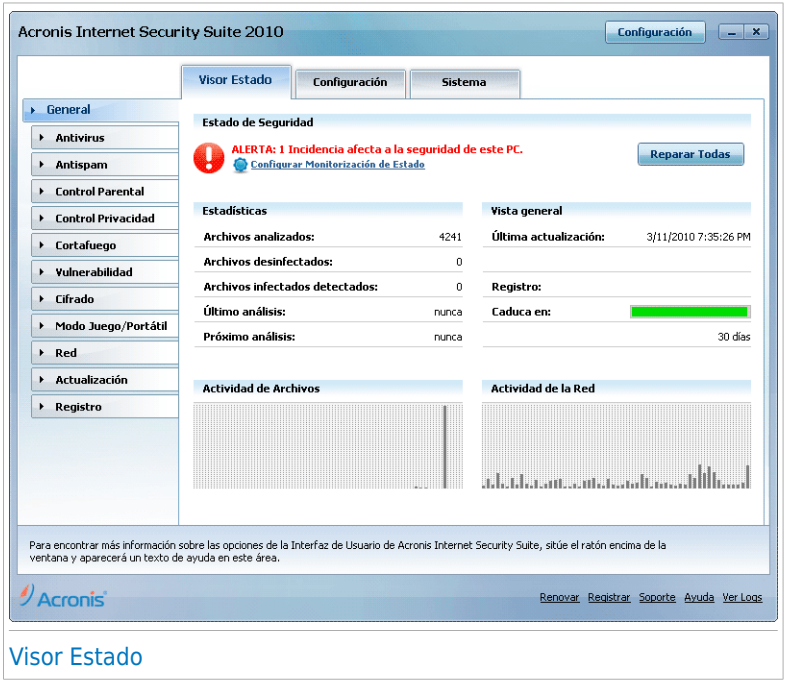
Modo Avanzado

16. General

El módulo General le ofrece información sobre la actividad de Acronis Internet Security Suite 2010 y su sistema. Desde aquí también puede cambiar algunos aspectos del comportamiento general de Acronis Internet Security Suite 2010.

16.1. Visor Estado

Para ver si alguna incidencia afecta a su equipo, así como estadísticas sobre la actividad del producto y su estado de registro, diríjase a **General>Visor Estado** en el Modo Avanzado.



Visor Estado

El Visualizador consta de varios apartados:

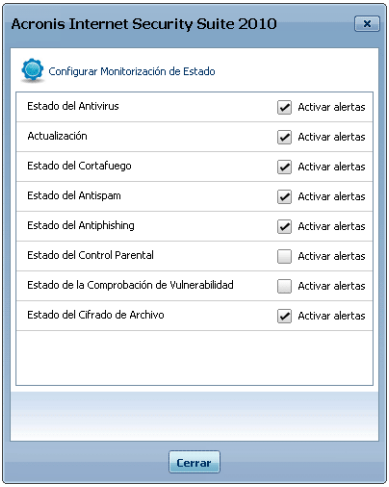
- **Estado de Seguridad** - Le informa de cualquier incidencia de seguridad que afectan a la seguridad de su equipo.
- **Estadísticas** - Muestra información importante sobre la actividad de Acronis Internet Security Suite 2010.
- **General** - Muestra el estado de la actualización, el estado del registro e información de la licencia.

- **Actividad de Archivo** - Indica la evolución del número de objetos analizados por Acronis Internet Security Suite 2010 Antimalware. La altura de la barra indica la intensidad del tráfico durante ese intervalo de tiempo.
- **Actividad Internet** - Indica la evolución del tráfico de red filtrado por el Cortafuego de Acronis Internet Security Suite 2010. La altura de la barra indica la intensidad del tráfico durante ese intervalo de tiempo.

16.1.1. Estado General

Desde aquí puede encontrar el número de incidencias que están afectando a la seguridad de sus equipo. Para eliminar todas las amenazas, haga clic en **Reparar Todas**. Se iniciará el asistente de Reparar Todas.

Para configurar que los módulos serán monitorizados por Acronis Internet Security Suite 2010, haga clic en **Configurar las Alertas de Estado**. Aparecerá una nueva ventana:



Configure las Alertas de Estado

Si desea que Acronis Internet Security Suite 2010 monitorice un componente, seleccione la casilla **Activar Alertas** para este componente. El estado de los siguientes componentes de seguridad pueden ser monitorizados por Acronis Internet Security Suite 2010:

- **Antivirus** - Acronis Internet Security Suite 2010 monitoriza el estado de dos componentes del módulo Antivirus: protección en tiempo real y análisis bajo demanda. El problema más común de una incidencia para este componente se muestra en la siguiente tabla.

Incidencia	Descripción
Protección en Tiempo Real desactivada	Los archivos no son analizados, ya que esta accediendo usted o bien una aplicación que se esta ejecutando en el sistema.
Nunca ha analizado su equipo en busca de malware	Nunca se ha realizado un análisis de sistema bajo demanda para comprobar si los archivos guardados en su equipo están libre de malware.
El último análisis de sistema iniciado fue abortado antes de finalizar	Un análisis completo de sistema fué iniciado pero no se completó.
El Antivirus está en un estado crítico	La protección en Tiempo Real esta desactivada y un análisis de sistema se ha retrasado.

- **Actualizar** - Acronis Internet Security Suite 2010 monitoriza si están las firmas de malware al día. El problema más común de una incidencia para este componente se muestra en la siguiente tabla.

Incidencia	Descripción
Actualizaciones Automáticas están desactivadas	Las firmas de malware en su producto Acronis Internet Security Suite 2010 no están siendo actualizadas automáticamente de forma periódica.
No se ha realizado ninguna actualización en los últimos x días	Las firmas de malware de su producto Acronis Internet Security Suite 2010 están obsoletas.

- **Cortafuego** - Acronis Internet Security Suite 2010 monitoriza el estado del Cortafuego. Si este no está activado, la incidencia **Cortafuego desactivado** se mostrará.
- **Antispam** - Acronis Internet Security Suite 2010 monitoriza el estado del Antispam. Si este no está activado, la incidencia **Antispam está desactivado** se mostrará.
- **Antiphishing** - Acronis Internet Security Suite 2010 monitoriza el estado de la función del Antiphishing. Si no esta activada para todas las aplicaciones soportados, la incidencia **Antiphishing esta desactivada** será informada.
- **Control Parental** - Acronis Internet Security Suite 2010 monitoriza el estado del Control Parental. Si este no está activado, la incidencia **Control Parental desactivado** se mostrará.

- **Comprobación de Vulnerabilidades** - Acronis Internet Security Suite 2010 mantiene la monitorización de la función de Comprobación de Vulnerabilidad. La comprobación de Vulnerabilidad le permite conocer si necesita instalar alguna actualización de Windows, actualizaciones de aplicaciones o si necesita fortalecer cualquier contraseña.

  El problema más común de una incidencia para este componente se muestra en la siguiente tabla.

Estado	Descripción
Comprobación de Vulnerabilidades desactivada	Acronis Internet Security Suite 2010 no comprueba las vulnerabilidades potenciales con respecto a actualizaciones de windows ausentes, actualizaciones de aplicaciones o contraseñas inseguras.
Se han detectado múltiples vulnerabilidades	Acronis Internet Security Suite 2010 encontró actualizaciones que faltan de aplicaciones/Windows y/o contraseñas inseguras.
Actualizaciones Críticas de Microsoft	Actualizaciones Criticas de Microsoft están disponibles pero no instaladas.
Otras actualizaciones de Microsoft	Actualizaciones no criticas de Microsoft están disponibles pero no instaladas.
Actualizaciones Automáticas de Windows están desactivadas	Actualizaciones de seguridad de Windows no serán instaladas automáticamente tan pronto como estén disponibles.
`Aplicación` (obsoleta)	Una nueva versión de la `Aplicación` está disponible pero no instalada.
`Usuario` (Contraseña insegura)	Una contraseña de usuario es fácil de descubrir por delincuentes con software especializado.

- **Cifrado** monitoriza el estado del Blindaje de Archivo. Si no esta activado, la incidencia **Cifrado desactivado** se mostrará.

Importante

Para asegurar que su sistema esta totalmente protegido, por favor, active monitorizar todos los componentes y repare todas las incidencias mostradas.

16.1.2. Estadísticas

Si desea controlar la actividad de Acronis Internet Security Suite 2010, puede empezar por el apartado Estadísticas. Puede ver los siguientes elementos:

Elemento	Descripción
Archivos analizados	Indica el número de archivos que han sido analizados en busca de malware durante el último análisis.
Archivos desinfectados	Indica el número de archivos han sido desinfectados durante el último análisis.
Archivos infectados detectados	Indica el número de archivos infectados que se han encontrado en el sistema durante el último análisis.
Último análisis de sistema	Muestra cuando su equipo fue analizado por última vez. Si el último análisis se realizó hace más de una semana, por favor analice su equipo lo antes posible. Para analizar el equipo entero, vaya a **Antivirus**, pestaña Análisis, y ejecute un Análisis Completo de Sistema o un Análisis en Profundidad.
Siguiente análisis	Indica la siguiente vez que su equipo se analizará.

16.1.3. Vista general

Aquí es donde usted puede ver el estado de actualización, registro y la información de licencia.

Elemento	Descripción
Última actualización	Incida cuando su producto Acronis Internet Security Suite 2010 se actualizó por última vez. Por favor realice actualizaciones periódicamente para tener un sistema completamente protegido.
Registro	Le indica el tipo de licencia utilizada y su estado. Para mantener su equipo protegido, debería renovar o actualizar su licencia de Acronis Internet Security Suite 2010 una vez haya caducado.
Caduca en	Indica el número de días restantes hasta que caduque la licencia. Si su licencia caduca en los próximos días, por favor registre el producto con un nuevo número de licencia. Para adquirir una licencia o renovar su licencia, haga clic en el enlace **Comprar/Renovar**, ubicado en la parte de abajo de la ventana.

16.2. Configuración

Para configurar las opciones generales de Acronis Internet Security Suite 2010 y administrar estas opciones, diríjase a **General>Configuración** en Modo Avanzado.

Configuración General

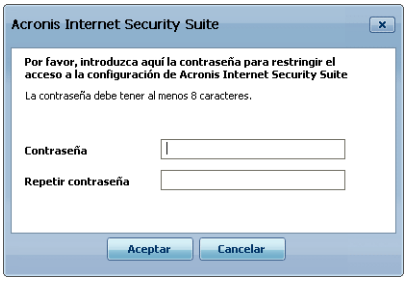
Aquí puede ajustar el comportamiento general de Acronis Internet Security Suite 2010. Por defecto, Acronis Internet Security Suite 2010 inicia con Windows y sigue funcionando minimizado en la barra de tareas.

16.2.1. Configuración General

- **Activar protección por contraseña** - pemite introducir una contraseña para proteger la configuración de Acronis Internet Security Suite 2010.

  Nota
  Si usted no es la única persona con derechos de administrador utilizando este equipo, recomendamos que proteja la configuración de Acronis Internet Securuty Suite 2010 con una contraseña.

  Si selecciona esta opción, aparecerá la siguiente ventana:



Confirmar contraseña

Introduzca la contraseña en el campo **Contraseña**, introdúzcala de nuevo en el campo **Repetir contraseña** y haga clic en **Aceptar**.

Una vez definida la contraseña, se le solicitará introducirla para poder cambiar la configuración de Acronis Internet Security Suite 2010. Los otros administradores de sistema (si hay) también tendrán que introducir esta contraseña para cambiar la configuración de Acronis Internet Security Suite 2010.

Si quiere que se le solicite la contraseña sólo cuando cambie la configuración del Control Parental, marque la opción **Preguntar/aplicar contraseña sólo para el Control Parental**. Por otro lado, si ha definido una contraseña sólo para el Control Parental y desmarca esta opción, se solicitará la respectiva contraseña al cambiar cualquier opción de Acronis Internet Security Suite 2010.

Importante

Si olvidó la contraseña tendrá que reparar el programa para poder cambiar la configuración de Acronis Internet Security Suite 2010.

- **Preguntarme si deseo configurar la contraseña al activar el Control Parental** - se le pedirá que configure una contraseña cuando active el Control Parental y no haya ninguna contraseña definida. Al introducir una contraseña, impedirá que los otros usuarios administradores cambien las opciones del Control Parental que ha configurado exclusivamente para un usuario.
- **Mostrar Noticias de Acronis Internet Security Suite(notificaciones relacionadas con la seguridad)** - Muestra noticias acerca de las epidemias de virus, enviadas por el servidor Acronis.
- **Mostrar pop-ups (notas en pantalla)** - muestra pop-ups acerca del estado del producto. Puede configurar Acronis Internet Security Suite 2010 para ver las ventanas emergentes solo cuando la interfaz está en Modo Básico / Intermedio o en Modo Experto.
- **Mostrar la barra de Actividad del Análisis (gráfico en pantalla de la actividad de producto)** - muestra la barra de Actividad de Análisis siempre que inicie sesión en Windows. Desmarque esta casilla si no desea que la Barra de Actividad se muestre más.

Barra de Actividad del Análisis

Nota

Esta opción sólo puede configurarse para la cuenta de usuario de Windows en uso. La barra de Actividad del Análisis está disponible solo cuando la interfaz esta en Modo Avanzado.

16.2.2. Configuración del Informe de Virus

- **Enviar informe de virus** - permite enviar automáticamente alertas acerca de estos virus a los Laboratorios Acronis. Nos ayuda a mantener un registro de las epidemias de virus.

  Los informes no contendrán datos confidenciales, tales como su nombre, dirección IP u otras informaciones, y no serán empleados con fines comerciales. Los datos proporcionados incluirán solamente el nombre del país y del virus y serán utilizados exclusivamente para crear informes y estadísticas.

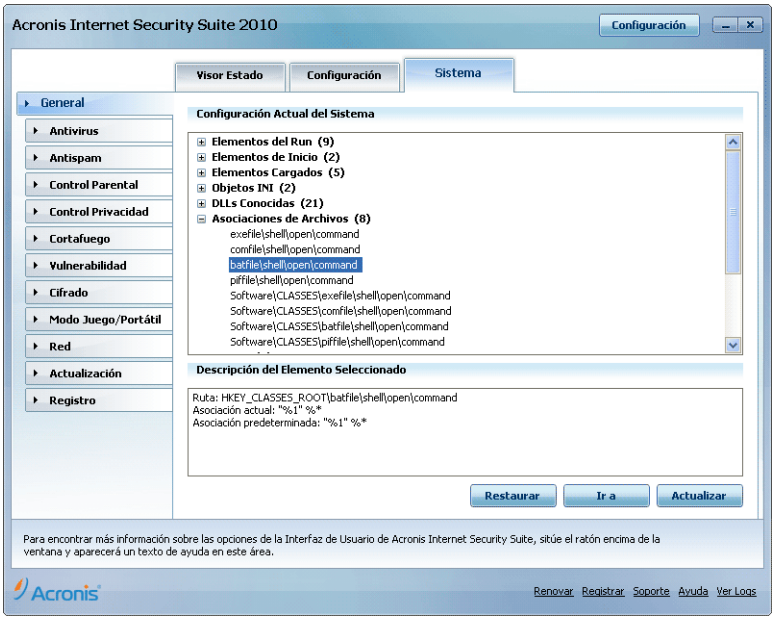
- **Activar la Detección de Epidemias de Acronis Internet Security Suite** - envía a los Labs de Acronis informes acerca de posibles epidemias de virus.

  Los informes no contendrán datos confidenciales, tales como su nombre, dirección IP u otra información, y no serán empleados con fines comerciales. La información enviada sólo contiene el posible virus y sólo será utilizada para detectar nuevos virus.

16.3. Información del Sistema

Acronis Internet Security Suite 2010 le permite ver, desde una sola ventana, todas las opciones y aplicaciones registradas para ejecutarse al iniciar el sistema. De esta manera, podrá monitorizar la actividad del sistema y de las aplicaciones instaladas, así como identificar posibles infecciones del sistema.

Para obtener información del sistema, diríjase a **General>Sistema** en el Modo Avanzado.



Información del Sistema

La lista contiene todos los objetos cargados cuando se inicia el sistema así como los objetos cargados por diferentes aplicaciones.

Hay tres botones disponibles:

- **Restaurar** - restaura la asociación actual del archivo a la asociación predeterminada. ¡Sólo disponible en la opción **Asociaciones de Archivos**!
- **Ir a** - abre una ventana para mostrar la ubicación del objeto seleccionado (el **Registro** por ejemplo).

> **Nota**
> En función del elemento seleccionado, puede que el botón **Ir a** no aparezca.

- **Refrescar** - re-abre la sección **Sistema**.

17. Antivirus

Acronis Internet Security Suite 2010 protege a su equipo frente a todo tipo de malware (virus, troyanos, spyware, rootkits y otros). La protección que ofrece Acronis Internet Security Suite 2010 está dividida en dos apartados:

- Protección en tiempo real - impide que las nuevas amenazas de malware entren en su sistema. Por ejemplo, Acronis Internet Security Suite 2010 analizará un documento de Word cuando lo abra, o los mensajes de correo a medida que los vaya recibiendo.

  Nota

  La protección en tiempo real también se denomina análisis al acceder, y se encarga de analizar los archivos a medida que los usuarios acceden a los mismos.

- Análisis bajo demanda - permite detectar y eliminar el malware que ya reside en el sistema. Este es el clásico análisis iniciado por el usuario - usted elije que unidad, carpeta o archivo debe analizar Acronis Internet Security Suite 2010, y Acronis Internet Security lo analizará bajo demanda. Las tareas de análisis le permiten crear rutinas de análisis personalizadas, que pueden planificarse para que se ejecuten regularmente.

17.1. Protección en tiempo real

Acronis Internet Security Suite 2010 le ofrece una protección ininterrumpida (Protección en Tiempo Real) frente a todo tipo de amenazas de malware, al analizar todos los archivos a los que accede, los mensajes y las comunicaciones a través de aplicaciones de mensajería instantánea (ICQ, NetMeeting, Yahoo! Messenger, MSN Messenger). El Antiphishing de Acronis Internet Security Suite 2010 le impide revelar información personal mientras navega por Internet, al avisarle cada vez que detecte una página web de phishing en potencia.

Para configurar la protección en Tiempo Real y Antiphishing, diríjase a **Antivirus>Residente** en Modo Avanzado.

Protección en tiempo real

Puede ver si la Protección en Tiempo Real está activada o desactivada. Si desea cambiar el estado de la Protección en Tiempo Real, desmarque o marque la casilla correspondiente.

Importante
Para impedir que los virus infecten su ordenador manenga la **Protección en Tiempo Real** activada.

Para iniciar un análisis de sistema, haga clic en **Analizar Ahora**.

17.1.1. Configurando el Nivel de Protección

Puede elegir el nivel de protección que mejor se adapte a sus necesidades de seguridad. Arrastre el deslizador a lo largo de la escala para elegir el nivel de protección adecuado.

Hay 3 niveles de seguridad:

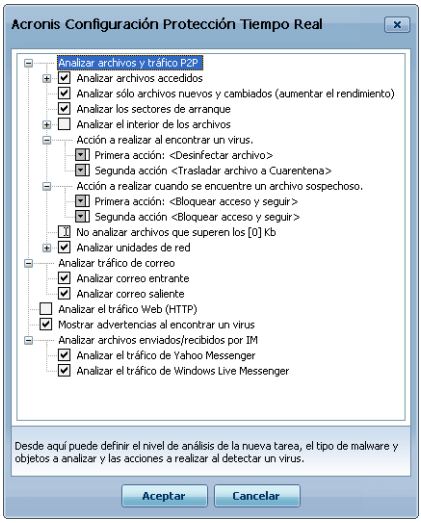
Nivel de Protección	Descripción
Tolerante	Cubre necesidades básicas de seguridad. El nivel de consumo de recursos es muy bajo. Los programas y mensajes entrantes se analizan sólo en busca de virus. Además del clásico análisis basado en firmas, se usa también el análisis heurístico. Las acciones que se realizan cuando se detectan archivos infectados son las siguientes: desinfectar archivo/mover archivo a cuarentena.
Por Defecto	Ofrece seguridad estándar. El nivel de consumo de recursos es bajo. Todos los archivos y correos entrantes&salientes son analizados por virus y spyware. Además del clásico análisis basado en firmas, se usa también el análisis heurístico. Las acciones que se realizan cuando se encuentran archivos infectados son las siguientes: desinfectar archivo/mover archivo a cuarentena.
Agresivo	Ofrece seguridad de alta calidad. El nivel de consumo de recursos es moderado. Todos los archivos y correos entrantes&salientes y el tráfico de web se analiza por virus y spyware. Además del clásico análisis basado en firmas, se usa también el análisis heurístico. Las acciones que se realizan cuando se encuentran archivos infectados son las siguientes: desinfectar archivo/mover archivo a la cuarentena.

Para aplicar la configuración predeterminada de la protección en tiempo real haga clic en **Por Defecto**.

17.1.2. Personalizando el Nivel de Protección

Los usuarios avanzados querrán aprovechar las opciones de análisis que Acronis Internet Security Suite 2010 ofrece. El análisis puede configurarse para que sólo se analicen un tipo de extensiones definidas, para buscar amenazas específicas, o para omitir archivos comprimidos. Esta característica permite disminuir notablemente los tiempos de análisis y mejorar el rendimiento de su equipo durante un análisis.

Puede personalizar la **Protección en Tiempo Real** haciendo clic en **Personalizado**. Se le mostrará la siguiente ventana:



Configuración de la Protección en Tiempo Real

Las opciones de análisis están organizadas en forma de menú extensible, de manera similar a los de Windows. Haga clic en la casilla "+" para desplegar una opción o en "-" para cerrarla.

Nota

Observará que ciertas opciones de análisis, aunque aparezca la seña "+" correspondiente, no se pueden extender debido a que estas opciones no han sido todavía seleccionadas. Notará que al seleccionarlas, se podrán extender.

- **Analizar ficheros accedidos y transferencias P2P** - analiza los ficheros accedidos y las comunicaciones mediante aplicaciones de mensajería instantánea (ICQ, NetMeeting, Yahoo! Messenger, MSN Messenger). Luego seleccione el tipo de ficheros a analizar.

Opción		Descripción
Analizar archivos accedidos	**Analizar todos los archivos**	Todos los ficheros serán analizados, independientemente de su tipo.
	Analizar sólo programas	Únicamente se analizarán los archivos con las siguientes extensiones: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`;

Opción		Descripción
		.wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml y .nws.
	Analizar extensiones definidas	Para analizar sólo los ficheros que tienen las extensiones especificadas por el usuario. Dichas extensiones deben estar separadas por ";".
	Analizar en busca de software de riesgo	Analizar en busca de software de riesgo. Los archivos detectados con este método se tratarán como archivos infectados. El software que incluya componentes de adware puede funcionar incorrectamente si esta opción está activada. Seleccionar **Omitir dialers y aplicaciones del análisis** y/o **Omitir keyloggers del análisis** si desea excluir este tipo de archivos del análisis.
Analizar sólo archivos nuevos y modificados		Analiza sólo ficheros que no han sido analizados anteriormente o que se han modificado desde la última vez que fueron analizados. Seleccionado esta opción, mejorará considerablemente el rendimiento general del sistema con una mínima compensación en seguridad.
Analizar los sectores de arranque		Para analizar el sector de arranque del sistema.
Analizar el interior de los archivos comprimidos		Para analizar el contenido de los archivos comprimidos. Con esta opción activada su ordenador puede ralentizarse un poco. Puede establecer el tamaño máximo de archivos que se analizaran (en kb, fijar 0 si desea que todos los archivos se analicen) y el tamaño máximo de archivo a analizar.
Primera acción		En el menú desplegable, seleccione la primera acción que desea realizar al encontrar archivos infectados o sospechosos.

Opción		Descripción
	Bloquear acceso y seguir	Si se detecta un archivo infectado, se bloqueará el acceso al mismo.
	Desinfectar archivo	Elimina el código de malware de los archivos infectados.
	Eliminar archivo	Elimina los archivos infectados inmediatamente y sin previa advertencia.
	Mover archivo a la cuarentena	Para trasladar los archivos infectados a la cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado.
Segunda acción		En el menú desplegable, seleccione la segunda acción que desea realizar al encontrar archivos infectados o sospechosos, en caso que falle la primera acción.
	Bloquear acceso y seguir	Si se detecta un archivo infectado, se bloqueará el acceso al mismo.
	Eliminar archivo	Elimina los archivos infectados inmediatamente y sin previa advertencia.
	Mover archivo a la cuarentena	Para trasladar los archivos infectados a la cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado.
No analizar archivos que superen los [x] Kb		Introduzca el tamaño máximo de los archivos a analizar. Si el tamaño es 0 Kb, se analizarán todos los archivos, independientemente de su tamaño.
Analizar recursos compartidos de red	**Analizar todos los archivos**	Todos los ficheros de la red serán analizados, independientemente de su tipo.
	Analizar sólo programas	Únicamente se analizarán los archivos con las siguientes extensiones: `.exe`; `.bat`; `.com`; `.dll`; `.ocx`; `.scr`; `.bin`; `.dat`; `.386`; `.vxd`; `.sys`; `.wdm`; `.cla`; `.class`; `.ovl`; `.ole`; `.exe`; `.hlp`; `.doc`; `.dot`; `.xls`; `.ppt`; `.wbk`; `.wiz`; `.pot`; `.ppa`; `.xla`; `.xlt`; `.vbs`; `.vbe`; `.mdb`; `.rtf`; `.htm`; `.hta`; `.html`; `.xml`; `.xtp`; `.php`; `.asp`; `.js`; `.shs`; `.chm`;

Opción		Descripción
		.lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml y .nws.
	Analizar extensiones definidas	Para analizar sólo los ficheros que tienen las extensiones especificadas por el usuario. Dichas extensiones deben estar separadas por ";".

- **Analizar correo** - analiza el correo electrónico.

  Tiene las siguientes opciones a su disposición:

Opción	Descripción
Analizar correo entrante	Analiza todos los correos entrantes.
Analizar correo saliente	Analiza todos los correos salientes.

- **Analizar el tráfico HTTP** - analiza el tráfico HTTP.
- **Mostrar advertencias al encontrar un virus** - mostrará una ventana de advertencia al detectarse un virus en un archivo o correo electrónico.

  Para un archivo infectado, la ventana de alerta mostrará el nombre del virus, la ruta y la acción ejecutada en el archivo infectado. Para un e-mail infectado, la ventana de alerta contendrá también información sobre el remitente y el receptor.

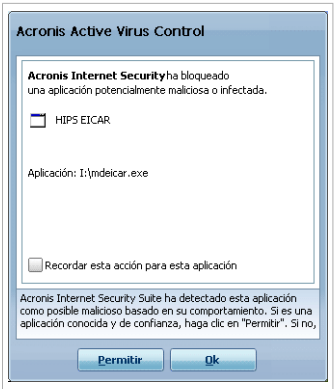
  Si el programa detecta ficheros sospechosos, puede iniciar el asistente desde la ventana de alertas para enviar el fichero al Laboratorio Acronis. Una vez analizado, puede recibir información por mail a la dirección mencionada en el asistente.
- **Analizar archivos enviados/recibidos por IM.** Para analizar los archivos que reciba o envíe a través de Yahoo Messenger o Windows Live Messenger, seleccione la casilla correspondiente.

Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

17.1.3. Configurar Active Virus Control

La tecnología Active Virus Control de Acronis Internet Security Suite 2010 proporcionar una capa de protección contra nuevas amenazas para las cuales todavia no existe una firma de malware. Monitoriza y analiza constantemente el comportamiento de las aplicaciones que se ejecutan en su equipo y le avisa si alguna aplicación tiene un comportamiento sospechoso.

Active Virus Control puede ser configurado para avisarle y pedirle que realice una acción cuando una aplicación intentar realizar una posible acción maliciosa.



Alerta de Active Virus Control

Si conoce y confía en la aplicación detectada, haga clic en **Permitir**.

Si desea cerrar la aplicación de inmediato, haga clic en **Aceptar**.

Marque la casilla **Recordar esta acción para esta aplicación** antes de hacer su elección y Acronis Internet Security Suite 2010 realizará la misma acción cuando la aplicación se detecte en el futuro. La regla que ha creado se mostrará en la ventana de configuración de Active Virus Control

Para configurar Active Virus Control, haga clic en **Opciones Avanzadas**.

Opciones Active Virus Control

Seleccione la casilla correspondiente para activar el Active Virus Control.

Importante

Mantenga el Active Virus Control activado para estar protegido frente a virus desconocidos.

Si desea que se le avise y se le pida una acción a realizar por el Active Virus Control cuando una aplicación intentar realizar una acción posiblemente maliciosa, seleccione la casilla **Preguntarme antes de realizar una acción**.

Configurando el Nivel de Protección

El nivel de protección de Active Virus Control cambia cuando establece un nuevo nivel de protección en tiempo real. Si no está satisfecho con el nivel de protección predeterminado, puede configurar manualmente el nivel de protección.

Nota

Recuerde que si cambia el actual nivel de protección en tiempo real, el nivel de protección de Active Virus Control cambiará en consecuencia. Si establece la protección en tiempo real en **Tolerante**, Active Virus Control se desactivará automáticamente. En este caso, puede activar Active Virus Control manualmente si desea utilizarlo.

Mueva el control deslizante hasta el nivel de protección que mejor se ajuste a sus necesidades.

Nivel de Protección	Descripción
Crítico	Monitorización estricta para todas las aplicaciones por posibles acciones maliciosas.
Por Defecto	El ratio de detección es alto y son posibles falsos positivos.
Mediana	La monitorización es moderada, algunos falsos positivos son aun posibles.
Tolerante	El ratio de detección es bajo y no hay falsos positivos.

Administrar Aplicaciones De confianza / Desconfianza

Usted puede añadir aplicaciones que conozca y en las que confie a la lista de aplicaciones de confianza. Estas aplicaciones no serán comprobadas por el control de virus activo y automáticamente se les permitirá acceso.

Las aplicaciones para las que ha creado reglas están listadas en la tabla de **Exclusiones**. La ruta de la aplicación y la acción que ha establecido para esta (Permitido o Bloqueado) es visualizada para cada regla.

Para cambiar la acción para una aplicación, haga clic en la acción actual y selecciones otra acción desde el menú.

Para administrar la lista, utilice los botones colocados encima de la tabla:

- **Añadir** - añadir una nueva aplicación a la lista.
- **Eliminar** - eliminar una aplicación de la lista.
- **Editar** - editar una regla de aplicación.

17.1.4. Desactivando la Protección en Tiempo Real

Si decide desactivar la protección en tiempo real, aparecerá una ventana de advertencia. Para confirmar su elección, deberá indicar durante cuanto tiempo desea desactivar la protección. Puede desactivar la protección durante 5, 15 o 30 minutos, durante una hora, de forma permanente, o hasta que reinicie el sistema.

Aviso

Se trata de una cuestión crítica para la seguridad de su sistema. Recomendamos desactivar la protección en tiempo real durante el menor tiempo posible. Mientras la protección esté desactivada, no tendrá protección contra amenazas de malware.

17.1.5. Configurando la Protección Antiphishing

Acronis Internet Security Suite 2010 ofrece protección antiphishing en tiempo real para:

- Internet Explorer
- Mozilla Firefox
- Yahoo! Messenger
- Windows Live (MSN) Messenger

Puede elegir entre desactivar la protección antiphishing por completo, o sólo para alguna de estas aplicaciones.

Haga clic en **Lista Blanca** para configurar y administrar la lista de páginas web que no deben analizarse con los motores Antiphishing de Acronis Internet Security Suite 2010.

Lista Blanca Antiphishing

Puede ver las páginas web que no están siendo analizadas por Acronis Internet Security Suite 2010 en busca de phishing.

Para añadir una página a la Lista Blanca, introduzca la dirección en el campo **Nueva dirección** y haga clic en **Añadir**. La Lista Blanca sólo debería contener páginas web en las que confíe plenamente. Por ejemplo, añada las páginas web en las que realice compras online.

Nota

Puede añadir páginas web la Lista Blanca fácilmente desde la barra de herramientas de Acronis Antiphishing integrada en su navegador web. Para más información, por favor diríjase a *"Integración con Navegadores Web"* (p. 272).

Si desea quitar una página web de la Lista Blanca, haga clic en el botón **Quitar** correspondiente.

Haga clic en **Guardar** para guardar los cambios y cerrar la ventana.

17.2. Análisis bajo demanda

El objetivo principal de Acronis Internet Security Suite 2010 es mantener su ordenador libre de virus. Los primeros dos pasos para lograr tal meta constan en

impedir el acceso de nuevos virus a su sistema y en analizar sus mensajes de correo y cualquier fichero descargado o copiado en su PC.

Existe riesgo de que un virus haya ingresado en su sistema antes de que instale Acronis Internet Security Suite 2010. Por esta razón le recomendamos analizar su equipo antes de instalar Acronis Internet Security Suite 2010. Es definitivamente buena idea también realizar un análisis frecuente en su equipo en busca de virus.

Para configurar e iniciar un análisis bajo demanda, vaya a **Antivirus>Analizar** en Modo Avanzado.

Tareas de Análisis

El análisis bajo demanda se basa en tareas de análisis. Estas tareas indican las opciones y los objetivos a analizar. Puede analizar el equipo cuando desee ejecutar las tareas por defecto o creando sus tareas propias (tareas definidas por el usuario). También puede planificar las tareas para que se realicen en momentos en que el sistema esté inactivo y no interfieran con su trabajo.

17.2.1. Tareas de Análisis

Acronis Internet Security Suite 2010 incluye diferentes tareas predeterminadas que cubren las necesidades de seguridad más comunes. Pero también puede crear sus propias tareas de análisis personalizadas.

Existen 3 tipos de tareas de análisis:

- **Tareas de Sistema** - contiene una lista de tareas de sistema predeterminadas. Las siguientes tareas están disponibles:

Tarea Predeterminada	Descripción
Análisis en Profundidad	Analiza el sistema por completo. En la configuración predeterminada, analiza en busca de cualquier tipo de malware que pueda amenazar a su sistema, como virus, spyware, adware, rootkits y otros.
Análisis de sistema	Analiza todo el sistema, excepto los archivos comprimidos. En la configuración predeterminada, busca todos los tipos de malware distintos a rootkits.
Análisis Rápido del Sistema	Analiza las carpetas de `Windows` y `Archivos de Programa`. En la configuración predeterminada, analiza en busca de cualquier tipo de malware, excepto rootkits, pero no analiza la memoria, el registro ni las cookies.
Análisis del Autologon	Analiza los elementos que se ejecutan cuando un usuario inicia sesión en Windows. Por defecto, el análisis automático al iniciar sesión está desactivado. Si desea utilizar esta tarea, haga clic derecha sobre ella, seleccione **Programar** y configure la tarea para ejecutarse **al iniciar el sistema**. Puede especificar cuanto tiempo después del inicio del sistema debe ejecutarse la tarea (en minutos).

Nota

A través de las tareas **Análisis en Profundidad** y **Análisis Completo** puede analizar el sistema por completo, pero el proceso requerirá bastante tiempo. Por ello, recomendamos ejecutar estas tareas con baja prioridad, o preferiblemente, cuando no utilice el equipo.

- **Tareas del Usuario** - contiene las tareas definidas por el usuario.

  Existe una tarea llamada `Mis Documentos`. Utilice esta tarea para analizar las carpetas del usuario que está utilizando: `Mis Documentos`, `Escritorio` e `Inicio`. Así se asegurará el contenido de sus documentos, un espacio de trabajo seguro y que las aplicaciones iniciadas al cargar el sistema están limpias.

- **Otras tareas** - contiene una lista de otras tareas de análisis. Estas tareas de análisis se refieren a tipos de análisis alternativos que no se pueden ejecutar desde esta ventana. Sólo puede modificar sus opciones o ver los informes de análisis.

Cada tarea tiene una ventana de **Propiedades** que le permite configurarlas y ver los informes de análisis. Para abrir esta ventana, doble clic en la tarea o clic en el botón **Propiedades** que precede al nombre de la tarea. Para más información, por favor diríjase a "*Configurando una Tarea de Análisis*" (p. 128).

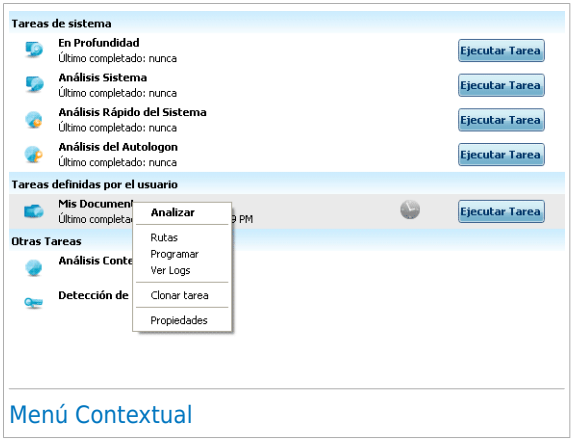
Para ejecutar una tarea de análisis de sistema o definida por el usuario, haga clic en el botón correspondiente a **Ejecutar Tarea**. El Asistente de Análisis Antivirus aparecerá y le guiará a través del proceso de análisis.

Cuando una tarea esta programada para ejecutarse automáticamente, más tarde o regularmentem, el botón **Programar** se mostrará en la derecha de la tarea. Haga clic en este botón para abrir la ventana de **Propiedades**, pestaña Programador, donde puede ver la tarea programada y modificarla.

Si ya no necesita una tarea de analisis que ha creado (tarea definida por el usuario), puede eliminarla haciendo clic en el botón **Eliminar**, ubicado a la derecha de la tarea. No puede eliminar tareas del sistema o misceláneas.

17.2.2. Utilizando el Menú Contextual

Dispone de un menú contextual para cada tarea. Haga clic con el botón derecho sobre la tarea seleccionada para abrirlo.



Menú Contextual

Para las tareas de sistema y las definidas por el usuario, las opciones están disponibles en el menú:

- **Analizar** - ejecuta la tarea seleccionada, iniciando inmediatamente el análisis.
- **Ruta** - abre la ventana de **Propiedades**, pestaña Ruta, dónde podrá cambiar el objetivo del análisis de la tarea seleccionada.

Nota
En las tareas del sistema, esta opción será reemplazada por **Mostrar rutas de Análisis**, donde podrá ver las rutas que se analizarán.

- **Programador** - abre la ventana de **Propiedades**, pestaña Programador, dónde podrá cambiar la planificación de la tarea seleccionada.
- **Ver Informes** - abre la ventana de **Propiedades**, pestaña Informes, dónde podrá ver los informes generados tras la realización del análisis.
- **Duplicar** - duplica la tarea seleccionada. Esta opción es muy útil para crear nuevas tareas, ya que puede modificar las opciones de la tarea duplicada.
- **Eliminar** - elimina la tarea seleccionada.

Nota
No disponible para tareas de sistema. No se puede eliminar una tarea de sistema.

- **Propiedades** - abre la ventana de **Propiedades**, pestaña General, dónde podrá cambiar las opciones de la tarea seleccionada.

Debido a la particular naturaleza de las **Otras Tareas**, sólo estarán disponibles las opciones **Propiedades** y **Ver Informes de Análisis**.

17.2.3. Creando tareas de análisis

Para crear una tarea de análisis, utilice uno de estos métodos:

- Duplicar una regla existente, cambie su nombre y haga las modificaciones necesarias en la ventana Propiedades.
- Haga clic en **Nueva tarea** para crear una nueva tarea y configurarla.

17.2.4. Configurando una Tarea de Análisis

Cada tarea de análisis tiene su ventana de **Propiedades**, donde puede configurar las opciones de análisis, el objeto de análisis, programar la tarea o ver los informes. Para abrir esta ventana haga clic en el botón **Propiedades**, situado a la izquierda de la tarea (o haga doble clic sobre la tarea y clic en **Propiedades**). También puede hacer doble clic en la tarea.

Nota
Para ver más información de los informes y la pestaña **Ver Informes**, por favor diríjase a "*Viendo los Informes del Análisis*" (p. 148).

Configurando las Opciones de Análisis

Para configurar las opciones de análisis de una tarea de análisis, haga clic derecho y seleccione **Propiedades**. Aparecerá la siguiente pantalla:

Vista general

Aquí puede ver información acerca de la tarea (nombre, última ejecución y próxima ejecución programada) y configurar las opciones de análisis.

Seleccionando el nivel de Análisis

Puede configurar fácilmente las opciones de análisis a través del deslizador. Arrastre el deslizador a lo largo de la escala para elegir el nivel de análisis deseado.

Hay 3 niveles de análisis:

Nivel de Protección	Descripción
Tolerante	Ofrece un nivel razonable de eficacia de detección. El nivel del consumo de recursos es bajo. Sólo los programas se analizan en busca de virus. Además del clásico análisis basado en firmas de virus, se usa también el análisis heurístico.
Mediana	Ofrece un buen nivel de eficacia de detección. El nivel del consumo de recursos es moderado. Todos los archivos se analizan en busca de virus y spyware. Además del clásico análisis basado en fimas de virus, se usa también el análisis heurístico.
Agresivo	Ofrece un alto nivel de eficacia de detección. El nivel del consumo de recursos es alto.

Nivel de Protección	Descripción
	Todos los archivos comprimidos se analizan en busca de virus y spyware. Además del clásico análisis basado en fimas de virus, se usa también el análisis heurístico.

También hay disponibles una serie de opciones generales para el proceso de análisis:

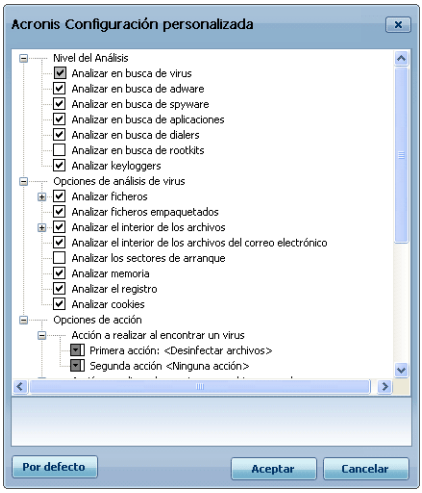
- **Ejecutar el análisis con prioridad baja.** Disminuye la prioridad del proceso de análisis. De este modo los otros programas funcionarán más rápido, pero incrementará el tiempo necesario para realizar el análisis.
- **Minimizar Asistente de Análisis a la barra de tareas.** Minimiza la ventana de análisis a la barra de tareas. Doble click en el icono de Acronis para abrirla.
- **Apagar el equipo al finalizar el análisis, si no se han detectado amenazas**

Haga clic en **Aceptar** para guardar los cambios realizados y cerrar la ventana. Para ejecutar la tarea sólo tiene que hacer clic en **Analizar**.

Optimizando el nivel de análisis

Los usuarios avanzados querrán aprovechar las opciones de análisis que Acronis Internet Security Suite 2010 ofrece. El análisis puede configurarse para que sólo se analicen un tipo de extensiones definidas, para buscar amenazas específicas, o para omitir archivos comprimidos. Esta característica permite disminuir notablemente los tiempos de análisis y mejorar el rendimiento de su equipo durante un análisis.

Haga clic en **Personalizado** para configurar sus propias opciones de análisis. Aparecerá una nueva ventana.



Opciones de análisis

Las opciones de análisis están organizadas en forma de menú extensible, de manera similar a los de Windows. Haga clic en la casilla "+" para desplegar una opción o en "-" para cerrarla.

Las opciones de análisis se agrupan en 3 categorías:

- **Nivel de Análisis.** Seleccione el tipo de malware que desea analizar con Acronis Internet Security Suite 2010 y las opciones deseadas desde la categoría **Nivel de Análisis**.

Opción	Descripción
Analizar en busca de virus	Analizar en busca de virus conocidos. Acronis Internet Security Suite 2010 detecta también cuerpos de virus incompletos, eliminando así cualquier posible amenaza que pueda afectar la seguridad de su sistema.
Analizar en busca de adware	Analiza en busca de adware. Estos archivos se tratarán como si fuesen archivos infectados. El software que incluya componentes adware puede dejar de funcionar si esta opción está activada.
Analizar en busca de spyware	Analiza en busca de spyware. Estos archivos se tratarán como si fuesen archivos infectados.

Opción	Descripción
Analizar en busca de aplicaciones	Analiza en busca de aplicaciones legítimas que pueden utilizarse como herramientas de espionaje, para ocultar aplicaciones maliciosas u otros fines maliciosos.
Analizar en busca de dialers	Analiza en busca de dialers de números de alta tarificación. Estos ficheros se tratarán como fuesen si ficheros infectados. El software que incluya componentes dialer puede dejar de funcionar si esta opción está activada.
Analizar en busca de Rootkits	Analizar en busca de objetos ocultos (archivos y procesos), generalmente denominados rootkits.

- **Opciones de análisis de virus.** Indique el tipo de objetos a analizar (tipos de archivo, comprimidos y otros) seleccionado las opciones adecuadas en la categoría **Opciones de análisis de virus**.

Opción		Descripción
Analizar ficheros	**Analizar todos los archivos**	Se analizarán todos los archivos, independientemente de su tipo.
	Analizar sólo programas	Para analizar sólo archivos con las siguientes extensiones: exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; exe; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml and nws.
	Analizar extensiones definidas	Para analizar sólo los ficheros que tienen las extensiones especificadas por el usuario. Dichas extensiones deben estar separadas por ";".
Analizar archivos empaquetados		Para analizar en el interior de los programas empaquetados.
Analizar el interior de los archivos comprimidos		Analizar en el interior de archivos comunes, como .zip, .rar, .ace, .iso y otros. Seleccionar la casilla de **Análisis de instaladores y archivos chm** si desea que estos tipos de archivos sean analizados.

Opción	Descripción
	El análisis de los archivos comprimidos incrementa el tiempo de análisis y requiere más recursos del sistema. Puede establecer el tamaño máximo de los archivos que serán analizados en Kilobytes (KB)escribiendo el tamaño en esta celda **Limitar el tamaño de archivo a analizar a**.
Analizar los archivos adjuntos del correo	Para analizar el interior de los archivos comprimidos del correo electrónico.
Analizar los sectores de arranque	Para analizar el sector de arranque del sistema.
Analizar memoria	Analiza la memoria en busca de virus y otros tipos de malware.
Analizar registro	Analiza las entradas del registro.
Analizar cookies	Analiza los archivos cookie.

- **Opciones de acción.** Especificar que acciones se deben realizar en cada una de las categorías de los archivos detectados utilizando las opciones en esta categoría.

  Nota

  Para establecer una nueva acción, haga clic la actual **Primera acción** y seleccione la opción deseada desde el menú. Especificar una **Segunda acción** que se realizará en caso de que la primera falle.

  ▶ Seleccione la acción a realizar cuando se detecte un archivo infectado. Tiene las siguientes opciones a su disposición:

Acción	Descripción
Ninguna Acción	No se realizará ninguna acción con los ficheros infectados. Estos ficheros aparecerán en el informe de análisis.
Desinfectar archivos	Elimina el código de malware de los archivos infectados detectados.
Eliminar archivos	Elimina los archivos infectados inmediatamente y sin previa advertencia.
Mover a la Cuarentena	Para trasladar los archivos infectados a la cuarentena. Los archivos en cuarentena no pueden

Acción	Descripción
	ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado.

▶ Seleccione la acción que desea que se realice al encontrar archivos sospechosos. Tiene las siguientes opciones a su disposición:

Acción	Descripción
Ninguna Acción	No se realizará ninguna acción con los archivos sospechosos. Estos archivos aparecerán en el informe de análisis.
Eliminar archivos	Elimina los archivos sospechosos inmediatamente y sin previa advertencia.
Mover a la Cuarentena	Trasladar los archivos sospechosos a la cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado.

Nota

Si durante el análisis se detectan archivos sospechosos, se le solicitará enviarlos a los Laboratorios de Acronis.

▶ Seleccione la acción a realizar cuando se detecten objetos ocultos (rootkits). Tiene las siguientes opciones a su disposición:

Acción	Descripción
Ninguna Acción	No se realizará ninguna acción con los archivos ocultos. Estos archivos aparecerán en el informe de análisis.
Renombrar ficheros	Renombra los ficheros ocultos añadiendo `.bd.ren` a su nombre. Como resultado, podrá buscar y encontrar estos ficheros en su equipo, en caso de que existan.
Mover a la Cuarentena	Trasladar los archivos infectados a la cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado.

Nota

Por favor tenga en cuenta que estos ficheros ocultos no son ficheros que usted ocultó de Windows. Son fichero ocultados por programas especiales, conocidos como rootkits. Los rootkits no son maliciosos por naturaleza. De todas maneras, son utilizados normalmente para hacer que los virus o spyware no sean detectados por programas normales antivirus.

▶ **Opciones de acción para archivos protegidos por contraseña y cifrados.** Ficheros cifrados utilizando Windows pueden ser importantes para usted. Por esta razón puede configurar distintas acciones para los ficheros infectados o sospechosos que están cifrados por Windows. Otra categoría de archivos que necesitan acciones especiales son los archivos protegidos por contraseña. Los archivos comprimidos protegidos con contraseña no pueden ser analizados, a no ser que introduzca la contraseña. Utilice estas opciones para configurar las acciones a realizar en los archivos protegidos por contraseña y los archivos cifrados por Windows.

– **Acción a realizar al encontrar un archivo cifrado.** Seleccione la acción a realizar en los ficheros infectados cifrados por Windows. Tiene las siguientes opciones a su disposición:

Acción	Descripción
No Realizar Ninguna Acción	Sólo guardar en el informe los ficheros infectados que están cifrados por Windows. Al finalizar el proceso de análisis, puede abrir el informe para ver información sobre estos archivos.
Desinfectar archivos	Elimina el código de malware de los archivos infectados detectados. La desinfección puede fallar en algunos casos, por ejemplo, cuando el archivo infectado se encuentra dentro de un archivo de datos del correo.
Eliminar archivos	Elimina de forma inmediata los archivos infectados, sin mostrar advertencia alguna.
Mover a la Cuarentena	Traslada los archivos infectados de su ubicación original a la carpeta de la cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado.

- **Acción a realizar al encontrar un archivo cifrado sospechoso.** Seleccione la acción a realizar en los ficheros sospechosos que están cifrados con Windows. Tiene las siguientes opciones a su disposición:

Acción	Descripción
No Realizar Ninguna Acción	Sólo guardar en el informe los ficheros sospechosos que están cifrados por Windows. Al finalizar el proceso de análisis, puede abrir el informe para ver información sobre estos archivos.
Eliminar archivos	Elimina los archivos sospechosos inmediatamente y sin previa advertencia.
Mover a la Cuarentena	Trasladar los archivos sospechosos a la cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado.

- **Acción a realizar al encontrar un archivo protegido por contraseña.** Seleccione la acción a realizar al detectar archivos protegidos con contraseña. Tiene las siguientes opciones a su disposición:

Acción	Descripción
Sólo registro	Sólo registra los archivos comprimidos protegidos con contraseña en el informe del análisis. Al finalizar el proceso de análisis, puede abrir el informe para ver información sobre estos archivos.
Solicitar contraseña	Al detectar un archivo comprimido protegido con contraseña, solicitará la contraseña al usuario para poder analizar el contenido del archivo.

Si hace clic en **Por defecto** cargará la configuración predeterminada. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

Estableciendo el Objetivo del Análisis

Para configurar el objetivo de análisis en una tarea de análisis especifica de usuario, haga clic derecho en la tarea y seleccione **Rutas**. Alternativamente, si ya está en la venta de Propiedades de la tarea, seleccione la pestaña **Rutas**. Aparecerá la siguiente pantalla:

Objetivo del Análisis

Puede ver la lista de unidades locales, de red o extraibles, así como las carpetas y los archivos añadidos anteriormente si existen. Todos los elementos seleccionados serán analizados cuando ejecute la tarea.

Dispone de los siguientes botones:

- **Añadir Archivo(s)** - abre una ventana de exploración desde la que podrá seleccionar el archivo(s) / carpeta(s) que desea analizar.

  Nota
  En la sección de análisis puede añadir ficheros o directorios para ser analizados, seleccionándolos y arrastrándolos.

- **Eliminar elementos** - borra del listado de análisis el fichero / directorio seleccionado anteriormente.

  Nota
  Solamente los ficheros / carpetas añadidos posteriormente se podrán borrar, pero no aquellos automáticamente "vistos" por Acronis Internet Security Suite 2010.

Además de estos botones, también hay algunas opciones que le permite seleccionar más rápido las ubicaciones de análisis.

- **Unidades locales** - para analizar las particiones locales.
- **Unidades de red** - para analizar las particiones de red.

- **Unidades extraíbles** - para analizar las unidades extraíbles (CD-ROM, disqueteras).
- **Todas las unidades** - para analizar todas las particiones, independientemente de que sean locales, de red o extraíbles.

Nota

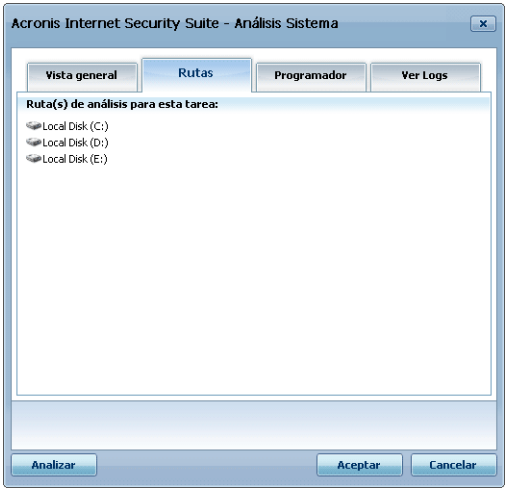
Si desea analizar todo el sistema en busca de virus, seleccione la casilla correspondiente a **Todas las unidades**.

Haga clic en **Aceptar** para guardar los cambios realizados y cerrar la ventana. Para ejecutar la tarea sólo tiene que hacer clic en **Analizar**.

Visualizando los el Objeto de Análisis de las Tareas del Sistema

No puede modificar los objetos de análisis de las tareas de la categoría **Tareas del Sistema**. Sólo podrá ver su objeto de análisis.

Puede ver el objetivo de análisis de una tarea de sistema, clic derecho en la tarea y seleccione **Mostrar Ruta de Análisis**. Por ejemplo, en la tarea **Análisis Completo**, aparecerá la siguiente ventana:



Objetos de Análisis de Sistema.

Las tareas **Análisis Completo** y **Análisis en Profundidad** analizarán todas las unidades locales, mientras que la tarea **Análisis Rápido del Sistema** sólo analizará las carpetas `Windows` y `Archivos de Programa`.

Haga clic en **Aceptar** para cerrar la ventana. Para iniciar la tarea, haga clic en **Analizar**.

Programando Tareas de Análisis

Si realiza un análisis complejo, el proceso de análisis requerirá bastante tiempo, y funcionará mejor si se cierran los otros programas que puedan estar abiertos. Por esta razón es aconsejable que programe este tipo de tareas con antelación, para que se inicien en aquellos momentos en los que no utilice el ordenador y éste se encuentre inactivo.

Para ver la planificación de una tarea especifica o modificarla, clic derecho en la tarea y seleccionar **Planificación**. Si ya esta en una ventana de Propiedades de tarea, seleccione la pestaña **Planificar**. Aparecerá la siguiente pantalla:

Programador

Podrá ver la planificación de la tarea.

Al programar una tarea, debe seleccionar una de las siguientes opciones:

- **No** - inicia la tarea sólo cuando el usuario lo solicita.
- **Una sola vez** - inicia el análisis sólo una vez, en determinado momento. Indique la fecha y hora de inicio en los campos **Fecha y hora de inicio**.
- **Periódicamente** - lanza el análisis periódicamente, a ciertos intervalos de (minutos, horas, días, semanas, meses, años) empezando por una fecha y hora específicas.

  Si quiere repetir el análisis cada cierto tiempo, seleccione la casilla **Periódicamente** e indique en **Cada** casilla el número de minutos/horas/días/semanas/meses/años indicando la frecuencia con la que desea

repetir el proceso. También puede indicar la fecha y hora de inicio en los campos **Fecha y hora de inicio**.

- **Al iniciar el sistema** - inicia un análisis cuando transcurran los minutos indicados después que el usuario inicie sesión en Windows.

Haga clic en **Aceptar** para guardar los cambios realizados y cerrar la ventana. Para ejecutar la tarea sólo tiene que hacer clic en **Analizar**.

17.2.5. Analizando los Archivos y Carpetas

Antes de iniciar un proceso de análisis, debe asegurarse que Acronis Internet Security Suite 2010 esta actualizado con sus firmas de malware. Analizar su equipo utilizando la base de firmas no actualizada puede impedir que Acronis Internet Security Suite 2010 detecte nuevo malware encontrado desde la última actualización. Para verificar cuando se realizó la última actualización, diríjase a **Actualización** en modo avanzado.

Nota

Para hacer un análisis completo de su sistema con Acronis Internet Security Suite 2010 es necesario cerrar todos los programas abiertos. Especialmente, es importante cerrar su cliente de correo electrónico (por ejemplo: Outlook, Outlook Express o Eudora).

Consejos de Análisis

Aquí puede encontrar algunos consejos de análisis que pueden ser de utilidad:

- Dependiendo del tamaño de su disco duro, la ejecución de un análisis completo de su equipo (como por ejemplo un Análisis Completo de Sistema o un Análisis en Profundidad) puede tardar un tiempo (hasta una hora o más). Por esta razón, debe realizar estos análisis cuando no necesita utilizar su equipo durante un tiempo (por ejemplo, por la noche).

  Puede programar un análisis para iniciarse cuando le sea necesario. Asegúrese de dejar su equipo encendido. Con Windows Vista, asegúrese de que su equipo no está en modo hibernación cuando la tarea está programada para ejecutarse.

- Si descarga frecuentemente archivos desde Internet en una carpeta específica, cree una nueva tarea de análisis y configure esa carpeta como ruta de análisis.. Programe la tarea para ejecutarse cada día o más a menudo.

- Existe un tipo de malware que se configura para ejecutarse al inicio del sistema cambiando opciones de Windows. Para proteger su equipo frente a este tipo de malware, puede programar una tarea de **Análisis del Autologon** para ejecutarse al inicio del sistema. Por favor tenga en cuenta que el análisis del autologon puede afectar el rendimiento del sistema por un período limitado después del inicio.

Métodos de Análisis

Acronis Internet Security Suite 2010 proporciona cuatro tipo de análisis bajo demanda:

- Análisis Inmediato - ejecuta una de las tareas de análisis del sistema o definidas por el usuario.
- Análisis Contextual - haga clic con el botón derecho en el fichero o carpeta que desee analizar y seleccione **Analizar con Acronis Internet Security Suite**.
- Análisis Arrastrar y Soltar - arrastre y suelte un archivo o la carpeta sobre la Barra de Actividad de Análisis.
- Análisis Manual - utilice el Análisis Manual de Acronis para seleccionar directamente los archivos y carpetas a analizar.

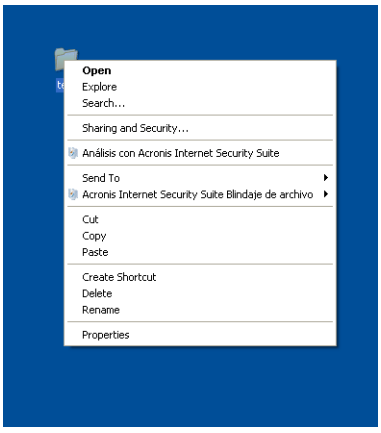
Análisis Inmediato

Para analizar su sistema o parte del mismo, puede usar las tareas de análisis predeterminadas o crear sus propias tareas de análisis. A esto se le llama análisis inmediado.

Para ejecutar una tarea de análisis de sistema o definida por el usuario, haga clic en el botón correspondiente a **Ejecutar Tarea**. El Asistente de Análisis Antivirus aparecerá y le guiará a través del proceso de análisis.

Análisis Contextual

Para analizar un archivo o carpeta sin tener que configurar una nueva tarea, puede utilizar el menú contextual. A esto se le llama análisis contextual.



Análisis Contextual

Haga clic derecho en el archivo o carpeta que desee analizar y seleccione la opción **Analizar con Acronis Internet Security Suite**. El Asistente de Análisis Antivirus aparecerá y le guiará a través del proceso de análisis.

Puede modificar las opciones del análisis o ver los informes en la ventana **Propiedades** de la tarea **Análisis del Menú Contextual**.

Análisis al Arrastrar y Soltar

Arrastre el archivo o la carpeta que desea analizar y suéltelo sobre la **Barra de Actividad del Análisis**, tal y como se puede ver en las siguientes imágenes.

Arrastrar Archivo

Soltar Archivo

El Asistente de Análisis Antivirus aparecerá y le guiará a través del proceso de análisis.

Análisis Manual

El análisis manual consiste en seleccionar directamente el objeto a analizar utilizando la opción Análisis Manual Acronis desde el grupo de programas de Acronis Internet Security Suite 2010 en el menú Inicio.

Nota
El análisis manual es muy útil, y puede utilizarse cuando inicie Windows en modo seguro.

Para seleccionar el objeto a ser analizado por Acronis Internet Security Suite 2010, en el menú Inicio de Windows, siga la ruta **Inicio → Programas → Acronis → Acronis Internet Security Suite 2010 → Acronis Análisis Manual**. Aparecerá la siguiente pantalla:

Análisis Manual

Haga clic en **Añadir Carpeta**, seleccione la ubicación que desea analizar y haga clic en **Aceptar**. Si desea analizar múltiples carpetas, repita esta acción para cada ubicación adicional.

Las rutas de las ubicaciones seleccionadas aparecerán en la columna **Ruta**. Si cambia de idea y desea eliminar alguno de los elementos seleccionados, simplemente haga clic en el botón **Quitar** situado junto a este elemento. Haga clic en el botón **Eliminar todas las Rutas** para eliminar todas las ubicaciones que están en la lista.

Cuando ha seleccionado las ubicaciones, haga clic en **Continuar**. El Asistente de Análisis Antivirus aparecerá y le guiará a través del proceso de análisis.

Asistente del análisis Antivirus

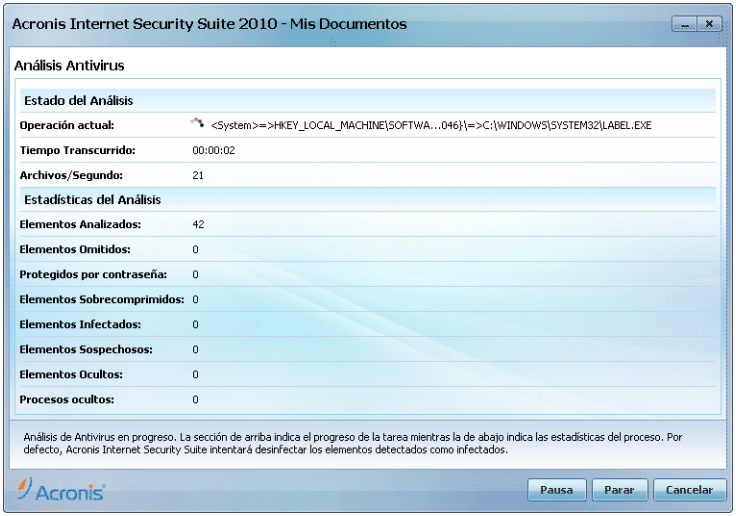
Cuando ejecute un análisis bajo demanda aparecerá el Asistente del análisis Antivirus. Siga el proceso guiado de tres pasos para completar el proceso de análisis.

Nota

Si el asistente de análisis no aparece, puede que el análisis esté configurado para ejecutarse en modo silencioso, en segundo plano. Busque en el icono de progreso de análisis en la barra de tareas. Puede hacer clic en este icono para abrir la ventana de análisis y ver el progreso del análisis.

Paso 1/3 – Analizando

Acronis Internet Security Suite 2010 comenzará el análisis de los objetos seleccionados.



Analizando

Puede ver el estado y las estadísticas del análisis (velocidad de análisis, número de archivos analizados / infectados / sospechosos / objetos ocultos y otros).

Espere a que Acronis Internet Security Suite 2010 finalice el análisis.

Nota
El análisis puede llevar un tiempo, dependiendo de la compejidad del análisis.

Archivos protegidos por contraseña. Si Acronis Internet Security Suite 2010 detecta un archivo protegido por contraseña durante el análisis y la acción por defecto es **Solicitar contraseña**, se le pedirá introducir la contraseña. Los archivos comprimidos protegidos con contraseña no pueden ser analizados, a no ser que introduzca la contraseña. Tiene las siguientes opciones a su disposición:

- **Contraseña.** Si desea que Acronis Internet Security Suite 2010 analice el archivo, seleccione esta opción e introduzca la contraseña. Si no conoce la contraseña, elija una de las otras opciones.
- **No preguntar por una contraseña y omitir este objeto del análisis.** Marque esta opción para omitir el análisis de este archivo.

- **Omitir todos los elementos protegidos con contraseña sin analizarlos.** Seleccione esta opción si no desea que se le pregunte acerca de archivos protegidos por contraseña. Acronis Internet Security Suite 2010 no podrá analizarlos, pero se guardará información acerca de ellos en el informe de análisis.

Haga clic en **Aceptar** para continuar el análisis.

Detener o pausar el análisis. Puede detener el análisis en cualquier momento, haciendo clic en botón **Parar**. Irá directamente al último paso del asistente. Para detener temporalmente el proceso de análisis, haga clic en **Pausa**. Para seguir con el análisis haga clic en **Reanudar**.

Paso 2/3 – Seleccionar Acciones

Cuando el análisis haya finalizado, aparecerá una nueva ventana donde podrá ver los resultados del análisis.

Acciones

Puede ver el número de incidencias que afectan a su sistema.

Los objetos infectados se muestran agrupados a partir del malware que los ha infectado. Haga clic en el enlace correspondiente a una amenaza para obtener más información sobre los objetos infectados.

Puede elegir una opción global que se aplicará a todas las incidencias, o bien elegir una opción por separado para cada una de las incidencias.

Una o varias de las siguientes opciones pueden aparecer en el menú:

Acción	Descripción
Ninguna Acción	No se realizará ninguna acción sobre los archivos detectados. Al finalizar el proceso de análisis, puede abrir el informe para ver información sobre estos archivos.
Desinfectar	Elimina el código de malware de los archivos infectados.
Eliminar	Elimina los archivos detectados.
Mover a Cuarentena	Traslada los archivos detectados a la cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado.
Renombrar ficheros	Renombra los ficheros ocultos añadiendo `.bd.ren` a su nombre. Como resultado, podrá buscar y encontrar estos ficheros en su equipo, en caso de que existan. Por favor tenga en cuenta que estos ficheros ocultos no son ficheros que usted ocultó de Windows. Son fichero ocultados por programas especiales, conocidos como rootkits. Los rootkits no son maliciosos por naturaleza. De todas maneras, son utilizados normalmente para hacer que los virus o spyware no sean detectados por programas normales antivirus.

Haga clic en **Continuar** para aplicar las acciones indicadas.

Paso 3/3 – Ver Resultados

Una vez Acronis Internet Security Suite 2010 ha finalizado la reparación de los problemas, aparecerán los resultados del análisis en una nueva ventana.

Sumario

Puede ver el resumen de los resultados. Si desea obtener información completa sobre el proceso de análisis, haga clic en **Mostrar Informe** para ver el informe de análisis.

Importante

En caso necesario, por favor, reinicie su equipo para completar el proceso de desinfección.

Haga clic en **Cerrar** para cerrar la ventana.

Acronis Internet Security Suite 2010 No Pudo Resolver Algunas Incidencias

En la mayoría de casos, Acronis Internet Security Suite 2010 desinfecta los archivos infectados detectados o aísla estos archivos en la Cuarentena. Sin embargo, algunas incidencias no pueden repararse.

En estos casos, le recomendamos que contacte con el equipo de soporte de Acronis en http://www.acronis.es/support/?ow=1. Nuestro equipo de representantes le ayudará a resolver las incidencias que experimente.

Acronis Internet Security Suite 2010 Detectó Archivos Sospechosos

Los archivos sospechosos son archivos detectados por el análisis heurístico como potencialmente infectados con malware, aunque su firma de virus todavía no se ha realizado.

Si durante el análisis se detectan archivos sospechosos, se le solicitará enviarlos a los Laboratorios de Acronis. Haga clic en **Aceptar** para enviar estos archivos al Laboratorio de Acronis para su posterior análisis.

17.2.6. Viendo los Informes del Análisis

Para ver los resultados del análisis de una tarea, haga clic derecho en la tarea y seleccione **Ver Logs**. Aparecerá la siguiente pantalla:

Informes

Aquí puede ver los archivos de informe generados cada vez que ejecuta la tarea. Cada archivo incluye información sobre su estado (infectado/desinfectado), la fecha y hora en que se realizó el análisis y un resumen de los resultados.

Hay dos botones disponibles:

- **Eliminar** - para eliminar el informe del análisis seleccionado.
- **Mostrar** - para ver el informe del análisis seleccionado. El informe del análisis se abrirá en su navegador predeterminado.

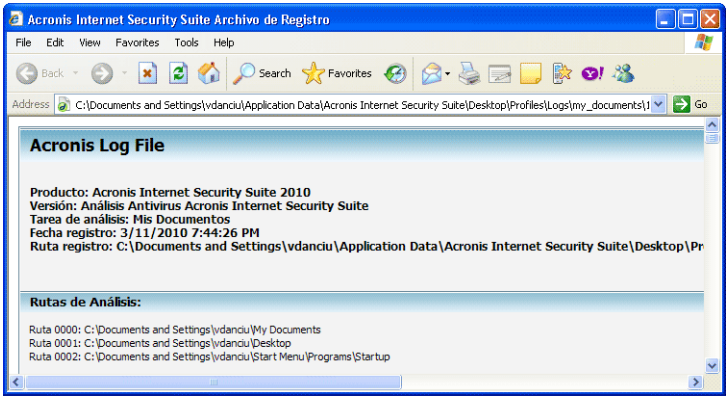
Nota

Para ver o eliminar un archivo también puede hacer clic derecho encima del archivo, y seleccionar la opción correspondiente en el menú contextual.

Haga clic en **Aceptar** para guardar los cambios realizados y cerrar la ventana. Para ejecutar la tarea sólo tiene que hacer clic en **Analizar**.

Ejemplo de Informe de Análisis

La siguiente imagen representa un ejemplo de informe de análisis:



Ejemplo de Informe de Análisis

El informe de análisis detalla información sobre el proceso de análisis, como las opciones del análisis, el objetivo del análisis, las amenazas detectadas y las acciones realizadas.

17.3. Elementos excluidos del análisis

En algunos casos puede necesitar excluir del análisis algunos elementos. Por ejemplo, si desea excluir el archivo del test EICAR del análisis en tiempo real, o los archivos `.avi` del análisis bajo demanda.

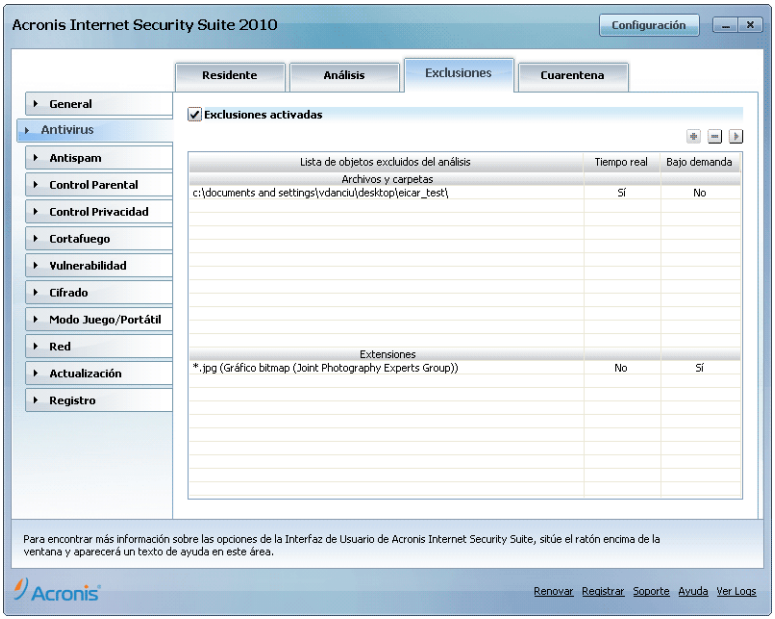
Acronis Internet Security Suite 2010 permite excluir algunos objetos del análisis bajo demanda, del análisis en tiempo real, o de ambos. Esta característica pretende disminuir el tiempo de análisis y evitar interferencias con su trabajo.

Pueden excluirse del análisis dos tipos de objetos:

- **Ruta** - el archivo o carpeta (incluyendo los objetos que contiene) indicado por la ruta será excluido del análisis.
- **Extensiones** - todos los archivos con la extensión indicada serán excluidos del análisis.

Nota
Los objetos excluidos del análisis en tiempo real no serán analizados, tanto si usted o una aplicación acceden al mismo.

Para ver y administrar los objetos excluidos del análisis, diríjase a **Antivirus>Excepciones** en Modo Avanzado.



Exclusiones

Aquí podrá ver todos los objetos (archivos, carpetas, extensiones) que han sido excluidos del análisis. En cada uno de los objetos podrá ver si ha sido excluido del análisis al acceder, bajo demanda, o ambos.

Nota

Las extensiones especificadas aquí NO se aplican al análisis contextual. El análisis contextual es un tipo de análisis bajo demanda: haga clic derecha sobre un fichero o carpeta que desee analizar y seleccione **Analizar con Acronis Internet Security Suite**.

Para eliminar un elemento de la tabla, selecciónelo y haga clic en el botón **Eliminar**.

Para editar un elemento de la tabla, selecciónelo y haga clic en el botón **Editar**. Aparecerá una nueva ventana donde podrá cambiar la extensión o la ruta a excluir, y el tipo de análisis del que desea excluirlo. Realice los cambios necesarios y pulse **Aceptar**.

Nota

También puede hacer clic derecho encima del elemento y utilizar las opciones del menú contextual para editarlo o eliminarlo.

Puede hacer clic en **Descartar** para cancelar los cambios realizados en la tabla, siempre y cuando no los hay guardado pulsando el botón **Aplicar**.

17.3.1. Excluyendo Rutas del Análisis

Para excluir una ruta del análisis, haga clic en el botón **Añadir**. El Asistente de Configuración que aparecerá le guiará a través del proceso de exclusión de rutas del análisis.

Paso 1/4 – Seleccione el Tipo de Objeto

Tipo de Objeto

Seleccione la opción de exclusión de ruta de análisis.

Haga clic en **Siguiente**.

Paso 2/4 – Indique las Rutas a Excluir

Rutas Excluidas

Para indicar las rutas a excluir siga cualquiera de estos métodos:

- Haga clic en **Explorar**, seleccione el archivo o carpeta que desea excluir del análisis y a continuación haga clic en **Añadir**.
- Introduzca la ruta que desea excluir del análisis en el campo editable, y haga clic en **Añadir**.

Nota

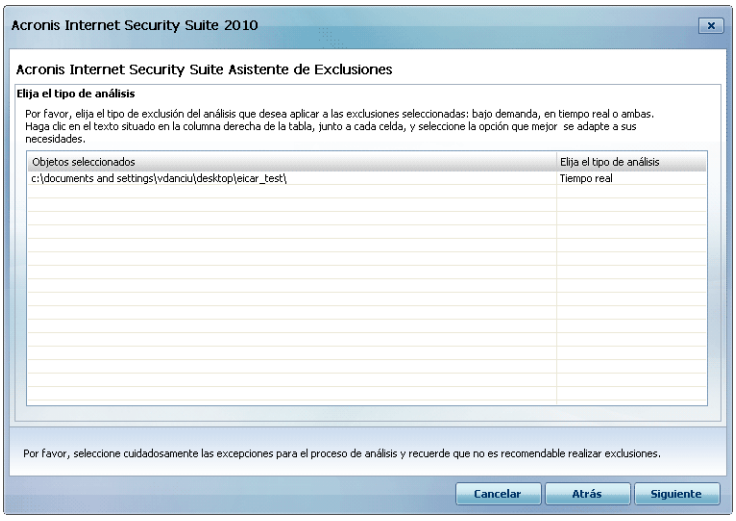
Si la ruta seleccionada no existe, aparecerá un mensaje de error. Haga clic en **Aceptar** y compruebe la validez de ruta.

Las rutas aparecerán en la tabla a medida que las vaya añadiendo. Puede añadir tantas rutas como desee.

Para eliminar un elemento de la tabla, selecciónelo y haga clic en el botón **Eliminar**.

Haga clic en **Siguiente**.

Paso 3/4 – Seleccione el Tipo de Análisis



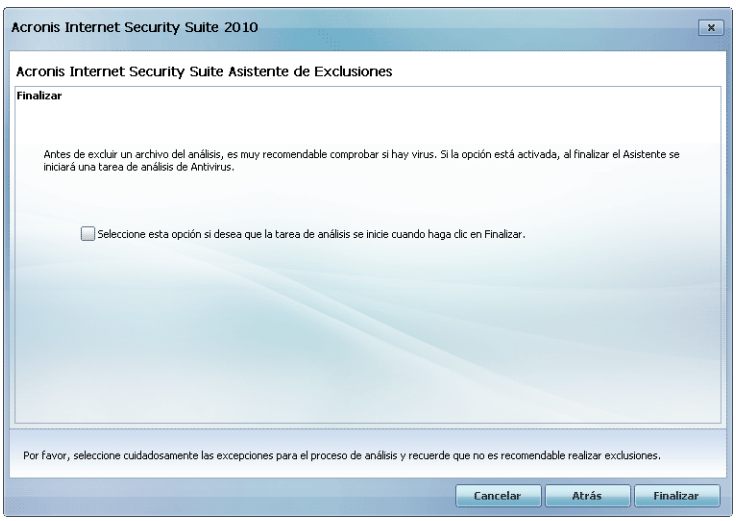
Tipo de Análisis

Verá una tabla que contiene las rutas a excluir y el tipo de análisis del que están excluidas.

Por defecto, las rutas seleccionadas se excluyen de los dos tipos de análisis (al acceder y bajo demanda). Si desea modificar el tipo de análisis, haga clic en la columna derecha y seleccione la opción deseada de la lista.

Haga clic en **Siguiente**.

Paso 4/4 – Analice los Archivos Excluidos



Analice los Archivos Excluidos

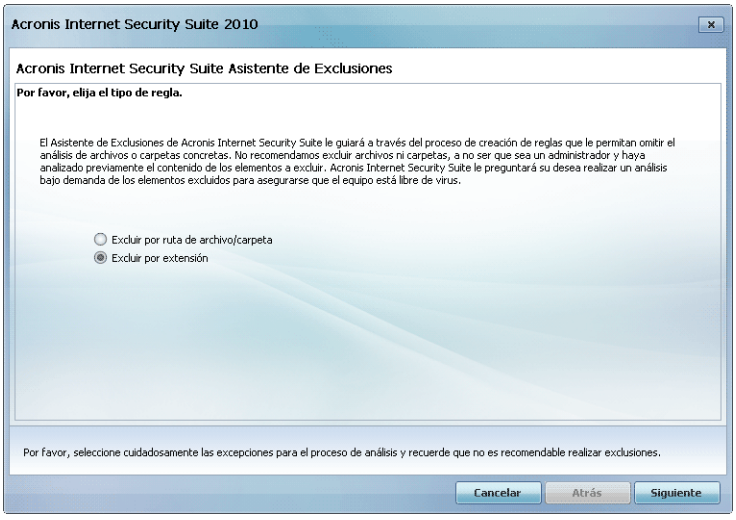
Es muy recomendable analizar los archivos de las rutas excluidas para asegurarse que no están infectados. Seleccione la casilla para analizar estos archivos antes de excluirlos del análisis.

Haga clic en **Finalizar**.

17.3.2. Excluyendo Extensiones del Análisis

Para excluir extensiones del análisis, haga clic en el botón **Añadir**. Aparecerá un asistente que le guiará a través del proceso de exclusión de extensiones.

Paso 1/4 – Seleccione el Tipo de Objeto

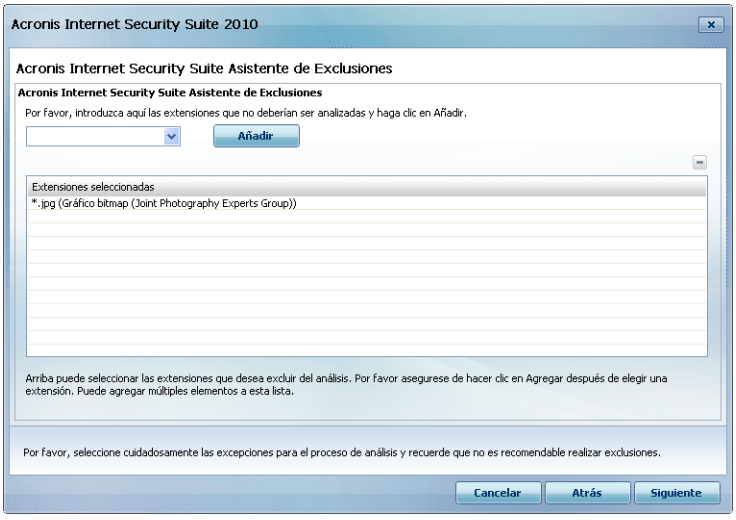


Tipo de Objeto

Seleccione la opción de exclusión del análisis de una extensión.

Haga clic en **Siguiente**.

Paso 2/4 – Indique las Extensiones Excluidas



Extensiones Excluidas

Para especificar las extensiones a excluir del análisis, utilice cualquiera de los siguientes métodos:

- Seleccione, desde el menú, la extensión que será excluida del análisis y a continuación haga clic en **Añadir**.

> **Nota**
> El menú contiene una lista de todas las extensiones registradas en su sistema. Cuando seleccione una extensión, podrá ver su descripción (si existe).

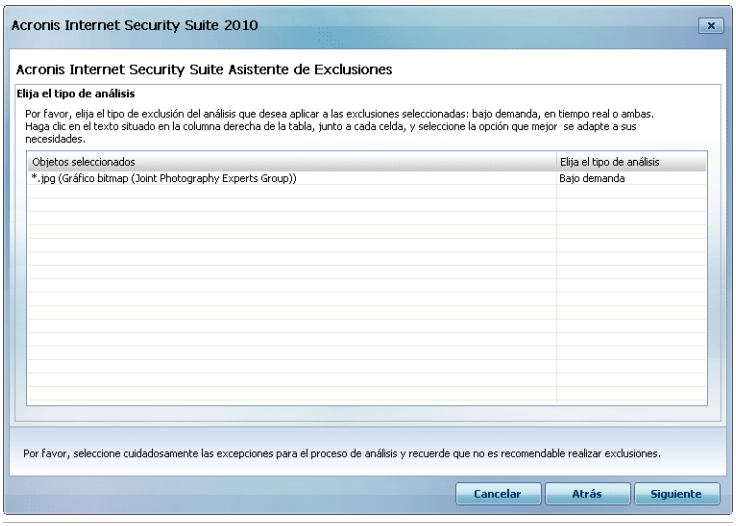
- Introduzca la extensión que desea excluir en el campo editable, y haga clic en **Añadir**.

Las extensiones aparecerán en la tabla a medida que las vaya añadiendo. Puede añadir tantas extensiones como desee.

Para eliminar un elemento de la tabla, selecciónelo y haga clic en el botón **Eliminar**.

Haga clic en **Siguiente**.

Paso 3/4 – Seleccione el Tipo de Análisis



Tipo de Análisis

Verá una tabla que contiene las extensiones a excluir y el tipo de análisis del que han sido excluidas.

Por defecto, las extensiones seleccionadas se excluyen de los dos tipos de análisis (al acceder y bajo demanda). Si desea modificar el tipo de análisis, haga clic en la columna derecha y seleccione la opción deseada en la lista.

Haga clic en **Siguiente**.

Paso 4/4 – Seleccione el Tipo de Análisis

Tipo de Análisis

Es muy recomendable analizar los archivos que tienen las extensiones indicadas para asegurarse que no están infectados.

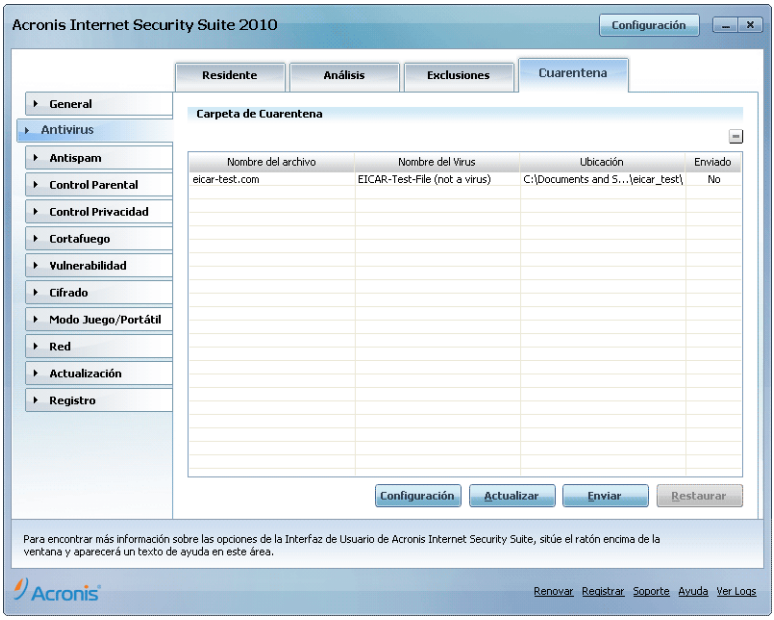
Haga clic en **Finalizar**.

17.4. Área de Cuarantena

Acronis Internet Security Suite 2010 permite aislar los archivos infectados o sospechosos en una área segura, llamada cuarentena. Aislando estos archivos en la cuarentena, el riesgo de infectarse desaparece y, al mismo tiempo, tiene la posibilidad de enviar estos archivos para un análisis al Lab. de Acronis.

Adicionalmente, Acronis Internet Security Suite 2010 analiza los ficheros de la cuarentena después de cada actualización de firmas de malware. Los ficheros desinfectados serán trasladados automáticamente a su ubicación original.

Para ver y administrador los archivos en cuarentena y configurar su opciones, diríjase **Antivirus>Cuarentena** en Modo Avanzado.



Cuarentena

El apartado Cuarentena muestra todos los archivos actualmente aislados en la carpeta Cuarentena. Podrá ver el nombre del archivo, nombre del virus detectado, ruta de su ubicación original y fecha de traslado a cuarentena de cada uno de los archivos en Cuarentena.

Nota
Cuando un virus está aislado en la cuarentena no puede hacer daño alguno, al no poder ejecutarse ni leerse.

17.4.1. Administrando los Archivos en Cuarentena

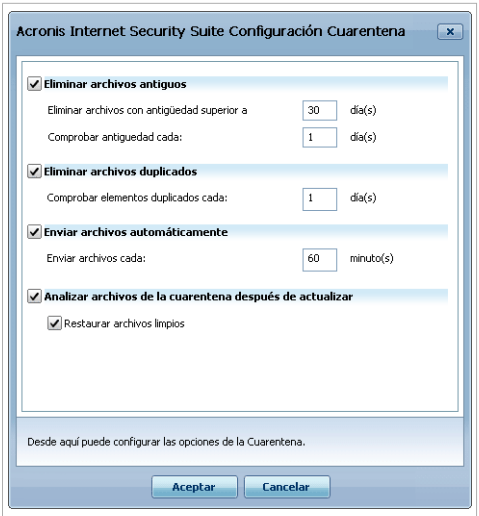
Puede enviar cualquier archivo de la cuarentena a los Laboratorios de Acronis haciendo clic en **Enviar**. Acronis Internet Security Suite 2010 enviará por defecto, cada 60 minutos, los archivos en cuarentena.

Para eliminar un archivo de la cuarentena haga clic en el botón **Eliminar**. Si quiere restaurar un archivo a su ubicación inicial haga clic en **Restaurar**.

Menú contextual. A través del menú contextual podrá gestionar los archivos de la cuarentena fácilmente. También puede seleccionar **Actualizar** para actualizar el apartado de Cuarentena.

17.4.2. Configurando las Opciones de Cuarentena

Para modificar la configuración de la Cuarentena, haga clic en **Configurar**. Aparecerá una nueva ventana.



Configuración de la Cuarentena

Al utilizar las opciones de la cuarentena conseguirá que Acronis Internet Security Suite 2010 realice automáticamente las siguientes acciones:

Eliminar archivos antiguos. Para eliminar automáticamente los archivos antiguos de la cuarentena, marque la casilla correspondiente. Debe indicar el número de días tras los cuales se eliminarán los archivos de la cuarentena, y la frecuencia con la que Acronis Internet Security Suite 2010 comprobará si existen.

Nota
Por defecto, Acronis Internet Security Suite 2010 comprobará si existen archivos antiguos cada día, y eliminará los más antiguos a 30 días.

Eliminar archivos duplicados. Para eliminar automáticamente los archivos duplicados de la cuarentena, marque la opción correspondiente. Debe indicar el número de días tras los cuales se comprobará si existen duplicados.

Nota
Por defecto, Acronis Internet Security Suite 2010 comprobará diariamente si hay archivos duplicados en la cuarentena.

Enviar archivos automáticamente. Para enviar automáticamente los archivos en cuarentena, marque la opción correspondiente. Debe indicar la frecuencia con la enviar los archivos.

Nota

Acronis Internet Security Suite 2010 enviará por defecto, cada 60 minutos, los archivos en cuarentena.

Analizar archivos de la cuarentena después de actualizar. Para analizar automáticamente los archivos de la cuarentena después de cada actualización, marque la casilla correspondiente. Puede restaurar los archivos desinfectados a su ubicación original, seleccionando la opción **Restaurar archivos limpios**.

Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

18. Antispam

Acronis Antispam emplea sorprendentes innovaciones tecnológicas y filtros antispam estándares en la industria para impedir que el spam llegue a su bandeja de entrada.

18.1. Comprensión del Antispam

El correo no solicitado se ha convertido en un problema cada vez más agobiante, tanto para los usuarios individuales como para las empresas. No es agraciado, no quiere que sus hijos lo vean, puede dejarlo sin trabajo (al perder mucho tiempo con el spam o al recibir contenidos pornográficos en su cuenta de empresa) y no puede hacer nada para impedirlo. Lo mejor acerca del correo no solicitado es, obviamente, dejar de recibirlo. Desgraciadamente, el correo no solicitado llega en una gran variedad de formas y tamaños y siempre en una cantidad increíble.

18.1.1. Los Filtros Antispam

El motor Acronis Internet Security Suite 2010 Antispam incorpora varios filtros para mantener su Bandeja de Entrada libre de SPAM: Lista de Amigos, Lista de Spammers, Filtro de Caracteres, Filtro de Imágenes, Filtro URL, Filtro NeuNet (heurístico) y Filtro Bayesiano.

Nota

Puede activar/desactivar cada uno de estos filtros desde el apartado Configuración del módulo **Antispam**.

Lista de Amigos y Lista de Spammers

La mayoría de la gente se suele comunicar con el mismo grupo de personas, o recibe mensajes de empresas y organizaciones de la misma área laboral. Al usar la **Lista de Amigos o de Spammers**, podrá distinguir fácilmente entre las personas cuyos mensajes desea recibir independientemente de su contenido (amigos), de aquellas cuyos mensajes no desea recibir más (spammers).

La lista de Amigos /Spammers puede administrarse en la interfaz Modo Avanzado o desde la Barra de Herramientas Antispam integrada dentro de los clientes de correo más utilizados.

Nota

Le recomendamos agregar los nombres y las direcciones de correo de sus amigos al **Listado de Amigos**. Acronis Internet Security Suite 2010 no bloquea los mensajes provenientes de las personas incluidas en este listado; por consiguiente, al agregar a sus conocidos en el Listado de Amigos se asegura que los mensajes legítimos llegarán sin problemas a su Bandeja de entrada.

Filtro de Caracteres

Gran parte del Spam está redactado con caracteres asiáticos o cirílicos. El Filtro de Caracteres detecta este tipo de mensajes y los marca como SPAM.

Filtro de Imágenes

El evitar la detección del filtro heurístico se ha convertido en todo un reto, hoy en día, las carpetas de entradas están llenas con más y más mensajes que sólo contienen una imagen con contenido no solicitado. Para hacer frente a este problema, el **Filtro de Imagen** compara la firma de imagen del correo con la base de datos de Acronis Internet Security Suite 2010. En caso de que coincida el correo se marcará como SPAM.

Filtro URL

La mayor parte de los mensajes de spam incluyen enlaces a varias páginas web. Estas páginas normalmente contienen más publicidad y la posibilidad de comprar cosas, e incluso a veces, se utilizan para el phishing.

Acronis mantiene una base de datos con este tipo de links. El Filtro URL comprueba todos los enlaces de los mensajes y comprueba si están incluidos en la base de datos. Si están incluidos en la base de datos, el mensaje se etiquetará como SPAM.

Filtro NeuNet (Heurístico)

El **Filtro NeuNet (Heurístico)** realiza pruebas en todos los componentes del mensaje (por ejemplo, no sólo en el encabezado, sino también en el cuerpo del mensaje, tanto en formato texto como HTML). Busca palabras, frases o enlaces característicos del SPAM. Basándose en los resultados del análisis, añade una puntuación de SPAM al mensaje.

El filtro también detecta mensajes y los marca como `SEXUALLY-EXPLICIT:` en el Asunto del mensaje, y los marca como SPAM.

Nota

Desde el 19 de Mayo del 2004, culaquier mensaje Spam que incluya contenido sexual debe incluir la advertencia `SEXUALLY EXPLICIT:` (SEXUALMENTE EXPLÍCITO) en la línea Asunto; de lo contrario se enfrentarán a multas por violación de la ley federal.

Filtro Bayesiano

El **Filtro Bayesiano** clasifica los mensajes según las informaciones estadísticas referentes a la tasa de aparición de ciertas palabras específicas en mensajes marcados como SPAM en comparación con aquellos declarados NO-SPAM (por el usuario o el filtro heurístico).

Esto significa que, si alguna palabra de cuatro letras (por ejemplo, una que empiece con c) aparece frecuentemente en los mensajes SPAM, es lógico asumir que hay

una alta probabilidad para que el siguiente mensaje que incluya dicha palabra sea SPAM. Todas las palabras relevantes en un mensaje están tomadas en consideración. Al sintetizar la información estadística relevante, se calcula la probabilidad general para que el mensaje sea considerado SPAM.

Este módulo también presenta otra característica interesante: puede aprender. Se adapta rápidamente al tipo de mensajes recibidos por un usuario y almacena toda la información. Para que funcione eficaz, el filtro debe ser "educado", es decir, se le tienen que presentar muestras de SPAM y de mensajes legítimos, así como se pone cebo al perro para que siga un rastro. A veces el filtro debe ser corregido, cuando su decisión resulta errónea.

Importante

Puede corregir las decisiones del Filtro Bayesiano utilizando los botones **Es Spam** y **No Spam** desde la Barra de Herramientas Antispam.

18.1.2. Funcionamiento del Antispam

El motor de Acronis Internet Security Suite 2010 Antispam utiliza todos los filtros combinados para determinar si un correo puede entrar en su **Bandeja de Entrada** o no.

Importante

Los mensajes de spam detectados por Acronis Internet Security Suite 2010 se marcan con el prefijo [SPAM] en el asunto. Acronis Internet Security Suite 2010 automáticamente mueve los mensajes spam a una carpeta específica de la siguiente manera:

- En Microsoft Outlook, los mensajes de spam se mueven a la carpeta **Spam**, ubicada en la carpeta **Elementos eliminados**. La carpeta **Spam** se ha creado durante la instalación de Acronis Internet Security Suite 2010.
- En Outlook Express y Windows Mail, los mensajes spam se mueven directamente a **Elementos eliminados**.
- En Mozilla Thunderbird, los mensajes spam se mueven a la carpeta **Spam**, ubicada en la carpeta **Papelera**. La carpeta **Spam** se ha creado durante la instalación de Acronis Internet Security Suite 2010.

Si usa otros clientes de correo, debe crear una regla para mover los mensajes de correo electrónico marcados como [SPAM] por Acronis Internet Security Suite 2010 a una carpeta de cuarentena personalizada.

Cualquier mensaje que provenga de Internet pasará primero por los filtros Lista de Amigos/Lista de Spammers. Si el remitente se encuentra en la Lista de Amigos el mensaje será trasladado directamente a su **Bandeja de Entrada**.

De lo contrario, el filtro de Lista de Spammers verificará si la dirección del remitente esta en su lista. Si la dirección se encuentra en la lista. El mensaje será marcado

com SPAM y será trasladado a la carpeta **Spam**(ubicada en Microsoft Outlook) si ha sido detectada un coincidencia.

Si el remitente no se encuentra en ninguno de los dos listados el Filtro de carácteres verificará si el mensaje está escrito con caracteres cirílicos o asiáticos. En tal caso, el mensaje será marcado como SPAM y trasladado a la carpeta **Spam**.

Si el mensaje no está escrito con caracteres cirílicos o asiáticos pasará al Filtro de Imagen. El **Filtro de imágenes** detectará todos los mensajes electrónicos que contienen imágenes de spam.

El Filtro URL buscará enlaces y los comparará con los enlaces de la base de datos de Acronis Internet Security Suite 2010. Al encontrar algún enlace de este tipo, un coeficiente de Spam será añadido al mensaje de correo.

El Filtro NeuNet (heurístico) realiza prueba en todos los componentes del mensaje, buscando palabras, frases, enlaces u otras características del SPAM. Como resultado, también añade una puntuación de SPAM al mensaje analizado.

Nota

Si el correo está marcado como SEXUALMENTE EXPLÍCITO en la línea del asunto, Acronis Internet Security Suite 2010 lo considerará SPAM.

El Filtro Bayesiano clasifica los mensajes según datos estadísticos referentes a la proporción de aparición de ciertas palabras en mensajes clasificados como SPAM en comparación con aquellos declarados NO-SPAM (por el admin o por el filtro heurístico). Un coeficiente de SPAM será añadido al mensaje analizado.

Si la puntuación total (puntuación de los filtros URL + heurístico + Bayesiano) supera la puntuación máxima de SPAM (establecida por el usuario en el apartado Estado como nivel de tolerancia), entonces el mensaje se considerará SPAM.

18.1.3. Actualizaciones de Antispam

Cada vez que usted efectúa una actualización:

- se añaden nuevas firmas al **Filtro de Imágenes**.
- se añaden nuevos enlaces al **Filtro URL**.
- se añaden nuevas reglas al **Filtro NeuNet (Heurístico)**.

De esta manera se aumenta la eficacia de los motores Antispam.

Para protegerle contra el correo no solicitado, Acronis Internet Security Suite 2010 puede realizar actualizaciones automáticas. Mantenga activada la opción **Actualizar automáticamente**.

18.2. Estado

Para configurar la protección Antispam, diríjase a **Antispam>Estado** en el Modo Avanzado.

Estado Antispam

Podrá ver si la protección Antispam está activada o desactivada. Si desea cambiar el estado del Antispam, desmarque o marque la casilla correspondiente.

Importante
Mantenga activado el filtro **Antispam**, para evitar que el spam llegue a su **Bandeja de Entrada**.

En el apartado **Estadísticas** podrá ver las estadísticas del módulo Antispam. Los resultados pueden mostrarse por sesión (desde que inició por última vez el ordenador) o bien ver un resumen de la actividad antispam (desde la instalación de Acronis Internet Security Suite 2010).

18.2.1. Estableciendo el Nivel de Protección

Puede elegir el nivel de protección que mejor se adapte a sus necesidades de seguridad. Arrastre el deslizador a lo largo de la escala para elegir el nivel de protección adecuado.

Hay 5 niveles de protección:

Nivel de Protección	Descripción
Tolerante	Ofrece protección para cuentas que reciben muchos mensajes comerciales legítimos. El filtro dejará pasar a la mayoría de los mensajes, pero puede producir falsos negativos (mensajes spam clasificados como legítimos).
De Permisivo a Moderado	Ofrece protección para cuentas que reciben algunos mensajes comerciales legítimos. El filtro dejará pasar a la mayoría de los mensajes, pero puede producir falsos negativos (mensajes spam clasificados como legítimos).
Moderado	Ofrece protección para cuentas habituales. Este filtro bloqueará la mayoría de los mensajes no deseados, mientras evita falsos positivos.
Moderado a Agresivo	Ofrece protección para cuentas que reciben un gran volumen de spam habitualmente. El filtro deja pasar una cantidad muy baja de spam, pero puede generar falsos positivos (mensajes legítimos marcados incorrectamente como spam). Configure las **Listas de Amigos/Spammers** y entrene el **Motor de Aprendizaje** para reducir el número de falsos positivos.
Agresivo	Ofrece protección para cuentas que reciben un gran volumen de spam habitualmente. El filtro deja pasar una cantidad muy baja de spam, pero puede generar falsos positivos (mensajes legítimos marcados incorrectamente como spam). Añade sus contactos a la **Lista de Amigos** para reducir el número de falsos positivos.

Para restaurar el nivel de protección predeterminado (**Moderado a Agresivo**) haga clic en el botón **Por Defecto**.

18.2.2. Configurando la Lista de Amigos

La **Lista de Amigos** es una lista que contiene todas las direcciones de e-mail de las que quiere recibir mensajes, independientemente de su contenido. Los mensajes de sus amigos no serán marcados como spam, aunque su contenido tenga múltiples características del correo no solicitado.

Nota
Cualquier mensaje que provenga de una dirección incluida en la **Lista de Amigos** llegará directamente a su Bandeja de Entrada.

Para configurar la Lista de Amigos, haga clic en **Amigos** (o haga clic en el botón **Amigos** de la Barra de Herramientas Antispam).

Lista de Amigos

Aquí puede agregar o eliminar entradas en el **listado de amigos**.

Si desea agregar una dirección de correo, haga clic en el campo **Dirección**, introduzca la dirección y luego haga clic . La dirección aparecerá en el **Lista de Amigos**.

Importante
Sintaxis: nombre@dominio.com.

Si desea añadir un dominio, haga clic en el campo **Dominio**, introduzca el dominio y luego clic en el botón . El dominio aparecerá en la **Lista de Amigos**.

Importante
Sintaxis:

- @dominio.com, *dominio.com y dominio.com - todos los mensajes provenientes de dominio.com llegarán a su **Bandeja de entrada** independientemente de su contenido;

- *dominio* - todos los mensajes provenientes de dominio (independientemente de los sufijos del dominio) llegarán a su **Bandeja de entrada** independientemente de su contenido;
- *com - todos mensajes con tales sufijos de dominios com llegarán a su **Bandeja de entrada** independientemente de sus contenidos;

Para eliminar un elemento de la lista, selecciónelo y haga clic en el botón **Eliminar**. Para eliminar todas las entradas de la lista, haga clic en el botón **Vaciar Lista** y después en **Si** para confirmar.

Puede guardar la lista de Amigos a un archivo la cual puede utilizarse en otro equipo o después de reinstalar el producto. Para guardar la lista de Amigos, haga clic en el botón **Guardar** y guárdela en la ubicación deseada. El archivo tendrá la extensión `.bwl`.

Para cargar una lista de Amigos previamente guardada, haga clic en el botón **Cargar** y abra el correspondiente archivo `.bwl`. Para resetear el contenido de la lista existente cuando carga una lista previamente guardad, seleccione **Sobrescribir la actual lista**.

Nota

Le recomendamos agregar los nombres y las direcciones de correo de sus amigos al **Listado de Amigos**. Acronis Internet Security Suite 2010 no bloquea los mensajes provenientes de las personas incluidas en este listado; por consiguiente, al agregar a sus conocidos en el Listado de Amigos se asegura que los mensajes legítimos llegarán sin problemas a su Bandeja de entrada.

Haga clic en **Aplicar** y **Aceptar** para guardar y cerrar el **listado de amigos**.

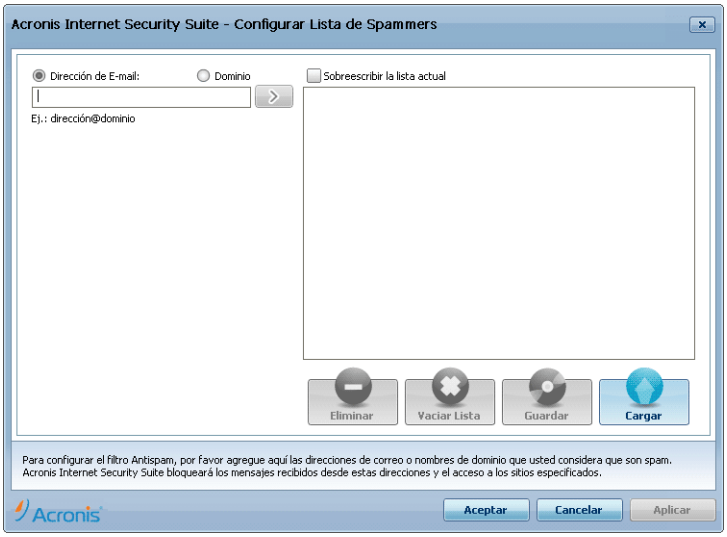
18.2.3. Configurando la Lista de Spammers

El **Listado de Spammers** es un listado que reúne todas las personas cuyos mensajes no desea recibir más, independientemente de sus formatos o contenidos.

Nota

Cualquier mensaje proveniente de una dirección incluida en su **listado de spammers** será automáticamente marcada como spam, sin procesamientos ulteriores.

Para configurar la Lista de Spammers, haga clic en **Administrar Spammers** (o haga clic en el botón **Spammers** de la Barra de Herramientas Antispam).



Lista de Spammers

Aquí puede agregar o eliminar entradas en el **listado de spammers**.

Si desea añadir una dirección de correo, haga clic en el campo **Dirección**, introduzca la dirección y luego clic en el botón . La dirección aparecerá en el **Lista de Spammers**.

Importante
Sintaxis: nombre@dominio.com.

Si desea añadir un dominio, haga clic en el campo **Dominio**, introduzca el dominio y luego clic en el botón . El dominio aparecerá en la **Lista de Spammers**.

Importante
Sintaxis:

- @dominio.com, *dominio.com y dominio.com - todos los mensajes provenientes de dominio.com serán marcados como SPAM;
- *dominio* - todos los mensajes provenientes de dominio (independientemente de los sufijos del dominio) serán marcados como SPAM;
- *com - todos mensajes con tales sufijos de dominios com serán marcados como SPAM.

Aviso

No agregar dominio legítimos de correo basados en servicios web (como un Yahoo, Gmail, Hotmail u otros) a la lista de Spammers. De lo contrario, los mensajes recibidos de cualquier usuario registrados en estos servicios serán detectados como spam. Si, por ejemplo, añade `yahoo.com` a la lista de Spammers, todas las direcciones de correo que vengan de `yahoo.com` serán marcados como `[spam]`.

Para eliminar un elemento de la lista, selecciónelo y haga clic en el botón **Eliminar**. Para eliminar todas las entradas de la lista, haga clic en el botón **Vaciar Lista** y después en **Si** para confirmar.

Puede guardar la lista de Spammers en un archivo la cual puede utilizarla en otro equipo o después de reinstalar el producto. Para guardar la lista Spammers, haga clic en el botón **Guardar** y guárdela en la ubicación deseada. El archivo tendrá la extensión `.bwl`.

Para cargar una lista de Spammers previamente guardad, haga clic en el botón **Cargar** y abra el archivo correspondiente `.bwl`. Para resetear el contenido de la lista existente cuando carga una lista previamente guardad, seleccione **Sobrescribir la actual lista**.

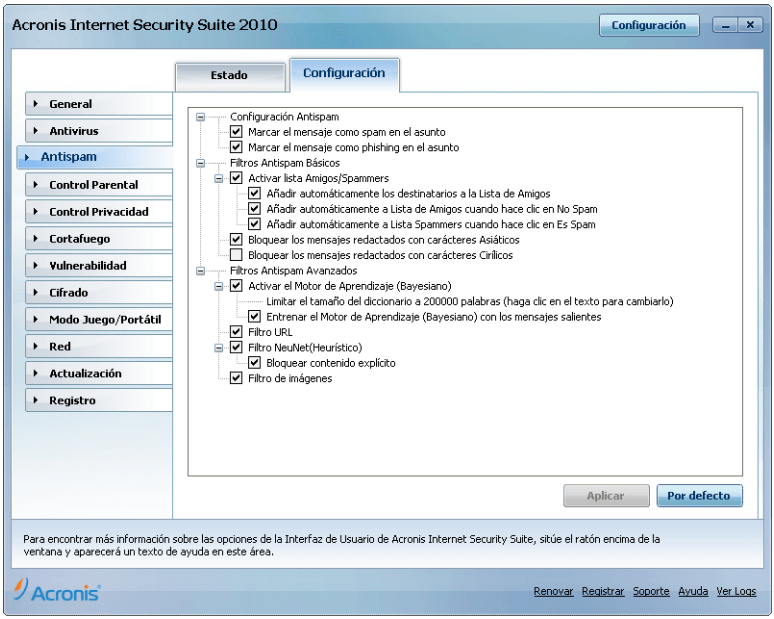
Haga clic en **Aplicar** y **Aceptar** para guardar y cerrar el **listado de spammers**.

Importante

Si desea reinstalar Acronis Internet Security Suite 2010, recomendamos guardar las listas de **Amigos** / **Spammers** antes de iniciar el proceso, para así volver a cargarlas cuando finalice la reinstalación.

18.3. Configuración

Para modificar la configuración del antispam y los filtros, diríjase a **Antispam>Configuración** en Modo Avanzado.



Configuración Antispam

Hay 3 categorías de opciones disponibles (**Configuración Antispam**, **Filtros Antispam Básicos** y **Filtros Antispam Avanzados**) organizados en un menú expandible, similar a los menús de Windows.

Nota
Haga clic en la casilla marcada "+" para abrir una categoría, o en la casilla marcada "-" para cerrar una categoría.

Para activar/desactivar una opción, seleccione/desmarque la casilla correspondiente.

Si desea aplicar la configuración predeterminada, haga clic en **Por Defecto**.

Haga clic en **Aplicar** para guardar los cambios.

18.3.1. Configuración Antispam

- **Marcar el mensaje como spam en el asunto** - si selecciona esta opción todos los mensajes considerados Spam serán marcados como SPAM en el asunto.
- **Marcar el mensaje como phishing en el asunto** - todos los correos considerados como phishing se marcarán como SPAM en el Asunto.

18.3.2. Filtros Antispam Básicos

- **Lista de Amigos / Spammers** - filtra los mensajes a partir de las listas de Amigos / Spammers.
  - ▶ **Añadir automáticamente a la Lista de Amigos** - para añadir los remitentes a la Lista de Amigos.
  - ▶ **Añadir automáticamente a la Lista de Amigos** - cuando haga clic en el botón **No Spam** de la Barra de Herramientas Antispam, el remitente será añadido automáticamente a la Lista de Amigos.
  - ▶ **Añadir automáticamente a la Lista de Spammers** - cuando haga clic en el botón **Es Spam** de la Barra de Herramientas Antispam, el remitente será añadido automáticamente a la Lista de Spammers.

Nota
Los botones **No Spam** y **Es Spam** se utilizan para entrenar al filtro Bayesiano.

- **Bloquear mensajes redactados con caracteres Asiáticos** - bloquea los mensajes redactados con caracteres Asiáticos.
- **Bloquear mensajes redactados con caracteres Cirílicos** - bloquea los mensajes redactados con caracteres Cirílicos.

18.3.3. Filtros Antispam Avanzados

- **Activar el Motor de Aprendizaje** - activa/desactiva el Motor de Aprendizaje.
  - ▶ **Limitar el tamaño del diccionario a 200000 palabras** - esta opción le ofrece la posibilidad de configurar el tamaño del diccionario Bayesiano - reducido funciona más rápido, enriquecido tiene mayor precisión.

Nota
El tamaño recomendado es de: 200.000 palabras.

  - ▶ **Entrenar al Motor de Aprendizaje (bayesiano) con los correos salientes** - entrena el Motor de Aprendizaje (bayesiano) con los mensajes salientes.
- **Filtro URL** - activa/desactiva el Filtro URL.
- **Filtro NeuNet(Heurístico)** - activa/desactiva el Filtro NeuNet(Heurístico).
  - ▶ **Bloquear contenido explícito** - activa/desactiva la detección de mensajes con SEXUALLY EXPLICIT en la línea Asunto.
- **Filtro de imágenes** - activa/desactiva el Filtro de imágenes.

19. Control Parental

El Control Parental de le permite controlar el acceso a Internet y a determinadas aplicaciones para cada una de las cuentas de usuario del sistema.

Puede configurar Control Parental para que bloquee:

- páginas web con contenido inadecuado.
- la conexión a Internet durante determinados periodos de tiempo (por ejemplo, en las horas de estudio).
- páginas web, mensajes de correo y conversaciones de mensajería instantánea que contengan determinadas palabras clave.
- aplicaciones como juegos, chat, aplicaciones de intercambio de archivos u otros.
- mensajes enviados por contactos de mensajería instantánea que no provengan de los contactos permitidos.

Importante

Sólo los usuarios con permisos de administrador (administradores del sistema) pueden acceder y configuar el Control Parental. Para asegurarse que nadie modifica la configuración del Control Parental de los usuarios, puede proteger la configuración con una contraseña. Se le pedirá configurar una contraseña cuando active el Control Parental de un usuario determinado.

Para configurar correctamente el Control Parental y restringir las actividades online y en el equipo de sus hijos, debe completar estas tareas:

1. Crear una cuenta de usuario de Windows limitada (estándar) para sus hijos.

Nota

Para aprender a crear cuentas de usuario de Windows, diríjase al Centro de Ayuda y Soporte Técnico de Windows (en el menú Inicio, haga clic en **Ayuda y soporte técnico**).

2. Configure el Control Parental de las cuentas de usuario de Windows que ha creado para sus hijos.

Para configurar el Control Parental, diríjase a **Control Parental** en Modo Avanzado.

Control Parental

Puede ver informaciones relacionadas con el estado de Control Parental para cada cuenta de usuario de Windows. La categoría de edad esta listada a continuación para cada nombre de usuario si el Control Parental esta activado. Si el Control Parental esta desactivado, el estado es **no configurado**.

Además, puede ver el estado del Control Parental por usuario:

Círculo Verde con una marca de verificación: La configuración está activada.
Circulo Rojo con un marca de exclamación: La configuración está desactivada.

Haga clic en el botón **Editar** del nombre de usuario para abrir una ventana en donde puede configurar el Control Parental para la respectiva cuenta de usuario.

En los siguientes apartados de este capítulo se le presentan las características del Control Parental y cómo configurarlas.

19.1. Configurar Control Parental a un usuario

Para configurar el Control Parental para una cuenta de usuario específica, haga clic en el botón **Editar** correspondiente a esta cuenta de usuario y entonces haga clic en la pestaña **Estado**.

Estado del control parental

Para configurar el Control Parental de este usuario, siga estos pasos:

1. Active el Control Parental para esta cuenta de usuario marcando la casilla situada junto a **Control Parental**.

   Importante
   Mantenga el módulo **Control Parental** activado para proteger a sus hijos contra el contenido inapropiado usando sus reglas de acceso personalizadas.

2. Establezca una contraseña para proteger la Configuración del Control Parental. Para más información, por favor, consulte el apartado *"Protegiendo la Configuración del Control Parental"* (p. 177) de esta guía.
3. Establezca la categoría de edad para permitir a sus hijos acceder sólo a paginas web apropiadas para esta edad. Para mas información, por favor diríjase a *"Configure la Categoría de Edad"* (p. 178).
4. Configurar las opciones de monitorización para este usuario, según sea necesario:
   - **Enviarme un informe de actividad a través del correo.** Se envía una notificación por correo cada vez que el Control Parental de bloquea una actividad para este usuario.

- **Guarda un informe del tráfico de Internet.** Registro de las páginas web visitadas por el usuario.

Para más información, por favor diríjase a "*Monitorizar la Actividad de los Niños*" (p. 181).

5. Haga clic en un icono o en una pestaña para configurar las características correspondientes al Control Parental:
   - **Web** - para filtrar la navegación web según las reglas establecidas en el apartado Web.
   - **Control de Aplicaciones** - para bloquear el acceso a las aplicaciones que ha especificado en el apartado Control de Aplciaciones.
   - **Filtro de Palabras Clave** - para filtrar el acceso a páginas web, correo y mensajería instantánea según las reglas que ha establecido en el apartado Palabras Clave.
   - **Control Mensajería Instantánea** - para permitir o bloquear los chats con los contactos IM según las reglas establecidas en el apartado Tráfico IM.
   - **Limitador de Tiempo Web** - para permitir el acceso según el horario especificado en el apartado Limitador Tiempo.

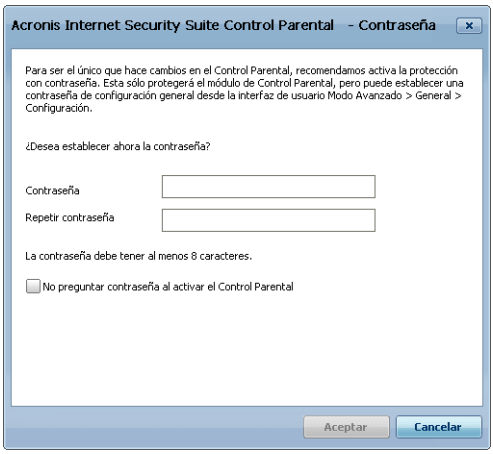
   Nota
   Para aprender a configurar este módulo, diríjase a los siguientes temas de este capítulo.

Para bloquear completamente el acceso a Internet, haga clic en el botón **Bloquear Internet**.

19.1.1. Protegiendo la Configuración del Control Parental

Si no es el único usuario con permisos de administrador que utiliza este ordenador, es recomendable que proteja su configuración del Control Parental con una contraseña. Al introducir una contraseña, impedirá que los otros usuarios administradores cambien las opciones del Control Parental que ha configurado exclusivamente para un usuario.

Cuando active el Control Parental, Acronis Internet Security Suite 2010 le solicitara introducir una contraseña.



Establecer la Protección por Contraseña

Para establecer la protección por contraseña, realice lo siguiente:

1. Introduzca la contraseña en el campo **Contraseña**.
2. Para confirmar la contraseña, introdúzcala de nuevo en el campo **Repetir contraseña**.
3. Haga clic en **Aceptar** para guardar la contraseña y cerrar la ventana.

De ahora en adelante, si quiere cambiar la configuración del Control Parental, se le solicitará introducir la contraseña. Los otros administradores del equipo (si existen) también tendrán que introducir esta contraseña para cambiar la configuración del Control Parental.

Nota
Esta contraseña no protegerá otras configuraciones de Acronis Internet Security Suite 2010.

En el caso que no introduzca ninguna contraseña y no desea que vuelva a aparecer esta ventana, marque la casilla **No solicitar la contraseña al activar el Control Parental**.

19.1.2. Configure la Categoría de Edad

El filtro web heurístico analiza las páginas web y bloquea aquellas con contenido potencialmente inapropiado.

Para filtrar el acceso web a partir de unas reglas predeterminadas para diferentes edades, deberá cambiar el nivel de tolerancia. Arrastre el control deslizante a través

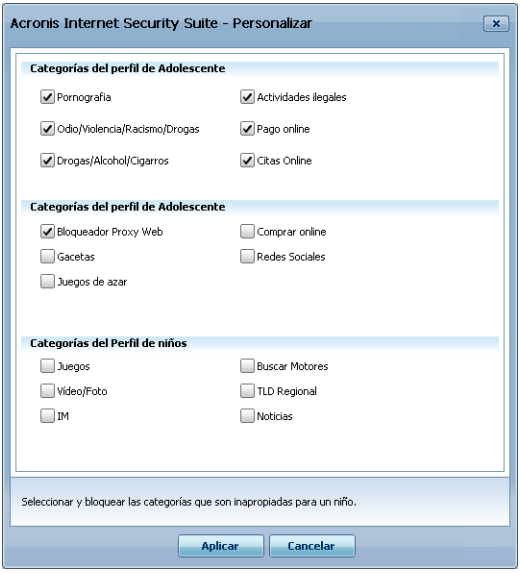
de la escala para fijar el nivel de protección que considere apropiado para el usuario seleccionado.

Hay 3 niveles de tolerancia:

Nivel de tolerancia	Descripción
Bajo	Se bloqueará el acceso a páginas web según la configuración recomendada. Se bloqueará el acceso a las páginas web con contenido potencialmente dañino para los niños (porno, sexualidad, drogas, hacking, etc).
Medio	Se bloqueará el acceso a páginas web según la configuración recomendada. Se bloqueará el acceso a las páginas web con contenido sexual, pornográfico o adulto.
Alto	Ofrece un acceso sin restricción a todas las páginas web, independientemente de su contenido.

Haga clic en **Por Defecto** para posicionar el deslizador en el nivel predeterminado.

Si desea más control sobre el tipo de contenido que el usuario puede ver en Internet, puede definir las categorías del contenido de web, las cuales serán bloqueadas por el filtro web. Para elegir que tipos de contenido web se bloquearán, haga clic **Personalizar Categorías**. Aparecerá una nueva ventana:



Categorías del Filtro Web

Seleccione la casilla correspondiente a una categoría que desea bloquear y al usuario no se le permitirá más acceder a páginas web que coincidan con esta categoría. Para hacer más fácil la selección, las categorías del contenido web están clasificadas según el grupo de edad que se considere oportuno:

- **Categoría Perfil Niño** incluye el contenido que los niños menores de 14 años podrán tener acceso.

Categoría	Descripción
Juegos	Páginas web que ofrecen juegos, foros de discusión de juegos, descargas de juegos, trampas, recorridos, etc.
Vídeo/Foto	Páginas Web que alojan galerías de fotos o vídeos.
IM	Aplicaciones de Mensajería Instantánea
Motores de Búsqueda	Motores de búsqueda y portales de búsqueda.
TLD Regional	Páginas Web que tienen un nombre de dominio fuera de su región.
Noticias	Periódicos Online.

- **Categoría Perfil Adolescente** incluye contenido que puede ser considerado seguro para un niño entre 14 y 18 años.

Categoría	Descripción
Bloqueador Proxy Web	Páginas Web utilizadas para ocultar la URL de una web solicitada.
Gacetas	Revistas Online.
Juegos de azar	Casino online, páginas de apuestas, páginas que ofrecen consejos de apuestas, foros de apuestas, etc.
Compras Online	Tiendas y almacenes online.
Redes Sociales	Páginas de Redes Sociales.

- **Categoría Perfil Adulto** incluye contenido que es inapropiado para niños y adolescentes.

Categoría	Descripción
Pornografía	Páginas web que alojan contenido pornográfico.
Odio / Violencia / Racismo / Estupefacientes	Las páginas Web que alojan contenido violento o racista, promocionando terrorismo o uso de estupefacientes.
Drogas/Alcohol/Tabaco	Páginas Web que venden o publicitan drogas, alcohol o productos de tabaco.
Actividades Ilegales	Páginas Web que promociona piratería o alojan contenido pirateado.
Pago Online	Formularios Web para pagos online y secciones de compra para tiendas online. El usuario puede navegar por tiendas online, pero los intentos de compras están bloqueados.
Citas Online	Citas para adultos en páginas web con chat, foto o vídeo compartido.

Haga clic en **Aplciar** para guardar las categorías para el contenido web bloqueado para el usuario.

19.2. Monitorizar la Actividad de los Niños

Acronis Internet Security Suite 2010 le ayuda a realizar el seguimiento de lo que sus hijos están haciendo en el equipo incluso cuando usted está fuera. Las alertas

pueden ser enviadas a su correo cada vez que el módulo de Control Parental bloquea una actividad. También puede guardar un informe con el historial de las páginas web visitadas.

Seleccionar las opciones que desea activar:

- **Enviarme un informe de actividad a través del correo.** Se envía una notificación por correo cada vez que el Control Parental de bloquea una actividad.
- **Guarda un informe del tráfico de Internet.** Registro de las páginas web visitadas por los usuarios para los cuales el Control Parental esta activado.

19.2.1. Comprobación de Páginas Web Visitadas

Acronis Internet Security Suite 2010 registra por defecto las páginas web visitadas por sus hijos.

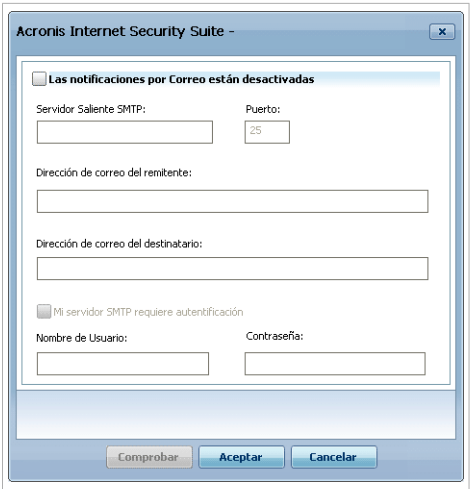
Para ver el registro, haga clic en **Ver Logs** para abrir el Historial&Eventos y seleccionar **Registro de Internet**.

19.2.2. Configurar Notificaciones por Correo.

Para recibir notificaciones por correo cuando el Control Parental bloquea una actividad, seleccionar **Enviarme un informe de actividad vía correo electrónico** en la ventana de configuración general del Control Parental. Se le pedirá la configuración de su cuenta de correo para configurarlo. Haga clic en **Si** para abrir la ventana de configuración.

Nota

Puede abrir la ventana de configuración más tarde haciendo clic en **Notificar por correo**.



Configuración de Correo

Debe introducir la configuración de su cuenta de correo de la siguiente manera:

- **Servidor de Salida SMTP** - Escriba la dirección del servidor de correo que utiliza para enviar mensajes de correo.
- Si el servidor utiliza un puerto diferente del puerto predeterminado 25, introdúzcalo en el campo correspondiente.
- **Dirección de correo del Remitente** - introduzca la dirección que desea que aparezca en el campo **De** en el correo.
- **Dirección de correo del Destinatario** - Introduzca la dirección de correo en la cual desea que reciba los informes enviados.
- Si el servidor requiere autentificación, seleccione la casilla **Mi servidor SMTP requiere autentificación** e introduzca su nombre de usuario y contraseña en los campos correspondientes.

Nota

Si no sabe que configuración es, abra su cuenta de correo y compruebe los ajustes de su cuenta de correo.

Para validar la configuración, haga clic en el botón **Comprobar**. Si se encuentra alguna incidencia durante la validación, Acronis Internet Security Suite 2010 le informará que áreas requieren su atención.

Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

19.3. Control Web

El **Control Web** le ayuda a bloquear el acceso a los sitios web con contenido inapropiado. Una lista de candidates para bloquear tanto los sitios como partes de los mismos serán proporcionados y actualizados por Acronis Internet Security Suite 2010, como parte del proceso regular de actualización.

Para configurar el Control de Web para una cuenta de usuario específica, haga clic en el botón **Modificar** correspondiente a esta cuenta de usuario y haga clic en la pestaña **Web**.

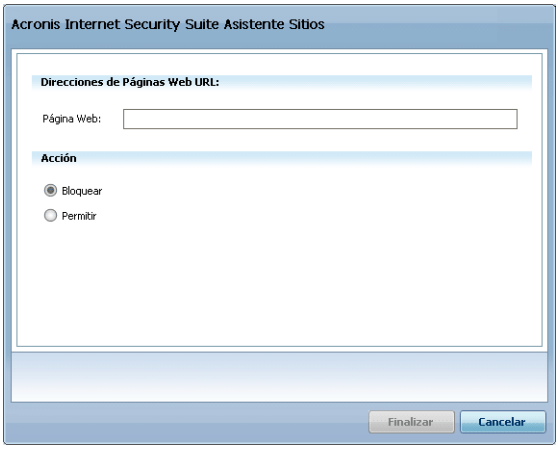
Control Web

Para activar esta protección seleccione la casilla correspondiente a **Activar Control Web**.

19.3.1. Creación de Reglas de Control Web

Para permitir o bloquear el acceso a una página web, siga estos pasos:

1. Haga clic en **Permitir Web** or **Bloquear Web**. Aparecerá una nueva ventana:



Especifique la página Web

2. Introduzca la dirección de la página web en el campo **Página Web**.
3. Seleccionar la acción deseada para esta regla - **Permitir** o **Bloquear**.
4. Haga clic en **Finalizar** para añadir la regla.

19.3.2. Administrar la Reglas de Control Web

Las regla de Control de Páginas Web han sido configuradas y están listadas en la tabla en la parte inferior de la ventana. La dirección Web y el actual estado esta listado para cada regla de Control de Página Web.

Para editar una regla, selecciónela, haga clic en el botón **Editar** y realice los cambios necesarios en la ventana de configuración. Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar**.

Debe seleccionar que acción debería realizar el Control Parental de Acronis Internet Security Suite 2010 en las páginas web que no tienen reglas de Control de páginas Web:

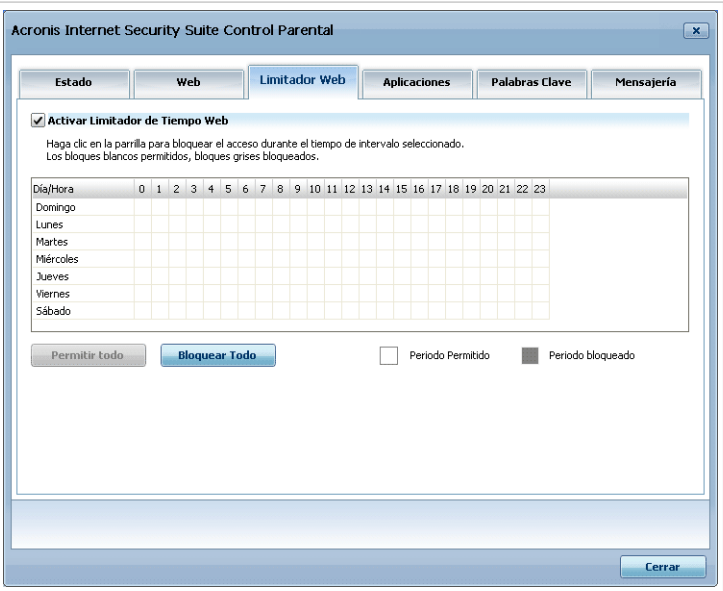
- **Permitir todos los sitios, excepto las que están en la lista**. Seleccione esta opción para permitir el acceso a todas las páginas web excepto las que ha establecido la acción **Bloquear**.
- **Bloquear todos los sitios, excepto los que estan en la lista**. Seleccione esta opción para bloquear el acceso a todas las páginas web excepto las que ha establecido la acción **Permitir**.

19.4. Limitador de tiempo para Web

El **Limitador de Tiempo Web** le ayuda a permitir o bloquear el acceso web a los usuarios o apliaciones durante los intervalos de tiempo indicados.

Nota
Acronis Internet Security Suite 2010 se actualizará independientemente de la configuración del **Limitador de Tiempo Web**.

Para configurar el Limitador de Tiempo web para un usuario específico, haga clic en el botón **Modificar** correspondiente para esta cuenta de usuario y haga clic en la pestaña **Limitador Web**.



Limitador de tiempo para Web

Para activar esta protección marque la casilla correspondiente a **Activar el limitador de tiempo para Web**.

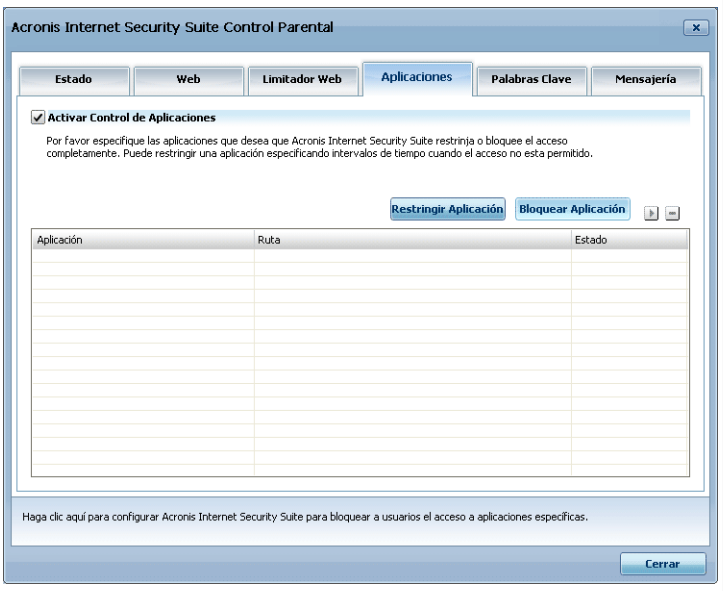
Seleccione los intervalos de tiempo para todas las conexiones de Internet que serán bloqueadas. Puede hacer clic en las celdas individuales, o puede hacer clic y arrastrar para cubrir largos periodos. Además, puede hacer clic en **Marcar Todos** para seleccionar todas las celdas y, implícitamente, bloquear todos los accesos a páginas web. Si hace clic en **Quitar Todos**, se permitirán todas las conexiones a Internet en todo momento.

Importante
Las casillas coloreadas en gris representan intervalos de tiempo en los que todas las conexiones a internet son bloqueadas.

19.5. Control de Aplicaciones

El **Control de Aplicaciones** ayuda a bloquear cualquier aplicación de ser ejecutada. Juegos, media y software de mensajería, así como otras categories de software y malware pueden ser bloqueadas de esta forma. Aplicaciones bloqueadas de esta manera también están protegidas contra modificiaciones y no pueden ser copiadas o movidas. Puede bloquear aplicaciones permanentes o justo durante ciertos intervalos de tiempos, tales como las de sus hijos cuando deberían estar haciendo sus tareas.

Para configurar el Control de Aplicaciones para una cuenta de usuario específica, haga clic en el botón **Modificar** correspondiente a esta cuenta de usuario y haga clic en la pestaña **Aplicaciones**.



Control de Aplicaciones

Para activar esta protección marque la casilla correspondiente a **Activar Control de Aplicación**.

19.5.1. Creando Reglas de Control de Aplicaciones

Para bloquear o restringir el acceso a una aplicación, siga estos pasos:

1. Haga clic en **Bloquear Aplicación** o **Restringir Aplicación**.

Especificar Aplicación

2. Haga clic en **Explorar** para localizar la aplicación que desea bloquear/restringir el acceso.
3. Seleccione la acción de la regla:
   - **Bloquear permanentemente** para bloquear el acceso a la aplicación completamente.
   - **Bloquear basado en este calendario** para restringir el acceso en ciertos intervalos de tiempo.

   Si selecciona restringir el acceso en lugar de bloquear la aplicación completamente, también debe seleccionar los días y el intervalo de tiempo de la tabla durante el cual el acceso esta bloqueado. Puede hacer clic en celdas individuales, o puede hacer clic y arrastrar para cubrir largos periodos. Además, puede hacer clic en **Marcar todo** para seleccionar todas las celdas, y, implícitamente, bloquear la aplicación completamente. Si hace clic **Desmarcar todo**, se permitirá el acceso a la aplicación en todo momento.
4. Haga clic en **Finalizar** para añadir la regla.

19.5.2. Administrar Reglas de Control de Aplicación

Las reglas de Control de Aplicación esta siendo configurado listado en la tabla en la parte inferior de la ventana. El nombre de la aplicación, la ruta y el actual estado esta listado para cada regla de Control de Aplicación.

Para editar una regla, selecciónela, haga clic en el botón **Editar** y realice los cambios necesarios en la ventana de configuración. Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar**.

19.6. Control de Palabras Clave

El Filtro de Palabras Clave le ayuda a bloquear a los usuarios el acceso a correos, páginas web y mensajes instantáneos que contengan las palabras específicas. Utilizando el Filtro de Palabras Clave, puede prevenir que sus hijos no vean palabras o frases inapropiadas cuando están conectados a Internet.

Nota
El Filtro de de Palabras Clave de la mensajería instantánea sólo está disponible para Yahoo Messenger y Windows Live (MSN) Messenger.

Para configurar el Filtro de Palabras Clave para una cuenta de usuario especifica, haga clic en el botón **Modificar** correspondiente a esta cuenta de usuario y haga clic en la pestaña **Palabras Clave**.

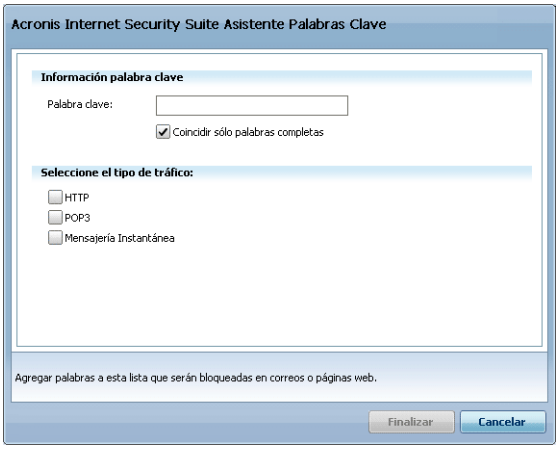
Control de Palabras Clave

Seleccionar la casilla **ACtivar Filtro de Palabras Clave** si desea utilizar esta característica.

19.6.1. Creando Reglas del Filtro de Palabras Clave

Para bloquear una palabra o frase, siga estos pasos:

1. Haga clic en **Bloquear Palabras Clave**. Aparecerá una nueva ventana:



Especificar Palabra Clave

2. Escriba la palabra o frase que desea bloquear en la celda. Si desea únicamente palabras completas que sean detectadas, seleccione la casilla **Coincidir sólo palabras completas**.
3. Seleccione el tipo de tráfico que Acronis Internet Security Suite 2010 debe analizar para la palabra específica.

Opción	Descripción
HTTP	Las páginas web que contengan la palabra clave serán bloqueados.
POP3	Los e-mails que contengan la palabra clave serán bloqueados.
Mensajería Instantánea	Los mensajes de mensajería instantánea que contengan la palabra clave serán bloqueados.

4. Haga clic en **Finalizar** para añadir la regla.

19.6.2. Administrar Reglas del Filtro de Palabras Clave

El Filtro de Palabras Clave ha sido configurado y está listado en la tabla de la parte inferior de la ventana. Las palabras y el actual estado para el diferente tipo de tráfico está listado para cada regla del Filtro de Palabras Clave.

Para editar una regla, selecciónela, haga clic en el botón **Editar** y realice los cambios necesarios en la ventana de configuración. Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar**.

19.7. Control de Mensajería Instantánea (IM)

El Control de Mensajería Instantánea (IM) le permite especificar los contactos con los que sus hijos pueden chatear.

Nota
El Control de Mensajería Instantánea (IM) sólo está disponible para Yahoo Messenger y Windows Live (MSN) Messenger.

Para configurar el Control IM para una cuenta de usuario específica, haga clic en el botón **Modificar** correspondiente a esta cuenta de usuario y haga clic en la pestaña **Tráfico IM**

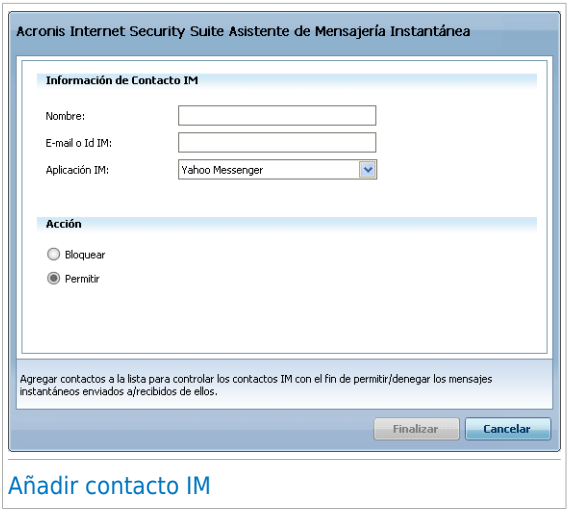
Control de Mensajería Instantánea

Marque la casilla **Control de Mensajería Instantánea** si desea utilizar esta característica.

19.7.1. Crear regla de Control de Mensajería Instantánea (IM)

Para permitir o bloquear mensajes instantáneos con un contacto, siga estos pasos:

1. Haga clic en **Bloquear ID IM** o **Permitir ID IM**. Aparecerá una nueva ventana:



Añadir contacto IM

2. Introduzca el nombre del contacto en el campo **Nombre**.
3. Introduzca la dirección de correo o el nombre de usuario utilizado por el contacto de IM en el campo **Correo o ID IM**.
4. Seleccione el programa de mensajería asociado a este contacto.
5. Seleccionar la acción para esta regla - **Bloquear** o **Permitir**.
6. Haga clic en **Finalizar** para añadir la regla.

19.7.2. Administrar reglas de Control de Mensajería Instantánea (IM)

Las reglas de Control IM se ha configurado y están listadas en la tabla en la parte inferior de la ventana. El nombre, ID IM, aplicación IM y el actual estado esta listado cada regla de Control IM.

Para editar una regla, selecciónela, haga clic en el botón **Editar** y realice los cambios necesarios en la ventana de configuración. Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar**.

Debería seleccionar que acción debe tomar el Control Parental de Acronis Internet Security Suite 2010 en los contactos de IM que han sido creados y no tienen reglas. Seleccione **Bloquear** o **Permitir IM con todos los contactos, excepto los que están en la lista**.

20. Control Privacidad

Acronis Internet Security Suite 2010 monitoriza docenas de puntos clave potenciales en su sistema dónde puede actuar el spyware, y también comprueba cualquier cambio que se haya producido en el sistema o software. Su función es bloquear troyanos u otras herramientas instaladas por hackers, que intenten comprometer su privacidad y envien información personal (como números de tarjetas de crédito) desde su equipo hacia el hacker.

20.1. Estado del control de privacidad

Para configurar el Control Privacidad y para ver la información relacionada con esta actividad, diríjase a **Control Privacidad>Estado** en Modo Avanzado.

Estado del control de privacidad

Puede ver si el Control de Privacidad está activado o desactivado. Si desea cambiar el estado del Control de Privacidad, desmarque o marque la casilla correspondiente.

Importante
Para impedir el robo de datos y proteger su privacidad, mantenga activado el **Control de Privacidad**.

El Control de Privacidad protege su equipo a través de los siguientes importantes controles de protección:

- Control de Identidad - protege sus datos confidenciales filtrando todo el tráfico web (HTTP), de correo (SMTP) y mensajería instantánea saliente según las reglas creadas en el apartado Identidad.
- Control del Registro - le pedirá permiso cada vez que un programa intente modificar un entrada del registro para ejecutarse cuando inicie Windows.
- Control de Cookies - le pedirá permiso cada vez que una nueva página web intente guardar una cookie.
- Control de Scripts - le pedirá permiso cada vez que una página web intente activar un script u otro tipo contenido activo.

En la parte inferior de este apartado puede ver las **Estadísticas del Control de Privacidad**.

20.1.1. Configurando el Nivel de Protección

Puede elegir el nivel de protección que mejor se adapte a sus necesidades de seguridad. Arrastre el deslizador a lo largo de la escala para elegir el nivel de protección adecuado.

Hay 3 niveles de seguridad:

Nivel de Protección	Descripción
Tolerante	Todos los controles de protección están desactivados.
Por Defecto	Sólo el **Control del Identidad** está activado.
Agresivo	**Control de Identidad**, **Control de Registro**, **Control de Cookie** y **Control de Script** está activado.

Puede personalizar el nivel de protección haciendo clic en **Personalizado**. En ventana que aparecerá, seleccione los controles de protección que desea activar y haga clic en **Aceptar**.

Haga clic en **Por Defecto** para posicionar el deslizador en el nivel predeterminado.

20.2. Control de Identidad

Mantener a salvo los datos personales es una cuestión que nos preocupa a todos. El robo de datos ha ido evolucionando al mismo ritmo que el desarrollo de las comunicaciones en Internet, utilizando nuevos métodos para engañar al usuario y conseguir su información privada.

Tanto si se trata de su dirección de e-mail o como de su número de tarjeta de crédito, cuando esta información no cae en buenas manos puede resultar peligrosa: puede

ahogarse entre una multitud de mensajes de spam o encontrar vacía su cuenta bancaria.

El Control de Identidad le protege del robo de información personal mientras está conectado a Internet. En función de las reglas que cree, el Control de Identidad analizará el tráfico web, e-mail y mensajería instantánea que sale de su equipo en busca de las cadenas de texto indicadas (por ejemplo, su número de tarjeta de crédito). En caso de coincidencia, se bloqueará la página web, correo o mensaje instantáneo correspondiente.

Puede crear reglas para proteger cualquier tipo de información que considere personal o confidencial, desde su número de teléfono o e-mail hasta información de su cuenta bancaria. Soporte multiusuario se incluye, para que los usuarios que inicien sesión en diferentes cuentas de usuario de Windows puedan usar sus propias reglas de protección de la identidad. Si su cuenta de Windows es una cuenta de Administrador, las reglas que cree pueden ser configuradas para que se apliquen también cuando otros usuarios del equipo inician sesión en Windows con sus cuentas.

¿Por qué usar el Control de Identidad?

- El Control de Identidad es muy efectivo bloqueando spyware de tipo keylogger. Este tipo de aplicaciones maliciosas capturan lo que escribe a través del teclado y lo envían a hackers o cibercriminales a través de Internet. El hacker puede encontrar información personal entre los datos robados, como números de cuentas bancarias o contraseñas, pudiendo utilizarlos para su propio beneficio.

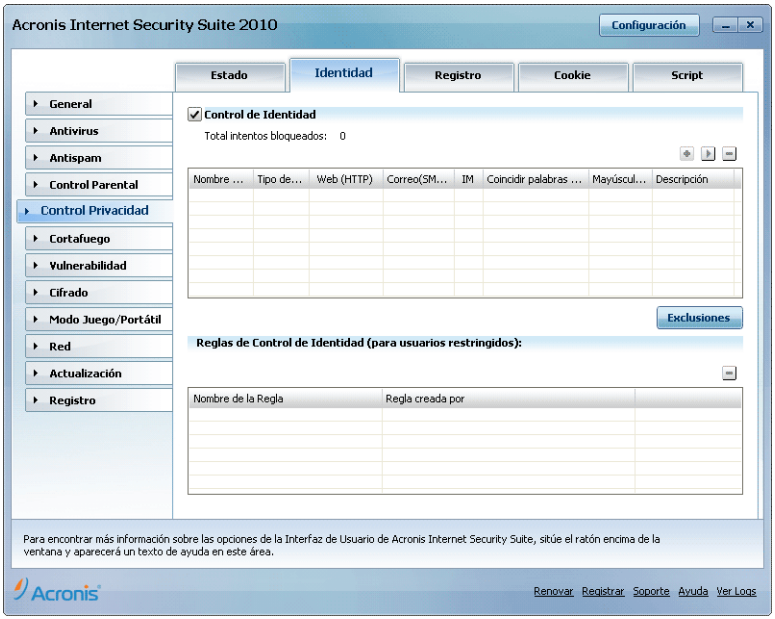
  Imaginemos que una aplicación de este tipo consigue eludir la detección antivirus. Si ha creado las reglas de protección de la identidad adecuadas, el keylogger no podría enviar información personal por e-mail web ni mensajería instantánea.

- El Control de Identidad puede protegerle de tentativas de phishing (intentos de robo de información personal). El tipo de phishing más habitual utiliza mensajes engañosos para inducirle a enviar información personal a través de una página web falsa.

  Por ejemplo, puede recibir mensajes que simulan provenir de su banco/caja y le soliciten actualizar su información bancaria urgentemente. Este mensaje incluye un enlace a una página web en la que debe introducir la información personal actualizada. Aunque puedan parecer legítimos, tanto la dirección de correo como la página a la que le dirige el enlace engañoso son falsos. Si hace clic en el enlace del mensaje y envía su información personal a través de la página web falsa, en realidad estará revelando sus datos a las personas que han organizado el intento de phishing.

  Si configura las reglas de protección de la identidad adecuadas, no podrá enviar información personal (como el número de su tarjeta de crédito) a través de una página web, a menos que la haya definido explícitamente como excepción a las reglas.

Para configurar el Control de Identidad, diríjase a **Control Privacidad>Identidad** en Modo Avanzado.



Control de Identidad

Si desea usar el Control de Identidad, siga estos pasos:

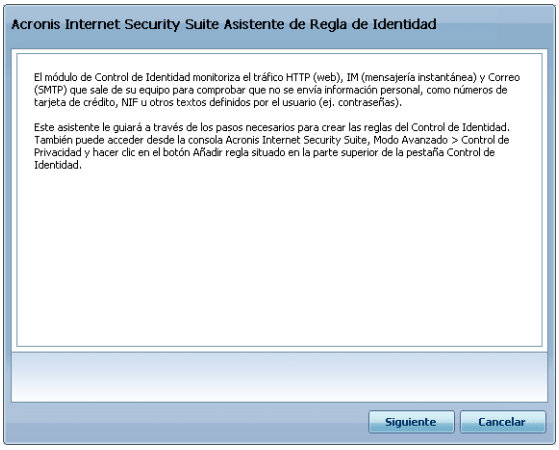
1. Marque la casilla **Activar Control de Identidad**.
2. Cree las reglas necesarias para proteger su información personal. Para más información, por favor, consulte el apartado "*Creando Reglas de Identidad*" (p. 198) de esta guía.
3. En caso necesario, puede definir excepciones a las reglas que ha creado. Para más información, por favor, consulte el apartado "*Definiendo las Excepciones*" (p. 201).
4. Si usted es un administrador del equipo, puede excluirse de las reglas de identidad creadas por otros administradores.

   Para más información, por favor, consulte el apartado "*Reglas Definidas por Otros Administradores*" (p. 203).

20.2.1. Creando Reglas de Identidad

Para crear una regla de protección de la identidad, haga clic en el botón **Añadir** y siga los pasos del asistente de configuración.

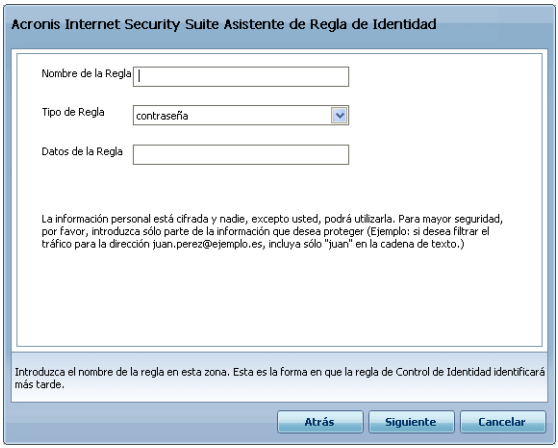
Paso 1/4 - Ventana de Bienvenida



Ventana de Bienvenida

Haga clic en **Siguiente**.

Paso 2/4 - Seleccione el Tipo de Regla y los Datos



Seleccionar el tipo y datos de la regla

Debe configurar los siguientes parámetros:

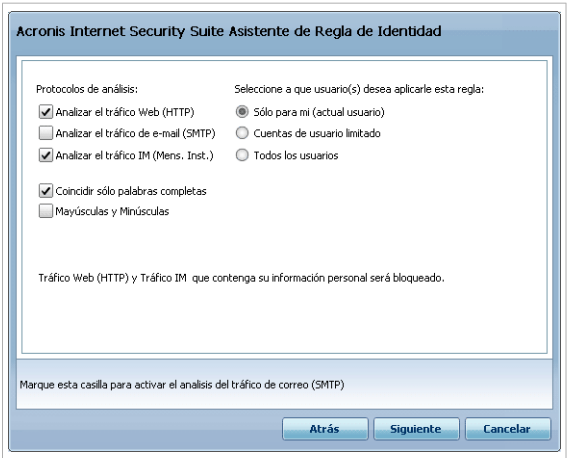
- **Nombre de la Regla** - introduzca el nombre de la regla en este campo editable.
- **Tipo de Regla** - elija el tipo de regla (dirección, nombre, tarjeta de crédito, PIN, etc).
- **Datos de la Regla** - introduzca los datos que desee proteger en este campo editable. Por ejemplo, si quiere proteger su número de tarjeta de crédito, introduzca toda la secuencia de números, o parte de ésta, en este campo.

> **Nota**
> Si introduce menos de tres caracteres, se le pedirá que valide los datos. Recomendamos escribir por lo menos tres caracteres para evitar confusiones durante el bloqueo de mensajes y páginas web.

Todos los datos que introduzca serán cifrados. Para mayor seguridad, no introduzca todos los datos que desee proteger.

Haga clic en **Siguiente**.

Paso 3/4 - Seleccionar el Tipo de Tráfico y Usuarios



Seleccionar el Tipo de Tráfico y Usuarios.

Seleccione el tipo de tráfico que desea que Acronis Internet Security Suite 2010 analice. Tiene las siguientes opciones a su disposición:

- **Analizar HTTP** - analiza el tráfico HTTP (web) y bloquea los datos salientes que coinciden con los datos de la regla.
- **Analizar SMTP** - analiza el tráfico SMTP (mail) y bloquea los mensajes salientes que coinciden con los datos de la regla.
- **Analizar Mensajería Instantánea** - analiza el tráfico de Mensajería Instantánea y bloquea los mensajes de chat salientes que coinciden con los datos de la regla.

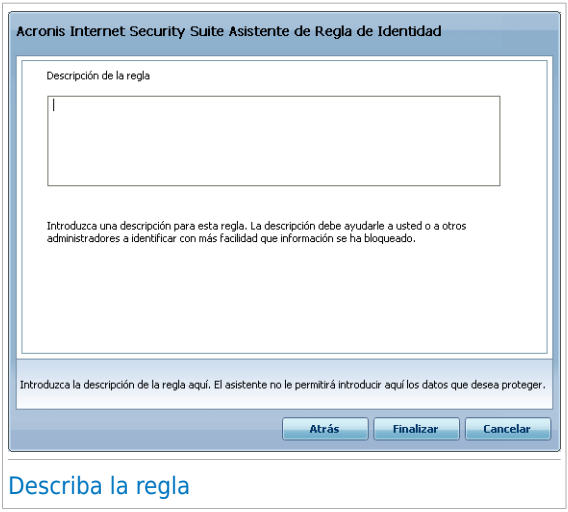
Puede elegir entre aplicar las reglas sólo si los datos de la regla coinciden completamente con las palabras, o si los datos de la regla y la cadena de texto detectada coinciden en mayúsculas y minúsculas.

Indique los usuarios para los que desea aplicar la regla.

- **Sólo para mi (actual usuario)** - la regla se aplicará sólo a su cuenta de usuario.
- **Cuentas de usuario limitadas** - la regla se aplicará a usted y a todos las cuentas de Windows limitadas.
- **Todos los usuarios** - La regla se aplicará a todas las cuentas de Windows.

Haga clic en **Siguiente**.

Paso 4/4 – Describa la Regla



Describa la regla

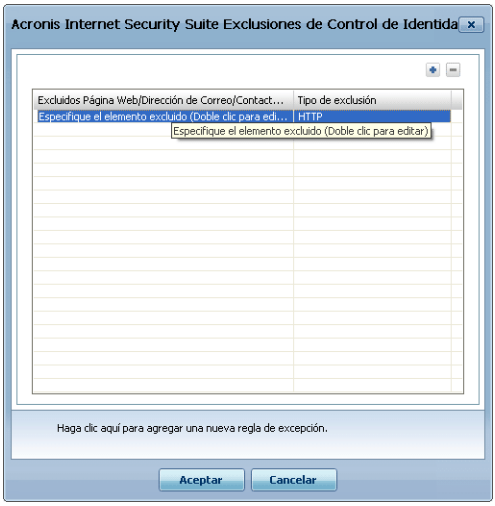
Introduzca una breve descripción de la regla en el campo editable. Como los datos bloqueados (las cadena de texto) no se muestran en texto plano cuando accede a la regla, es importante introducir una breve descripción que le ayude a identificar fácilmente los datos que protege.

Haga clic en **Finalizar**. La nueva regla aparecerá en la tabla.

20.2.2. Definiendo las Excepciones

En algunos casos, es necesario crear excepciones a las reglas de identidad. Imaginemos que ha creado una regla para impedir el envío de su número de tarjeta de crédito en páginas web. En el momento que su número de tarjeta se envíe a una página web, la página en cuestión se bloqueará. Pero si realmente quisiera comprar una película DVD en una tienda online segura, tendría que crear una excepción para dicha regla.

Para abrir la ventana dónde puede crear excepciones, haga clic en **Excepciones**.



Exclusiones

Para añadir una excepción, siga estos pasos:

1. Haga clic en el botón **Añadir** para añadir una nueva entrada en la tabla.
2. Haga doble clic en **Indique las direcciones permitidas** e introduzca la dirección de la página, el correo electrónico o el contacto de mensajería que desea añadir como excepción.
3. Haga doble clic en **Seleccionar tipo** y en el menú, seleccione la opción correspondiente al tipo de dirección que ha introducido previamente.
   - Si ha introducido una página web, seleccione la opción **HTTP**.
   - Si ha introducido una dirección de e-mail, seleccione la opción **SMTP**.
   - Si ha introducido un contacto de mensajería instantánea, seleccione **IM**.

Para eliminar un elemento de la tabla, selecciónelo y haga clic en el botón **Eliminar**.

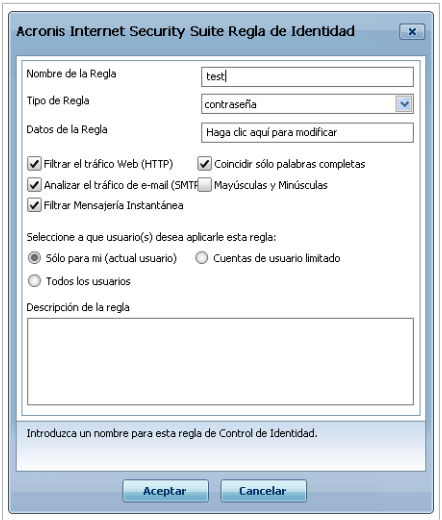
Haga clic en **Aceptar** para guardar los cambios.

20.2.3. Administrando las Reglas

Puede ver las reglas listadas hasta el momento en la tabla.

Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar**.

Para editar una regla selecciónela y haga clic en el botón **Editar** o haga doble clic en ella. Aparecerá una nueva ventana.



Editar Regla

Aquí puede cambiar el nombre, la descripción y los parámetros de la regla (tipo, datos y tráfico). Haga clic en **Aceptar** para guardar los cambios.

20.2.4. Reglas Definidas por Otros Administradores

Cuando usted no es el único usuario con derechos de administrador en su equipo, otros administradores pueden crear reglas de identidad para su cuenta. En caso de que desee que las reglas creadas por otros usuarios no se apliquen cuando inicien sesión, Acronis Internet Security Suite 2010 le permitirá excluirse de cualquier reglas que no haya creado usted.

Puede ver una lista de reglas creadas por otros administradores en la tabla **Reglas de Control de Identidad**. Para cada regla, su nombre y el usuario que la creado se muestra en la tabla.

Para excluirse de una regla, seleccione la regla en la tabla y haga clic en el botón. y haga clic en el botón **Eliminar**.

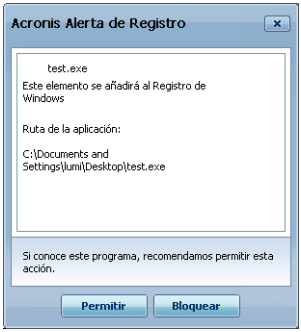
20.3. Control del Registro Windows

El **Registro** es un componente muy importante de Windows. El sistema operativo emplea el registro para guardar su configuración, los programas instalados, los datos del usuario etc.

El **Registro** también es utilizado para definir los programas que se puedan lanzar automáticamente con cada inicio de Windows. Esta posibilidad es frecuentemente

usada por los virus para lanzarse automáticamente cuando el usuario reinicie su ordenador.

El **Control del Registro** monitoriza toda la actividad del Registro Windows – acción que puede resultar muy útil para detectar Troyanos. Este módulo le advierte cada vez que un programa intenta modificar una entrada en el registro para poder ejecutarse con cada inicio del sistema.



Alerta de Registro

Podrá ver el nombre de la aplicación que intenta modificar el Registro de Windows.

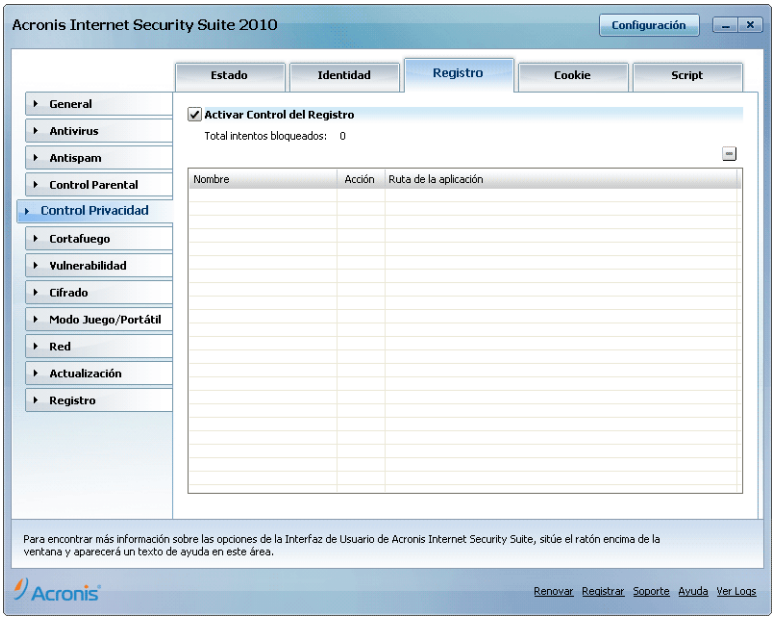
Si no reconoce esta aplicación y le parece sospechosa, haga clic en **Bloquear** para impedir que modifique el Registro de Windows. De lo contrario, haga clic en **Permitir** para autorizar la modificación.

A partir de su respuesta, se creará una regla que quedará listada en la tabla de reglas. Se aplicará la acción que ha indicado cada vez que esta aplicación intente modificar el Registro de Windows.

Nota

Generalmente, Acronis Internet Security Suite 2010 le envía alertas cuando usted instala nuevos programas que deben ejecutarse después del próximo reinicio del ordenador. En la mayoría de los casos, estos programas son legítimos y de confianza.

Para configurar el Control de Registro, diríjase a **Control Privacidad>Registro** en Modo Avanzado.



Control del Registro Windows

Puede ver las reglas listadas hasta el momento en la tabla.

Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar**.

20.4. Control de Cookies

Las Cookies son elementos muy comunes en Internet. Se trata de pequeños archivos que se almacenan en su equipo. Las páginas web crean estas cookies para rastrear información sobre sus hábitos.

Las Cookies están hechas para hacerle la vida más fácil. Por ejemplo, pueden ayudar al sitio web "recordar" su nombre y preferencias, para que no tenga que introducir estos datos cada vez que visita dicha página.

Pero las cookies también pueden ser empleadas para comprometer su privacidad, al monitorizar sus preferencias mientras navega en Internet.

Para evitar estos casos, use nuestro **Control de cookie**. Si se lo mantiene activado, **Control de cookies** le pedirá la autorización cada vez que un nuevo sitio web intenta enviar una cookie:

Alerta de Cookie

Podrá ver el nombre de la aplicación que trata de enviar la cookie.

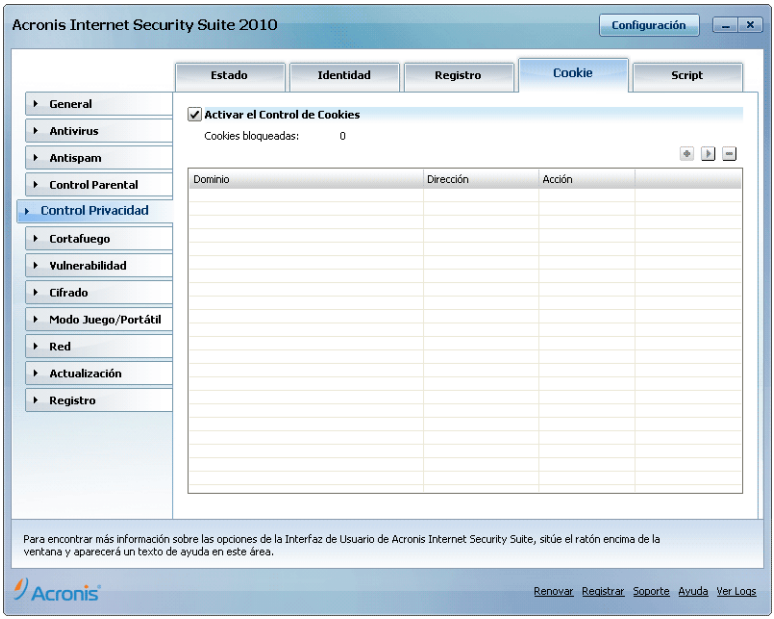
Haga clic en **Si** o **No** y una regla será creada, aplicada y listada en la tabla de reglas.

Esto le ayudará a decidir cuáles serán los sitios web de confianza.

Nota

Debido al gran número de cookies que se usan hoy en día en Internet, el **Control de Cookies** puede resultar un poco molesto al principio. Recibirá muchas preguntas sobre las páginas que intentan enviar cookies a su equipo. Pero, en cuanto añada sus páginas de confianza al listado de reglas, navegar por Internet volverá a ser tan fácil como antes.

Para configurar el Control de Cookies, diríjase a **Control Privacidad>Cookie** en Modo Avanzado.



Control de Cookies

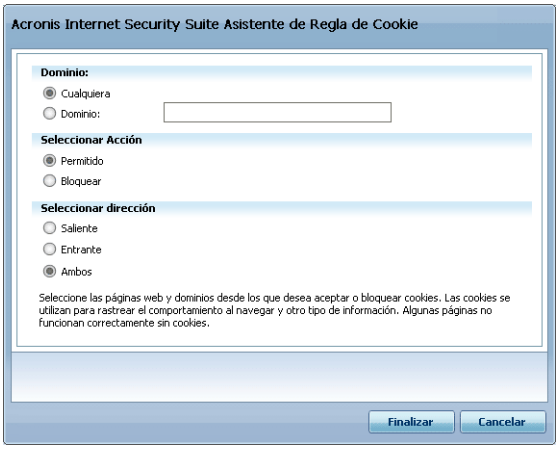
Puede ver las reglas listadas hasta el momento en la tabla.

Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar**. Para modificar los parámetros de la regla, seleccione la regla y haga clic en el botón **Editar** o haga doble clic en ella. Realice los cambios deseados en la ventana de configuración.

Para añadir manualmente una regla, haga clic en el botón **Añadir** y configure los parámetros de la regla en la ventana de configuración.

20.4.1. Ventana de Configuración

Cuando edite una regla o al añadir una regla manualmente, aparecerá la ventana de configuración.



Seleccione los Dominios y/o URLs, la Acción y la Dirección

Puede configurar los parámetros:

- **Introducir dominio** - permite introducir el nombre del dominio donde quiere que se aplique la regla.
- **Seleccionar acción** - seleccione la acción para la regla.

Acción	Descripción
Permitir	La aplicación será permitida.
Bloquear	La aplicación será bloqueada.

- **Dirección** - seleccione la dirección del tráfico.

Tipo	Descripción
Saliente	La regla será aplicada sólo para las cookies enviadas al sitio web conectado.
Entrante	La regla se aplicará sólo a las cookies recibidas desde la página web indicada.
Ambos	La regla aplicará en ambas direcciones.

Nota

Puede aceptar cookies, pero nunca debe enviarlas. Para bloquear su envío, cambie la acción a **Bloquear** y la dirección a **Saliente**.

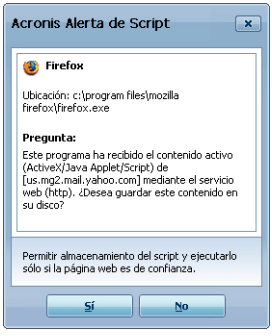
Haga clic en **Finalizar**.

20.5. Control de Scripts

Los Scripts y otros códigos, tales como los mandos ActiveX y los Java applets, empleados para crear páginas web interactivas, pueden ser programados para tener efectos dañinos. Los elementos ActiveX, por ejemplo, pueden obtener el acceso total a sus datos y, por consiguiente, pueden leer los datos de su ordenador, borrar información, copiar contraseñas e interceptar mensajes mientras esté conectado a Internet. No debe aceptar contenidos activos pertenecientes a sitios web que no conoce y no contempla con absoluta confianza.

Acronis Internet Security Suite 2010 le permite optar por ejecutar estos elementos o bien por bloquearlos.

Con el **Control del Script** usted decidirá cuáles serán los sitios web de confianza. Acronis Internet Security Suite 2010 le pedirá una confirmación de permiso todas las veces que un sitio intente activar un script u otros contenidos activos:

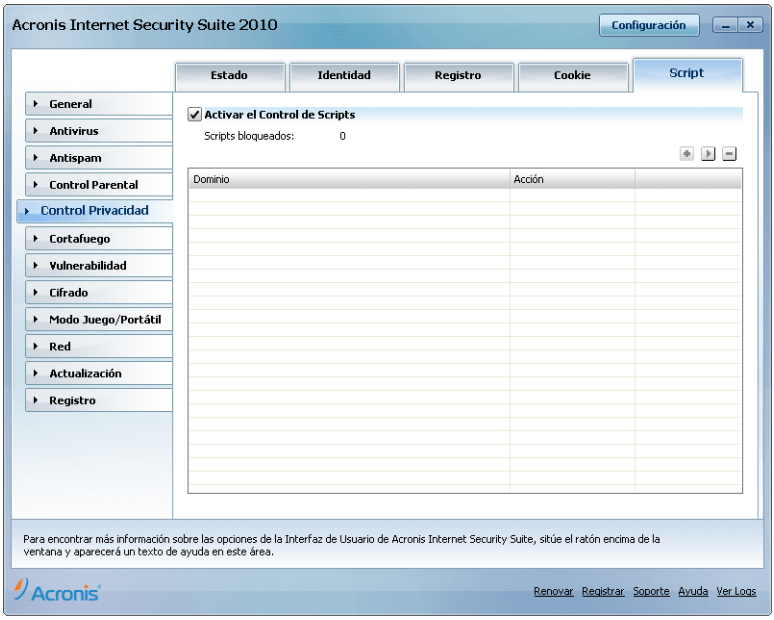


Alerta de Script

Puede ver el nombre del recurso.

Haga clic en **Si** o **No** y una regla será creada, aplicada y listada en la tabla de reglas.

Para configurar el Control de Script, diríjase a **Control Privacidad>Cookie** en Modo Avanzado.



Control de Scripts

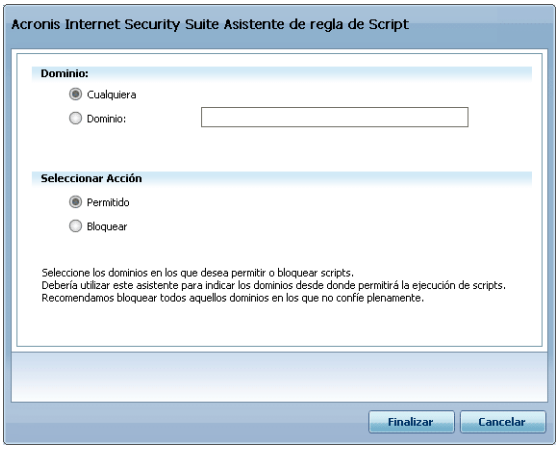
Puede ver las reglas listadas hasta el momento en la tabla.

Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar**. Para modificar los parámetros de la regla, seleccione la regla y haga clic en el botón **Editar** o haga doble clic en ella. Realice los cambios deseados en la ventana de configuración.

Para añadir manualmente una regla, haga clic en el botón **Añadir** y configure los parámetros de la regla en la ventana de configuración.

20.5.1. Ventana de Configuración

Cuando edite una regla o al añadir una regla manualmente, aparecerá la ventana de configuración.



Seleccione la Dirección y la Acción

Puede configurar los parámetros:

- **Introducir dominio** - permite introducir el nombre del dominio donde quiere que se aplique la regla.
- **Seleccionar acción** - seleccione la acción para la regla.

Acción	Descripción
Permitir	La aplicación será permitida.
Bloquear	La aplicación será bloqueada.

Haga clic en **Finalizar**.

21. Cortafuego

El Cortafuego protege su sistema de los intentos de conexión externos o internos no autorizados. Es algo parecido a tener un guardia en la puerta – vigilará su conexión a Internet y controlará todas las conexiones que decida autorizar o bloquear.

Nota
Un cortafuegos es esencial si tiene conexión de ancha banda o DSL.

Con el modo Oculto su ordenador "se oculta" del software malintencionado y los hackers. El módulo Cortafuego es capaz de detectar y protegerle automáticamente de los análisis de puertos (flujo de paquetes enviados a una máquina para encontrar "puntos de acceso", y que a menudo son una preparación para un ataque).

21.1. Configuración

Para configurar la protección de cortafuego, diríjase a **Cortafuego>Configuración** en el Modo Avanzado.

Configuración del Cortafuego

Puede ver si el cortafuego de Acronis Internet Security Suite 2010 está activado o desactivado. Si desea cambiar el estado del Cortafuego, marque o desmarque la casilla correspondiente.

Importante
Para estar protegido contra los ataques de Internet mantenga el **Cortafuego** activado.

Existen dos tipos de categorías de información:

- **Resumen de la Configuración de la Red.** Puede ver el nombre de su equipo, su dirección IP y la puerta de enlace predeterminada. Si dispone de más de un adaptador de red (es decir, si está conectado a más de una red), verá la dirección IP y puerta de enlace de cada uno de los adaptadores.
- **Estadísticas.** Puede ver varias estadísticas relacionadas con la actividad del Cortafuego:
  - ▶ número de bytes enviados.
  - ▶ número de bytes recibidos.
  - ▶ número de puertos analizados detectados y bloqueados por Acronis Internet Security Suite 2010. Los análisis de puertos son una herramienta frecuentemente utilizada por los hackers que buscan puertos abiertos en su equipo para intentar aprovecharse de ellos.
  - ▶ número de paquetes perdidos.
  - ▶ número de puertos abiertos.
  - ▶ número de conexiones entrantes activas.
  - ▶ número de conexiones salientes activas.

Para ver las conexiones activas y los puertos abiertos, diríjase a la pestaña Actividad.

En la parte de abajo puede ver las estadísticas de Acronis Internet Security Suite 2010 referentes al tráfico saliente y entrante. El gráfico muestra el volumen de tráfico de internet en los últimos dos minutos.

Nota
El gráfico aparece aunque el **Cortafuego** esté desactivado.

21.1.1. Estableciendo la Acción Predeterminada

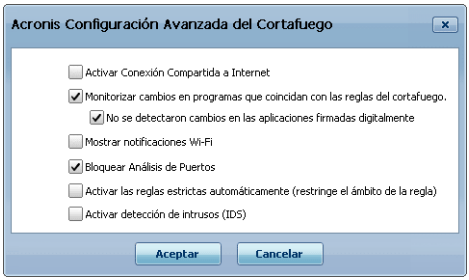
Por defecto, Acronis Internet Security Suite 2010 permite el acceso a Internet y a la red a todas los programas conocidos recopilados en su lista blanca. Para el resto de programas, Acronis Internet Security Suite 2010 le preguntará la acción a realizar a través de una ventana de alerta. La acción indicada se aplicará siempre que la aplicación intente acceder a Internet o a la red.

Arrastre el control deslizante a través de la escala para establecer la acción predeterminada que se realizará cuando una aplicación intente conectarse a la red/Internet. Dispone de las siguientes acciones:

Acción predeterminada	Descripción
Permitir todo	Aplica las reglas actuales y permite todo el tráfico que no coincida con las reglas actuales sin preguntar. Esta política no es en absoluto recomendable, pero puede resultar útil para los administradores de red y jugadores.
Permitir Programas Conocidos	Aplique las reglas actuales y permita todas las conexiones de salida de programas que se saben que son legítimos (lista blanca) por Acronis Internet Security Suite 2010 sin preguntarle. Para el resto de intentos de conexión, Acronis Internet Security Suite 2010 le solicitará permiso. La lista blanca está formada por las aplicaciones más utilizadas por los usuarios. Esto incluye los navegadores web más comunes, reproductores de audio y vídeo, programas de mensajería instantánea e intercambio de archivos, y también clientes de servidores (Correo, FTP..) o aplicaciones del sistema operativo. Para ver la lista blanca completa, haga clic en **Ver Lista Blanca**.
Informe	Aplica las reglas y le consulta sobre el tráfico que no coincide con ninguna de las reglas actuales.
Bloquear todo	Aplica las reglas existentes y bloquea todos los intentos de conexión que no coincidan con ninguna de las reglas existentes.

21.1.2. Modificando las Opciones Avanzadas del Cortafuego

Puede hacer clic en **Ajustes Avanzados** para modificar la configuración avanzada del Cortafuego.



Configuración Avanzada del Cortafuego

Tiene las siguientes opciones a su disposición:

- **Activar soporte Conexión compartida a Internet (ICS)** - activa el soporte para Conexión Compartida a Internet (ICS).

  Nota
  Esta opción no activa automáticamente ICS en su ordenador, solamente permite este tipo de conexión en caso de que la active desde su sistema operativo.

  Conexión Compartida a Internet (ICS) permite a los miembros de las redes locales conectarse a Internet a través de su ordenador. Esto es muy útil en caso de que tenga una conexión especial/particular a Internet (ej. conexiones de red inalámbricas) y desea compartirla con los otros miembros de su red.

  Al compartir su conexión a Internet con los miembros de su red local puede experimentar un mayor nivel de consumo de recursos y puede implicar riesgos. También le quita algunos de sus puertos (aquellos abiertos por los miembros que usan su conexión de Internet).

- **Detecta aplicaciones que han cambiado desde que la regla de cortafuego fue creada** - comprueba que aplicaciones intentan conectarse a Internet para ver si estas han sido cambiadas desde que se añadió la regla que controla el acceso. Si la aplicación ha sido cambiada, le avisará una alerta para permitir o denegar el acceso de la aplicación a Internet.

  A menudo, las aplicaciones cambian debido a actualizaciones. Sin embargo, existe el riesgo de que hayan sido modificadas por aplicaciones de malware con la intención de infectar a su equipo u otros equipos de la red.

  Nota
  Recomendamos mantener marcada esta opción y permitir el acceso sólo a aquellas aplicaciones que imaginaba que habrían cambiado desde la creación de la regla de acceso.

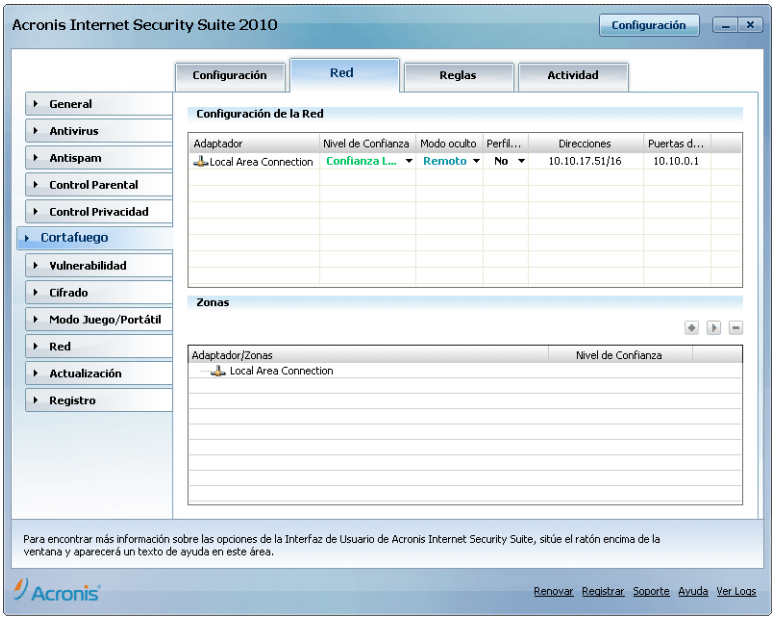
Las aplicaciones firmadas suelen ser aplicaciones de confianza con un alto grado de seguridad. Puede marcar la opción **Ignorar cambios de los procesos firmados** para permitir el acceso a Internet a aquellas aplicaciones firmadas que hayan sufrido algún cambio, sin recibir ningún mensaje de alerta.

- **Activar Notificaciones Wi-Fi** - si está conectado a una red Wi-Fi, se mostrarán ventanas con información sobre diferentes eventos de red (por ejemplo, cuando un equipo se conecta a la red).
- **Bloquear Análisis de Puertos** - detecta y bloquea los ataques que intentan averiguar qué puertos tiene abiertos.

  Los análisis de puertos son una herramienta frecuentemente utilizada por los hackers para averiguar los puertos abiertos en su equipo. Si encuentran un puerto vulnerable o inseguro, pueden intentar entrar en su equipo sin su autorización.
- **Reglas Automáticas Estrictas** - crea reglas estrictas a través de las alertas del Cortafuego. Con esta opción seleccionada, Acronis Internet Security Suite 2010 le preguntará la acción a realizar y creará reglas para cada uno de los procesos que abran la aplicación que solicita el acceso a la red o Internet.
- **Sistema de Detección de Intrusiones (SDI)** - activa la monitorización heurística de las aplicaciones que intentan acceder a los servicios de la red o a Internet.

21.2. Red

Para modificar la configuración del cortafuego, diríjase a **Cortafuego>Red** en Modo Avanzado.



Red

Las columnas de la tabla **Configuración de la Red** muestra información sobre las redes a las que está conectado:

- **Adaptador** - el adaptador de red que utiliza su equipo para conectarse a Internet.
- **Nivel de Confianza** - el nivel de confianza asignado al adaptador de red. En función de la configuración del adaptador de red, Acronis Internet Security Suite 2010 puede asignar automáticamente un nivel de confianza al adaptador o solicitarle más información.
- **Modo Oculto** - indica si quiere que otros ordenadores detecten a su equipo o no.
- **Perfil Genérico** - indica si las reglas genéricas se aplican a esta conexión o no.
- **Direcciones** - la dirección IP configurada en el adaptador.
- **Puertas de Enlace** - la dirección IP que utiliza su equipo para disponer de conexión a Internet.

21.2.1. Cambiando el Nivel de Confianza

Acronis Internet Security Suite 2010 asigna a cada adaptador de red un nivel de confianza. El nivel de confianza asignado al adaptador de red indica la fiabilidad de la red correspondiente.

A partir del nivel de confianza, se crean reglas específicas para el adaptador que indican cómo accederán a la red / Internet los procesos del sistema y Acronis Internet Security Suite 2010.

Puede ver el nivel de confianza configurado en cada adaptador en la tabla **Configuración de Red**, columna **Nivel de Confianza**. Para cambiar el nivel de confianza, haga clic en la flecha de la columna **Nivel de Confianza** y seleccione el nivel deseado.

Nivel de confianza	Descripción
Confianza Total	Desactiva el Cortafuego en el respectivo adaptador.
Confianza Local	Permite todo el tráfico entre su equipo y los equipos de la red local.
Seguro	Permite compartir recursos con los equipos de la red local. Este es el nivel que se establece automáticamente para las redes local (doméstica u oficina).
Inseguro	Impide que los equipos de la red o Internet se conecten a su equipo. Este es el nivel que se establece automáticamente para las redes públicas (si recibe una dirección IP desde un Proveedor de Servicios de Internet).
Bloqueo Local	Bloquea todo el tráfico entre su equipo y los equipos de la red local, aunque le ofrecerá acceso a Internet. Este es el nivel que se establece automáticamente para las redes Wi-Fi inseguras (abiertas).
Bloqueado	Bloquea por completo el tráfico de la red e Internet del adaptador de red correspondiente.

21.2.2. Configurando el Modo Oculto

El Modo Oculto hace que su ordenador sea invisible al software malintencionado y a los hackers de la red / Internet. Para configurar el Modo Oculto, haga clic en la flecha ▾ de la columna **Oculto** y seleccione la opción deseada.

Opciones del Modo Oculto	Descripción
Activado	El Modo Oculto está activado. Su equipo no será visible ni desde la red local ni desde Internet.
Desactivado	El Modo Oculto está desactivado. Cualquier usuario de la red local o Internet puede enviarle un ping y detectar su equipo.
Remoto	Su equipo no puede ser detectado desde Internet. Los usuarios de la red pueden enviarle pings y detectar su equipo.

21.2.3. Modificando la Configuración Genérica

Si la dirección IP del adaptador de red cambia, Acronis Internet Security Suite 2010 modificará el nivel de confianza en consecuencia. Si desea mantener el mismo nivel de confianza, haga clic en la flecha de la columna **Genérico** y seleccione **Si**.

21.2.4. Zonas de Red

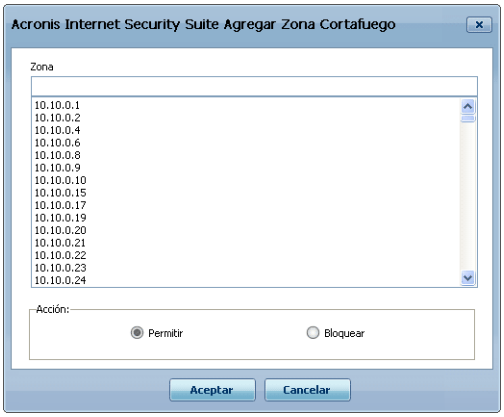
Puede añadir equipos de confianza o inseguros a un adaptador de red específico.

Una zona de confianza es un equipo en el que confía plenamente. Se permitirá todo el tráfico entre su equipo y un equipo de confianza. Para compartir recursos con algunos de los equipos que forman parte de una red Wi-Fi insegura, añádalos como equipos permitidos.

Una zona bloqueada es un equipo en el que no confía y con el que no desea comunicarse.

La tabla **Zonas** muestra las zonas de red existentes en cada adaptador.

Para añadir una zona, haga clic en el botón **Añadir** .



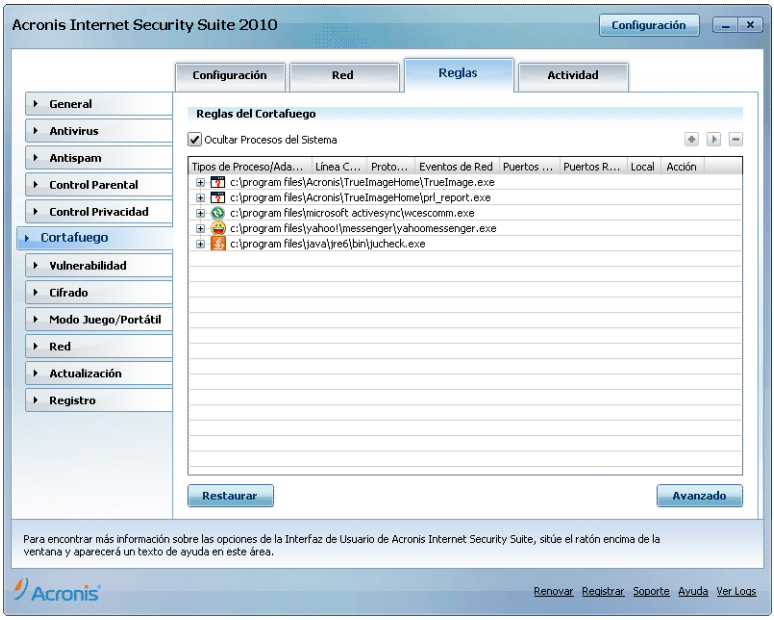
Añadir zona

Siga estos pasos:

1. Seleccione la dirección IP del equipo que desea añadir.
2. Seleccione la acción:
   - **Permitir** - para permitir todo el tráfico entre su equipo y el equipo seleccionado.
   - **Bloquear** - para bloquear todo el tráfico entre su equipo y el equipo seleccionado.
3. Haga clic en **Aceptar**.

21.3. Reglas

Para administrar las reglas del cortafuego que controlan el acceso de las aplicaciones a los recursos de la red e Internet, diríjase a **Cortafuego>Reglas** en Modo Avanzado.



Reglas del Cortafuego

Puede ver las aplicaciones (procesos) para las cuales se han creado reglas del cortafuego. Desmarque la casilla **Ocultar procesos del sistema** para ver las reglas correspondientes a los proceso del sistema o Acronis Internet Security Suite 2010.

Para ver las reglas creadas para una aplicación específica, haga clic en la casilla + situada junto a la respectiva aplicación. Puede ver más información sobre cada regla a partir de las columnas de la tabla:

- **Tipos de Proceso/Adaptador** - los tipos de proceso y adaptador de red a los que se aplica la regla. Las reglas se crean automáticamente para filtrar el tráfico de la red / Internet a través de cualquier adaptador. Puede crear reglas manualmente o editar reglas existentes y así filtrar el acceso a la red/Internet de una aplicación en un adaptador de red específico (por ejemplo, un adaptador de red Wi-Fi).
- **Línea de Comando** - el comando utilizado para iniciar el proceso en la interfaz de línea de comandos de Windows (**cmd**).
- **Protocolo** - el protocolo IP sobre el que se aplica la regla. Puede ver uno de los siguientes:

Protocolo	Descripción
Cualquiera	Incluye todos los protocolos IP.
TCP	Transmisión Control Protocol – TCP habilita dos hosts para establecer una conexión e intercambia partes de datos. TCP garantiza la entrega de los datops y también que los paquetes serán entregados en el mismo orden en el que fueron enviados.
UDP	User Datagram Protocol – UDP es un transporte basado en IP diseñado para un mayor rendimiento. Los juegos y otras aplicaciones basadas en vídeo a menudo utilizan UDP.
Un número	Representa un protocolo IP específico (que no sea TCP ni UDP). Puede encontrar una lista completa de los números asignados a los protocolos IP en www.iana.org/assignments/protocol-numbers.

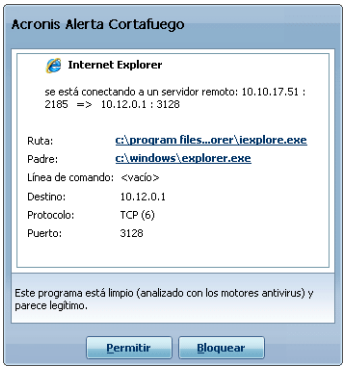
- **Eventos de Red** - los eventos de red a los que se aplica la regla. Puede producirse los siguientes eventos:

Evento	Descripción
Conectar	Intercambio preliminar de mensajes estándar usados por protocolos orientados a conexiones (como TCP) para establecer una conexión. En los protocolos orientados a conexiones, el tráfico de datos entre dos equipos sólo se produce después de establecer la conexión.
Tráfico	Flujo de datos entre dos equipos.
Escucha	Estado en el cual una aplicación monitoriza la red a la espera de establecer una conexión o de recibir información desde una aplicación igual.

- **Puertos Locales** - los puertos de su equipo sobre los que se aplica la regla.
- **Puertos Remotos** - los puertos del equipo remoto sobre los que se aplica la regla.
- **Local** - indica si la regla sólo se aplica a los equipos de la red local o no.
- **Acción** - indica si la aplicación tiene acceso o no a la red/Internet bajo las circunstancias especificadas.

21.3.1. Añadir Reglas Automáticamente

Con el **Cortafuego** activado, Acronis Internet Security Suite 2010 le pedirá permiso siempre que se realice una conexión a Internet:



Alerta de Cortafuego

En la alerta encontrará la siguiente información: la aplicación que está intentando acceder a Internet, la ruta de la aplicación, el destino, el protocolo utilizado y el puerto al que la aplicación está intentando conectarse.

Haga clic en **Permitir** para permitir todo el tráfico (entrante y saliente) generado por las aplicaciones ejecutadas localmente hacia cualquier IP de destino y en todos los puertos. Si selecciona **Bloquear**, se bloqueará el acceso de la aplicación a Internet.

En función de su respuesta, se creará una regla, se aplicará y añadirá a la lista. La próxima vez que la aplicación intente conectarse, se aplicará dicha regla.

Importante
Permita los intentos de conexión entrantes sólo de aquellas IPs y dominios en los que confíe plenamente.

21.3.2. Eliminando y Restableciendo Reglas

Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar Regla(s)**. Puede seleccionar y eliminar varias reglas a la vez.

Si desea eliminar todas las reglas creadas para una aplicación concreta, seleccione la aplicación en la lista y haga clic en el botón **Eliminar Regla(s)**.

Si desea cargar la regla establecida por defecto para el nivel de confianza seleccionado, haga clic en **Resetear Reglas**.

21.3.3. Creando y Modificando Reglas

Crear nuevas reglas manualmente o modificar las existentes, consiste en configurar los parámetros de la regla en la ventana de configuración.

Creando reglas. Para crear una nueva regla manualmente, siga estos pasos:

1. Haga clic en el botón **Añadir regla**. Aparecerá la ventana de configuración.
2. Configure los parámetros principales y avanzados según sus necesidades.
3. Haga clic en **Aceptar** para añadir la nueva regla.

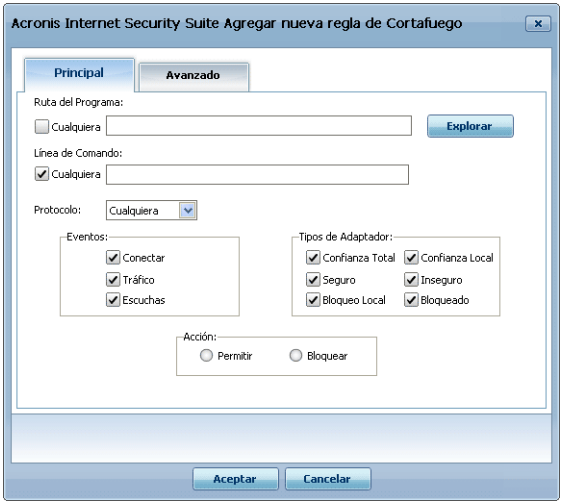
Modificando las reglas. Para modificar una regla existente, siga estos pasos:

1. Haga clic en el botón **Editar regla** o haga doble clic en la regla. Aparecerá la ventana de configuración.

2. Configure los parámetros principales y avanzados según sus necesidades.
3. Haga clic en **Aceptar** para guardar los cambios.

Configurando los Parámetros Principales

La pestaña **Principal** de la ventana de configuración le permite configurar los parámetros básicos.



Parámetros Principales

Puede configurar los siguientes parámetros:

- **Ruta del Programa.** Haga clic en **Explorar** y seleccione la aplicación a la que quiere aplicar la regla. Si desea aplicar la regla a todas las aplicaciones, seleccione **Cualquiera**.
- **Línea de comando.** Si sólo desea aplicar la regla cuando la aplicación seleccionada se abra con un comando específico de la interfaz de línea de comandos de Windows, desmarque la casilla **Cualquiera** e introduzca el comando correspondiente en el campo de texto editable.
- **Protocolo.** En el menú, seleccione el protocolo IP sobre el que desea aplicar la regla.
  - ▶ Si desea aplicar la regla a todos los protocolos, seleccione la casilla **Cualquiera**.
  - ▶ Si desea aplicar la regla para TCP, seleccione **TCP**.
  - ▶ Se desea aplicar la regla para UDP, seleccione **UDP**.

▶ Si sólo desea aplicar la regla a un protocolo concreto, seleccione la casilla **Otros**. Aparecerá un campo de texto editable. Introduzca el número asignado al protocolo que desea filtrar en el campo editable.

Nota

Los números de los protocolos IP están asignados por la Internet Assigned Numbers Authority (IANA). Puede encontrar una lista completa de los números asignados a los protocolos IP en www.iana.org/assignments/protocol-numbers.

- **Eventos.** Según el protocolo seleccionado, seleccione los eventos de la red a los que se aplica la regla. Puede producirse los siguientes eventos:

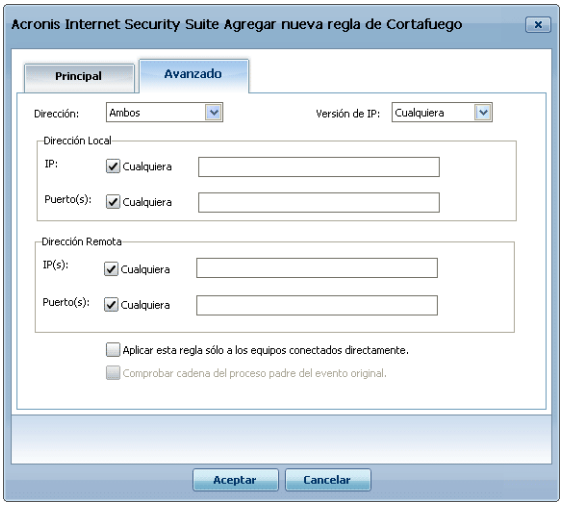
Evento	Descripción
Conectar	Intercambio preliminar de mensajes estándar usados por protocolos orientados a conexiones (como TCP) para establecer una conexión. En los protocolos orientados a conexiones, el tráfico de datos entre dos equipos sólo se produce después de establecer la conexión.
Tráfico	Flujo de datos entre dos equipos.
Escucha	Estado en el cual una aplicación monitoriza la red a la espera de establecer una conexión o de recibir información desde una aplicación igual.

- **Tipos de Adaptador.** Seleccionar el tipo de adaptador al que aplicar la regla.
- **Acción.** Seleccione una de las acciones disponibles:

Acción	Descripción
Permitir	Se permitirá el acceso de la aplicación especificada a la red / Internet bajo las condiciones indicadas.
Bloquear	Se bloqueará el acceso de la aplicación especificada a la red / Internet bajo las condiciones indicadas.

Configurando los Parámetros Avanzados

La pestaña **Avanzado** de la ventana de configuración le permite configurar los parámetros avanzados de la regla.



Parámetros Avanzados

Puede configurar los siguientes parámetros avanzados:

- **Dirección.** En el menú, seleccione la dirección del tráfico a la que se aplicará la regla.

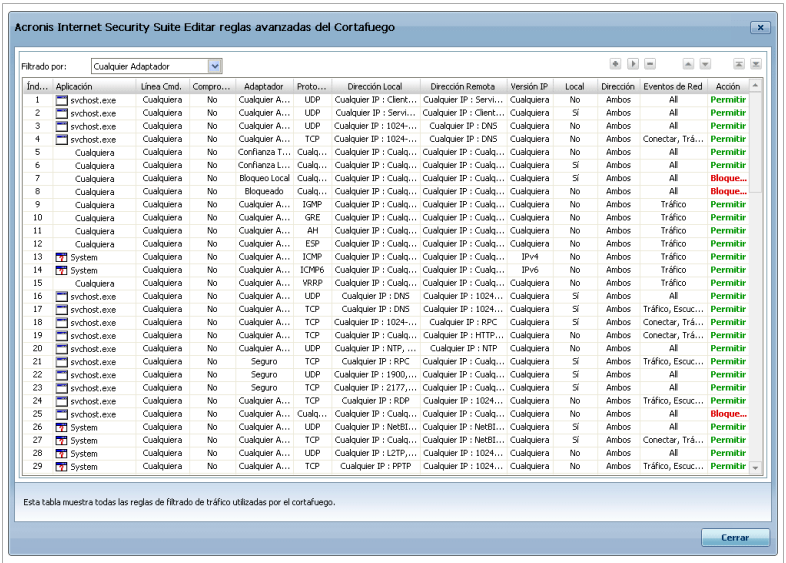
Dirección	Descripción
Saliente	La rula aplicará sólo para el tráfico saliente.
Entrante	La rula aplicará sólo para el tráfico entrante.
Ambos	La regla aplicará en ambas direcciones.

- **Versión de IP.** En el menú, seleccione la versión de IP (IPv4, IPv6 o cualquiera) a la que se aplicará la regla.
- **Dirección Local.** Indique la dirección IP local y el puerto a los que se aplicará la regla, como se indica:
  - ▶ Si dispone de más de un adaptador de red, puede desmarcar la casilla **Cualquiera** e introduzca una dirección IP específica.
  - ▶ Si ha seleccionado TCP o UDP como protocolo, puede indicar si la regla debe aplicarse a un puerto específico, o un rango entre 0 y 65535. Si quiere que la regla aplique a todos los puertos seleccione **Cualquiera**.

- **Dirección Remota.** Indique la dirección IP remota y el puerto a los que se aplicará la regla, como se indica:
  - ▶ Para filtrar el tráfico entre su equipo y un equipo concreto, desmarque la casilla **Cualquiera** e introduzca una dirección IP específica.
  - ▶ Si ha seleccionado TCP o UDP como protocolo, puede indicar si la regla debe aplicarse a un puerto específico, o un rango entre 0 y 65535. Si quiere que la regla aplique a todos los puertos seleccione **Cualquiera**.
- **Aplicar esta regla sólo a los equipos conectados directamente.** Seleccione esta opción desea que la regla se aplique sólo a los intentos de tráfico local.
- **Comprobar cadena del proceso padre del evento original.** Sólo puede modificar esta parámetro si ha seleccionado la opción **Reglas Automáticas Estrictas** (diríjase a la pestaña Configuración y haga clic en **Opciones Avanzadas**). Las reglas estrictas harán que Acronis Internet Security Suite 2010 le solicite la acción a realizar cada vez que el proceso padre de una aplicación que intenta acceder a la red/Internet sea diferente.

21.3.4. Configuración Avanzada de las Reglas

Si necesita un control avanzado sobre las reglas del Cortafuego, haga clic en **Avanzado**. Aparecerá una nueva ventana.



Configuración Avanzada de las Reglas

Puede ver las reglas del Cortafuego listadas para poder consultarlas. Las columnas de la tabla le proporcionan información sobre cada regla.

Nota

Cuando se produce un intento de conexión (tanto entrante como saliente), Acronis Internet Security Suite 2010 aplica la acción de la primera regla que coincide con la respectiva conexión. Por lo tanto, es muy importante el orden con el que se comprueban la reglas.

Para eliminar una regla, selecciónela y haga clic en el botón **Eliminar Regla(s)**.

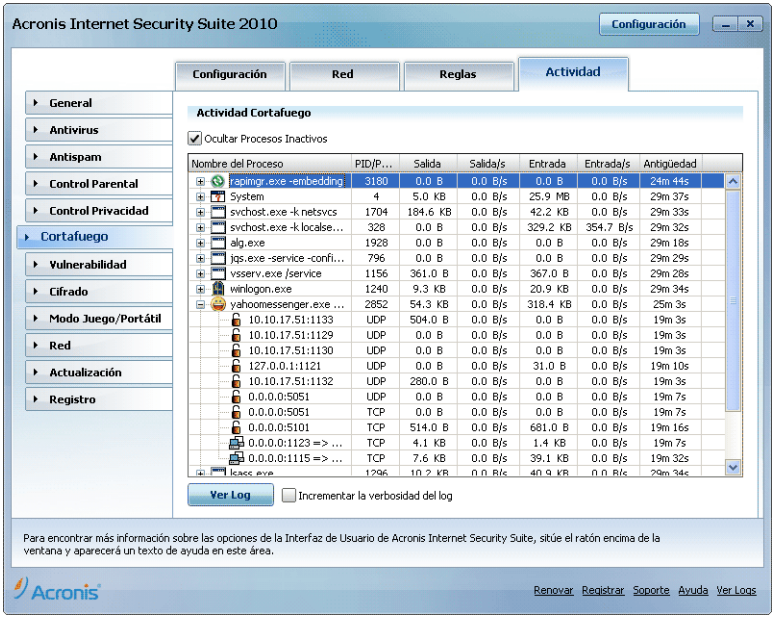
Para editar una regla existente, selecciónela y haga clic en el botón **Editar regla** o simplemente haga doble clic en la regla.

Puede subir o bajar la prioridad de una regla. Haga clic en el botón **Subir** para subir la prioridad de la regla seleccionada, o haga clic en el botón **Bajar** para bajar la prioridad de la regla seleccionada. Para dar la máxima prioridad a una regla, haga clic en el botón **Primera**. Para dar la mínima prioridad a una regla, haga clic en el botón **Última**.

Haga clic en **Cerrar** para cerrar la ventana.

21.4. Control de Conexiones

Para monitorizar la red actual/actividad de Internet (TCP y UDP) clasificadas por aplicaciones o para abrir el informe del Cortafuego de Acronis Internet Security Suite 2010, diríjase a **Cortafuego>Actividad** en Modo Avanzado.



Control de Conexiones

Puede ver el tráfico total ordenado por el nombre de las aplicaciones. Para cada aplicación, podrá ver las conexiones y puertos abiertos, así como estadísticas sobre la velocidad del tráfico entrante y saliente o la cantidad de datos enviados / recibidos.

Si también quiere ver los procesos inactivos, desmarque la opción **Ocultar procesos inactivos**.

A continuación se indica el significado de los iconos:

- Indica una conexión saliente.
- Indica una conexión entrante.
- Indica un puerto abierto en su equipo.

Esta ventana muestra la actividad de red / Internet en tiempo real. Si las conexiones o los puertos están cerrados, verá que las estadísticas correspondientes están oscurecidas y que, finalmente, desaparecen. Lo mismo sucede con todas las estadísticas correspondientes a las aplicaciones que generen tráfico o abran puertos que usted ha cerrado.

Para ver una lista completa de los eventos relacionados con el uso del módulo Cortafuego (activación/desactivación del cortafuego, bloqueo de tráfico, modificación de la configuración) o las actividades detectadas (análisis de puertos, bloqueo de

intentos de conexión o tráfico según las reglas), puede consultar el registro del Cortafuego de Acronis Internet Security Suite 2010 haciendo clic en **Mostrar Log**.

Si desea que el archivo log registre más información, marque la opción **Incrementar nivel de detalle del Log**.

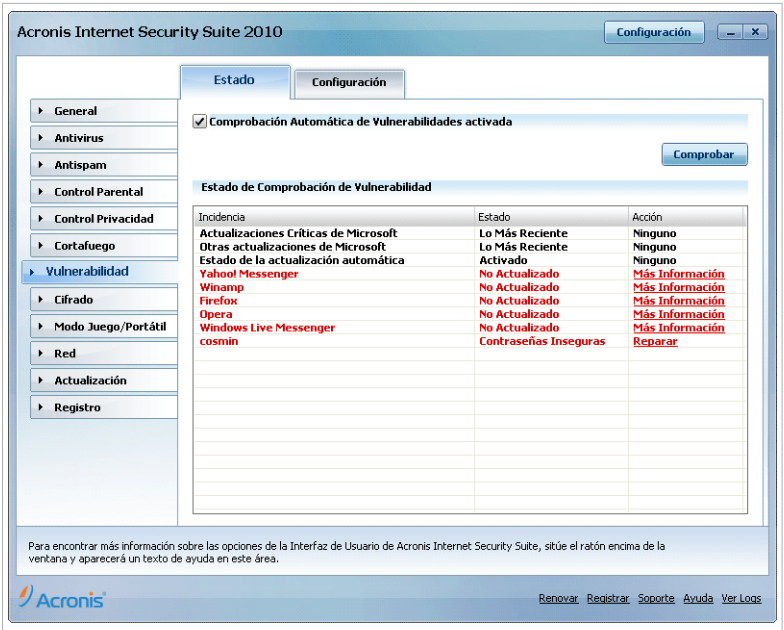
22. Vulnerabilidad

Un requisito importante para la protección de su equipo frente a aplicaciones malintencionadas y atacantes, es mantener actualizado su sistema operativo y las aplicaciones que utiliza habitualmente. Además, para impedir el acceso físico no autorizado a su equipo, debería utilizar contraseñas seguras (que no puedan adivinarse fácilmente) en todas las cuentas de usuario de Windows.

Acronis Internet Security Suite 2010 comprobará regularmente la existencia de vulnerabilidades en su sistema y le avisará en caso que existan incidencias.

22.1. Estado

Para configurar la comprobación automática de vulnerabilidad o ejecutar una comprobación de vulnerabilidad, diríjase a **Vulnerabilidad>Estado** en Modo Avanzado.



Estado de Vulnerabilidades

La tabla muestra las incidencias cubiertas en el último análisis de vulnerabilidades y su estado. Puede ver la acción que debe realizar para reparar cada vulnerabilidad,

en caso de que las haya. Si la acción es **Ninguna**, entonces la incidencia no representa una vulnerabilidad.

Importante

Para recibir notificaciones automáticas sobre las vulnerabilidades de su sistema o aplicaciones, mantenga activada la **Comprobación Automática de Vulnerabilidades**.

22.1.1. Reparar Vulnerabilidades

Dependiendo de la incidencia, para reparar una vulnerabilidad específica haga lo siguiente:

- Si las actualizaciones de Windows están disponibles, haga clic en **Instalar** en la columna **Acción** para instalarla.
- Si una aplicación no está actualizada, utilice el enlace **Página de Inicio** proporcionado para descargar e instalar la última versión de la aplicación.
- Si una cuenta de Windows ha detectado una contraseña insegura, haga clic en **Reparar** para forzar al usuario a cambiar la contraseña en el siguiente inicio de sesión o cambie la contraseña usted mismo. Para conseguir una contraseña segura, utilice una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (como #, $ o @).

Puede hacer clic en **Comprobar ahora** y seguir el asistente para reparar las vulnerabilidades paso a paso. Para más información, por favor diríjase a "*Asistente de Análisis de Vulnerabilidad*" (p. 57).

22.2. Configuración

Para modificar la configuración de la Comprobación Automática de Vulnerabilidades, diríjase a **Vulnerabilidad>Configuración** en Modo Avanzado.

Configuración de la Comprobación Automática de Vulnerabilidades

Marque las casillas correspondientes a las vulnerabilidades del sistema que desee comprobar con regularidad.

- **Actualizaciones Críticas de Windows**
- **Actualizaciones Regulares de Windows**
- **Actualizaciones de Aplicaciones**
- **Contraseñas Débiles**

Nota

Si desmarca la casilla correspondiente a una vulnerabilidad específica, Acronis Internet Security Suite 2010 dejará de informarle sobre las incidencias relacionadas con la ésta.

23. Cifrado

Acronis Internet Security Suite 2010 ofrece funciones de cifrado para proteger sus documentos confidenciales y las conversaciones de mensajería instantánea a través de Yahoo Messenger y MSN Messenger.

23.1. Cifrado de Mensajería Instantánea (IM)

Por defecto, Acronis Internet Security Suite 2010 cifra todas sus sesiones de chat por mensajería instantánea siempre y cuando:

- Su pareja de chat tiene un producto Acronis instalado que soporta cifrado de IM y el cifrado IM está activado para la aplicación de mensajería instantánea utilizada para chatear.
- Su contacto de chat utilice Yahoo Messenger o Windows Live (MSN) Messenger.

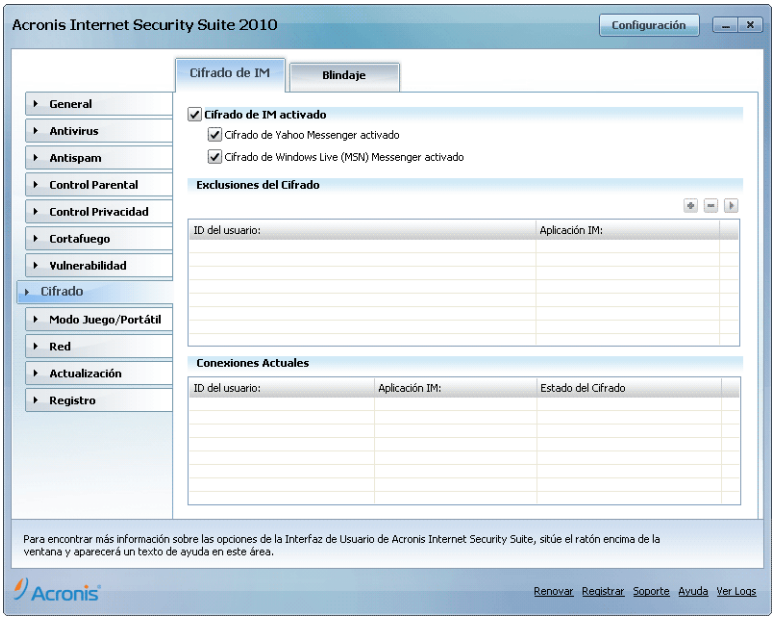
Importante

Acronis Internet Security Suite 2010 no cifrará la conversación si su contacto utiliza una aplicación web para chatear, como Meebo, o si uno de los contactos utiliza Yahoo! y el otro Windows Live (MSN).

Para configurar el cifrado de mensajería instantánea, diríjase a **Cifrado>Cifrado de IM** en Modo Avanzado.

Nota

Puede configurar fácilmente el cifrado de la mensajería instantánea usando la barra de herramientas de Acronis en la ventana de chat. Para más información, por favor diríjase a “*Integración con Programas de Mensajería Instantánea*” (p. 275).



Cifrado de Mensajería Instantánea

Por defecto, el Cifrado de IM está activado tanto para Yahoo Messenger como para Windows Live (MSN) Messenger. Puede elegir entre desactivar el Cifrado de IM por completo, o sólo para alguna de las aplicaciones citadas.

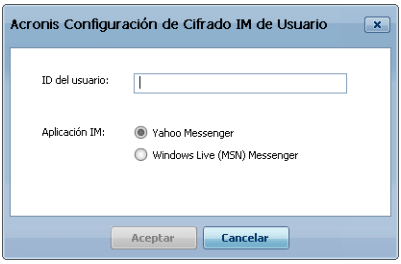
Se mostrarán dos tablas:

- **Exclusiones del Cifrado** - lista los IDs de usuario y el programa de mensajería asociado para el cual el cifrado está desactivado. Para eliminar un contacto de la lista, selecciónelo y haga clic en el botón **Quitar**.
- **Conexiones Actuales** - lista las conexiones de mensajería instantánea establecidas actualmente (ID de usuario y programa IM asociado) e indica si el cifrado está activado o no. Una conexión puede no cifrarse por alguna de las siguientes razones:
  - Ha desactivado explícitamente el cifrado para las conversaciones con el respectivo contacto.
  - Su contacto no tiene instalada un producto Acronis que soporte cifrado IM.

23.1.1. Desactivando el Cifrado para Usuarios Específicos

Para desactivar el cifrado de un contacto determinado, siga estos pasos:

1. Haga clic en el botón **Añadir** para abrir la ventana de configuración.



Añadiendo Contactos

2. Introduzca el ID de usuario de su contacto en el campo de texto editable.
3. Seleccione la aplicación de mensajería instantánea asociada a este contacto.
4. Haga clic en **Aceptar**.

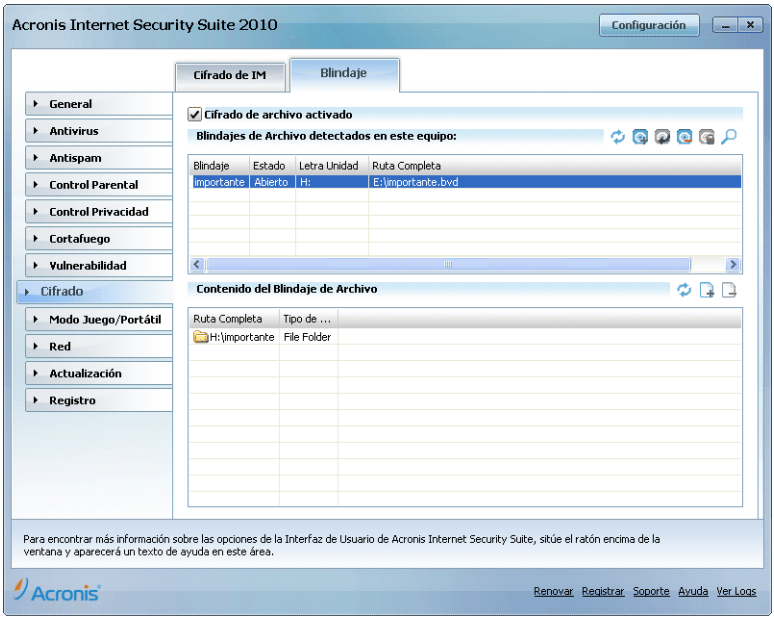
23.2. Cifrado de Archivo

El Blindaje de Archivo de le permite crear unidades logicas cifradas y protegidos por contraseña en su equipo, en los que puede almacenar sus documentos confidenciales y sensibles. Sólo la persona que conozca la contraseña podrá acceder a los datos almacenados en los blindajes.

La contraseña le permite abrir el blindaje, almacenar datos en éste y cerrarlo, a la vez que asegura su protección. Cuando un blindaje está abierto, puede añadir nuevos archivos, abrir los archivos que contiene y modificarlos.

Físicamente, el blindaje es un archivo cifrado almacenado en su equipo cuya extensión es bvd. Aunque es posible acceder a los archivos físicos de las unidades blindadas desde diferentes sistemas operativos (como Linux), la información almacenada en los mismos no puede leerse al estar cifrada.

Para administrar los blindajes de archivo en su equipo, diríjase a **Cifrado>Cifrado de Archivo** en Modo Avanzado.



Blindaje

Para desactivar el Cifrado de Archivo, desmarcar la casilla **Cifrado de Archivo Activado** y haga clic en **Si** para confirmar. Si desactiva el Blindaje de Archivos, se bloquearán todos los blindajes existentes y no podrá acceder a los archivos que contienen.

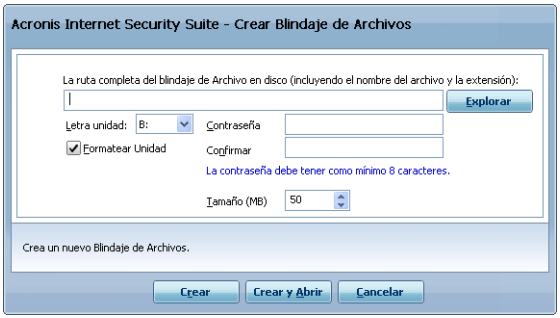
La tabla de la parte superior muestra los blindajes de su equipo. Puede ver el nombre, el estado (abierto/bloqueado), la letra de la unidad y la ruta completa del blindaje. La tabla de la parte inferior muestra el contenido del blindaje seleccionado.

23.2.1. Creando un Blindaje

Para crear un nuevo blindaje, siga cualquiera de estos métodos:

- Haga clic en **Crear Blindaje**.
- Haga clic derecho en la tabla de blindajes y seleccione la opción **Crear**.
- Haga clic derecho en el Escritorio o en una carpeta de su equipo, sitúe el cursor encima de la opción **Blindaje de Archivos de Acronis Internet Security Suite** y seleccione **Crear**.

Aparecerá una nueva ventana.



Crear Blindaje de Archivos

Siga estos pasos:

1. Indique la ubicación y el nombre del archivo de blindaje.
   - Haga clic en **Explorar**, seleccione la ubicación del blindaje y guarde el archivo de blindaje con el nombre deseado.
   - Escriba sólo el nombre del blindaje en el campo correspondiente para crearlo en Mis Documentos. Para abrir Mis Documentos, haga clic en start el menú Inicio de Windows y después en **Mis Documentos**.
   - Introduzca la ruta completa del archivo de blindaje en el disco. Por ejemplo, `C:\my_vault.bvd`.
2. Seleccione la letra de la unidad en el menú. Al abrir un blindaje, en Mi PC aparecerá un nuevo disco virtual con la letra de unidad seleccionada.
3. Introduzca la contraeña deseada para el Blindaje en los campos **Nueva Contraseña** y **Confirmar contraseña**. Cada vez que alguien que intente abrir el blindaje y acceder a sus archivos, deberá introducir la contraseña.
4. Seleccione la opción **Formatear unidad** para formatear la unidad virtual asignada al blindaje. Debe formatear la unidad antes de poder añadir archivos al blindaje.
5. Si desea modificar el tamaño predeterminado del blindaje (50 MB), introduzca el valor deseado en el campo **Tamaño del Blindaje**.
6. Haga clic en **Crear** si sólo desea crear el Blindaje en la ubicación deseada. Para crear un blindaje y mostrarlo como una unidad de disco virtual en Mi PC, haga clic en **Crear y Abrir**.

Acronis Internet Security Suite 2010 le informará inmediatamente sobre el resultado de la operación. En caso de que haya ocurrido un error, utilice el mensaje de error para solucionar la incidencia. Haga clic en **Aceptar** para cerrar la ventana.

Nota
Podría ser conveniente guardar todos los blindajes de archivos en la misma ubicación. De esta manera, puede localizarlos fácilmente.

23.2.2. Abriendo un Blindaje

Para poder acceder y trabajar con los archivos almacenados en el Blindaje, antes debería abrirlo. Al abrir un Blindaje, aparecerá una unidad de disco virtual en Mi PC. Esta unidad estará etiquetada con la letra de unidad asignada al Blindaje.

Para abrir un blindaje, use cualquiera de estos métodos:

- Seleccione un blindaje de la lista y haga clic en **Abrir Blindaje**.
- Haga clic derecho en la tabla y seleccione la opción **Abrir**.
- Haga clic derecho en el archivo de blindaje de su equipo, sitúe el cursor encima de la opción **Blindaje de Archivos de Acronis Internet Security Suite** y seleccione **Abrir**.

Aparecerá una nueva ventana.

Abrir Blindaje de Archivos

Siga estos pasos:

1. Seleccione la letra de la unidad en el menú.
2. Introduzca la contraseña del blindaje en el campo **Contraseña**.
3. Haga clic en **Abrir**.

Acronis Internet Security Suite 2010 le informará inmediatamente sobre el resultado de la operación. En caso de que haya ocurrido un error, utilice el mensaje de error para solucionar la incidencia. Haga clic en **Aceptar** para cerrar la ventana.

23.2.3. Bloqueando un Blindaje

Cuando acabe de trabajar con el blindaje de archivos, debería bloquearlo para proteger sus datos. Al bloquear el blindaje, la unidad de disco virual desaparecerá de Mi PC. En consecuencia, el acceso a los datos guardados en el blindaje será completamente bloqueado.

Para bloquear un blindaje, use cualquiera de estos métodos:

- Seleccione un blindaje de la tabla y haga clic en **Bloquear Blindaje**.
- Haga clic derecho en un blindaje de la tabla y seleccione **Bloquear**.
- Haga clic derecho en la unidad de disco virtual de Mi PC correspondiente al Blindaje, sitúe el cursor encima de la opción **Blindaje de Archivos de Acronis Internet Security Suite** y seleccione **Bloquear**.

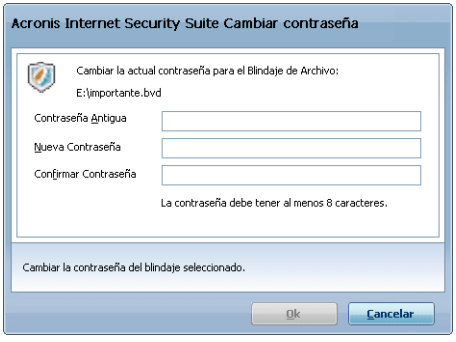
Acronis Internet Security Suite 2010 le informará inmediatamente sobre el resultado de la operación. En caso de que haya ocurrido un error, utilice el mensaje de error para solucionar la incidencia. Haga clic en **Aceptar** para cerrar la ventana.

23.2.4. Cambiando la Contraseña del Blindaje

El blindaje debe bloquearse antes de cambiar la contraseña. Para cambiar la contraseña del blindaje, use cualquiera de estos métodos:

- Seleccione un blindaje de la tabla y haga clic en **Cambiar contraseña**.
- Haga clic derecho en un blindaje de la tabla y seleccione la opción **Cambiar contraseña**.
- Clic derecho en el blindaje de archivo en su equipo, sitúe el cursor en **Acronis Internet Security Suite Blindaje de Archivo** y seleccione **Cambiar contraseña del blindaje**.

Aparecerá una nueva ventana.



Cambiar Contraseña del Blindaje

Siga estos pasos:

1. Introduzca la contraseña del blindaje existente en el campo **Contraseña Antigua**.
2. Introduzca la nueva contraseña del blindaje en los campos **Nueva Contraseña** y **Confirmar Nueva Contraseña**.

Nota

La contraseña debe tener como mínimo 8 caracteres. Para conseguir una contraseña segura, utilice una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (como #, $ o @).

3. Haga clic en **Aceptar** para cambiar la contraseña.

Acronis Internet Security Suite 2010 le informará inmediatamente sobre el resultado de la operación. En caso de que haya ocurrido un error, utilice el mensaje de error para solucionar la incidencia. Haga clic en **Aceptar** para cerrar la ventana.

23.2.5. Añadiendo Archivos a un Blindaje

Para añadir archivos a un blindaje, siga estos pasos:

1. Selecciona de la tabla de blindajes el blindaje en el que quiere añadir archivos.
2. Si esl blindaje está bloqueado, primero debe abrirlo (clic derecho y seleccionar **Abrir blindaje**).
3. Haga clic **Añadir archivo**. Aparecerá una nueva ventana.
4. Seleccione el archivo / carpeta que desea añadir al blindaje.
5. Haga clic en **Aceptar** para copiar los objetos seleccionados al blindaje.

Una vez el blindaje está abierto, puede utilizar directamente la unidad virtual correspondiente al blindaje. Siga estos pasos:

1. Abra Mi PC (haga clic en el start menú Inicio de Windows y después en **Mi PC**).
2. Entre en la unidad de disco virtual correspondiente al blindaje. Busque la letra de la unidad que asignó al blindaje al abrirlo.
3. Copie-pegue o arraste&suelte archivos o carpetas directamente a la unidad de disco virtual.

23.2.6. Eliminando Archivos de un Blindaje

Para eliminar un archivo de un blindaje, siga estos pasos:

1. Seleccione el blindaje de la tabla que contiene el archivo a eliminar.
2. Si esl blindaje está bloqueado, primero debe abrirlo (clic derecho y seleccionar **Abrir blindaje**).

3. Seleccione el archivo a eliminar en la tabla que muestra el contenido del blindaje.
4. Haga clic en **Eliminar archivos/carpetas**.

Si el blindaje está abierto, puede eliminar directamente los archivos en la unidad de disco virtual asignada al blindaje. Siga estos pasos:

1. Abra Mi PC (haga clic en el menú Inicio de Windows y después en **Mi PC**).
2. Entre en la unidad de disco virtual correspondiente al blindaje. Busque la letra de la unidad que asignó al blindaje al abrirlo.
3. Elimina archivos o carpetas como lo hace en Windows (por ejemplo, clic derecho en un archivo que quiere eliminar y seleccione **Eliminar**).

24. Modo Juego / Portátil

Los Modos Juego / Portátil le permiten configurar modos especiales de funcionamiento de Acronis Internet Security Suite 2010:

- El Modo Juego modifica temporalmente las opciones de seguridad para minimizar su impacto y sacar el máximo rendimiento a su experiencia de juego.
- El Modo Portátil modifica temporalmente las opciones de seguridad para modificar su impacto y prolongar la duración de su batería.

24.1. Modo Juego

El Modo Juego modifica temporalmente las opciones de seguridad para minimizar su impacto sobre el rendimiento del sistema. Cuando activa el Modo Juego, se aplica la siguiente configuración:

- Todas las alertas y ventanas emergentes de Acronis Internet Security Suite 2010 están desactivadas.
- El nivel de protección en tiempo real de Acronis Internet Security Suite 2010 queda fijado a **Permisivo**.
- El cortafuego de Acronis Internet Security Suite 2010 está establecido en **Permitir todo**. Esto significa que todas las conexiones nuevas (tanto entrantes como salientes) se aceptarán de forma automática, independientemente del puerto y protocolo que utilicen.
- Por defecto, no se realizarán actualizaciones.

  Nota
  Para modificar esta opción, diríjase al apartado Actualización > Configuración y desmarque la casilla **No actualizar si el Modo Juego está activado**.

- Las tareas de análisis programadas se desactivarán de forma predeterminada.

Por defecto, Acronis Internet Security Suite 2010 automáticamente entra en Modo Juego cuando inicia un juego desde la lista de juegos conocidos o cuando una aplicación va a pantalla completa. Puede activar manualmente el Modo Juego usando la combinación de teclas predeterminada, `Ctrl+Alt+Shift+G`. Es sumamente recomendable desactivar el Modo Juego cuando acabe de jugar (puede utilizar la misma combinación de teclas, `Ctrl+Alt+Shift+G`).

Nota
Mientras en Modo Juego, puede ver la letra G sobre el icono Acronis.

Para configurar el Modo Juego, diríjase a **Modo Juego/Portátil>Modo Juego** en Modo Avanzado.

Modo Juego

En la parte superior de este apartado puede ver el estado del Modo Juego: Puede hacer clic en **Activar Modo Juego** o **Salir del Modo Juego** para cambiar el estado.

24.1.1. Configurando el Modo Juego Automático

El Modo Juego Automático permite que Acronis Internet Security Suite 2010 active automáticamente el Modo Juego cuando se detecte un juego. Puede configurar las siguientes opciones:

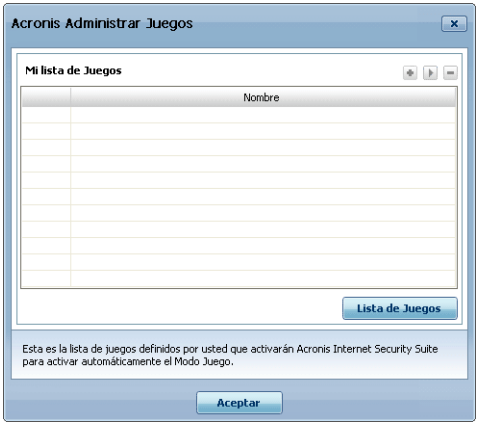
- **Use la lista predeterminada de juegos proporcionada por Acronis Internet Security Suite** - para entrar automáticamente en Modo Juego cuando inicie un juego de la lista de juegos conocidos de Acronis Internet Security Suite 2010. Para ver esta lista, haga clic en **Administrar Juegos** y a continuación **en Lista de Juegos** .
- **Activar modo juego al entrar en modo pantalla completa** - para activar automáticamente el Modo Juego cuando inicie una aplicación en modo pantalla completa.
- **¿Añadir la aplicación a la lista de juego?** - para preguntar si desea añadir la nueva aplicación a la lista de juegos cuando salga del modo pantalla completa.

Al añadir una nueva aplicación a la lista de juegos, Acronis Internet Security Suite 2010 activará automáticamente el Modo Juego la próxima vez que la inicie.

Nota
Si no desea que Acronis Internet Security Suite 2010 active automáticamente el Modo Juego, desmarque la casilla **Modo Juego Automático**.

24.1.2. Administrando la Lista de Juegos

Acronis Internet Security Suite 2010 activará automáticamente el Modo Juego cuando inicie una aplicación de la lista de juegos. Para ver y gestionar la lista de juegos, haga clic en **Administrar Juegos**. Aparecerá una nueva ventana.



Lista de Juegos

Se añadirán automáticamente nuevas aplicaciones a la lista cuando:

- Ha iniciado un juego de la lista de juegos conocidos de Acronis Internet Security Suite 2010. Para ver esta lista, haga clic en **Juegos Permitidos**.
- Cuando salga del modo pantalla completa, añada la aplicación a la lista de juegos desde la ventana de aviso.

Si desea desactivar el Modo Juego Automático para una aplicación concreta de la lista, desmarque su casilla correspondiente. Debe desactivar el Modo Juego Automático para aquellas aplicaciones de uso habitual que utilizan el modo pantalla completa, como navegadores web o reproductores de vídeos y películas.

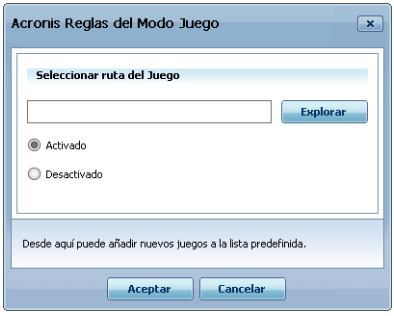
Para administrar la lista de juegos, puede utilizar los botones situados en la parte superior de la tabla:

- **Añadir** para añadir una nueva aplicación a la lista de juegos.

- **Eliminar** - para eliminar una aplicación de la lista de juegos.
- **Editar** - editar una entrada existente en la lista de juegos.

Añadiendo o Editando Juegos

Cuando añada o edite una entrada de la lista de juegos, aparecerá la siguiente ventana:



Añadir Juego

Haga clic en **Explorar** para seleccionar la aplicación deseada, o introduzca la ruta de la aplicación en el campo de texto editable.

Si no desea activar automáticamente el Modo Juego al iniciar la aplicación seleccionada, seleccione **Desactivar**.

Haga clic en **Aceptar** para añadir la entrada a la lista de juegos.

24.1.3. Modificando la Configuración del Modo Juego

Para modificar el comportamiento de las tareas programadas, utilice las siguientes opciones:

- **Activar este módulo para modificar las tareas planificadas de análisis de Antivirus** - Prevenir que se ejecuten las tareas planificadas de análisis mientras esta en Modo Juego. Puede seleccionar una de de las siguientes opciones:

Opción	Descripción
Omitir Tarea	Para no iniciar la tarea programada.
Posponer Tarea	Para iniciar la tarea programada inmediatamente después de desactivar el Modo Juego.

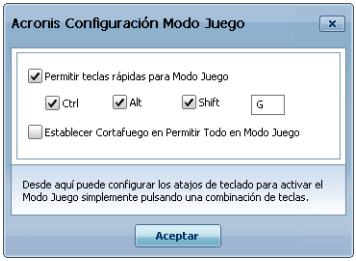
Para desactivar automáticamente el cortafuego de Acronis Internet Security Suite 2010 mientras está en Modo Juego, siga estos pasos:

1. Haga clic en **Opciones Avanzadas**. Aparecerá una nueva ventana.
2. Seleccionar el **Establecer Cortafuego en permitir todo (Modo Juego) cuando marque el Modo Juego**.
3. Haga clic en **Aceptar** para guardar los cambios.

24.1.4. Cambiando el Atajo de Teclado del Modo Juego

Puede activar manualmente el Modo Juego usando la combinación de teclas predeterminada, `Ctrl+Alt+Shift+G`. Si desea cambiar el atajo de teclado, siga estos pasos:

1. Haga clic en **Opciones Avanzadas**. Aparecerá una nueva ventana.



Opciones Avanzadas

2. Debajo de la opción **Usar Atajos de Teclado**, configure la combinación de teclas deseada:
   - Elija las teclas que desea utilizar seleccionado alguna de las siguientes: Control (`Ctrl`), Shift (`Shift`) o Alternate (`Alt`).
   - En el campo editable, escriba la tecla que desea utilizar en combinación con la tecla indicada en el paso anterior.

   Por ejemplo, si desea utilizar la combinación de teclas `Ctrl+Alt+D`, marque sólo `Ctrl` y `Alt`, y a continuación escriba la tecla `D`.

   Nota
   Si desmarca la casilla correspondiente a **Usar Atajos de Teclado**, desactivará las combinaciones de teclas.

3. Haga clic en **Aceptar** para guardar los cambios.

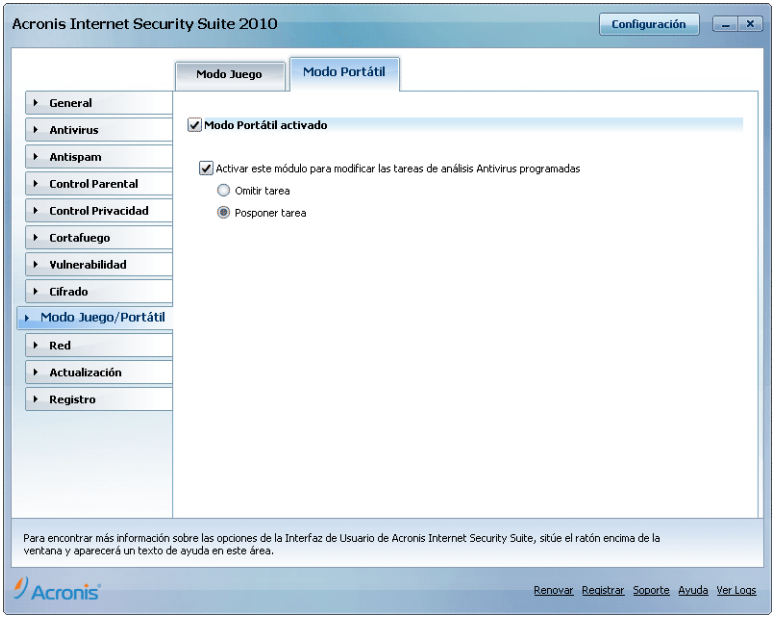
24.2. Modo Portátil

El Modo Portátil está especialmente para usuarios de portátiles. Su objetivo es minimizar el impacto de Acronis Internet Security Suite 2010 en el consumo de energía cuando estos dispositivos funcionan con batería.

Cuando el Modo Portátil esté activado, por defecto, las tareas programadas no se realizarán.

Acronis Internet Security Suite 2010 detecta cuando su portátil hace uso de la batería y activa automáticamente el Modo Portátil. Asimismo, Acronis Internet Security Suite 2010 desactivará automáticamente el Modo Portátil cuando detecte que el portátil ha dejado de funcionar con batería.

Para configurar el Modo Portátil, diríjase a **Modo Juego/Portátil>Modo Portátil** en Modo Avanzado.



Modo Portátil

Podrá ver si el Modo Portátil está activado o no. Si el Modo Portátil está activado, Acronis Internet Security Suite 2010 aplicará la configuración definida mientras el equipo funcione con batería.

24.2.1. Configurando las Opciones del Modo Portátil

Para modificar el comportamiento de las tareas programadas, utilice las siguientes opciones:

- **Activar este módulo para modificar las tareas planificadas de análisis de Antivirus** - Prevenir que se ejecuten las tareas planificadas de análisis mientras esta en Modo Portátil. Puede seleccionar una de de las siguientes opciones:

Opción	Descripción
Omitir Tarea	Para no iniciar la tarea programada.
Posponer Tarea	Para iniciar la tarea programada inmediatamente después de desactivar el Modo Portátil.

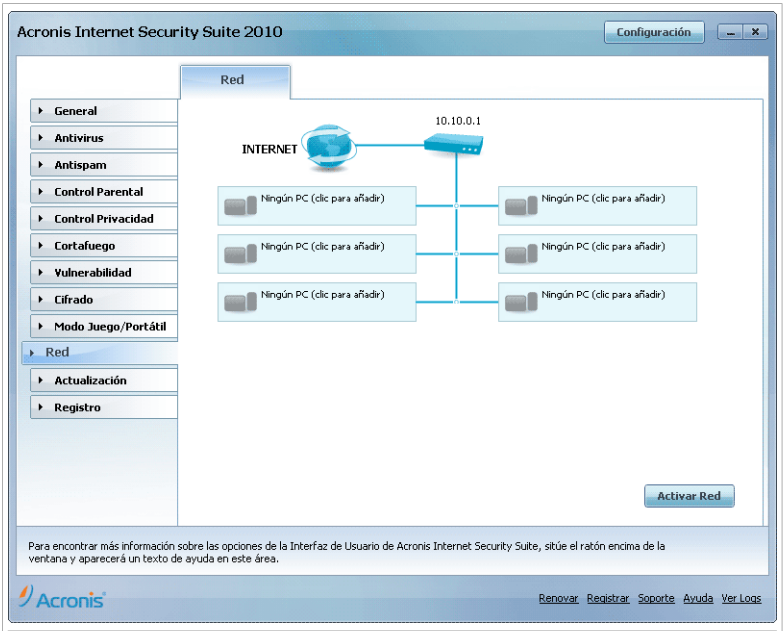
25. Red

El módulo Red le permite administrar los productos Acronis instalados en los equipos de una pequeña red desde un único equipo.

Importante

Usted solamente puede gestionar los siguientes productos de seguridad Acronis:

- Acronis AntiVirus 2010
- Acronis Internet Security Suite 2010
- Acronis Backup and Security 2010



Mapa de la Red

Para poder administrar los productos Acronis de los otros equipos de la pequeña red, debe seguir estos pasos:

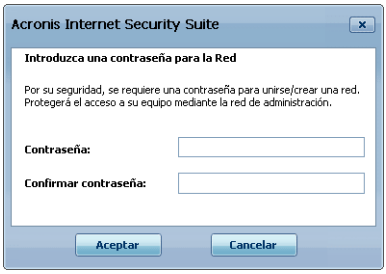
1. Únase a la red de administración de Acronis desde su equipo. Unirse a una red consiste en establecer una contraseña de administración para gestionar la red de administración.
2. Diríjase a cada unos de los equipos que desee administrar remotamente y únalos a la red (defina una contraseña).

3. Vuelva a su equipo y añada los equipos que desee administrar.

25.1. Uniéndose a la red de Acronis

Para unirse a la red de administración de Acronis, siga estos pasos:

1. Haga clic en **Activar Red**. Se le solicitará configurar la contraseña de administración de red.



Configurar Contraseña

2. Introduzca la misma contraseña en cada uno de los campos de texto.
3. Haga clic en **Aceptar**.

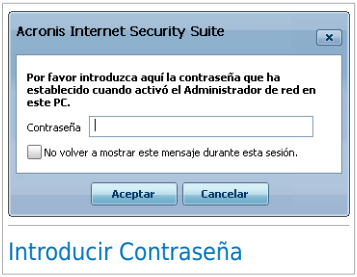
Podrá ver como el nombre del equipo aparece en el mapa de la red.

25.2. Añadiendo Equipos a la Red de Acronis

Antes de que usted pueda añadir un equipo a la red de Acronis, usted debe configurar la contraseña de gestión doméstica de Acronis en el equipo correspondiente.

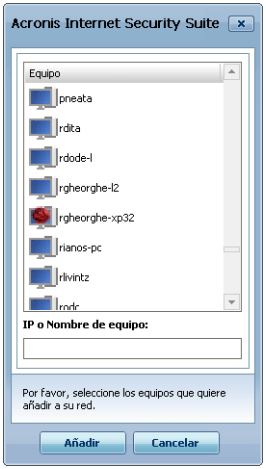
Para añadir un equipo a la red de administración de Acronis, siga estos pasos:

1. Haga clic en **Agregar Equipo**. Se le solicitará introducir la contraseña de administración de red local.



Introducir Contraseña

2. Introduzca la contraseña de administración de red y haga clic en el botón **Aceptar**. Aparecerá una nueva ventana.



Añadir Equipo

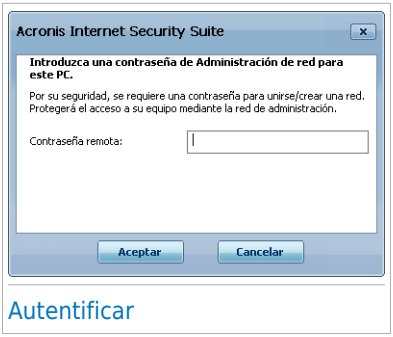
Podrá ver la lista de los equipos de la red. A continuación se explica el significado de los iconos:

Indica un equipo conectado con ningún producto gestionable Acronis instalado.

Indica un equipo conectado con productos gestionables Acronis instalados.

Indica un equipo no conectado con un producto gestionable Acronis instalado.

3. Realice una de estas acciones:
   - Seleccione un equipo de la lista para añadirlo.
   - Introduzca la dirección IP o el nombre del equipo a añadir en el campo editable correspondiente.
4. Haga clic en **Añadir**. Se le solicitará la contraseña de administración de red del equipo correspondiente.



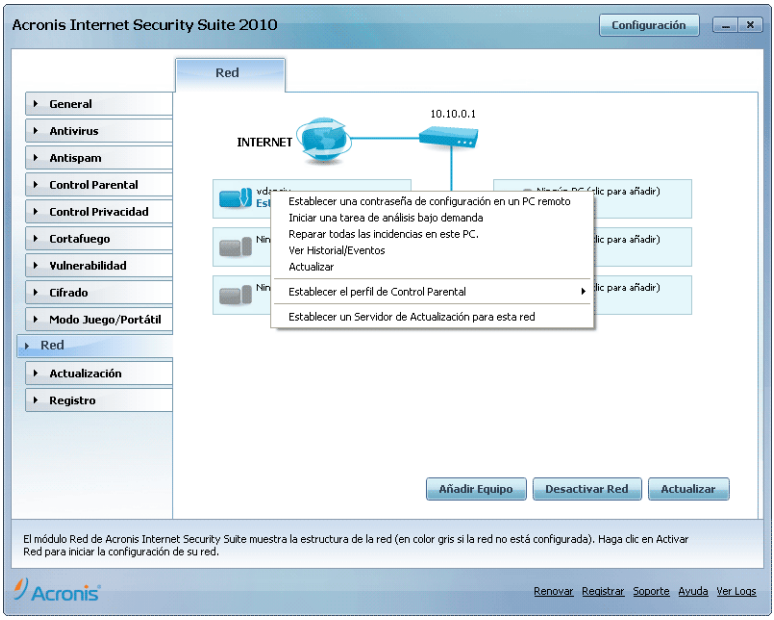
Autentificar

5. Introduzca la contraseña de administración de red configurada en el equipo correspondiente.
6. Haga clic en **Aceptar**. Si ha introducido la contraseña correcta, el nombre del equipo seleccionado aparecerá en el mapa de la red.

Nota
Puede añadir hasta cinco equipos en el mapa de la red.

25.3. Gestionando la red de Acronis

Una vez haya creado con éxito una red doméstica de Acronis, usted puede gestionar todos los productos Acronis desde un único equipo.



Mapa de la Red

Si situa el cursor del ratón encima de un equipo del mapa de red, podrá ver información sobre el (nombre, dirección IP, número de incidencias que afectan a la seguridad del sistema).

Si hace clic en el nombre del equipo del mapa de red, puede ver todas las tareas administrativas que pueden ejecutarse en un equipo remoto.

- **Quitar Pc de la red**

  Permite eliminar un PC de la red.

- **Establecer contraseña de configuración en un PC remoto**

  Permite crear una contraseña para restringir el acceso a la configuración de Acronis en este PC.

- **Ejecutar una tarea de Análisis bajo demanda**

  Permite ejecutar un análisis bajo demanda en un equipo remoto. Puede realizar cualquiera de las siguiente tareas de análisis: Analizar Mis Documentos, Análisis de sistema o Análisis en Profundidad.

- **Reparar todas las incidencias en este PC**

Le permite reparar todas las incidencias que están afectando a la seguridad de este equipo siguiendo el asistente Reparar Todas.

- **Historial**

  Le permite acceder al módulo **Historial&Eventos** en el producto instalado de Acronis en este equipo.

- **Actualizar ahora**

  Inicia el proceso de actualización para el producto Acronis instalado en este equipo.

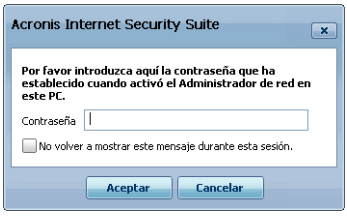
- **Establecer Perfil de Control Parental**

  Le permite establecer la categoría de edad que será utilizada por el filtro web del Control Parental en este equipo: niños, adolescentes o adultos.

- **Establecer un Servidor de Actualizaciones para esta Red**

  Permite establecer este equipo como servidor de actualización para todos los productos Acronis instalados en los equipos de esta red. Utilice esta opción para reducir el tráfico de Internet, porque sólo se conectará un equipo de esta red a Internet para descargar las actualizaciones.

Antes de ejecutar una tarea en un equipo determinado, se le solicitará la contraseña de administración de red local.



Introducir Contraseña

Introduzca la contraseña de administración de red y haga clic en el botón **Aceptar**.

Nota

Si tiene previsto ejecutar varias tareas, puede interesarle la opción **No volver a mostrar este mensaje durante esta sesión**. Al seleccionar esta opción, no se le volverá a solicitar esta contraseña durante la actual sesión.

26. Actualizar

Cada día se encuentran nuevas amenazas de malware. Por esta razón es muy importante mantener Acronis Internet Security Suite 2010 actualizado con las últimas firmas de malware.

Si está conectado a Internet a través de una conexión de banda ancha o ADSL, Acronis Internet Security Suite 2010 se actualizará sólo. Por defecto, comprueba si existen nuevas actualizaciones al encender su equipo y a cada **hora** a partir de ese momento.

Al detectar una actualización, se le puede solicitar su confirmación para realizar la actualización o puede realizarse de forma automática, según lo que haya definido en la Configuración de la actualización automática.

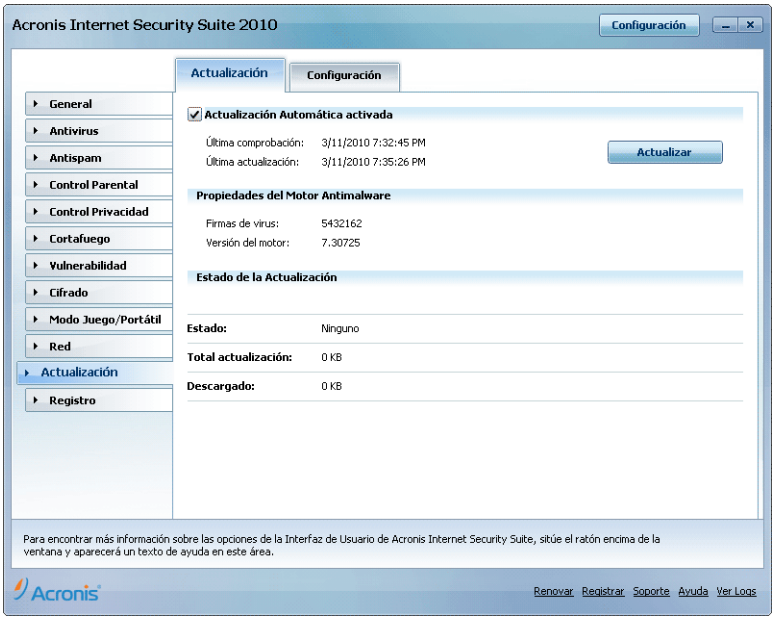
El proceso de actualización se realiza al instante, actualizando o reemplazando los archivos antiguos progresivamente. De este modo, el proceso de actualización no afecta al rendimiento del producto, a la vez que se evita cualquier riesgo.

El proceso de actualización se aplica para tres elementos:

- **Actualización de los motores antivirus** - a medida que se detecten nuevas amenazas, los ficheros incluyendo las firmas de virus deberán actualizarse para asegurar una protección permanente contra los virus. Este tipo de actualización está conocido como **Actualización de las firmas de virus**.
- **Actualizaciones de los motores antispam** - nuevas reglas serán añadidas a los filtros heurístico y URL, lo cual aumentará la eficiencia de su motor Antispam. Este tipo de actualización está conocido como **Actualización de Antispam**.
- **Actualizaciones para los motores antispyware** - nuevas firmas de spyware serán añadidas a la base de datos. Esta actualización también es conocida como **Actualización Antispyware**.
- **Actualizaciones del producto** - al estrenar una nueva versión de producto, nuevas funcionalidades y técnicas de análisis serán introducidas para mejorar los rendimientos del producto. Este tipo de actualización está conocido como **Actualización del producto**.

26.1. Actualizaciones automáticas

Para ver la información relacionada con las actualizaciones y realizar actualizaciones automáticas, diríjase a **Actualizar>Actualizar** en Modo Avanzado.



Actualizaciones automáticas

Desde aquí podrá ver cuando se ha realizado la última comprobación y la última actualización (si se ha realizado con éxito o con errores). Además, también verá información sobre la versión de los motores y el número de firmas de virus.

Si abre este apartado durante una actualización podrá ver el estado de la descarga.

Importante
Para estar protegido contra las últimas amenazas mantenga la **Actualización automática** activada.

26.1.1. Solicitando una Actualización

Puede realizar una actualización automática en cualquier momento haciendo clic en **Actualizar**. Este tipo de actualización también se conoce como **Actualización por petición del usuario**.

El módulo **Actualizar** se conectará al servidor de actualizaciones de Acronis y comprobará si hay alguna actualización disponible. Si se detecta una actualización, según las opciones elegidas en el apartado de Configuración de la Actualización Manual se le pedirá que confirme la actualización o bien ésta se realizará automáticamente.

Importante

Podría ser necesario reiniciar el equipo cuando haya completado la actualización. Recomendamos hacerlo lo más pronto possible.

Nota

Si está conectado a Internet a través de una conexión por módem analógico, es recomendable actualizar Acronis Internet Security Suite 2010 manualmente.

26.1.2. Desactivando la Actualización Automática

Si decide desactivar la actualización automática, aparecerá una ventana de advertencia. Para confirmar su elección, deberá seleccionar durante cuanto tiempo desea desactivar la actualización. Puede desactivar la actualización durante 5, 15 o 30 minutos, durante una hora, de forma permanente, o hasta que reinicie el sistema.

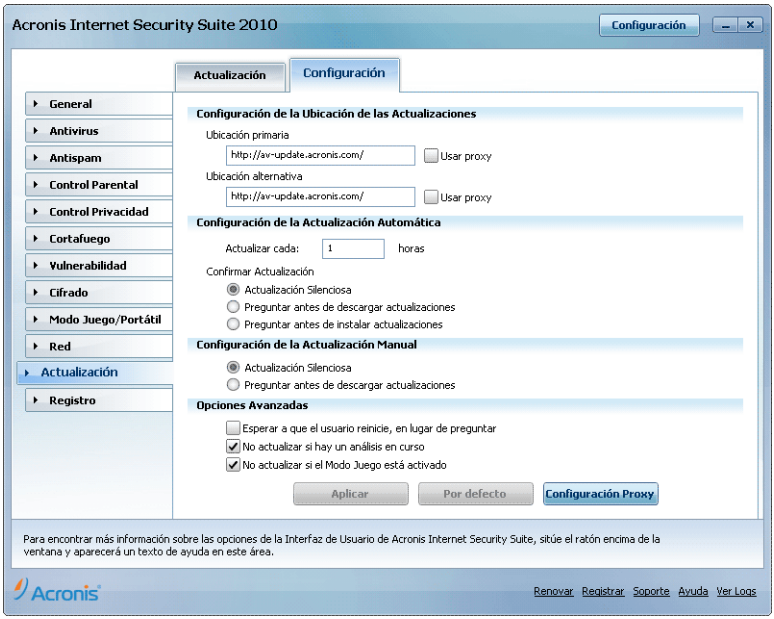
Aviso

Esta es una incidencia de seguridad crítica. Recomendamos desactivar la actualización automática el menor tiempo posible. Si Acronis Internet Security Suite 2010 no se actualiza regularmente, no estará protegido de las últimas amenazas.

26.2. Configuración de la Actualización

Las actualizaciones se pueden realizar desde la red local, por Internet, directamente o mediante un servidor proxy. Por defecto, Acronis Internet Security Suite 2010 comprobará si existen actualizaciones cada hora, a través de Internet, e instalará las actualizaciones disponibles sin alertarle.

Para modificar la configuración de actualización y el proxy, diríjase a **Actualizar>Configuración** en Modo Avanzado.



Configuración de la Actualización

Las opciones de actualización están agrupadas en 4 categorías (**Configuración de la Ubicación de las Actualizaciones**, **Configuración de la Actualización Automática**, **Configuración de la Actualización Manual** y **Opciones Avanzadas**). Cada categoría se describirá por separado.

26.2.1. Configuración de la Ubicaciones de las Actualizaciones

Para modificar las ubicaciones de descarga de las actualizaciones, utilice las opciones de la categoría **Configuración de la Ubicación de las Actualizaciones**.

Importante
Modifique estas opciones sólo si está conectado a una red local que almacene las firmas de malware de Acronis localmente, o si se conecta a Internet a través de un servidor proxy.

Para modificar una de las ubicaciones de descarga, indique la URL del servidor espejo en el campo **URL** correspondiente a la ubicación que desea cambiar.

Nota

Recomendamos poner el servidor espejo local en la ubicación primaria y no cambiar la ubicación alternativa. Así, en caso que falle el servidor local, siempre tendrá disponible el servidor de la ubicación alternativa.

Si su empresa utiliza un servidor proxy para conectarse a Internet, marque la casilla **Usar proxy** y haga clic en **Opciones Proxy** para modificar la configuración. Para más información, por favor, consulte el apartado "*Administrando los Proxies*" (p. 261).

26.2.2. Configurando la Actualización Automática

Para configurar el proceso de actualización automática de Acronis Internet Security Suite 2010, utilice las opciones en la categoría **Configuración de Actualización Automática**.

Puede indicar el número de horas entre dos actualizaciones consecutivas en el campo **Intervalo de tiempo**. Por defecto, el tiempo de intervalo es de 1 hora.

Para indicar cómo debe realizarse las actualizaciones automáticas, seleccione una de las siguientes opciones:

- **Actualización silenciosa** - Acronis Internet Security Suite 2010 descarga e instala las actualizaciones automáticamente.
- **Preguntar antes de descargar actualizaciones** - cada vez que exista una actualización disponible, se le preguntará si desea descargarla.
- **Preguntar antes de instalar actualizaciones** - cada vez que se haya descargado una actualización, se le pedirá permiso para instalarla.

26.2.3. Configurando la Actualización Manual

Para indicar cómo debe realizarse la actualización manual (actualización por petición del usuario), seleccione una de las siguientes opciones en la categoría **Configuración de la Actualización Manual**:

- **Actualización silenciosa** - la actualización manual se realizará automáticamente en segundo plano, sin la intervención del usuario.
- **Preguntar antes de descargar actualizaciones** - cada vez que exista una actualización disponible, se le preguntará si desea descargarla.

26.2.4. Modificando las Opciones Avanzadas

Para impedir que el proceso de actualización de Acronis interfiera en su trabajo, modifique las opciones en la categoría **Opciones Avanzadas**:

- **Esperar a que el usuario reinicie, en lugar de preguntar** - Si una actualización requiere el reinicio del equipo, el producto funcionará con los archivos antiguos hasta que reinicie el sistema. No se le pedirá al usuario que reinicie, de

manera que el proceso de actualización de Acronis Internet Security Suite 2010 no interferirá con el trabajo de los usuarios.

- **No actualizar si el análisis está en progreso** - Acronis Internet Security Suite 2010 no se actualizará si un procesos de análisis está en progreso. De esta manera, el proceso de actualización de Acronis Internet Security Suite 2010 no interferirá con las tareas de análisis.

Nota

Si actualiza Acronis Internet Security Suite 2010 mientras se está realizando un análisis, el análisis se abortará.

- **No actualizar si el Modo Juego está activado** - Acronis Internet Security Suite 2010 no se actualizará mientras el modo juego esté activado. De esta manera podrá minimizar el impacto del producto en el rendimiento del sistema mientras juega.

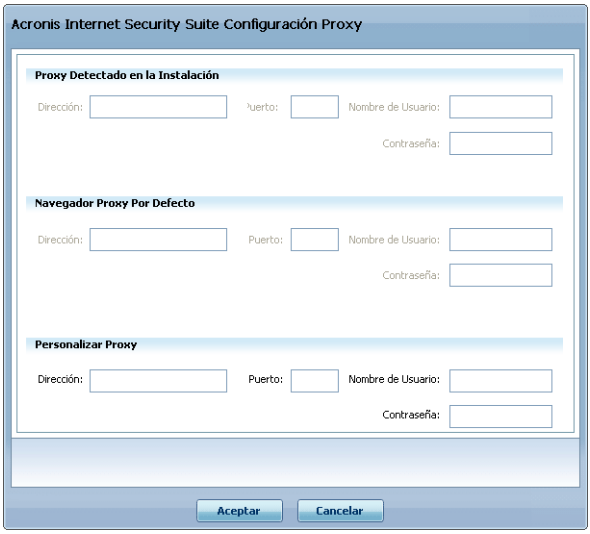
26.2.5. Administrando los Proxies

Si su empresa utiliza un servidor proxy para conectarse a Internet, deberá introducir la configuración del proxy para que Acronis Internet Security Suite 2010 pueda actualizarse. En caso contrario, se utilizará la configuración introducida por el administrador, o la configuración indicada en el navegador web.

Nota

La configuración del proxy sólo puede realizarse por los usuarios que tengan permisos de administrador o los usuarios que conozcan la contraseña de configuración del producto.

Para configurar el proxy, haga clic en **Configuración Proxy**. Aparecerá una nueva ventana.



Administrador de Proxy

Existen 3 tipos de configuración de proxy:

- **Detectado proxy durante la instalación)** - configuración de proxy detectada en la cuenta de administrador durante la instalación del producto, pero sólo podrá modificarse si ha iniciado sesión como Administrador. Si el servidor proxy necesita nombre de usuario y contraseña, deberá indicarlos en los campos correspondientes.
- **Proxy Predeterminado del Navegador** - los ajustes del proxy para el actual usuario, extraído del navegador actual. Si el servidor proxy requiere un nombre y un uausio, debe especificarlos en los campos correspondientes.

  Nota
  Los navegadores web soportados son Internet Explorer, Mozilla Firefox y Opera. Si utiliza otro navegador, Acronis Internet Security Suite 2010 no será capaz de reconocer la configuración de proxy del usuario en uso.

- **Sus propias opciones de proxy** - configuración del proxy que puede modificar si ha iniciado sesión como administrador.

  Deben indicarse las siguientes opciones:
  - ▶ **Dirección** - introduzca la IP del servidor proxy.
  - ▶ **Puerto** - introduzca el puerto que Acronis Internet Security Suite 2010 debe utilizar para conectarse con el servidor proxy.
  - ▶ **Nombre** - escriba un nombre de usuario que el proxy reconozca.

▶ **Contraseña** - escriba una contraseña válida para el usuario indicado anteriormente.

Al intentar conectarse a Internet, se prueba cada una de las configuraciones simultáneamente, hasta que Acronis Internet Security Suite 2010 consiga conectarse.

En primer lugar se prueba su propia configuración para conectarse a Internet. Si no funciona, se probará la configuración detectada durante la instalación. Finalmente, si tampoco funciona, se importará la configuración desde el navegador predeterminado para intentar conectarse.

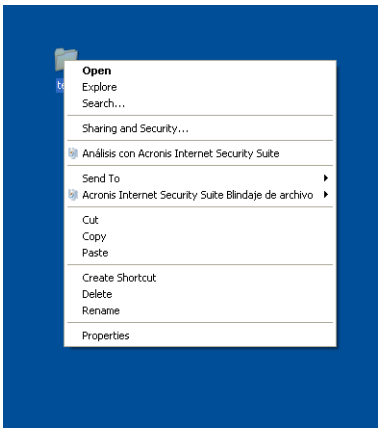
Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

Haga clic en **Aplicar** para guardar los cambios realizados, o en **Por defecto** para cargar la configuración inicial.

Integrado en Windows y software de terceros

27. Integración en el Menú Contextual de Windows

El menú contextual de Windows aparece siempre que hace clic derecha sobre un fichero o carpeta de su equipo o en objetos de su escritorio.



Menú Contextual de Windows

Acronis Internet Security Suite 2010 se integra dentro del menú contextual de Windows para ayudarle a analizar fácilmente los ficheros en busca de virus y evitar que otros usuarios accedan a sus ficheros privados. Puede localizar rápidamente las opciones de Acronis Internet Security Suite 2010 en el menú buscando el icono de Acronis.

- Analizar con Acronis Internet Security Suite
- Blindaje de Archivo Acronis Internet Security Suite

27.1. Analizar con Acronis Internet Security Suite

Puede analizar fácilmente ficheros, carpetas o incluso las particiones enteras del disco duro utilizando el menú contextual de Windows. Haga clic derecha sobre un objeto que desea analizar y seleccione **Analizar con Acronis Internet Security Suite** desde el menú. El Asistente de Análisis Antivirus aparecerá y le guiará a través del proceso de análisis.

Configurar las opciones del análisis. Las opciones de análisis están preconfiguradas para mejores resultados de detección. Si se detectan ficheros infectados, Acronis Internet Security Suite 2010 intentará desinfectarlos (eliminar el código malicioso). Si la desinfección falla, el Asistente de Análisis Antivirus le permitirá especificar otras acciones a realizar con los ficheros infectados.

Si desea modificar las opciones de análisis, siga estos pasos:

1. Abra Acronis Internet Security Suite 2010 y cambie la interfaz de usuario al Modo Avanzado.
2. Haga clic en **Antivirus** del menú de la izquierda.
3. Haga clic en la pestaña **Análisis**.
4. Haga clic derecha en la tarea **Análisis contextual** y seleccione **Abrir**. Aparecerá una ventana.
5. Haga clic en **Personalizado** y configure las opciones de análisis según sus necesidades. Para ver la descripción de una acción, mantenga el cursor encima y lea la descripción en la parte de abajo de la ventana.
6. Haga clic en **Aceptar** para guardar los cambios.
7. Haga clic en **Aceptar** para confirmar y aplicar las nuevas opciones de análisis.

Importante

No debería modificar las opciones de análisis de este método a no ser que tenga una buena razón para hacerlo.

27.2. Blindaje de Archivo Acronis Internet Security Suite

El Blindaje de Archivos de Acronis Internet Security Suite le ayuda a guardar con seguridad sus documentos confidenciales en su equipo a través del uso de blindajes de archivos.

- El Blindaje de Archivos es un área de almacenamiento protegida, situada dentro de su equipo, en la que puede guardar información personal o archivos confidenciales.
- El Blindaje de Archivos se basa en un archivo cifrado en su equipo, cuya extensión es bvd. Al estar cifrado, los datos que contiene este archivo no son vulnerables a robos o agujeros de seguridad.
- Cuando monte este archivo bvd, aparecerá una nueva partición lógica (una unidad nueva). Puede entender fácilmente este proceso si imagina que funciona de forma similar al montaje de una imagen ISO en una unidad de CD virtual.

  Abra Mi PC y verá una nueva unidad basada en el archivo de blindaje, desde la que podrá realizar operaciones con los archivos (copiar, eliminar, modificar, etc.). Los archivos estarán protegidos mientras residan en esta unidad (ya que para la operación de montaje es necesario introducir una contraseña).

  Al finalizar, bloquee (desmonte) su blindaje para empezar a proteger su contenido.

Puede identificar fácilmente el blindaje de archivo de Acronis Internet Security Suite 2010 en su equipo mediante el icono Acronis y la extensión .bvd.

Nota

Este apartado le enseña a crear y administrar blindajes de archivos de Acronis Internet Security Suite 2010 utilizando las opciones disponibles en el menú contextual de Windows. También puede crear y administrar blindajes de archivos desde la interfaz de Acronis Internet Security Suite 2010.

- En Modo Intermedio, diríjase a la pestaña Almacenamiento y utilice las opciones del área de **Tareas Rápidas**. Un asistente le ayudará a completar cada tarea.
- Para una opción más directa, cambie a la interfaz de usuario en Modo Avanzado y haga clic en **Cifrado** del menú de la izquierda. En la pestaña Cifrado, puede ver y administrar los blindajes de archivos existentes y su contenido.

27.2.1. Crear Blindaje

Tenga en cuenta que un blindaje es sólo un fichero con la extensión `.bvd`. Sólo cuando abre el blindaje, un disco virtual aparece en Mi PC y puede guardar con seguridad ficheros dentro de él. Al crear un blindaje, debe especificar dónde y con qué nombre lo quiere guardar en su equipo. También debe especificar una contraseña para proteger su contenido. Sólo los usuarios que conocen la contraseña pueden abrir el blindaje y tener acceso a los documentos y datos guardados dentro de él.

Para crear un blindaje siga estos pasos:

1. Haga clic derecho en el Escritorio o en una carpeta de su equipo, sitúe el cursor encima de la opción **Acronis Internet Security Suite Blindaje de Archivo** y seleccionar **Crear Blindaje de Archivo**. Aparecerá la siguiente pantalla:

Crear Blindaje de Archivos

2. Indique la ubicación y el nombre del archivo de blindaje.
   - Haga clic en **Explorar**, seleccione la ubicación del blindaje y guarde el archivo de blindaje con el nombre deseado.

- Escriba sólo el nombre del blindaje en el campo correspondiente para crearlo en Mis Documentos. Para abrir Mis Documentos, haga clic en start el menú Inicio de Windows y después en **Mis Documentos**.
- Introduzca la ruta completa del archivo de blindaje en el disco. Por ejemplo, `C:\my_vault.bvd`.

3. Seleccione la letra de la unidad en el menú. Al abrir un blindaje, en Mi PC aparecerá un nuevo disco virtual con la letra de unidad seleccionada.
4. Introduzca la contraeña deseada para el Blindaje en los campos **Nueva Contraseña** y **Confirmar contraseña**. Cada vez que alguien que intente abrir el blindaje y acceder a sus archivos, deberá introducir la contraseña.
5. Seleccione la opción **Formatear unidad** para formatear la unidad virtual asignada al blindaje. Debe formatear la unidad antes de poder añadir archivos al blindaje.
6. Si desea modificar el tamaño predeterminado del blindaje (50 MB), introduzca el valor deseado en el campo **Tamaño del Blindaje**.
7. Haga clic en **Crear** si sólo desea crear el Blindaje en la ubicación deseada. Para crear un blindaje y mostrarlo como una unidad de disco virtual en Mi PC, haga clic en **Crear y Abrir**.

Acronis Internet Security Suite 2010 le informará inmediatamente sobre el resultado de la operación. En caso de que haya ocurrido un error, utilice el mensaje de error para solucionar la incidencia. Haga clic en **Aceptar** para cerrar la ventana.

Nota

Podría ser conveniente guardar todos los blindajes de archivos en la misma ubicación. De esta manera, puede localizarlos fácilmente.

27.2.2. Abrir Blindaje

Para poder acceder y trabajar con los archivos almacenados en el Blindaje, antes debería abrirlo. Al abrir un Blindaje, aparecerá una unidad de disco virtual en Mi PC. Esta unidad estará etiquetada con la letra de unidad asignada al Blindaje.

Para abrir un blindaje, siga estos pasos:

1. Localice en su equipo el fichero `.bvd` que representa el blindaje que desea abrir.
2. Haga clic derecho en el archivo, sitúe el cursor en **Acronis Internet Security Suite Blindaje de Archivo** y seleccione **Abrir**. Alternativas más rápidas serían hacer doble clic sobre el fichero, o clic derecha y seleccionar **Abrir**. Aparecerá la siguiente pantalla:

Abrir Blindaje de Archivos

3. Seleccione la letra de la unidad en el menú.
4. Introduzca la contraseña del blindaje en el campo **Contraseña**.
5. Haga clic en **Abrir**.

Acronis Internet Security Suite 2010 le informará inmediatamente sobre el resultado de la operación. En caso de que haya ocurrido un error, utilice el mensaje de error para solucionar la incidencia. Haga clic en **Aceptar** para cerrar la ventana.

27.2.3. Bloquear Blindaje

Cuando acabe de trabajar con el blindaje de archivos, debería bloquearlo para proteger sus datos. Al bloquear el blindaje, la unidad de disco virual desaparecerá de Mi PC. En consecuencia, el acceso a los datos guardados en el blindaje será completamente bloqueado.

Para bloquear un blindaje, siga estos pasos:

1. Abra Mi PC (haga clic en el start menú Inicio de Windows y después en **Mi PC**).
2. Identifique la unidad de disco virtual correspondiente al blindaje que desea cerrar. Busque la letra de la unidad que asignó al blindaje al abrirlo.
3. Haga clic derecha en la unidad de disco virtual correspondiente, sitúe el cursor encima de la opción **Blindaje de Archivos de Acronis Internet Security Suite** y haga clic en **Cerrar**.

También puede hacer clic derecho en el archivo `.bvd` que representa al blindaje, sitúese encima de **Acronis Internet Security Suite Blindaje de Archivo** y haga clic en **Cerrar**.

Acronis Internet Security Suite 2010 le informará inmediatamente sobre el resultado de la operación. En caso de que haya ocurrido un error, utilice el mensaje de error para solucionar la incidencia. Haga clic en **Aceptar** para cerrar la ventana.

Nota

Si hay varios blindaje abiertos, sería conveniente utilizar la interfaz de Modo Avanzado de Acronis Internet Security Suite 2010. Si va a **Cifrado**, pestaña Cifrado de Archivo, puede ver una tabla que proporciona la información de los blindajes existentes. Esta información indica si el blindaje esta abierto, y en caso de que así sea, la letra de unidad que fue asignada.

27.2.4. Añadir Archivo al Blindaje

Antes de añadir ficheros o carpetas a un blindaje, deberá abrir el blindaje. Una vez el blindaje esté abierto, puede guardar fácilmente ficheros o carpetas dentro de él utilizando el menú contextual. Haga clic derecho en el archivo o carpeta que desea copiar al blindaje, sitúe el cursor en **Acronis Internet Security Suite Blindaje de Archio** y haga clic en **Añadir al Blindaje de Archivo**.

- Si sólo hay un blindaje abierto, el fichero o carpeta será copiado directamente a ese blindaje.
- Si hay varios blindajes abiertos, se le pedirá elegir a qué blindaje copiar el elemento. Seleccione desde el menú la letra correspondiente al blindaje deseado y haga clic en **Aceptar** para copiar el elemento.

También puede utilizar la unidad de disco virtual correspondiente al blindaje. Siga estos pasos:

1. Abra Mi PC (haga clic en el start menú Inicio de Windows y después en **Mi PC**).
2. Entre en la unidad de disco virtual correspondiente al blindaje. Busque la letra de la unidad que asignó al blindaje al abrirlo.
3. Copie-pegue o arraste&suelte archivos o carpetas directamente a la unidad de disco virtual.

27.2.5. Quitar del blindaje de archivos

Para eliminar archivos o carpetas de un blindaje, el blindaje debe estar abierto. Para eliminar un archivo de un blindaje, siga estos pasos:

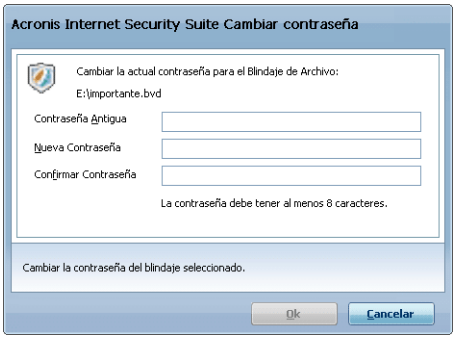
1. Abra Mi PC (haga clic en el start menú Inicio de Windows y después en **Mi PC**).
2. Entre en la unidad de disco virtual correspondiente al blindaje. Busque la letra de la unidad que asignó al blindaje al abrirlo.
3. Elimina archivos o carpetas como lo hace en Windows (por ejemplo, clic derecho en un archivo que quiere eliminar y seleccione **Eliminar**).

27.2.6. Cambiar Contraseña del Blindaje

La contraseña protege el contenido de un blindaje de accesos sin autorización. Sólo los usuarios que conocen la contraseña pueden abrir el blindaje y tener acceso a los documentos y datos guardados dentro de él.

El blindaje debe bloquearse antes de cambiar la contraseña. Para cambiar la descripción de una política, siga estos pasos:

1. Localice en su equipo el archivo `.bvd` correspondiente al blindaje.
2. Haga clic derecho en el archivo, sitúe el cursor en **Acronis Internet Security Suite Blindaje de Archivo** y seleccionar **Cambiar Contraseña del Blindaje**. Aparecerá la siguiente pantalla:



Cambiar Contraseña del Blindaje

3. Introduzca la contraseña actual para el blindaje en el campo **Contraseña Antigua**.
4. Introduzca la nueva contraseña para el blindaje en los campos **Nueva Contraseña** y **Confirmar Nueva Contraseña**.

> **Nota**
>
> La contraseña debe tener como mínimo 8 caracteres. Para conseguir una contraseña segura, utilice una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (como #, $ o @).

5. Haga clic en **Aceptar** para cambiar la contraseña.

Acronis Internet Security Suite 2010 le informará inmediatamente sobre el resultado de la operación. En caso de que haya ocurrido un error, utilice el mensaje de error para solucionar la incidencia. Haga clic en **Aceptar** para cerrar la ventana.

28. Integración con Navegadores Web

Acronis Internet Security Suite 2010 le protege contra los intentos de phishing mientras navega por Internet. Analiza las páginas web a las que accede y le alerta si detecta alguna amenaza de phishing. Puede configurar la Lista Blanca de páginas web que no serán analizadas por Acronis Internet Security Suite 2010.

Acronis Internet Security Suite 2010 se integra a través de una barra de herramientas muy intuitiva y fácil de usar en los siguientes navegadores:

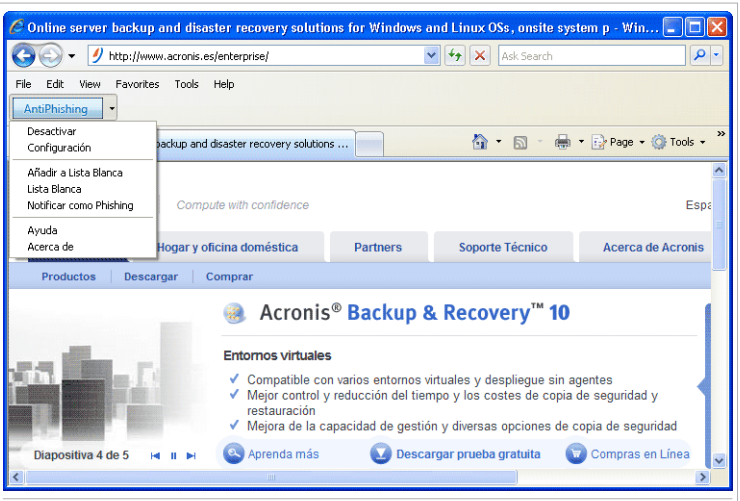
- Internet Explorer
- Mozilla Firefox

Puede administrar la protección antiphishing y la Lista Blanca fácilmente a través de la barra de herramientas de Acronis Antiphishing, integrada en los navegadores citados anteriormente.

La herramienta antiphishing está ubicada en la parte superior del navegador. Haga clic para abrir el menú de la barra de herramientas.

Nota

Si no puede ver la barra de herramientas, abra el menú **Ver**, diríjase a la opción **Barras de herramientas** y marque la opción **Acronis Toolbar**.



Barra de Herramientas Antiphishing

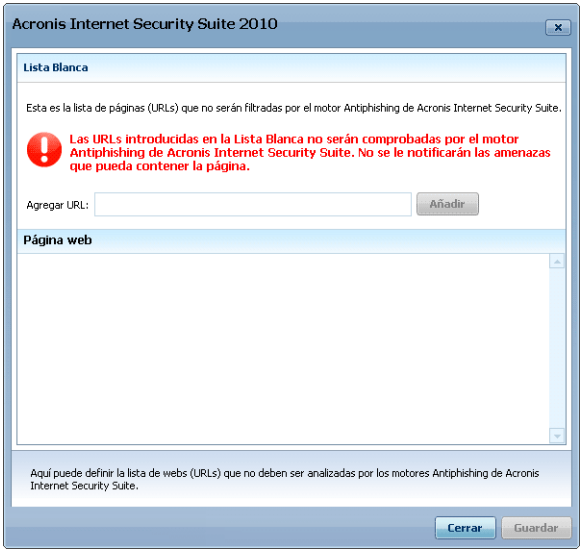
Dispone de los siguientes comandos en la barra de herramientas:

- **Activar/Desactivar** - activar/desactivar la protección Antiphishing de Acronis Internet Security Suite 2010 en el actual navegador web.
- **Opciones** - abre una ventana dónde puede modificar la configuración de la barra de herramientas. Tiene las siguientes opciones a su disposición:
  - ▶ **Protección Antiphishing Web en Tiempo Real** - detecta y le notifica en tiempo real si una web está comprometida (configurada para robar información personal). Esta opción controla la protección antiphishing de Acronis Internet Security Suite 2010 solamente en el navegador actual.
  - ▶ **Preguntar antes de añadir a la lista blanca** - se le preguntará si está seguro de añadir la página web en la Lista Blanca.
- **Añadir a la Lista Blanca** - añade la página web actual a la Lista Blanca.

Nota

Añadir una página web a la Lista Blanca significa que Acronis Internet Security Suite 2010 no analizará nunca más la página en busca de intentos de phishing. Recomendamos añadir a la Lista Blanca sólo las páginas en las que confíe plenamente.

- **Lista Blanca** - abre la Lista Blanca.



Lista Blanca Antiphishing

Puede ver la lista de todas las páginas web que no serán analizadas por los motores antiphishing de Acronis Internet Security Suite 2010. Si desea eliminar

una página web de la Lista Blanca, para detectar los posibles intentos de phishing existentes en la página, haga clic en el botón **Eliminar** situado justo al lado.

Puede añadir las páginas en las que confíe a la Lista Blanca, de modo que no sean analizadas por los motores antiphishing. Para añadir una página a la Lista Blanca, escriba la dirección en la casilla correspondiente y haga clic en **Añadir**.

- **Notificar como Phishing** - informa al Laboratorio de Acronis de que considera que esta página web puede ser utilizada para phishing. Notificando las páginas web sospechosas de phishing ayuda a proteger a otras personas frente al robo de identidad.
- **Ayuda** - abre la ventana de asistencia electrónica.
- **Acerca de** - abre la ventana dónde puede verse información sobre Acronis Internet Security Suite 2010 y dónde encontrar ayuda en caso necesario.

29. Integración con Programas de Mensajería Instantánea

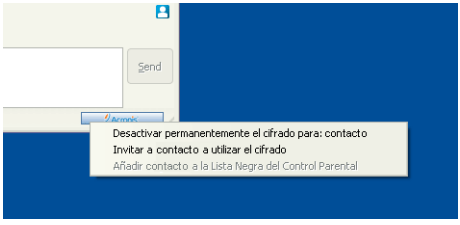
Acronis Internet Security Suite 2010 ofrece funciones de cifrado para proteger sus documentos confidenciales y las conversaciones de mensajería instantánea a través de Yahoo Messenger y MSN Messenger.

Por defecto, Acronis Internet Security Suite 2010 cifra todas sus sesiones de chat por mensajería instantánea siempre y cuando:

- Su pareja de chat tiene un producto Acronis instalado que soporta cifrado de IM y el cifrado IM está activado para la aplicación de mensajería instantánea utilizada para chatear.
- Su contacto de chat utilice Yahoo Messenger o Windows Live (MSN) Messenger.

Importante
Acronis Internet Security Suite 2010 no cifrará la conversación si su contacto utiliza una aplicación web para chatear, como Meebo, u otras aplicaciones que soportan Yahoo Messenger o MSN.

Puede configurar fácilmente el cifrado de la mensajería instantánea usando la barra de herramientas de Acronis en la ventana de chat. La barra de herramientas debería estar ubicada en la parte derecha arriba de la ventana de chat. Busque el logo de Acronis para encontrarla.



Barra de Herramientas Acronis

Nota
La barra de herramientas indica si una conversación está cifrada mostrando una pequeña clave al lado del logo de Acronis.

Haciendo clic en la barra de herramientas de Acronis se le mostrarán las siguientes opciones:

- **Desactivar permanentemente el cifrado para el contacto.**
- **Invitar contacto a usar cifrado.** Para cifrar sus conversaciones, su contacto debe instalar Acronis Internet Security Suite 2010 y utilizar un programa IM compatible.
- **Añadir contacto a la lista negra del Control Parental.** Si añade un contacto a la lista negra del Control Parental y el Control Parental está activado, no podrá ver los mensajes enviados por dicho contacto. Para eliminar un contacto de la lista negra, haga clic en la barra de herramientas y seleccione **Eliminar contacto de la lista negra del Control Parental**.

30. Integración en Clientes de Correo

Acronis Internet Security Suite 2010 incluye un módulo Antispam. El módulo Antispam verifica los correos que recibe e identifica cuales de ellos son spam. Los mensajes de spam detectados por Acronis Internet Security Suite 2010 se marcan con el prefijo [SPAM] en el asunto.

Nota

Protección Antispam disponible para todos los clientes de correo POP3/SMTP.

Acronis Internet Security Suite 2010 se integra directamente a través de una barra de herramientas intuitiva y fácil de utilizar dentro de los siguientes clientes de correo:

- Microsoft Outlook
- Outlook Express
- Windows Mail
- Mozilla Thunderbird

Acronis Internet Security Suite 2010 automáticamente mueve los mensajes spam a una carpeta específica de la siguiente manera:

- En Microsoft Outlook, los mensajes de spam se mueven a la carpeta **Spam**, ubicada en la carpeta **Elementos eliminados**. La carpeta **Spam** se ha creado durante la instalación de Acronis Internet Security Suite 2010.
- En Outlook Express y Windows Mail, los mensajes spam se mueven directamente a **Elementos eliminados**.
- En Mozilla Thunderbird, los mensajes spam se mueven a la carpeta **Spam**, ubicada en la carpeta **Papelera**. La carpeta **Spam** se ha creado durante la instalación de Acronis Internet Security Suite 2010.

Si usa otros clientes de correo, debe crear una regla para mover los mensajes de correo electrónico marcados como [SPAM] por Acronis Internet Security Suite 2010 a una carpeta de cuarentena personalizada.

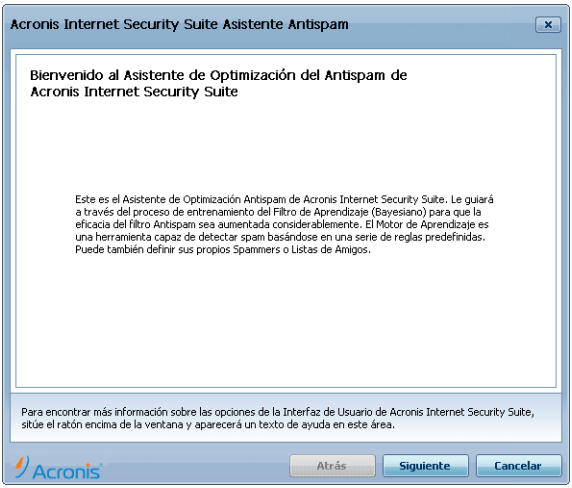
30.1. Asistente de Configuración Antispam

La primera vez que inicie su cliente de correo tras la instalación de Acronis Internet Security Suite 2010, aparecerá un asistente de bienvenida que le ayudará a configurar la Lista de Amigos y Lista de Spammers, así como entrenar el Filtro Bayesiano, que mejorarán la eficacia de los filtros Antispam.

Nota

Puede iniciar el asistente cuando quiera, haciendo clic en el botón **Asistente** de la Barra de Herramientas Antispam.

30.1.1. Paso 1/6 - Ventana de bienvenida



Ventana de Bienvenida

Haga clic en **Siguiente**.

30.1.2. Paso 2/6 - Completar la Lista de Amigos

Completar la Lista de Amigos

Aquí puede ver todas las direcciones de su **Libreta de Direcciones**. Por favor seleccione las que quiere agregar al **Listado de amigos** (le recomendamos seleccionarlas todas). Recibirá todos los mensajes de estas direcciones, independientemente de sus contenidos.

Para añadir sus contactos a la Lista de Amigos, compruebe **Seleccionar Todo**.

Si desea omitir este paso de la configuración, seleccione **Omitir este paso**. Haga clic en **Siguiente** para continuar.

30.1.3. Paso 3/6 - Borrar la base de datos del filtro Bayesiano

Eliminar la base de datos del filtro Bayesiano

Si nota que su filtro antispam está empezando a perder su eficiencia, esto se puede deber a una educación inadecuada (por ejemplo, usted ha marcado erróneamente un número de mensajes legítimos como Spam, o viceversa). Si su filtro es muy impreciso, talvez tenga que borrar toda la base de datos del filtro y reeducar el filtro siguiendo los pasos indicados por el programa asistente, tal como se describe a continuación.

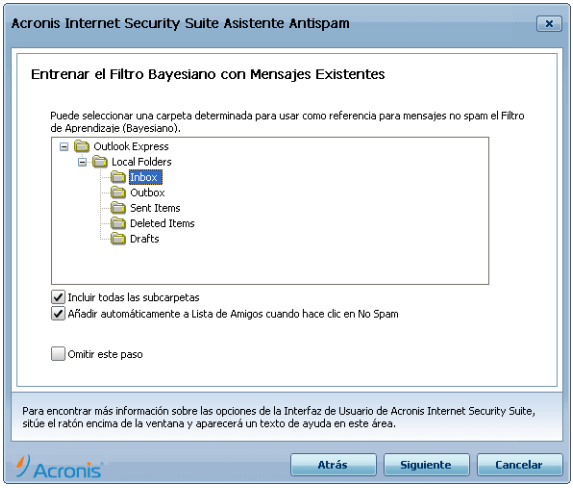
Seleccione la opción **Limpiar la base de datos del filtro Antispam** si desea reiniciar la base de datos del filtro Bayesiano.

Puede guardar la base de datos Bayesiano en un archivo el cual puede usarla con otro producto de AcroniS Internet Security Suite 2010 o después de reinstalar Acronis Internet Security Suite 2010. Para guardar la base de datos Bayesiana, haga clic en el botón **Guardar Bayes** y guardela en la ubicación deseada. El archivo tendrá una extensión `.dat`.

Para cargar una base datos Bayesiana previamente guardada, haga clic en el botón **Cargar Bayes** y abra el archivo correspondiente.

Si desea omitir este paso de la configuración, seleccione **Omitir este paso**. Haga clic en **Siguiente** para continuar.

30.1.4. Paso 4/6 - Entrenar el Motor de Aprendizaje con Mensajes Legítimos



Entrenar el Motor de Aprendizaje con Mensajes Legítimos

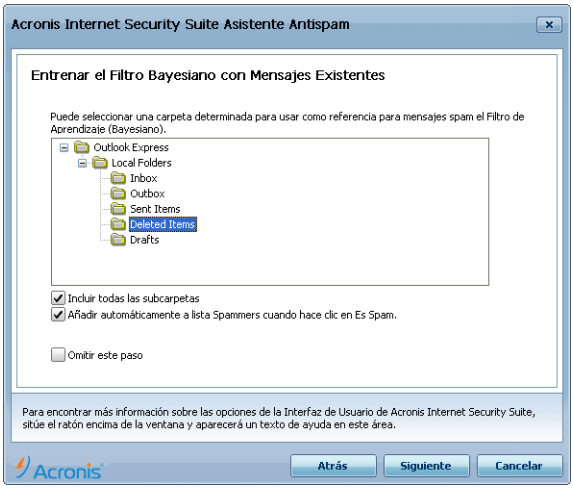
Por favor seleccione una carpeta que contiene mensajes legítimos. Estos mensajes serán utilizados para educar el filtro antispam.

Existen dos opciones debajo de la lista de carpetas:

- **Incluir todas las subcarpetas** - para incluir las subcarpetas en su selección.
- **Añadir automáticamente a la lista de Amigos** - para añadir los remitentes a la lista de Amigos.

Si desea omitir este paso de la configuración, seleccione **Omitir este paso**. Haga clic en **Siguiente** para continuar.

30.1.5. Paso 5/6 - Entrenar el Filtro Bayesiano con Spam



Entrenar el Filtro Bayesiano con Spam

Por favor seleccione una carpeta que contiene mensajes Spam. Estos mensajes serán empleados para educar el filtro Antispam.

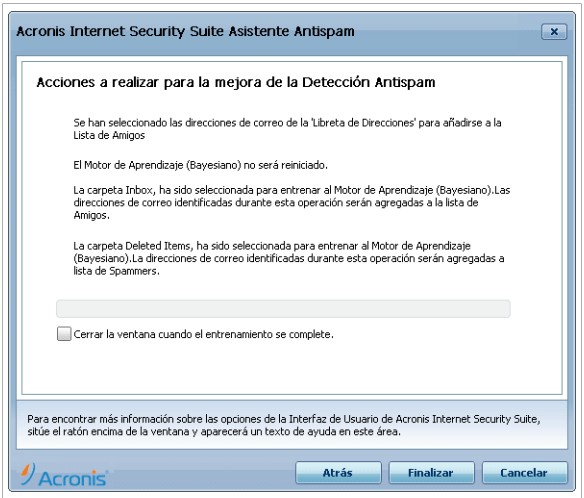
Importante
Por favor asegúrese que la carpeta seleccionada no contiene ningún mensaje legítimo, sino la eficiencia del filtro antispam será reducida considerablemente.

Existen dos opciones debajo de la lista de carpetas:

- **Incluir todas las subcarpetas** - para incluir las subcarpetas en su selección.
- **Añadir automáticamente a la lista de Spammers** - para añadir los remitentes a la lista de Spammers. Los mensajes de correos desde estos remitentes siempre serán marcados como SPAM y procesados en consecuencia.

Si desea omitir este paso de la configuración, seleccione **Omitir este paso**. Haga clic en **Siguiente** para continuar.

30.1.6. Paso 6/6 - Epílogo



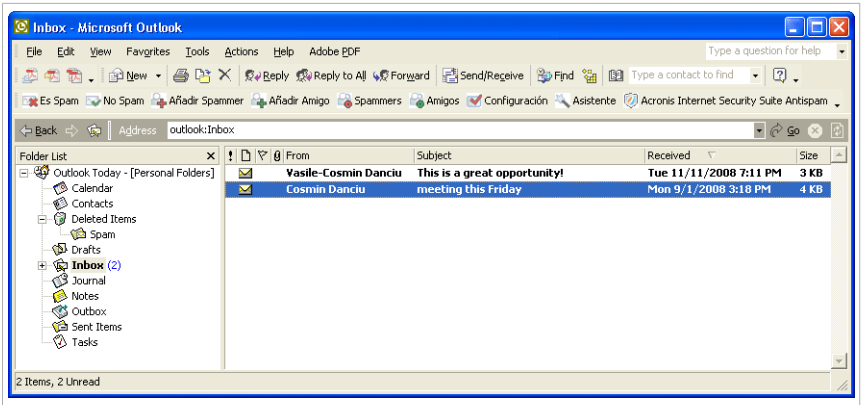
Sumario

En esta ventana se muestran todas las opciones para el programa asistente. Puede hacer cualquier modificación que considere oportuna, volviendo al paso anterior (haga clic en **Atrás**).

Si no quiere hacer ninguna modificación, haga click en **Finalizar** para cerrar el asistente.

30.2. La barra de herramientas Antispam

En el área superior de la ventana de su cliente de correo puede ver la barra Antispam. La barra Antispam le ayuda a administrar la protección antispam directamente desde su cliente de correo. Puede corregir fácilmente Acronis Internet Security Suite 2010 si este ha marcada un mensaje legítimo como SPAM.



La barra de herramientas Antispam

Cada botón de la barra de herramientas de Acronis Internet Security Suite 2010 se explica a continuación:

- **Es Spam** - envia un mensaje al módulo Bayesiano indicándole que dicho mensaje es spam. El mensaje seleccionado será trasladado a la carpeta **Spam**.

  Los próximos mensajes con las mismas características serán marcados como SPAM.

  Nota
  Puede seleccionar un solo mensaje o bien puede elegir todos los mensajes que quiera.

- **No es Spam** - envía un mensaje al módulo Bayesiano indicándole que este correo seleccionado no es spam y Acronis Internet Security Suite 2010 no debería marcarlo como tal. El correo será movido a la carpeta **Spam** de la **Bandeja de Entrada**.

  Los próximos mensajes con las mismas características ya no serán marcados como SPAM.

  Nota
  Puede seleccionar un solo mensaje o bien puede elegir todos los mensajes que quiera.

  Importante
  El botón **No Spam** se activa al seleccionar un mensaje marcado como spam por Acronis Internet Security Suite 2010 (normalmente, estos mensajes se almacenan en la carpeta **Spam**).

- **Añadir a Spammer** - añade el remitente del correo seleccionado a la lista de Spammers.

Añadir Spammer

Seleccione **No volver a mostrar este mensaje** si no quiere que se le solicite la confirmación al agregar una nueva dirección al listado de spammers.

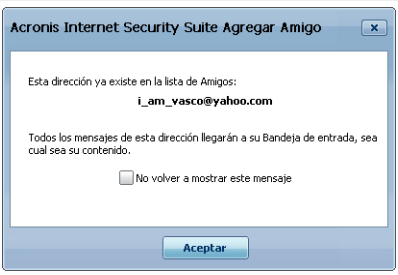
Haga clic en **Aceptar** para cerrar la ventana.

Los próximos mensajes provenientes de aquella dirección serán automáticamente trasladados a la carpeta SPAM.

Nota

Puede seleccionar un solo remitente o bien puede elegir todos los remitentes que quiera.

- **Añadir Amigo** - añade el remitente del correo seleccionado a la lista de Amigos.



Añadir Amigo

Seleccione **No volver a mostrar este mensaje** si no quiere que se le solicite la confirmación al agregar una nueva dirección al listado de amigos.

Haga clic en **Aceptar** para cerrar la ventana.

A partir de este momento, recibirá todos los mensajes provenientes de esta dirección, independientemente de su contenido.

Nota

Puede seleccionar un solo remitente o bien puede elegir todos los remitentes que quiera.

- **Spammers** - abre la **Lista de Spammers** que contiene todas las direcciones de correo electrónico de las cuales no quiere recibir mensajes, independientemente de su contenido.

  Nota
  Cualquier mensaje proveniente de una dirección incluida en su **listado de spammers** será automáticamente marcada como spam, sin procesamientos ulteriores.

Lista de Spammers

Aquí puede agregar o eliminar entradas en el **listado de spammers**.

Si desea añadir una dirección de correo, haga clic en el campo **Dirección**, introduzca la dirección y luego clic en el botón . La dirección aparecerá en la **Lista de Spammers**.

Importante
Sintaxis: nombre@dominio.com.

Si desea añadir un dominio, haga clic en el campo **Dominio**, introduzca el dominio y luego clic en el botón . El dominio aparecerá en la **Lista de Spammers**.

Importante
Sintaxis:

- @dominio.com, *dominio.com y dominio.com - todos los mensajes provenientes de dominio.com serán marcados como SPAM;
- *dominio* - todos los mensajes provenientes de dominio (independientemente de los sufijos del dominio) serán marcados como SPAM;
- *com - todos mensajes con tales sufijos de dominios com serán marcados como SPAM.

Aviso

No agregar dominio legítimos de correo basados en servicios web (como un Yahoo, Gmail, Hotmail u otros) a la lista de Spammers. De lo contrario, los mensajes recibidos de cualquier usuario registrados en estos servicios serán detectados como spam. Si, por ejemplo, añade `yahoo.com` a la lista de Spammers, todas las direcciones de correo que vengan de `yahoo.com` serán marcados como `[spam]`.

Para exportar las direcciones de e-mail de la **Libreta de Direcciones de Windows** / **Carpetas de Outlook Express** en **Microsoft Outlook** / **Outlook Express** / **Windows Mail**, seleccione la opción apropiada en el menú desplegable **Importar direcciones de correo desde**.

En **Microsoft Outlook Express / Windows Mail**, aparecerá una nueva ventana desde la que podrá indicar la carpeta que contiene las direcciones de correo que quiere añadir a la **lista de Spammers**. Selecciónela y haga clic en **Seleccionar**.

En ambos casos, la dirección de correo electrónico aparecerá en el listado de importación. Seleccione las direcciones que desee y haga clic en para añadirlasa la **Lista de Spammers**. Si hace clic en se añadirán todas las direcciones de correo al listado.

Para eliminar un elemento de la lista, selecciónelo y haga clic en el botón **Eliminar**. Para eliminar todas las entradas de la lista, haga clic en el botón **Vaciar Lista** y después en **Si** para confirmar.

Puede guardar la lista de Spammers en un archivo la cual puede utilizarla en otro equipo o después de reinstalar el producto. Para guardar la lista Spammers, haga clic en el botón **Guardar** y guárdela en la ubicación deseada. El archivo tendrá la extensión `.bwl`.

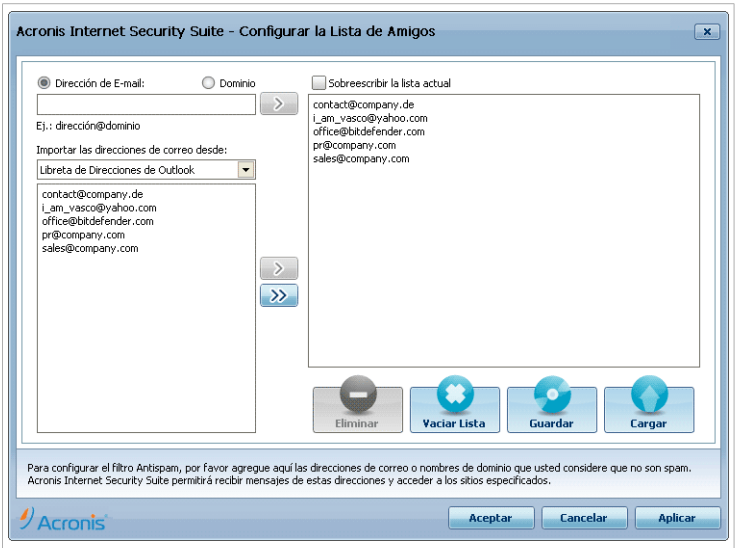
Para cargar una lista de Spammers previamente guardad, haga clic en el botón **Cargar** y abra el archivo correspondiente `.bwl`. Para resetear el contenido de la lista existente cuando carga una lista previamente guardad, seleccione **Sobrescribir la actual lista**.

Haga clic en **Aplicar** y **Aceptar** para guardar y cerrar el **listado de spammers**.

- **Amigos** - abre la **Lista de Amigos** que contiene todas las direcciones desde las que siempre quiere recibir mensajes, independientemente de su contenido.

Nota

Cualquier mensaje que provenga de una dirección incluida en la **Lista de Amigos** llegará directamente a su Bandeja de Entrada.



Lista de Amigos

Aquí puede agregar o eliminar entradas en el **listado de amigos**.

Si desea añadir una dirección de correo, haga clic en el campo **Dirección**, introduzca la dirección y luego haga clic en el botón. La dirección aparecerá en la **Lista de Amigos**.

Importante

Sintaxis: nombre@dominio.com.

Si desea añadir un dominio, haga clic en el campo **Dominio**, introduzca el dominio y luego clic en el botón. El dominio aparecerá en el **Lista de Amigos**.

Importante

Sintaxis:

- @dominio.com, *dominio.com y dominio.com - todos los mensajes provenientes de dominio.com llegarán a su **Bandeja de entrada** independientemente de su contenido;
- *dominio* - todos los mensajes provenientes de dominio (independientemente de los sufijos del dominio) llegarán a su **Bandeja de entrada** independientemente de su contenido;

▶ *com - todos mensajes con tales sufijos de dominios com llegarán a su **Bandeja de entrada** independientemente de sus contenidos;

Para exportar las direcciones de e-mail de la **Libreta de Direcciones de Windows** / **Carpetas de Outlook Express** en **Microsoft Outlook** / **Outlook Express** / **Windows Mail**, seleccione la opción apropiada en el menú desplegable **Importar direcciones de correo desde**.

En **Microsoft Outlook Express** / **Windows Mail** aparecerá una nueva ventana desde la que podrá indicar la carpeta que contiene las direcciones de correo que quiere añadir a la **Lista de Amigos**. Selecciónela y haga clic en **Seleccionar**.

En ambos casos, la dirección de correo electrónico aparecerá en el listado de importación. Seleccione las direcciones que desee y haga clic en to add them to the **Lista de Amigos**. Si hace clic en se añadirán todas las direcciones de correo al listado.

Para eliminar un elemento de la lista, selecciónelo y haga clic en el botón **Eliminar**. Para eliminar todas las entradas de la lista, haga clic en el botón **Vaciar Lista** y después en **Si** para confirmar.

Puede guardar la lista de Amigos a un archivo la cual puede utilizarse en otro equipo o después de reinstalar el producto. Para guardar la lista de Amigos, haga clic en el botón **Guardar** y guárdela en la ubicación deseada. El archivo tendrá la extensión `.bwl`.

Para cargar una lista de Amigos previamente guardada, haga clic en el botón **Cargar** y abra el correspondiente archivo `.bwl`. Para resetear el contenido de la lista existente cuando carga una lista previamente guardad, seleccione **Sobrescribir la actual lista**.

Nota

Le recomendamos agregar los nombres y las direcciones de correo de sus amigos al **Listado de Amigos**. Acronis Internet Security Suite 2010 no bloquea los mensajes provenientes de las personas incluidas en este listado; por consiguiente, al agregar a sus conocidos en el Listado de Amigos se asegura que los mensajes legítimos llegarán sin problemas a su Bandeja de entrada.

Haga clic en **Aplicar** y **Aceptar** para guardar y cerrar el **listado de amigos**.

- **Configuración** - abre la ventana **Configuración** en la que puede especificar algunas opciones del módulo **Antispam**.

Configuración

Tiene las siguientes opciones a su disposición:

- **Mover el mensaje a Elementos Eliminados** - para trasladar los mensajes Spam a la carpeta **Elementos Eliminados** (sólo para Microsoft Outlook Express / Windows Mail);
- **Marcar el mensaje como 'leído'** - para marcar todos los mensajes Spam como leídos, para que así los nuevos mensajes Spam no le molesten al llegar.

Si su filtro antispam es muy inexacto, es posible que necesite vaciar la base de datos y volver a entrenar al Filtro Bayesiano. Haga clic en **Limpiar la base de datos del Antispam** si quiere restaurar la base de datos del filtro Bayesiano.

Puede guardar la base de datos Bayesiano en un archivo el cual puede usarla con otro producto de AcroniS Internet Security Suite 2010 o después de reinstalar Acronis Internet Security Suite 2010. Para guardar la base de datos Bayesiana, haga clic en el botón **Guardar Bayes** y guardela en la ubicación deseada. El archivo tendrá una extensión `.dat`.

Para cargar una base datos Bayesiana previamente guardada, haga clic en el botón **Cargar Bayes** y abra el archivo correspondiente.

Haga clic en la pestaña **Alertas** si quiere acceder al apartado en el que puede desactivar las ventanas de confirmación de los botones **Añadir Spammer** y **Añadir Amigo**.

Nota

En la ventana **Alertas** puede activar/desactivar la aparición de la alerta **Por favor seleccione un mensaje de correo**. Esta alerta aparece cuando seleccione un grupo de mensajes en lugar de un mensaje de correo.

- **Asistente** - Abre el asistente de configuración de Antispam, el cual le ayudará a entrenar el filtro Bayesiano con el fin de seguir incrementando la eficiencia del filtro Antispam de Acronis Internet Security Suite 2010. Puede agregar direcciones desde la Libreta de Direcciones a la lista de Amigos/Spammers.
- **Acronis Internet Security Suite Antispam** - abra la interfaz de usuario de Acronis Internet Security Suite 2010.

Cómo

31. Cómo Analizar Ficheros y Carpetas

Analizar es fácil y flexible con Acronis Internet Security Suite 2010. Existen 4 maneras de configurar Acronis para que analice los ficheros y carpetas en busca de virus y otro malware:

- Utilizando el Menú Contextual de Windows
- Utilizando las Tareas de Análisis
- Usando Análisis Manual de Acronis
- Utilizando la Barra de Actividad del Análisis

Una vez iniciado un análisis, el asistente de Análisis Antivirus aparecerá y le guiará durante el proceso. Para información detallada acerca de este asistente, por favor consulte "*Asistente del análisis Antivirus*" (p. 45).

31.1. Utilizando el Menú Contextual de Windows

Ésta es la manera más fácil y recomendada para analizar un fichero o carpeta de su equipo. Haga clic derecha sobre un objeto que desea analizar y seleccione **Analizar con Acronis Internet Security Suite** desde el menú. Siga el asistente de Análisis Antivirus para finalizar el análisis.

Las situaciones típicas en las cuales debería utilizar este método de análisis incluyen las siguientes:

- Sospecha que un fichero o carpeta concreta está infectada.
- Siempre que descarga desde Internet ficheros que piensa que podrían ser peligrosos.
- Analizar una carpeta compartida en red antes de copiar ficheros a su ordenador.

31.2. Utilizando Tareas de Análisis

Si desea analizar su equipo o algunas carpetas regularmente, debería utilizar las tareas de análisis. Las tareas de análisis indican a Acronis Internet Security Suite 2010 qué ubicaciones analizar, con qué opciones y qué acciones realizar. Además, puede programarlas para que se ejecuten regularmente o en un momento específico.

Para analizar su equipo utilizando tareas de análisis, debe abrir la interfaz de Acronis Internet Security Suite 2010 y ejecutar la tarea de análisis deseada. Dependiendo de la vista de la interfaz de usuario, existen diferentes pasos a seguir para ejecutar la tarea de análisis.

Ejecutar Tareas de Análisis en Modo Básico

En Modo Básico, puede ejecutar solo un análisis estándar completo del equipo haciendo clic en **Analizar Ahora**. Siga el asistente de Análisis Antivirus para finalizar el análisis.

Ejecutar Tareas de Análisis en Modo Intermedio.

En Modo Intermedio, puede ejecutar un número de tareas de análisis pre configuradas. Siga estos pasos para ejecutar una tarea de análisis en el Modo Intermedio:

1. Haga clic en la pestaña **Seguridad**.
2. En el área superior Izquierda de la Tareas Rápidas, haga clic **Análisis Completo** para iniciar un análisis estándar entero del equipo. Para ejecutar una tarea de análisis diferente, haga clic en el botón de flecha y seleccione la tarea de análisis desea. Para configurar y ejecutar un análisis personalizado, haga clic en **Análisis**. Éstas son las tareas de análisis disponibles:

Tarea de Análisis	Descripción
Análisis de sistema	Analiza todo el sistema, excepto los archivos comprimidos. En la configuración predeterminada, busca todos los tipos de malware distintos a rootkits.
Análisis en Profundidad	Analiza el sistema por completo. En la configuración predeterminada, analiza en busca de cualquier tipo de malware que pueda amenazar a su sistema, como virus, spyware, adware, rootkits y otros.
Analizar Mis Documentos	Utilice esta tarea para analizar las carpetas del usuario que está utilizando: `Mis Documentos`, `Escritorio` e `Inicio`. Así se asegurará el contenido de sus documentos, un espacio de trabajo seguro y que las aplicaciones iniciadas al cargar el sistema están limpias.
Análisis Personalizado	Esta opción le ayuda a configurar y ejecutar una tarea de análisis personalizada, permitiéndole especificar el análisis y las opciones generales del análisis. Puede guardar las tareas de análisis personalizadas con el fin de acceder más tarde en el Modo Intermedio o en Modo Avanzado.

3. Siga el asistente de Análisis Antivirus para finalizar el análisis. Si ha seleccionado ejecutar un análisis personalizado, debe completar el Asistente de Análisis Personalizado.

Ejecutar Tareas de Análisis en Modo Avanzado

En Modo Avanzado, puede ejecutar todas las tareas de análisis preconfiguradas, y también modificar las opciones de análisis. Además, puede crear tareas de análisis personalizadas si dese analizar ubicaciones especificas en su equipo. Siga estos pasos para ejecutar una tarea de análisis en el Modo Avanzado:

1. Haga clic en **Antivirus** del menú de la izquierda.
2. Haga clic en la pestaña **Análisis**. Aquí puede encontrar un número de tareas de análisis predeterminadas y puede crear sus propias tareas de análisis. Éstas son las tareas de análisis predeterminadas que puede utilizar:

Tarea Predeterminada	Descripción
Análisis en Profundidad	Analiza el sistema por completo. En la configuración predeterminada, analiza en busca de cualquier tipo de malware que pueda amenazar a su sistema, como virus, spyware, adware, rootkits y otros.
Análisis de sistema	Analiza todo el sistema, excepto los archivos comprimidos. En la configuración predeterminada, busca todos los tipos de malware distintos a rootkits.
Análisis Rápido del Sistema	Analiza las carpetas de `Windows` y `Archivos de Programa`. En la configuración predeterminada, analiza en busca de cualquier tipo de malware, excepto rootkits, pero no analiza la memoria, el registro ni las cookies.
Mis Documentos	Utilice esta tarea para analizar las carpetas del usuario que está utilizando: `Mis Documentos`, `Escritorio` e `Inicio`. Así se asegurará el contenido de sus documentos, un espacio de trabajo seguro y que las aplicaciones iniciadas al cargar el sistema están limpias.

3. Haga doble clic sobre la tarea que desea ejecutar.
4. Siga el asistente de Análisis Antivirus para finalizar el análisis.

31.3. Usando Análisis Manual de Acronis

El Análisis Manual de Acronis le premite analizar una carpeta específica o una partición del disco duro sin tener que crear una tarea de análisis. Esta característica ha sido diseñada para ser utilizada cuando Windows se ejecuta en Modo Seguro. Si su sistema está infectado con un virus residente, puede intentar eliminarlo iniciando

Windows en Modo Seguro y analizando cada partición de su disco duro utilizando el Análisis Manual de Acronis.

Para analizar su equipo utilizando el Análisis Manual de Acronis, siga estos pasos:

1. En el menú Inicio de Windows, siga la ruta **Inicio → Programas → Acronis → Acronis Internet Security Suite 2010 → Acronis Análisis Manual**. Aparecerá una nueva ventana.
2. Haga clic en **Añadir Carpeta** para seleccionar el análisis. Aparecerá una nueva ventana.
3. Seleccione la ruta del análisis:
   - Para analizar su escritorio, seleccione **Escritorio**.
   - Para analizar una partición entera del disco duro, selecciónela desde Mi PC.
   - Para analizar una carpeta específica, explore y seleccione la carpeta.
4. Haga clic en **Aceptar**.
5. Haga clic en **Continuar** para iniciar el análisis.
6. Siga el asistente de Análisis Antivirus para finalizar el análisis.

¿Qué es el Modo Seguro?
El Modo Seguro es una manera especial de iniciar Windows, utilizado normalmente para solucionar incidencias que afectan el funcionamiento normal de Windows. Estos problemas pueden ser desde drivers conflictivos hasta virus que impidan el inicio normal de Windows. En Modo Seguro, Windows inicia sólo un mínimo de componentes y drivers básicos. Sólo algunas aplicaciones funcionan en Modo Seguro. Por esta razón los virus están inactivos en Modo Seguro y pueden ser eliminados fácilmente.
Para iniciar Windows en Modo Seguro, reinicie el equipo y presione la tecla F8 hasta que aparezca el Menú de Opciones Avanzadas de Windows. Puede elegir varias opciones para iniciar Windows en Modo Seguro. Puede seleccionar **Modo Seguro con Funciones de Red** con tal de tener acceso a Internet.

Nota

Para más información acerca del Modo Seguro, puede dirigirse a la Ayuda de Windows y Centro de Soporte (el menú Inicio, haga click en **Ayuda y Soporte**). También puede encontrar información de utilidad buscando en Internet.

31.4. Utilizar la barra de actividad del análisis

Barra de Actividad del Análisis

La **barra de análisis de la actividad** es una vista gráfica de la actividad de análisis de su sistema. Esta pequeña ventana esta disponible por defecto sólo en Modo Avanzado.

Puede utilizar la Barra de Actividad del Análisis para analizar rápidamente ficheros y carpetas. Arrastre & suelte el fichero o carpeta que desea analizar encima de la Barra de Actividad del Análisis. Siga el asistente de Análisis Antivirus para finalizar el análisis.

Nota

Para más información, por favor, consulte el capítulo "*Barra de Actividad del Análisis*" (p. 27).

32. Cómo Programar Análisis del Equipo

Analizando su equipo periódicamente es la mejor manera de mantener su equipo libre de malware. Acronis Internet Security Suite 2010 le permite programar tareas de análisis de manera que pueda analizar su equipo automáticamente.

Para programar Acronis Internet Security Suite 2010 para analizar su equipo, siga estos pasos:

1. Abra Acronis Internet Security Suite 2010 y cambie la interfaz de usuario al Modo Avanzado.
2. Haga clic en **Antivirus** del menú de la izquierda.
3. Haga clic en la pestaña **Análisis**. Aquí puede encontrar un número de tareas de análisis predeterminadas y puede crear sus propias tareas de análisis.
   - Las tareas de sistema están disponibles y se pueden ejecutar bajo cualquier cuenta de usuario de Windows.
   - Las tareas de usuario sólo están disponibles y se pueden ejecutar por el usuario que las ha creado.

   Éstas son las tareas de análisis predeterminadas que puede programar:

Tarea Predeterminada	Descripción
Análisis en Profundidad	Analiza el sistema por completo. En la configuración predeterminada, analiza en busca de cualquier tipo de malware que pueda amenazar a su sistema, como virus, spyware, adware, rootkits y otros.
Análisis de sistema	Analiza todo el sistema, excepto los archivos comprimidos. En la configuración predeterminada, busca todos los tipos de malware distintos a rootkits.
Análisis Rápido del Sistema	Analiza las carpetas de `Windows` y `Archivos de Programa`. En la configuración predeterminada, analiza en busca de cualquier tipo de malware, excepto rootkits, pero no analiza la memoria, el registro ni las cookies.
Análisis del Autologon	Analiza los elementos que se ejecutan cuando un usuario inicia sesión en Windows. Para utilizar esta tarea, debe programarla para que se ejecute al inicio del sistema. Por defecto, el análisis automático al iniciar sesión está desactivado.
Mis Documentos	Utilice esta tarea para analizar las carpetas del usuario que está utilizando: `Mis Documentos`,

Tarea Predeterminada	Descripción
	Escritorio e Inicio. Así se asegurará el contenido de sus documentos, un espacio de trabajo seguro y que las aplicaciones iniciadas al cargar el sistema están limpias.

Si ninguna de esta tareas cumple con sus necesidades, puede crear una nueva tarea, que puede programar según sus preferencias.

4. Haga clic derecha sobre la tarea de análisis y seleccione **Programar**. Aparecerá una nueva ventana.
5. Programe la tarea para ejecutarse según sus necesidades:
   - Para ejecutar la tarea sólo una vez, seleccione **Una vez** y especifique la fecha y hora de inicio.
   - Para ejecutar una tarea después del inicio de sistema, seleccione **Al iniciar el sistema**. Puede especificar cuanto tiempo después del inicio del sistema debe ejecutarse la tarea (en minutos).
   - Para ejecutar la tarea de análisis regularmente, seleccione **Periódicamente** y especifique la frecuencia y la fecha y hora de inicio.

   Nota

   Por ejemplo, para analizar su equipo cada sábado a las 2AM, debe configurar el horario de la siguiente manera:

   a. Seleccione **Periódicamente**.
   b. En el campo **Cada**, introduzca 1 y después seleccione **semanas** desde el menú. De esta manera, la tarea se ejecutará una vez a la semana.
   c. Configure como fecha de inicio el próximo sábado.
   d. Configure como hora de inicio `2:00:00 AM`.

6. Haga clic en **Aceptar** para guardar el horario. La tarea de análisis se ejecutará automáticamente según el horario que usted ha definido. Si el equipo está apagado cuando el análisis programado debe iniciarse, la tarea se ejecutará la próxima vez que inicie el equipo.

Solución de Problemas y Ayuda

33. Resolución de Problemas

Este capítulo presenta algunos problemas que pueden surgir cuando se utilice Acronis Internet Security Suite 2010 y le ofrece soluciones posibles para estos problemas. La mayoría de estos problemas pueden ser solucionados mediante la configuración adecuada de la configuración del producto.

Si no puede encontrar su problema aquí, o si la solución presentada no lo resuelve, puede contactar con el soporte técnico de Acronis como se representa en el capítulo "*Soporte*" (p. 316).

33.1. Problemas de Instalación

Este artículo le ayudara a solucionar los problemas más comunes de instalación con Acronis Internet Security Suite 2010. Estos problemas puede ser agrupados dentro de las siguientes categorías:

- Errores de Validación de Instalación: El asistente de instalación no puede ser ejecutado debido a las condiciones específicas de su sistema.
- Error de instalación: Ha iniciado una instalación desde el asistente de instalación, pero no fue completada con éxito.

33.1.1. Errores de Validación de Instalación

Cuando inicia el asistente de instalación, se verifican un número de condiciones para validar si la instalación puede ser iniciada. La siguiente tabla presenta los errores de validación de instalación más comunes y soluciones para superarlos.

Error	Descripción&Solución
Usted no tiene suficientes privilegios para instalar el programa.	Con el fin de ejecutar el asistente de instalación e instalación Acronis Internet Security Suite 2010 necesita privilegios de administrador. Realice una de estas acciones: ● Inicie sesión con en Windows con una cuenta de administrador y vuelva a ejecutar el asistente de instalación. ● Haga clic derecho en el archivo de instalación y seleccionar **Ejecutar como**. Escriba el nombre de usuario y contraseña de la cuenta de administrador de Windows en el sistema.
El instalador ha detectado una versión anterior de Acronis Internet Security	Acronis Internet Security Suite 2010 fue instalado previamente en su sistema, pero la instalación no fue totalmente desinstalada. Este condición bloquea una

Error	Descripción&Solución
Suite 2010 que no fue desinstalada correctamente.	nueva instalación de Acronis Internet Security Suite 2010. Para superar este error e instalar Acronis Internet Security Suite 2010, siga estos pasos: 1. Contactar con el soporte técnico de Acronis Inc. como se detalla en "*Soporte*" (p. 316) y pregunte por la herramienta de desinstalación. 2. Ejecute la herramienta de desinstalación utilizando privilegios administrativos. 3. Reinicie el equipo. 4. Inicie el asistente de instalación de nuevo para instalar Acronis Internet Security Suite 2010.
El producto de Acronis Internet Security Suite 2010 no es compatible con su sistema operativo.	Esta intentando instalar Acronis Internet Security Suite 2010 en un sistema operativo incompatible. Por favor compruebe el "*Requisitos del Sistema*" (p. 2) para averiguar los sistemas operativos donde pueden instalar Acronis Internet Security Suite 2010. Si su sistema operativo es Windows XP con Service Pack 1 o sin ningún service pack, puede instalar Service Pack 2 o superior y volver a ejecutar el asistente de instalación.
El archivo de instalación esta diseñado para un tipo diferente de procesador.	Si obtiene un error de este tipo, es que esta intentando ejecutar una versión incorrecta del archivo de instalación. Existen dos versiones del archivo de instalación de Acronis Internet Security Suite 2010: uno para procesadores de 32-bit y otra para procesadores de 64-bit. Para asegurarse que tiene la versión correcta para su sistema, descarga directamente el archivo desde http://www.acronis.es/.

33.1.2. Fallo en la Instalación

Existen varias posibilidades de que falle la instalación:

- Durante la instalación, aparece un error en pantalla. Se le puede pedir que cancele la instalación o puede proporcionar un botón para ejecutar una herramienta de desinstalación para que se limpie el sistema.

Nota

Inmediatamente después de que inicie la instalación, es posible que se le notifique no hay espacio libre suficiente en disco para instalar Acronis Internet Security Suite 2010, En ese caso, libere el espacio requerido en disco en la partición en donde desea instalar Acronis Internet Security Suite 2010 y luego reanude la instalación.

- La instalación se cuelga y, probablemente, su sistema se pare. Sólo un reinicio de sistema lo restaurará.
- La instalación fue completada, pero no puede utilizar alguno o todas las funciones de Acronis Internet Security Suite 2010.

Para solucionar los problemas con una instalación fallida e instalar Acronis Internet Security Suite 2010, siga estos pasos:

1. **Limpiar el sistema después de una instalación fallida.** Si la instalación falla, algunas claves de registro y archivos de Acronis Internet Security Suite 2010 permanecerán es su sistema. Estos restos pueden impedir una nueva instalación de Acronis Internet Security Suite 2010. También puede afectar al rendimiento del sistema y la estabilidad. Esto es porque debe eliminar los restos antes de intentar instalar el nuevo producto.

   Si la pantalla de error proporciona un botón para ejecutar una herramienta de desinstalación, haga clic en el botón para limpiar el sistema. De lo contrario, proceda de la siguiente manera:

   a. Contactar con el soporte técnico de Acronis Inc. como se detalla en "*Soporte*" (p. 316) y pregunte por la herramienta de desinstalación.

   b. Ejecute la herramienta de desinstalación utilizando privilegios administrativos.

   c. Reinicie el equipo.

2. Compruebe si tiene alguna otra solución de seguridad instalada porque esta puede perturbar la operación normal de Acronis Internet Security Suite 2010. Si este es el caso, le recomendamos que desinstale todas la otras soluciones de seguridad y luego reinstale Acronis Internet Security Suite 2010.
3. Vuelva a instalar Acronis Internet Security Suite 2010. Se recomienda que descargue y ejecute la última versión del archivo de instalación desde www.acronis.es.
4. Si la instalación vuelve a fallar, contacte con Acronis Inc para recibir soporte como se describe en la sección "*Soporte*" (p. 316).

33.2. Los Servicios de Acronis Internet Security Suite 2010 No Responden

Este artículo le ayuda a solucionar problemas del error *Servicios de Acronis Internet Security Suite 2010 no responden* Puede encontrar este error de la siguiente manera:

- El icono de Acronis en la barra de tareas está en gris y una ventana emergente le informa que los servicios de Internet Security Suite 2010 no responden.
- La ventana de Acronis Internet Security Suite 2010 indica que los servicios de Acronis Internet Security Suite 2010 no responden.

El error puede ser causado por una de las siguientes condiciones:

- una actualización importante esta instalándose.
- Errores temporales de comunicación entre los servicios de Acronis Internet Security Suite 2010.
- algunos de los servicios de Acronis Internet Security Suite 2010 están detenidos.
- otras soluciones de seguridad se están ejecutando en su equipo al mismo tiempo que Acronis Internet Security Suite 2010.
- los virus en su sistema afectan a la ejecución normal de Acronis Internet Security Suite 2010.

Para solucionar este problema, pruebe estas soluciones:

1. Espere unos momentos y mire si algo cambia. El error puede ser temporal.
2. Reinicie el equipo y espere unos minutos a que Acronis Internet Security Suite 2010 se inicie. Abra Acronis Internet Security Suite 2010 para ver si continua el error. Reiniciando el equipo normalmente soluciona el problema.
3. Compruebe si tiene alguna otra solución de seguridad instalada porque esta puede perturbar la operación normal de Acronis Internet Security Suite 2010. Si este es el caso, le recomendamos que desinstale todas la otras soluciones de seguridad y luego reinstale Acronis Internet Security Suite 2010.
4. Si el error continua, debe ser un problema serio mas grave (por ejemplo, puede estar infectado con un virus que interfiere con Acronis Internet Security Suite 2010). Por favor, contacte con Acronis Inc para recibir soporte como se describe en la sección “*Soporte*” (p. 316).

33.3. Compartir Impresoras y Archivos en red Wi-Fi (Wireless) no funciona

Este artículo le ayuda a solucionar los siguientes problemas con el cortafuego de Acronis Internet Security Suite 2010 en redes Wi-Fi:

- No se pueden compartir archivos con equipos en la red Wi-Fi.
- No puede acceder a la impresora compartida de red en la red Wi-Fi.
- No puede acceder a la impresora compartida por un equipo en la red Wi-Fi.
- No puede compartir su impresora con equipos en la red Wi-Fi.

Antes de solucionar estos problemas, debe conocer algunas cosas acerca de la seguridad y la configuración del cortafuego de Acronis Internet Security Suite 2010 en redes Wi-Fi. Desde un punto de vista de seguridad, las redes de Wi-Fi están dentro de una de estas categorías:

- **Seguridad en redes Wi-Fi.** Este tipo de red permite sólo a Wi-Fi autorizadas-dispositivos activados para conectarse. El acceso a Red está condicionado por una contraseña. Los ejemplos de redes Wi-Fi seguras serán las establecidas en redes de oficina.
- **Abrir Red Wi-Fi (no segura).** Cualquier dispositivo Wi-Fi activado dentro del rango en una red Wi-Fi no segura puede conectarse libremente. Las redes Wi-Fi no seguras son ampliamente utilizadas. Entre ellas se incluyen casi todas las redes Wi-Fi públicas (tales como campus de colegio, cibercafés, aeropuertos y otras). Una red que se configura utilizando un router inhalámbrico no está segura hasta que active la seguridad en el router.

  Una red Wi-Fi no segura presenta un gran riesgo de seguridad porque su equipo está conectado a equipos desconocidos. Sin la protección apropiada proporcionada por un cortafuego, cualquier persona conectada a la red puede acceder a sus elementos compartidos e incluso entrar dentro de su equipo.

Cuando se conecta a una red Wi-Fi no segura, Acronis Internet Security Suite 2010 automáticamente bloquea la comunicación con los equipos de esta red. Usted sólo puede tener acceso a Internet, pero no puede compartir archivos o impresoras con otros usuarios de la red.

Para activar la comunicación con un red Wi-Fi, dispone de estas dos soluciones:

- La solución "equipo de confianza" permite compartir carpetas e impresoras sólo con equipos específicos (equipos de confianza) de la red Wi-Fi. Utilice esta solución cuando esté conectado a una red Wi-Fi pública (por ejemplo, una red en un campus o en un cibercafé) y desee compartir archivos o una impresora con un amigo o acceder a la impresora de la red Wi-Fi.
- La solución "red segura" permite compartir archivos e impresoras en toda la red Wi-Fi (Red Segura). Esta solución no es recomendable por razones de seguridad, pero debe utilizarla en situaciones particulares (por ejemplo, puede utilizarla para una red Wi-Fi doméstica u oficina).

33.3.1. Solución "Equipo de Confianza"

Para configurar el cortafuego de Acronis Internet Security Suite 2010 para permitir compartir archivos e impresoras con un equipo en la red Wi-Fi, o acceder a una impresora de la red Wi-Fi, siga estos pasos:

1. Abra Acronis Internet Security Suite 2010 y cambie la interfaz de usuario al Modo Avanzado.
2. Haga clic en **Cortafuego** en el menú de la izquierda.

3. Haga clic en la pestaña **Red**.
4. En la tabla Zonas, seleccione la red Wi-Fi y haga clic en el botón **Añadir**.
5. Seleccione el equipo deseado o la impresora de la red Wi-Fi de la lista de los dispositivos detectados en la red Wi-Fi. Si el equipo o la impresor no ha sido detectada automáticamente, puede escribir la dirección IP en el campo **Zona**.
6. Seleccione la acción **Permitir**.
7. Haga clic en **Aceptar**.

Si aún no ha compartido archivos o una impresora con el equipo seleccionado, lo más probable es que esto no sea causado por el cortafuego de Acronis Internet Security Suite 2010 en su equipo. Comprobar otras causas potenciales, como las siguientes:

- El cortafuego en el otro equipo puede bloquear archivos e impresoras compartidas en red Wi-Fi no seguras (públicas).
  - ▶ Si el cortafuego de Acronis Internet Security Suite 2010 se utiliza, el mismo procedimiento debe ser seguido en otro que equipo para permitir compartir impresoras y archivos con su equipo.
  - ▶ Si se utiliza el Cortafuego de Windows, se puede configurar para permitir compartir archivos e impresoras de la siguiente manera: abra la ventana de configuración del Cortafuego de Windows, pestaña **Excepciones** y marque la casilla **Compartir Archivos e Impresoras**.
  - ▶ Si utiliza otro programa de cortafuego, por favor, consulte su documentación o archivo de ayuda.
- Condiciones generales que pueden impedir el uso o la conexión a la impresora compartida:
  - ▶ Puede necesitar iniciar sesión con una cuenta de Administrador de Windows para acceder a la impresora compartida.
  - ▶ Se establecen los permisos para permitir el acceso a la impresora compartida a los equipos y a los usuarios solamente. Si esta compartiendo su impresora, compruebe los permisos establecidos para esta impresora para ver si el usuario de otro equipo tiene permitido el acceso a la impresora. Si esta intentando conectarse a una impresora compartida, compruebe con el usuario del otro equipo si tiene permisos para conectarse a la impresora.
  - ▶ La impresora conectada a su equipo o a otro equipo no está compartida.
  - ▶ La impresora compartida no está agregada en el equipo.

Nota

Para aprender como administrar una impresora compartida (compartir una impresora, establecer o eliminar permisos para una impresora, conectar una

impresora de red o compartir impresora), diríjase a la Ayuda de Windows y Centro de Soporte (en el menú Inició, haga clic en **Ayuda y soporte técnico**).

Si no tiene acceso a la impresora de la red Wi-Fi, los más probable es que esta no sea causado por el cortafuego de Acronis Internet Security Suite 2010 en su equipo. Para acceder a la impresora de la red Wi-Fi puede estar restringida a equipo e usuarios solamente. Debería comprobar con el administrador en la red Wi-Fi si tiene permisos para conectarse con esta impresora.

Si sospecja que el problema es con el cortafuego de Acronis Internet Security Suite 2010, puede contactar con el soporte de Acronis Inc. como se describe en la sección "*Soporte*" (p. 316).

33.3.2. Solución "Red Segura"

Es recomendado que utilice esta solución solo para redes Wi-Fi en casa u oficina.

Para configurar el cortafuego de Acronis Internet Security Suite 2010 para permitir compartir archivos e impresoras con todas la red Wi-Fi, siga estos pasos:

1. Abra Acronis Internet Security Suite 2010 y cambie la interfaz de usuario al Modo Avanzado.
2. Haga clic en **Cortafuego** en el menú de la izquierda.
3. Haga clic en la pestaña **Red**.
4. En la tabla de Configuración de Red, la columna **Nivel de Confianza**, haga clic en la flecha en la celda correspondiente para la red Wi-Fi.
5. Dependiendo del nivel de seguridad que desea obtener, elija una de las siguientes opciones:
   - **Insegura** - para acceder a los archivos e impresoras compartidas en la red Wi-Fi, sin permitir el acceso a sus compartidos.
   - **Seguro** - para permitir compartir archivos e impresoras en ambos sentidos. Esto significa que los usuarios conectados a la red Wi-Fi pueden también tener acceso a sus archivos o impresoras compartidas.

Si aun no ha compartido archivos o una impresora con un equipo en la red Wi-Fi, lo más probable es que esto no sea causado por el cortafuego de Acronis Internet Security Suite 2010 en su equipo. Comprobar otras causas potenciales, como las siguientes:

- El cortafuego en el otro equipo puede bloquear archivos e impresoras compartidas en red Wi-Fi no seguras (públicas).
  - ▶ Si el cortafuego de Acronis Internet Security Suite 2010 se utiliza, el mismo procedimiento debe ser seguido en otro que equipo para permitir compartir impresoras y archivos con su equipo.

- ▶ Si se utiliza el Cortafuego de Windows, se puede configurar para permitir compartir archivos e impresoras de la siguiente manera: abra la ventana de configuración del Cortafuego de Windows, pestaña **Excepciones** y marque la casilla **Compartir Archivos e Impresoras**.
- ▶ Si utiliza otro programa de cortafuego, por favor, consulte su documentación o archivo de ayuda.

● Condiciones generales que pueden impedir el uso o la conexión a la impresora compartida:

- ▶ Puede necesitar iniciar sesión con una cuenta de Administrador de Windows para acceder a la impresora compartida.
- ▶ Se establecen los permisos para permitir el acceso a la impresora compartida a los equipos y a los usuarios solamente. Si esta compartiendo su impresora, compruebe los permisos establecidos para esta impresora para ver si el usuario de otro equipo tiene permitido el acceso a la impresora. Si esta intentando conectarse a una impresora compartida, compruebe con el usuario del otro equipo si tiene permisos para conectarse a la impresora.
- ▶ La impresora conectada a su equipo o a otro equipo no está compartida.
- ▶ La impresora compartida no está agregada en el equipo.

Nota

Para aprender como administrar una impresora compartida (compartir una impresora, establecer o eliminar permisos para una impresora, conectar una impresora de red o compartir impresora), diríjase a la Ayuda de Windows y Centro de Soporte (en el menú Inició, haga clic en **Ayuda y soporte técnico**).

Si no tiene acceso a la impresora de la red Wi-fi, lo más probable es que no sea causado por el cortafuego de Acronis Internet Security Suite 2010 en su equipo. Para acceder a la impresora de la red Wi-Fi puede estar restringida a equipo e usuarios solamente. Debería comprobar con el administrador en la red Wi-Fi si tiene permisos para conectarse con esta impresora.

Si sospecja que el problema es con el cortafuego de Acronis Internet Security Suite 2010, puede contactar con el soporte de Acronis Inc. como se describe en la sección "*Soporte*" (p. 316).

33.4. El Filtro Antispam no funciona correctamente

Este articulo le ayuda a solucionar los siguientes problemas con el funcionamiento del Filtro Antispam de Acronis Internet Security Suite 2010:

- Un número de mensajes de correo legítimos están marcados como `[spam]`.
- Algunos mensajes spam no están marcados de acuerdo con el filtro spam.

- El filtro antispam no ha detectado ningún mensaje antispam.

33.4.1. Mensajes Legítimos Están Marcados como [spam]

Mensajes Legítimos están marcados como `[spam]` simplemente porque el filtro Antispam de Acronis Internet Security Suite 2010 los ve como spam. Normalmente puede solventar este problema adecuando la configuración del filtro Antispam.

Acronis Internet Security Suite 2010 automáticamente añade los destinatarios de su mensajes de correo a la lista de Amigos. Los mensajes de correo recibidos de los contacto que estan en la lista de Amigos son considerados como legítimos. Estos no son verificados por el filtro antispam y, así, no serán marcados nunca como `[spam]`.

La configuración automática de la lista de Amigos no previene la detección de errores que pueden ocurrir en estas situaciones:

- Puede recibir muchos correos comerciales como resultado de suscribirse en varias páginas web. En esta caso, la solución en añadir la dirección de correo de la cual recibe tales mensajes a la lista de Amigos.
- Una parte significativa de sus correos legítimos es de gente con los cuales nunca antes se ha contactado, como clientes, posibles socios comerciales y otros. Se requieren otras soluciones en este caso.

Si está utilizando un de los clientes de correo integrados dentro de Acronis Internet Security Suite 2010, intente las siguientes soluciones:

1. Indicador de detección de errores. Este se utiliza para entrenar el Motor de Aprendizaje (Bayesiano) del filtro antispam y le ayuda a prevenir las futuras detecciones de errores. El Motor de Aprendizaje analiza los mensajes indicados y aprende de sus patrones. El siguiente mensaje de correo se ajusta al mismo patrón que se no será marcada como `[spam]`.
2. Disminuir el nivel de protección antispam. Para disminuir el nivel de protección, el filtro antispam necesitará más indicadores spam para clasificar un mensaje de correo como spam. Intentar esta solución sólo si muchos mensajes (incluyendo mensajes comerciales solicitados) son detectados incorrectamente como spam.
3. Reentrenar el Motor de Aprendizaje (filtro Bayesiano). Intente esta solución solo si las soluciones anteriores no han ofrecido resultados satisfactorios.

Nota

Acronis Internet Security Suite 2010 se integra dentro de los clientes de correo más utilizados mediante una barra de herramientas antispam fácil de utilizar. Para una lista completa de clientes de correo soportados, por favor diríjase a *"Software Soportado"* (p. 2).

Si esta utilizando un cliente de correo diferente, puede no indicar la detección de errores y entrenar el Motor de Aprendizaje. Para resolver el problema, intente disminuir el nivel de protección antispam.

Agregar Contactos a la Lista de Amigos

Si esta utilizando un cliente de correo compatible, puede añadir fácilmente los remitentes de los mensajes legítimos a la lista de Amigos. Siga estos pasos:

1. En su cliente de correo, seleccionar el mensaje de correo del remitente que desea añadir a la lista de Amigos.
2. Haga clic en el botón **Añadir Amigo** en la barra de herramientas antispam de Acronis Internet Security Suite 2010.
3. Puede pedir que admita las direcciones añadidas a la lista de Amigos. Seleccione **No volver a mostrar este mensaje** y haga clic en **Aceptar**.

A partir de este momento, recibirá todos los mensajes provenientes de esta dirección, independientemente de su contenido.

Si esta utilizando un cliente de correo diferente, puede añadir contactos a lista de Amigos desde la interfaz de Acronis Internet Security Suite 2010. Siga estos pasos:

1. Abra Acronis Internet Security Suite 2010 y cambie la interfaz de usuario al Modo Avanzado.
2. Haga clic en **Antispam** en el menú de la izquierda.
3. Haga clic en la pestaña **Estado**.
4. Haga clic en **Amigos**. Aparecerá una nueva ventana de configuración.
5. Introduzca la dirección de correo que desea siempre recibir los mensajes de correo y haga clic en el botón para añadir la dirección a la lista de Amigos.
6. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

Indicador de Detección de Errores

Si esta utilizando un cliente de correo compatible, puede corregir fácilmente el filtro antispam (indicando que mensajes de correo no deben ser marcados como `[spam]`). Si lo hace, mejorará considerablemente la eficiencia del filtro antispam. Siga estos pasos:

1. Abra su cliente de correo.
2. Diríjase a la carpeta de correo no deseado en donde se han movido los mensajes spam.
3. Seleccionar el mensaje legítimos marcado incorrectamente como `[spam]` por Acronis Internet Security Suite 2010.

4. Haga clic en el botón **Añadir Amigo** en la barra de herramientas antispam de Acronis Internet Security Suite 2010 para añadir los remitentes a la lista de Amigos. Puede que necesite hacer clic en **Aceptar** para admitirlo. A partir de este momento, recibirá todos los mensajes provenientes de esta dirección, independientemente de su contenido.
5. Haga clic en el botón **No Spam** en la barra de herramientas antispam de Acronis Internet Security Suite 2010 (normalmente ubicado en la parte superior en la ventana de correo). Esto le indica al motor de Aprendizaje que el mensaje seleccionado no es spam. El mensaje de correo se moverá a la carpeta Bandeja de Entrada. El siguiente mensaje de correo se ajusta al mismo patrón, el cual no será marcado como `[spam]`.

Disminuir el Nivel de Protección Antispam

Para disminuir el nivel de protección antispam, siga estos pasos:

1. Abra Acronis Internet Security Suite 2010 y cambie la interfaz de usuario al Modo Avanzado.
2. Haga clic en **Antispam** en el menú de la izquierda.
3. Haga clic en la pestaña **Estado**.
4. Mueva la barra de la escala hacia abajo.

Esto es recomendable para disminuir la protección a un sólo nivel y esperar suficiente tiempo para evaluar los resultados. Si algunos mensajes de correo legítimos están siendo aún marcados como `[spam]`, puede disminuir aún más el nivel de protección. Si nota que muchos mensajes no se detectan como spam, no debería disminuir el nivel de protección.

Reentrenar el Motor de Aprendizaje (Bayesiano)

Antes de entrenar el Motor de Aprendizaje (Bayesiano), prepare una carpeta que contenga sólo mensajes SPAM y otra que contenga sólo mensajes legítimos. El Motor de Aprendizaje analizará estos y aprenderá las características que definen el spam o mensajes legítimos que normalmente recibe. Con el fin de entrenarlo con eficacia debe haber más de 50 mensajes en cada categoría.

Para reiniciar la base de datos Bayesiano y reentrenar el Motor de Aprendizaje, siga estos pasos:

1. Abra su cliente de correo.
2. En la barra de herramientas antispam de Acronis Internet Security Suite 2010, haga clic en el botón **Asistente** para iniciar el asistente de configuración antispam. Se proporciona más información en la sección *"Asistente de Configuración Antispam"* (p. 276).
3. Haga clic en **Siguiente**.

4. Seleccionar **Omitir este paso** y haga clic en **Siguiente**.
5. Seleccionar **Limpiar base de datos del filtro antispam** y haga clic en **Siguiente**.
6. Seleccione la carpeta que contiene mensajes legítimos y haga clic en **Siguiente**.
7. Seleccione la carpeta que contiene mensajes SPAM y haga clic en **Siguiente**.
8. Haga clic en **Finalizar** para iniciar el proceso de aprendizaje.
9. Cuando el aprendizaje se ha completado, haga clic en **Cerrar**.

Solicitar Ayuda

Si esta información no le ayuda, puede contactar con el Soporte de Acronis como se describe en la sección "*Soporte*" (p. 316).

33.4.2. Muchos Mensajes SPAM No se han Detectado

Si está recibiendo muchos mensajes spam que no están marcados como `[spam]`, debe configurar el filtro antispam de Acronis Internet Security Suite 2010, con el fin de mejorar su eficiencia.

Si está utilizando uno de los clientes de correo integrados en Acronis Internet Security Suite 2010, intente las siguientes soluciones:

1. Indicador de mensajes spam no detectados. Este se utiliza para entrenar el Motor de Aprendizaje (Bayesiano) del filtro antispam y normalmente mejora la detección de antispam. El Motor de Aprendizaje analiza los mensajes indicados y aprende de sus patrones. Los siguientes mensajes de correos se ajustan al mismo patrón, los cuales serán marcados como `[spam]`.
2. Añadir spammers a la lista de Spammers. Los mensajes de correo recibidos de las direcciones que están en la lista de Spammer son marcados automáticamente como `[spam]`.
3. Incrementar el nivel de protección antispam. Para incrementar el nivel de protección, el filtro antispam necesitará más indicadores spam para clasificar un mensaje de correo como spam.
4. Reentrenar el Motor de Aprendizaje (filtro Bayesiano). Utilice esta solución cuando la detección antispam es muy insatisfactorio y que indica que la detección de spam no funciona.

Nota

Acronis Internet Security Suite 2010 se integra dentro de los clientes de correo más utilizados mediante una barra de herramientas antispam fácil de utilizar. Para una lista completa de clientes de correo soportados, por favor diríjase a "*Software Soportado*" (p. 2).

Si esta utilizando un cliente de correo diferente, no puede indicar los mensajes spam y entrenar el Motor de Aprendizaje. Para resolver el problema, intente disminuir el nivel de protección antispam y añade spammer a la lista de Spammers.

Indicador de Mensajes Spam No detectados.

Si esta utilizando un cliente de correo compatible, puede indicar fácilmente que mensajes de correo deben ser detectados como spam. Haciendo esto aumentará considerablemente la eficacia del filtro antispam. Siga estos pasos:

1. Abra su cliente de correo.
2. Diríjase a la carpeta Bandeja de Entrada.
3. Seleccione los mensajes spam no detectados.
4. Haga clic en el botón **Es Spam** en la barra de herramientas de Acronis Internet Security Suite 2010 (normalmente ubicacada en la parte superior de la ventana del cliente de correo). Esto le indica al Motor de Aprendizaje que los mensajes seleccionados son spam. Inmediatamente será marcado como `[spam]` y movido a la carpeta de correo no deseado. Los siguientes mensajes de correos se ajustan al mismo patrón, los cuales serán marcados como `[spam]`.

Añadir Spammers a la Lista de Spammers

Si esta utilizando cliente de correo compatible, puede fácilmente añadir los remitentes de los mensajes spam a la lista de Spammers. Siga estos pasos:

1. Abra su cliente de correo.
2. Diríjase a la carpeta de correo no deseado en donde se han movido los mensajes spam.
3. Seleccionar los mensajes marcados como `[spam]` por Acronis Internet Security Suite 2010.
4. Haga clic en el botón **Añadir Spammer** en la barra de herramientas de Acronis Internet Security Suite 2010.
5. Puede pedir que reconozca las direcciones añadidas a la Lista de Spammers. Seleccione **No volver a mostrar este mensaje** y haga clic en **Aceptar**.

Si esta utilizando un cliente de correo diferente, puede añadir spammers manualmente a la Lista de Spammers desde la interfaz de Acronis Internet Security Suite 2010. Es conveniente hacerlo sólo cuando ha recibido bastantes mensajes spam desde la misma de dirección de correo. Siga estos pasos:

1. Abra Acronis Internet Security Suite 2010 y cambie la interfaz de usuario al Modo Avanzado.
2. Haga clic en **Antispam** en el menú de la izquierda.
3. Haga clic en la pestaña **Estado**.

4. Haga clic en **Spammers**. Aparecerá una nueva ventana de configuración.
5. Introduzca la dirección de correo del spammer y haga clic en el botón para añadir la dirección a la lista de Spammers.
6. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

Incrementar el Nivel de Protección Antispam

Para incrementar el nivel de protección antispam, siga estos pasos:

1. Abra Acronis Internet Security Suite 2010 y cambie la interfaz de usuario al Modo Avanzado.
2. Haga clic en **Antispam** en el menú de la izquierda.
3. Haga clic en la pestaña **Estado**.
4. Mueva la barra de la escala hacia arriba.

Reentrenar el Motor de Aprendizaje (Bayesiano)

Antes de entrenar el Motor de Aprendizaje (Bayesiano), prepare una carpeta que contenga sólo mensajes SPAM y otra que contenga sólo mensajes legítimos. El Motor de Aprendizaje analizará estos y aprenderá las características que definen el spam o mensajes legítimos que normalmente recibe. Con el fin de entrenarlo con eficacia, debe hacer más de 50 mensajes en cada carpeta.

Para reiniciar la base de datos Bayesiano y reentrenar el Motor de Aprendizaje, siga estos pasos:

1. Abra su cliente de correo.
2. En la barra de herramientas antispam de Acronis Internet Security Suite 2010, haga clic en el botón **Asistente** para iniciar el asistente de configuración antispam. Se proporciona más información en la sección *"Asistente de Configuración Antispam"* (p. 276).
3. Haga clic en **Siguiente**.
4. Seleccionar **Omitir este paso** y haga clic en **Siguiente**.
5. Seleccionar **Limpiar base de datos del filtro antispam** y haga clic en **Siguiente**.
6. Seleccione la carpeta que contiene mensajes legítimos y haga clic en **Siguiente**.
7. Seleccione la carpeta que contiene mensajes SPAM y haga clic en **Siguiente**.
8. Haga clic en **Finalizar** para iniciar el proceso de aprendizaje.
9. Cuando el aprendizaje se ha completado, haga clic en **Cerrar**.

Solicitar Ayuda

Si esta información no le ayuda, puede contactar con el Soporte de Acronis como se describe en la sección "*Soporte*" (p. 316).

33.4.3. El Filtro Antispam No ha Detectando Ningún Mensaje Spam

Si no se marca el mensaje spam como `[spam]`, esto debe ser un problema con el filtro Antispam de Acronis Internet Security Suite 2010. Antes de resolver este problema, asegúrese que no esta causado por una de las siguientes condiciones:

- La protección Antispam de Acronis Internet Security Suite 2010 está disponible solo para clientes de correo configurados para recibir mensajes de correo mediante el protocolo POP3. Esto significa lo siguiente:
  - ▶ Los mensajes recibidos mediante servicios de correo basados en web (como Yahoo, Gmail, Hotmail u otro) no se filtran como spam por Acronis Internet Security Suite 2010.
  - ▶ Si su cliente de correo esta configurado para recibir mensajes de correo utilizando otro protocolo diferente a POP3 (por ejemplo, IMAP4), el filtro Antispam de Acronis Internet Security Suite 2010 no marcará estos como spam.

  Nota

  POP3 es uno de los protocolos más extensos utilizados para descargar mensajes de correo de un servidor de correo. Si no sabe el protocolo que utiliza su cliente de correo para descargas los mensajes, pregunte a la persona que ha configurado su correo.

- Acronis Internet Security Suite 2010 no analiza el tráfico POP3 de Lotus Notes.

Debe también verificar las siguientes causas posibles:

1. Asegúrese que el Antispam está activado.
   a. Abrir Acronis Internet Security Suite 2010.
   b. Haga clic en el botón **Ajustes** en la esquina superior derecha de la ventana.
   c. En la categoría de ajustes de seguridad, compruebe el estado del antispam.

   Si el Antispam esta desactivado, esto es lo que está causando el problema. Active y monitorice el antispam para ver si el problema se soluciona.
2. Aunque se muy poco probable, debería comprobar si ha configurado (o alguno más) Acronis Internet Security Suite 2010 que no marque los mensajes como `[spam]`.
   a. Abra Acronis Internet Security Suite 2010 y cambie la interfaz de usuario al Modo Avanzado.
   b. Haga clic en **Antispam** en el menú izquierdo y luego en la pestaña **Configuración**

c. Asegúrese que la opción **Marcar los mensajes spam en el asunto** está seleccionada.

Una posible solución esta para reparar o reinstalar el producto. Sin embargo, debería contactar con Acronis Inc para soporte, como se describe en esta sección "*Soporte*" (p. 316).

33.5. Error en la Desinstalación de Acronis Internet Security Suite 2010

Este artículo le ayuda a solucionar los problemas de errores que pueden ocurrir cuando desinstala Acronis Internet Security Suite 2010. Existen dos situaciones posibles:

- Durante la desinstalación, aparece un error en pantalla. La pantalla proporciona un botón para ejecutar una herramienta de desinstalación que limpiará el sistema.
- La instalación se cuelga y, probablemente, su equipo se pare. Haga clic en **Cancelar** para abortar la desinstalación. Si esto no funciona, reinicie el sistema.

Si la desinstalación falla, algunas claves de registro y archivos de Acronis Internet Security Suite 2010 permanecerán en su sistema. Estos restos pueden impedir una nueva instalación de Acronis Internet Security Suite 2010. Además puede afectar al rendimiento y estabilidad del sistema. Con el fin de completar la desinstalación de Acronis Internet Security Suite 2010 de su equipo, debe ejecutar la herramienta de desinstalación.

Si la desinstalación falla con un error en pantalla, haga clic en el botón ejecutar de la herramienta de desinstalación para limpiar su sistema. De lo contrario, proceda de la siguiente manera:

1. Contactar con el soporte técnico de Acronis Inc. como se detalla en "*Soporte*" (p. 316) y pregunte por la herramienta de desinstalación.
2. Ejecute la herramienta de desinstalación utilizando privilegios administrativos. La herramienta de desinstalación eliminará todos los archivos y claves del registro que no hayan sido eliminadas durante el proceso de desinstalación automático.
3. Reinicie el equipo.

Si esta información no le ayuda, puede contactar con el Soporte de Acronis como se describe en la sección "*Soporte*" (p. 316).

34. Soporte

Si tiene alguna pregunta sobre nuestros productos, o si necesita asistencia, visite nuestro sitio web en http://www.acronis.es.

Glosario

ActiveX

El ActiveX es un modelo para escribir programas de manera que otros programas y sistemas operativos puedan usarlos. La tecnología ActiveX se utiliza junto con Microsoft Internet Explorer para hacer páginas web interactivas que se vean y comporten como programas, y no como páginas estáticas. Con ActiveX, los usuarios pueden hacer o contestar preguntas, pulsar botones, interactuar de otras formas con una página web. Los controles ActiveX normalmente se escriben en Visual Basic.

ActiveX es notable por la ausencia absoluta de mandos de seguridad; los expertos de la seguridad computacional desaprueban desalientan el empleo de ActiveX en Internet.

Adware

El Adware habitualmente se combina con aplicaciones que son gratuitas a cambio que el usuario acepte la instalación del componente adware. Puesto que las aplicaciones adware generalmente se instalan después que el usuario acepte los términos de licencia que declaran el propósito de la aplicación, no se comete ningún delito. Sin embargo, los pop-up de publicidad pueden resultar molestos, y en algunos casos afectar al rendimiento del sistema. Además, la información que recopilan algunas de estas aplicaciones puede causar preocupación acerca de su privacidad a aquellos usuarios que no son plenamente conscientes de los términos de la licencia.

Sin embargo, las ventanas emergentes de publicidad pueden resultar molestas, y en algunos casos afectar al rendimiento del sistema. Además, la información que recopilan algunas de estas aplicaciones pueden causar problemas de privacidad a aquellos usuarios que no eran plenamente conscientes de los términos de la licencia.

Archivo Comprimido

Disco, cinta o directorio conteniendo ficheros almacenados.

Fichero conteniendo uno o varios ficheros en formato comprimido.

Backdoor

Se trata de un agujero de seguridad dejado intencionalmente por los diseñadores o los administradores. El objetivo de estos agujeros no es siempre dañino; algunos sistemas operativos funcionan con unas cuentas privilegiadas, creadas para los técnicos de servicio u operadores de mantenimiento.

Sector de arranque

Un sector al principio de cada disco y que identifica la arquitectura del disco (tamaño del sector, tamaño del cluster, etc). Para los discos de inicio, el sector de arranque también incluye un programa para cargar el sistema operativo.

Virus de boot

Es un virus que infecta el sector de arranque de un disco duro o disquete. Al intentar arrancar el sistema desde un disco infectado con un virus de boot, el virus quedará cargado en la memoria. A partir de ese momento, cada vez que intente arrancar el sistema, tendrá el virus activo en la memoria.

Explorador

Forma abreviada de Navegador de Web, aplicación de software empleada para ubicar y cargar las páginas web. Los dos navegadores más populares son Netscape Navigator y Microsoft Internet Explorer, sendos navegadores gráficos, lo cual significa que pueden mostrar tanto gráficos como textos. Además, la mayoría de los navegadores modernos incluyen información multimedia: sonido e imágenes, aunque requieran plugins para ciertos formatos.

Línea de comando

En una interfaz con línea de comando, el usuario puede introducir comandos en el espacio provisto directamente en la pantalla, usando un lenguaje de comando.

Cookie

En la industria del Internet, las cookies se describen como pequeños ficheros conteniendo información sobre los ordenadores individuales que se pueden analizar y usar por los publicistas para determinar los intereses y los gustos online de los usuarios respectivos. En este ambiente, la tecnología de las cookies se desarrolla con la intención de construir reclamos y mensajes publicitarios correspondientes a los intereses declarados por usted. Es un arma de doble filo para mucha gente porque, por un lado, es más eficiente y pertinente que usted vea publicidades relacionadas con sus intereses. Por otro lado, implica seguir cada paso suyo y cada clic que usted haga. Por consiguiente, es normal que haya resultado un debate sobre la privacidad y mucha gente se sintió ofendida por la idea de ser vista como "número de SKU" (el código de barras ubicado en la parte posterior de los paquetes analizados a la salida de los supermercados). Aunque esta perspectiva pueda parecer extremista, en algunos casos es cierta.

Unidad de disco

Es un dispositivo que lee la información y / o la escribe en un disco.

Una unidad de disco duro lee y escribe en los discos duros.

Una unidad de disquetera abre disquetes.

Las unidades de disco pueden ser internas (guardadas en el ordenador) o externas (guardadas en una caja separada conectada al ordenador).

Descargar

Para copiar informaciones (por lo general un fichero entero) desde una fuente principal a un dispositivo periférico. El término se usa a menudo para describir el proceso de copiar un fichero desde un servicio online al ordenador personal.

También se refiere al proceso de copiar ficheros desde un servidor de la red a un ordenador conectado a la red.

E-mail

Correo electrónico. Un servicio que envía mensajes a otros ordenadores mediante las redes locales o globales.

Eventos

Una acción o acontecimiento detectado por un programa. Los eventos pueden ser acciones, como por ejemplo hacer clic con el ratón o pulsar una tecla, o también pueden ser acontecimientos (agotar el espacio de memoria).

Falso positivo

Ocurre cuando un analizador identifica un fichero infectado, cuando de hecho éste no lo es.

Extensión de un archivo

La última parte del nombre de un fichero, que aparece después del punto e indica el tipo de información almacenada.

Hay varios sistemas operativos que utilizan extensiones de archivos (Por Ej. Unix, VMS, MS-DOS). Por lo general las extensiones tienen de uno a tres caracteres. Por ejemplo, "c" para archivos de código fuente en lenguaje C, "ps" para PostScript, "txt" para documentos de texto.

Heurístico

Es un método para identificar nuevos virus, que se basa en ciertas reglas y no en firmas específicas de los virus. La ventaja del análisis heurístico reside en la dificultad de engañarlo con una nueva versión de un virus ya existente. Sin embargo, ocasionalmente puede notificar sobre la existencia de unos códigos sospechosos en los programas normales, generando el "falso positivo".

IP

Internet Protocol - pertenece a la gama de protocolos TCP/IP y es responsable. Toda la comunicación en Internet se realiza mediante los dos protocolos para el intercambio de información: El Transmission Control Protocol (TCP, o Protocolo de Control de Transmisión) y el Internet Protocol (IP, o Protocolo de Internet). Estos protocolos son conocidos, en forma conjunta, como TCP/IP. No forman un único protocolo sino que son protocolos separados, pero sin embargo están estrechamente comunicados para permitir una comunicación más eficiente.

Applet de Java

Es un programa de Java diseñado para funcionar solamente en una página web. Para usarlo tendría que especificar el nombre del applet y la dimensión (de ancho y de largo --- en pixels) que éste usará. Al acceder a una página web, el navegador descarga el applet desde un servidor y lo abre en el ordenador del usuario (del cliente). Los applets difieren de las aplicaciones al ser gobernados por un protocolo de seguridad muy estricto.

Por ejemplo, aunque los applets se puedan ejecutar directamente en el ordenador del cliente, no pueden leer o escribir información en aquel ordenador. Además, los applets tienen restricciones en cuanto a leer y escribir información desde la misma área a la que pertenecen.

Virus de macro

Es un tipo de virus informático, que se encuentra codificado como un macro incluido en un documento. Muchas aplicaciones, como las de Microsoft Word o Excel, soportan fuertes lenguajes de macro.

Estas aplicaciones permiten introducir un macro en un documento y también que el macro se ejecute cada vez que se abra el documento.

Cliente de mail

Un cliente de e-mail es una aplicación que permite enviar y recibir mensajes.

Memoria

Área de almacenamiento interno en un ordenador. El término memoria se refiere al almacenamiento de información en forma de virutas y la palabra almacenamiento se emplea para la memoria guardada en cintas o disquetes. Cada ordenador tiene una cierta cantidad de memoria física, generalmente denominada memoria principal o RAM.

No Heurístico

Este método de análisis se basa en firmas de virus especificas. La ventaja del análisis no heurístico es que no se le puede engañar por algo que parecería ser un virus. Por consiguiente, no genera alarmas falsas.

Programas Empaquetados

Son ficheros en formato comprimido. Muchos sistemas operativos y varias aplicaciones contienen comandos que le permiten a usted empaquetar un fichero para que ocupe menos espacio en la memoria. Por ejemplo: tiene un fichero de texto conteniendo diez caracteres espacio consecutivos. Normalmente, para esto necesitaría diez bytes de almacenamiento.

Sin embargo, un programa que puede empaquetar ficheros podría reemplazar los caracteres mencionados por una serie a la que le sigue el número de espacios. En este caso, los diez espacios requieren dos bytes. Ésta es solamente una técnica para empaquetar programas o ficheros, hay muchas otras también.

Ruta

Las direcciones exactas de un fichero en un ordenador, generalmente descritas mediante un sistema jerárquico: se empieza por el límite inferior, mostrando un listado que contiene la unidad de disco, el directorio, los subdirectorios, el fichero mismo, la extensión del fichero si tiene alguna. Esta suma de informaciones es una ruta completamente válida.

La ruta entre dos puntos, como por ejemplo el canal de comunicación entre dos ordenadores.

Phishing

Es el acto de enviar un e-mail a un usuario simulando pertenecer a una empresa existente, e intentar estafarlo solicitándole información privada con la que después se efectuará el robo. El e-mail conduce al usuario a visitar una página Web en la que se le solicita actualizar información personal, como contraseñas y números de tarjetas de crédito, seguridad social y números de cuentas corrientes, que en realidad ya posee la organización auténtica. La página Web, en cambio, es una réplica fraudulenta, creada sólo para robar la información de los usuarios.

Virus Polimórfico

Son virus que se modifican en cada fichero que infectan. Al no tener una secuencia binaria constante, son muy difíciles de identificar.

Puerto

Interfaz en un ordenador a la que se puede conectar un dispositivo. Los ordenadores personales tienen distintos tipos de puertos. Hay varios puertos internos para conectar las unidades de disco, las pantallas, los teclados. Asimismo, los ordenadores personales tienen puertos externos para conectar módems, impresoras, ratones y otros dispositivos periféricos.

En las redes de tipo TCP/IP y UDP representa el punto final de una conexión lógica. El número de puerto indica el tipo del dicho puerto. Por ejemplo, el puerto 80 se usa para el tráfico http.

Archivo de informe

Es un fichero que lista las acciones realizadas. Acronis Internet Security Suite 2010 genera un archivo de informe (log) que contiene una lista de las rutas analizadas, las carpetas, el número de archivos y archivos comprimidos analizados, el número de archivos infectados y sospechosos que se han detectado.

Rootkit

Un rootkit es un conjunto de herramientas de software que ofrecen acceso al sistema a nivel de administrador. El término empezó a usarse con los sistemas operativos UNIX y se refería a las herramientas que proporcionaban permisos de administrador a los intrusos, permitiéndoles ocultar su presencia para no ser vistos por los administradores de sistema.

El papel principal de los rootkits es ocultar procesos, archivos, conexiones y logs. También pueden interceptar datos de terminales, conexiones de red o periféricos, si éstos incorporan el software apropiado.

Los rootkits no son maliciosos por naturaleza. Por ejemplo, los sistemas operativos y algunas aplicaciones esconden sus archivos críticos mediante rootkits. Sin embargo, normalmente se utilizan para esconder la presencia de malware o para encubrir la presencia de un intruso en el sistema. Cuando se combinan con malware, los rootkits representan una gran amenaza para la

seguridad e integridad de su sistema. Pueden monitorizar el tráfico, crear puertas traseras en el sistema, alterar archivos o logs, y evitar su detección.

Script

Es otro término para macro o fichero batch y se constituye de una lista de comandos que se pueden ejecutar sin la intervención del usuario.

Spam

Correo basura o los posts basura en grupos de noticias, también denominado correo no solicitado.

Spyware

Se trata de cualquier software que, en secreto, recopile información del usuario a través de su conexión a Internet sin su consentimiento, generalmente con fines comerciales. Las aplicaciones Spyware son, generalmente, componentes ocultos de programas freeware o shareware que pueden descargarse por Internet; sin embargo, debe observarse que la gran mayoría de aplicaciones shareware y freeware no contienen spyware. Una vez instalado, el spyware monitoriza la actividad del usuario en Internet y, en segundo plano, envía esa información a una tercera persona. El spyware también puede recoger información acerca de las direcciones de correo, e incluso contraseñas y números de tarjetas de crédito.

El spyware es similar al Troyano en el hecho que los usuarios los instalan inconscientemente cuando instalan otra aplicación. Una forma habitual de infectarse con spyware es descargando, a través de programas de intercambio de ficheros, un determinado archivo que intercambia el nombre de los productos compartidos.

A parte de las cuestiones de ética y privacidad, el spyware roba al usuario recursos de memoria y ancho de banda mientras envía la información al creador del Spyware a través de la conexión de Internet del usuario. Puesto que el spyware utiliza memoria y recursos del sistema, las aplicaciones que se ejecutan en segundo plano pueden provocar errores del sistema o inestabilidad general del mismo.

Elementos en Inicio

Todos los ficheros de esta carpeta se abren al iniciar el ordenador. Por ejemplo: una pantalla, un fichero audio, un calendario de tareas u otras aplicaciones pueden ser elementos de startup. Normalmente, se elige un alias del fichero para ubicar en esta carpeta y no directamente el fichero.

Área de notificación del Sistema

Elemento introducido con el sistema Windows 95,la bandeja de sistema está ubicada en la parte de debajo de la pantalla, al lado del reloj y contiene iconos miniaturales para acceder fácilmente a las funciones del sistema, como el fax, la impresora, el módem, el volumen etc. Al hacer doble clic o clic derecho en

el icono correspondiente, verá y abrirá los detalles y los mandos de los programas.

TCP/IP

Transmission Control Protocol/Internet Protocol - Es una gama de protocolos de red, extremadamente utilizados en Internet para proporcionar comunicaciones en las redes interconectadas, que incluyen ordenadores con distintas arquitecturas de hardware y varios sistemas operativos. TCP/IP ofrece estándares para el modo de comunicación entre ordenadores y convenciones para las redes interconectadas.

Troyano

Es un programa destructivo disfrazado como aplicación benigna. A diferencia de los virus, los caballos troyanos no se multiplican; sin embargo pueden ser igual de peligrosos. Unos de los tipos más insidiosos de Troyano es un programa que pretende desinfectar su ordenador y que en realidad introduce virus.

El término tiene origen en la famosa obra "La Ilíada" de Homero, en la cual Grecia entrega un gigantesco caballo de madera a sus enemigos, los Troyanos, como supuesta oferta de paz. Pero una vez los Troyanos arrastraron el caballo hasta el interior de las murallas de la ciudad, los soldados Griegos salieron de un hueco del vientre del caballo y abrieron las puertas de las murallas, permitiendo la entrada de sus compatriotas y la conquista de Troya.

Actualizar

Una nueva versión de un producto de software o hardware, diseñada para reemplazar una versión anterior del mismo producto. Además, durante la instalación se verifica si en su ordenador existe una versión anterior; si no se encuentra ninguna, no se instalará la actualización.

Acronis Internet Security Suite 2010 tiene su propio módulo para realizar las actualizaciones, permitiéndole a usted buscar manualmente las actualizaciones o bien hacer una actualización automática del producto.

Virus

Es un programa o una parte de un código cargado en su ordenador sin avisarle y en contra de su voluntad. La mayoría de los virus se pueden multiplicar. Todos los virus informáticos son artificiales, creados por una persona. Es muy simple producir un virus que se multiplique continuamente. Pero, aún así, sería muy peligroso porque dentro de poco tiempo estaría usando toda la memoria disponible y llevaría al bloqueo del sistema. Un tipo de virus todavía más peligroso es uno capaz de propagarse a través de redes y evitando los sistemas de seguridad.

Firma de virus

Es la secuencia binaria de un virus, utilizada por los antivirus para detectar y eliminar los virus.

Gusano

Es un programa que se propaga a través de la red, reproduciéndose mientras avanza. No se puede agregar a otros programas.