Introdução

Panda Antivirus

O **Panda Antivirus** é uma solução completa e eficaz para manter protegido o seu computador face a qualquer tipo de vírus. Incluem-se versões Windows 95, Windows NT Workstation, Windows 3.1x, DOS e OS/2 para que você esteja protegido seja qual for o seu sistema operativo. Esta ajuda é a correspondente ao **Panda Antivirus** para Windows NT Workstation.

Estratégias de protecção

O **Panda Antivirus** compreende várias estratégias de protecção frente aos vírus:

- **Protecção permanente:** a protecção permanente se encarrega de proteger o computador face aos vírus em todo o momento e sem requerer a intervenção do utilizador. A grande vantagem desta estratégia de protecção, é que permite ter protegido o computador de uma forma completamente automática.
- **Análise sob solicitação:** a análise sob solicitação permite analisar qualquer parte do computador a pedido do utilizador. Deve escolher-se a área a analisar e nesse momento começará a análise à procura de vírus na área assinalada.
- **Desinfecção:** uma vez encontrado um vírus, há várias possíveis acções a levar a cabo. Uma delas é a desinfecção que consiste em eliminar o vírus do ficheiro deixando este tal e como estava antes da infecção.
- **Análise heurística:** a análise heurística é uma técnica de análise alternativa às já mencionadas. A análise heurística funciona sob solicitação. Ou seja, o utilizador deve indicar que área do computador deseja analisar com este método em um momento determinado. Esta técnica de análise está preparada para encontrar vírus desconhecidos.
- **Procura de cadeias:** do mesmo modo que a análise heurística, é uma técnica de análise alternativa e também funciona sob pedido do utilizador. A sua utilidade é a procura de novos vírus a partir de dados oferecidos pelo suporte técnico da Panda Software.
- **Outras opções:** sob este item se englobam certas capacidades do antivírus destinadas a oferecer informação ou a facilitar a gestão do mesmo. Por exemplo, conta-se com um relatório de resultados no que se possam ver as diferentes incidências e operações que se tenham levado a cabo com o antivírus.

Soluções antivírus Panda Software

A Panda Software lhe oferece as seguintes soluções antivírus:

- **24h-365d® Seguro Antivirus® para PCs Individuais**. *Licenças.*
- **24h-365d® Seguro Antivirus® para PCs em rede** (distribuição automática desde servidores).
- **24h-365d® Seguro Antivirus® para Servidores de rede** (Novell NetWare e Windows NT Server).
- **24h-365d® Seguro Antivirus® para Redes Locais**.
- **24h-365d® Seguro Antivirus® para clientes de e-mail e Groupware**.
- **24h-365d® Seguro Antivirus® para Servidores de e-mail e Groupware**.
- **24h-365d® Seguro Antivirus® para Servidores de Correio SMTP**.
- **24h-365d® Seguro Antivirus® para PCs conectados a Internet**.
- **24h-365d® Seguro Antivirus® para Servidores de Internet (SMTP, FTP e HTTP)**.

- **24h-365d® Seguro Antivirus® para Proxys**.

O que é o 24h-365d Seguro Antivirus Panda Software?

O **24h-365d® Seguro Antivirus® Panda Software**, é um novo e revolucionário conceito de protecção antivírus que fornece ainda mais segurança. O **24h-365d® Seguro Antivirus® Panda Software** é uma extraordinária combinação de produtos e serviços que oferece os mais altos níveis de protecção face aos vírus. O **24h-365d® Seguro Antivirus® Panda Software** pode ser contratado com diferentes tempos de direito a actualizações e com diferentes períodos de actualização.

O produto o fornece o **Panda Antivirus**, um antivírus que conseguiu os certificados mais exigentes em detecção de vírus como são:

- O **Certificado ICSA:** outorgado pela prestigiosa organização norte-americana ICSA aos produtos antivírus que detectam periodicamente 100% dos vírus *In the Wild* (os vírus mais estendidos em cada momento) e mais de 90% da *Zoo Collection* (colecção de milhares de vírus menos estendidos).
- O **Certificado CheckMark:** outorgado pela revista inglesa especializada em Segurança Informática *Secure Computing*.

Se você não dispõe do **24h-365d® Seguro Antivirus® Panda Software**, pode contratá-lo utilizando a ordem de encomenda incluída no cartão de registo. Os serviços oferecidos pelo **24h-365d® Seguro Antivirus® Panda Software** são os seguintes:

- **Hot-Line:** durante UM ano solucionaremos os seus problemas técnicos por telefone, fax, Internet ou e-mail. Ligue quando ligue, a qualquer hora do dia ou da noite, você encontrará técnicos do outro lado, pessoas altamente qualificadas que estão a sua disposição 24 horas ao dia, os 365 dias do ano. Este é um serviço exclusivo da **Panda Software**.
- **S.O.S. Virus:** se você encontra algum vírus que o **Panda Antivirus** não detecta ou não elimina, enviaremos um mensageiro a seu domicílio (ou recolheremos a amostra suspeita de qualquer outro modo) e em menos de 24 horas desenvolveremos uma nova versão capaz de detectar e eliminar o novo vírus. Enviaremos-lhe esta nova versão sem custo algum.
- **Serviço de Actualizações com entrega a domicílio:** o seu antivírus estará totalmente actualizado. Você receberá em seu próprio domicílio actualizações mensais ou trimestrais em CD ou em disquetes se contratou a nossa solução **24h-365d® Seguro Antivirus® Panda Software**. Também poderá actualizar o produto através do nosso WEB tantas vezes quanto deseje durante um ano, garantindo-lhe no mínimo uma actualização nova a cada dia.
- **Serviço WEB:** resolução das dúvidas mais frequentes e informação sobre vírus.

Instalação

Requisitos

Para instalar o **Panda Antivirus** para Windows NT Workstation precisa-se dos seguintes elementos:

- Computador compatível com IBM com processador 486 ou superior.
- 16 Mb de RAM.
- 4 Mb de espaço em disco rígido.
- Sistema operativo Windows NT 3.51 ou superior.
- Unidade de CD-ROM.
- Rato.

Procedimento de instalação

Há duas versões do **Panda Antivirus** para Windows NT Workstation. Uma delas corresponde à versão 3.51 do mencionado sistema operativo e a outra à versão 4.0. Deve ter-se a precaução de instalar a versão correspondente a cada sistema operativo.

Ambas as versões podem instalar-se unicamente desde o CD-ROM que acompanha o produto. Para instalar qualquer uma das duas versões, há que executar o programa CDMENU.COM. Este programa apresenta um simples menu de opções. Em primeiro lugar há que escolher o idioma desejado e logo a versão que se quer instalar. Neste caso se deve escolher uma das duas versões do **Panda Antivirus** para Windows NT, a 3.51 ou a 4.0 em função do sistema operativo que se tenha instalado.

Para poder instalar a versão do **Panda Antivirus** para Windows NT Workstation é necessário que tenha direitos de administrador sobre a sua máquina. Isto é assim devido aos direitos necessários para instalar o driver que se encarrega da protecção permanente.

O procedimento de instalação consta dos seguintes passos:

1. Em primeiro lugar se apresenta um ecrã de boas-vindas.
2. Em seguida perguntam-se os dados do utilizador.
3. Pede-se o directório no que se deseja instalar a aplicação.
4. Solicita-se o grupo de programas no que se criarão os ícones de acesso ao antivírus.
5. Dá-se a escolher se se quer instalar a protecção permanente (driver **Sentinel**) ou não.
6. Começa a cópia de ficheiros ao disco rígido.
7. Uma vez que tenha acabado a cópia de ficheiros, recomenda-se reiniciar a máquina para que a protecção permanente entre em funcionamento.

Actualização do antivírus

Para actualizar uma versão com uma actualização recebida, basta instalar a nova versão sobre a antiga.

Desinstalação

Se se trata da versão para Windows NT 3.51, a desinstalação do **Panda Antivirus** se realiza mediante o programa UNINST que se encontra no grupo de programas da aplicação.

Se se trata da versão para Windows NT 4.0, a desinstalação do **Panda Antivirus** se realiza mediante a opção *Acrescentar ou tirar programas* do *Painel de Controlo*. Basta escolher **Panda Antivirus Windows NT W/S 4.0** da lista que se apresenta em dita opção e premir o botão *Acrescentar ou Tirar*. Para completar a desinstalação, é necessário reiniciar a máquina.

Não se deve tentar desinstalar a versão apagando a pasta onde tenha instalado o antivírus. Desinstale sempre seguindo o procedimento descrito.

O que é a protecção permanente

A protecção permanente é um programa que, desde o arranque da máquina, intercepta todas aquelas operações que supõem risco de contágio para verificar que nenhum vírus entre no sistema.

A protecção permanente funciona de maneira totalmente automática e sem requerer nenhuma intervenção por parte do utilizador. Apesar da vigilância constante, o rendimento do sistema não se vê afectado pelo que a instalação da protecção permanente é sempre aconselhável dado que aumenta consideravelmente a protecção do computador.

Como se usa a protecção permanente

A protecção permanente é uma das opções da instalação. Se se escolheu instalar a referida protecção, uma vez que se arranque a máquina, a protecção permanente (**Sentinel**) estará em funcionamento.

Se o sistema operativo é Windows NT Workstation 3.51, o **Sentinel** aparecerá como um ícone minimizado no escritório de Windows. Se o sistema operativo é Windows NT Workstation 4.0, o **Sentinel** aparecerá como um ícone junto ao relógio situado na barra de tarefas.

O funcionamento da protecção permanente é totalmente automático. Se, em alguma operação, o **Sentinel** detectar a presença de um vírus, avisaria de tal circunstância e levaria a cabo a acção pertinente.

Como se configura a protecção permanente

A protecção permanente pode ser configurada para se adaptar às necessidades de cada utilizador. Fazendo duplo clique sobre o ícone do **Sentinel**, aparece uma janela com várias fichas. Cada uma delas faz referência à configuração dos diferentes aspectos do **Sentinel**. As opções de configuração são as seguintes:

Estado

Nesta ficha se define o estado da protecção permanente.

- **Activado:** mediante esta opção, activa-se ou desactiva-se a protecção permanente. Há que ter em conta que, se se desactiva a protecção permanente, o computador ficará desprotegido face aos vírus.
- **Entradas:** estando a protecção permanente activada, esta opção indica que se devem analisar todas aquelas entradas de ficheiros na máquina. Também se analisarão as criações de ficheiros e as modificações dos mesmos.
- **Saídas:** estando a protecção permanente activada, esta opção indica que se devem analisar todas aquelas saídas de ficheiros da máquina. Analisar-se-ão também todas as aberturas e execuções de ficheiros.
- **Renomeado:** estando a protecção permanente activada, esta opção indica que se devem analisar, à procura de vírus, todas as operações de renomeação de ficheiros.
- **Rede Microsoft:** se a protecção permanente está activada, esta opção indica que se devem analisar em remoto todas as operações efectuadas sobre uma unidade de rede Microsoft.
- **Rede Novell:** se está activa a protecção permanente, esta opção indica que se analisem em remoto todas as operações efectuadas sobre uma unidade de rede Novell.

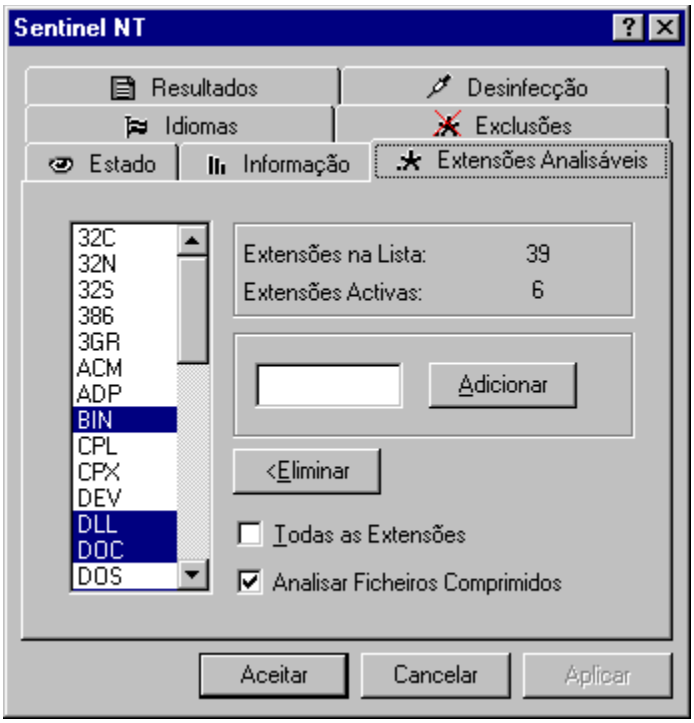
Informação

Nesta ficha se mostram diversas informações referentes à actividade da protecção permanente.

- **Revisados:** indica o número de ficheiros que a protecção permanente revisou, à procura de vírus, desde o início do sistema.
- **Infectados:** esta informação mostra o número de ficheiros infectados que se encontraram.
- **Desinfectados:** indica o número de ficheiros desinfectados pela protecção permanente.
- **Renomeados:** mostra-se aqui o número de ficheiros que a protecção permanente renomeou.
- **Apagados:** neste ponto se mostra o número de ficheiros apagados pela protecção permanente por estarem contaminados com vírus.
- **Movidos:** informa-se aqui de quantos ficheiros moveu a protecção permanente por estarem contaminados com vírus.
- **Vírus encontrados:** por último, indica-se aqui quantos vírus se encontraram.

Extensões analisáveis

Neste item se configuram as extensões que a protecção permanente deve analisar.



- **Lista de extensões:** na lista de extensões se podem marcar todas aquelas extensões que se desejam analisar. A protecção permanente intercepta sempre todos os ficheiros aos que se acede, porém somente analisará aqueles ficheiros que tenham uma das extensões seleccionadas. Independentemente da selecção de extensões que se faça, os ficheiros EXE e COM serão analisados sempre.
- **Extensões em lista:** este dado informa do número de extensões que há na lista.
- **Extensões activas:** este dado informa das extensões que se marcaram na lista para analisar.
- **Acrescentar extensão:** para acrescentar uma extensão à lista, deve escrever-se a extensão na casinha para tal efeito e premir o botão *Acrescentar*.
- **Eliminar extensão:** para eliminar uma extensão da lista, deve seleccionar-se na lista a extensão a eliminar e premir o botão *Eliminar*.
- **Todos os ficheiros:** se se marca esta opção, analisar-se-ão todos os ficheiros independentemente das extensões que se tenham seleccionado.
- **Analisar ficheiros comprimidos:** se se marca esta opção, analisar-se-ão os ficheiros comprimidos aos que se aceda.

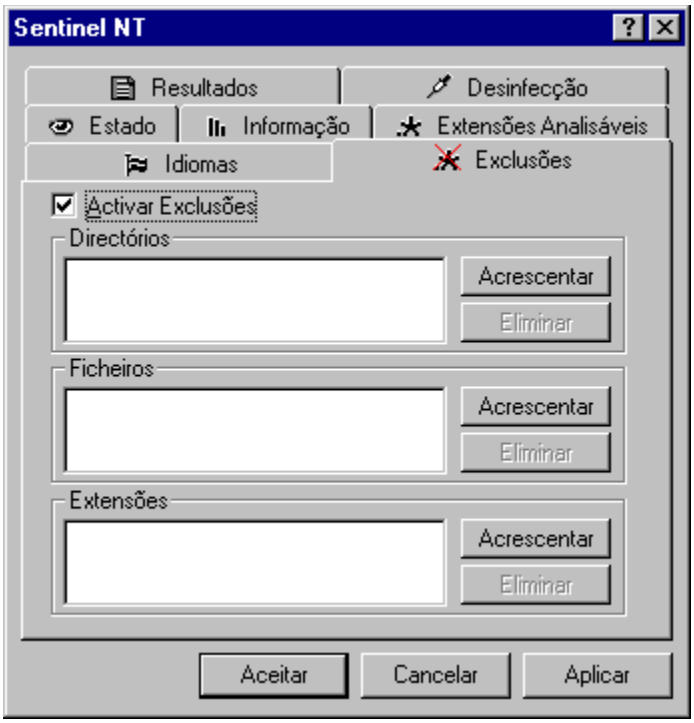
Idiomas

Nesta ficha se pode consultar o idioma no que se encontra a protecção permanente e também se pode escolher outro idioma na lista de idiomas disponíveis.

- **Idiomas disponíveis:** mostra-se uma lista com os diferentes idiomas disponíveis para a protecção permanente. Para mudar de idioma, basta seleccionar o idioma desejado e premir o botão *Aceitar* ou o botão *Aplicar*.
- **Idioma actual:** aqui se mostra o idioma no que se encontra nesse momento a protecção permanente.

Exclusões

Nesta ficha se podem indicar aquelas áreas, ficheiros ou extensões que não se desejem analisar. Independentemente do que se tenha indicado em *Extensões*, todas aquelas áreas, ficheiros ou extensões que se marquem aqui, **não se analisarão**.



- **Activar exclusões:** se se marca esta opção, activar-se-á a função de exclusão em função dos dados que se tenham indicado.
- **Directório:** neste item se mostra uma lista com todos aqueles directórios que não se deverão analisar.
- **Acrescentar directório:** mediante esta opção, podem-se acrescentar directórios à lista de directórios que não se analisarão.
- **Eliminar directório:** mediante esta opção, podem-se eliminar directórios da lista de directórios que não se analisarão.
- **Ficheiro:** neste item se mostra uma lista com os ficheiros que não se devem analisar.
- **Acrescentar ficheiro:** esta opção permite acrescentar um ficheiro à lista de ficheiros que não se analisam.
- **Eliminar ficheiro:** esta opção permite eliminar um ficheiro da lista de ficheiros que não se analisam.
- **Extensões:** neste item se mostra uma lista das extensões que não se devem analisar. Ainda que alguma destas extensões esteja na lista de extensões a analisar, não se analisará.
- **Acrescentar extensão:** graças a esta opção, pode-se acrescentar uma extensão à lista de extensões não analisáveis.
- **Eliminar extensão:** graças a esta opção, pode-se eliminar uma extensão da lista de extensões que não se analisam.

Resultados

Nesta ficha se configura o comportamento do sistema de relatórios de incidências encontradas pela protecção permanente.

- **Gerar relatório local:** se se activa esta opção, gerar-se-á um relatório com as diferentes incidências que encontre a protecção permanente.
- **Utilizador:** aqui se mostra o nome do utilizador da máquina.
- **Ver relatório:** este botão mostra o relatório com as incidências encontradas até o presente momento.
- **Imprimir relatório:** graças a este botão, pode-se imprimir o relatório de incidências.
- **Apagar relatório:** mediante este botão, pode-se apagar o relatório de incidências.

Desinfecção

Nesta ficha se configura o comportamento da desinfecção de ficheiros contaminados por vírus e detectados pela protecção permanente.

- **Cancelar:** se se marca esta opção, a operação na que se tenha detectado o vírus será cancelada. Se, por exemplo, o vírus foi detectado em um ficheiro que se tentava executar, cancelar-se-á a execução do mencionado ficheiro.
- **Ignorar:** com esta opção marcada, ainda que se encontre um vírus será ignorado o respectivo facto.
- **Desinfectar:** se se marca esta opção e a protecção permanente detecta um vírus, procederá a sua desinfecção deixando o ficheiro contaminado tal e como estava antes da infecção.
- **Renomear arquivo:** com esta opção marcada, se se detecta um vírus, o **Sentinel** renomeará o ficheiro para que tenha extensão VIR.
- **Apagar arquivo:** se se marca esta opção e o **Sentinel** detecta um vírus em um ficheiro, proceder-se-á a apagar o referido ficheiro.
- **Se não se pode desinfectar, renomear arquivo:** se esta opção está activa, quando o **Sentinel** detecte um vírus e tente desinfectá-lo, no caso de não poder realizar tal operação com êxito, o ficheiro será renomeado.
- **Se não se pode desinfectar, apagar arquivo:** se esta opção está activa, quando o **Sentinel** detecte um vírus e tente desinfectá-lo, no caso de não poder realizar a respectiva operação com êxito, o ficheiro será apagado.

O que é a análise sob solicitação

A análise sob solicitação lhe permite analisar qualquer área do seu computador no momento que você escolha. Cada análise que se realiza se pode configurar mediante um conjunto de simples opções.

Como se usa a análise sob solicitação

Para realizar uma análise sob solicitação, há que levar a cabo os seguintes passos:

1. **Executar o antivírus:** para executar o antivírus, vá ao grupo de programas onde se tenham criado os ícones que permitem a sua execução. Faça duplo clique sobre o ícone *Panda Antivirus*.
2. **Ir ao item de análise:** para ir a este item, prima o botão *Analisar* na barra de botões da aplicação. Aparecerá uma janela para especificar o que é que se deve analisar e como se deve fazê-lo.
3. **Escolher a área de análise:** deve escolher-se a área que se deseja analisar. Em uma lista se mostram as diferentes unidades reconhecidas no sistema. Também se pode indicar um directório ou um ficheiro concreto mediante os botões para tal efeito.
4. **Configurar as extensões:** este passo é opcional. O programa guarda a configuração das extensões que se querem analisar. Portanto, uma vez configuradas, não há porque repetir a configuração em cada análise.
5. **Configurar as opções de análise:** este passo também é opcional. O programa guarda a configuração das opções de análise. Portanto, uma vez configurada a análise, não há porque repetir a configuração em cada análise. Só se deverá variar a dita configuração quando se deseje escolher um conjunto de opções diferente. Conta com uma explicação mais detalhada das opções de análise nesta mesma documentação no item de configuração.
6. **Indicar se se quer analisar unicamente o boot:** este passo é opcional. Se se marca esta opção, das unidades seleccionadas só se analisará o boot e não os ficheiros. Se não se marca esta opção, serão analisados tanto o boot como os ficheiros em todas as unidades seleccionadas.
7. **Começar a análise:** o botão *Analisar* dá começo à análise à procura de vírus nas áreas seleccionadas e com as opções escolhidas.

Como se configura a análise sob solicitação

Tal e como se mencionou, em uma análise se deve indicar:

- Que área se quer analisar.
- Que extensões se considerarão na análise.
- Como se vai levar a cabo a análise.

A configuração de uma análise compreende indicar quais extensões vão-se considerar e as opções de análise.

Extensões

Premindo o botão *Extensões* aparece uma janela que permite indicar quais extensões se desejam analisar.

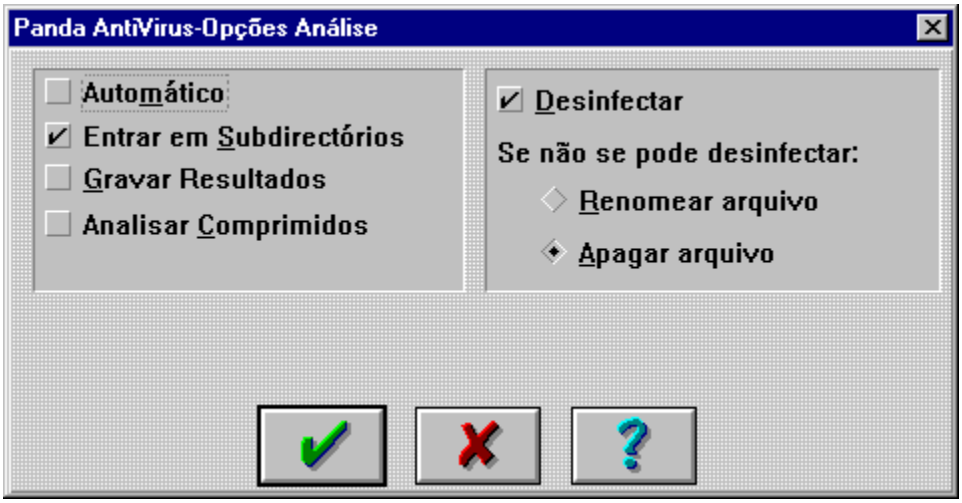
A opção *Todas* sobre a lista de extensões indica que se analisarão todos os ficheiros com independência da sua extensão. Se esta opção não está marcada, só se analisarão os ficheiros cuja extensão coincida com alguma das da lista.

Dois botões permitem acrescentar e eliminar extensões à lista. Por defeito, proporciona-se uma lista com as extensões mais comuns e uma selecção daquelas extensões susceptíveis de albergar vírus.

Independentemente da selecção de extensões que se faça, os ficheiros EXE e COM serão analisados sempre.

Opções de análise

Premindo o botão *Opções* aparece uma janela que permite escolher as opções de análise que são as seguintes:



- **Automático:** se se marca esta opção, o processo de análise será completamente automático. Se se encontram vírus, o processo informará disso porém continuará e não se verá interrompido. Isto é especialmente útil quando o computador tem muitos ficheiros infectados e se estão a desinfectar.
- **Entrar em subdirectórios:** se se marca esta opção, analisar-se-ão os subdirectórios encontrados nas áreas que se estejam a analisar. Se não se marca a dita opção, não se analisarão os subdirectórios encontrados com o que se se escolhe analisar uma unidade porém não se marca esta opção, unicamente analisar-se-á o directório raiz da mesma.
- **Gravar resultados:** se se marca esta opção, os dados relativos à análise em questão serão registrados no ficheiro de resultados.
- **Analisar comprimidos:** se se marca esta opção, analisar-se-ão os ficheiros comprimidos que se encontrem.
- **Desinfectar:** se se marca esta opção e se encontra um vírus, o antivírus tratará de desinfectá-lo.
- **Se não se pode desinfectar, renomear:** se se marca esta opção e se encontra um vírus que o antivírus não pode desinfectar, proceder-se-á a renomear o arquivo em questão.
- **Se não se pode desinfectar, apagar:** se se marca esta opção e se encontra um vírus que o antivírus não pode desinfectar, proceder-se-á a apagar o arquivo em questão.

O que é a análise heurística

A análise heurística é uma técnica de análise adicional especialmente pensada para detectar vírus desconhecidos.

Do mesmo modo que a análise sob solicitação, a análise heurística é imediata e a pedido do utilizador. O método de análise em que se baseia a análise heurística é completamente diferente do método de análise sob solicitação. Este último se baseia em tentar encontrar um dos vírus que o antivírus conhece enquanto que o heurístico tenta determinar se existe um vírus baseando-se em características gerais comuns na maioria dos vírus.

Dado que a análise heurística somente pode determinar que um ficheiro é suspeito de estar infectado por um vírus e que não se conta com informação suficiente sobre o suposto vírus, não se podem desinfectar aqueles supostos vírus detectados pela análise heurística.

É importante ter em conta que a análise heurística é um complemento da análise sob solicitação.

O funcionamento da análise heurística é similar à da análise sob solicitação.

Como se usa a análise heurística

Para realizar uma análise heurística, há que levar a cabo os seguintes passos:

1. **Executar o antivírus:** para executar o antivírus, vá ao grupo de programas onde se tenham criado os ícones que permitem a sua execução. Faça duplo clique sobre o ícone *Panda Antivirus*.
2. **Ir ao item de análise heurística:** para ir a este item, prima o botão *Investigar* na barra de botões da aplicação. Aparecerá uma janela para especificar o que se deve analisar mediante o método heurístico e como se deve fazer.
3. **Escolher a área de análise:** deve escolher-se a área que se deseja analisar. Em uma lista se mostram as diferentes unidades reconhecidas no sistema. Também se pode indicar um directório ou um ficheiro concreto mediante os botões para tal efeito.
4. **Configurar as opções da análise heurística:** este passo é opcional. O programa guarda a configuração das opções da análise heurística. Portanto, uma vez configurada a análise heurística, não há razão para repetir a configuração em cada análise deste tipo que se realize. Somente se deverá variar a referida configuração quando se deseje escolher um conjunto de opções diferente. Oferece-se uma explicação mais detalhada sobre as opções de análise heurística no item de configuração nesta mesma documentação.
5. **Começar a análise:** o botão *Analisar* dá começo à análise heurística à procura de vírus nas áreas seleccionadas e com as opções escolhidas.

Como se configura a análise heurística

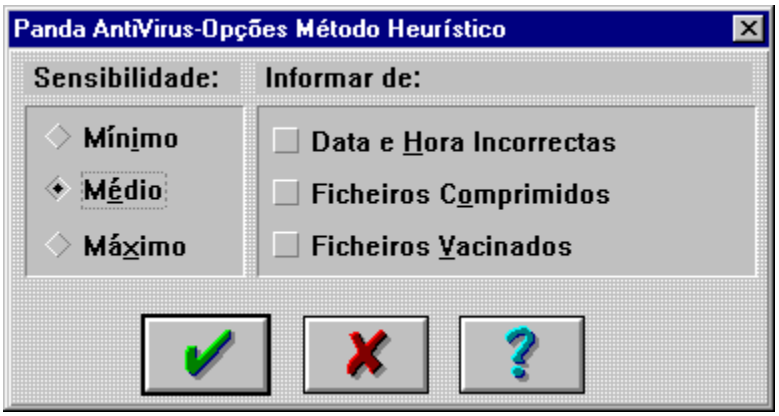
Tal e como se mencionou, em uma análise heurística deve indicar-se:

- Que área se quer analisar mediante este método.
- Como se vai levar a cabo a mencionada análise.

A configuração de uma análise heurística consiste nas opções do referido tipo de análise.

Opções de análise

Premindo o botão *Opções* aparece uma janela que permite escolher as opções de análise heurística que são as seguintes:



- **Sensibilidade mínima:** se se marca esta opção, a sensibilidade da análise heurística será baixa conseguindo assim que somente se indiquem como possíveis ficheiros contaminados aqueles muito suspeitos de conter um vírus.
- **Sensibilidade média:** se se marca esta opção, a análise heurística será levada a cabo com uma sensibilidade média. Desta forma, somente se indicarão como suspeitos aqueles ficheiros com bastante probabilidade de estarem contaminados.
- **Sensibilidade máxima:** se se marca esta opção, a sensibilidade da análise heurística será máxima indicando como suspeitos de infecção todos aqueles ficheiros nos que se detecte alguma possibilidade de se encontrar infectado. Apesar do mencionado, a possibilidade de que um ficheiro não infectado se mostre como suspeito inclusive com este nível de sensibilidade, é mínima.
- **Informar de data e hora incorrectas:** se se marca esta opção, avisar-se-á cada vez que se encontre um ficheiro com data ou hora incorrectas.
- **Informar de ficheiros comprimidos:** se se marca esta opção, avisar-se-á cada vez que se encontre um ficheiro comprimido.
- **Informar de ficheiros vacinados:** se se marca esta opção, avisar-se-á de todos aqueles ficheiros vacinados que se encontrem.

O que é a procura de cadeias

A análise sob solicitação se baseia em procurar nos ficheiros partes dos vírus que o antivírus conhece. Dado que cada dia surgem novos vírus, a análise sob solicitação vai ficando antiquada pouco a pouco.

A procura de cadeias usa o mesmo método que a análise sob solicitação porém se pode indicar uma cadeia (parte de um vírus) para que a procure. Desta maneira, o serviço de atenção ao cliente da **Panda Software** pode indicar a si uma cadeia correspondente a um novo vírus para que o antivírus a detecte apesar de não ter informação referente ao mencionado vírus no seu interior.

Do mesmo modo que a análise sob solicitação, a procura de cadeias é imediata e a pedido do utilizador.

Como se usa a procura de cadeias

Para realizar uma procura de cadeias, há que levar a cabo os seguintes passos:

1. **Executar o antivírus:** para executar o antivírus, vá ao grupo de programas onde se tenham criado os ícones que permitem a sua execução. Faça duplo clique sobre o ícone *Panda Antivirus*.
2. **Ir ao item de procura de cadeias:** para ir a este item, prima o botão *Localizar* na barra de botões da aplicação. Aparecerá uma janela para especificar que se deve analisar mediante a procura de cadeias e como se deve fazer.
3. **Escolher a área na que se vai realizar a procura:** deve escolher-se a área na que se deseja procurar. Em uma lista se mostram as diferentes unidades reconhecidas no sistema. Também se pode indicar um directório ou um ficheiro concreto mediante os botões para tal efeito.
4. **Indicar as cadeias que se devem procurar:** há que escrever as cadeias que o antivírus deve procurar ou escolher cadeias já introduzidas de uma lista. Dado que o programa guarda as cadeias que se tenham introduzido em outras ocasiões, se não se deseja acrescentar nenhuma cadeia nova não há razão para realizar este passo.
5. **Começar a procura:** o botão *Localizar* dá começo à procura das cadeias indicadas nas áreas escolhidas.

Como se configura a procura de cadeias

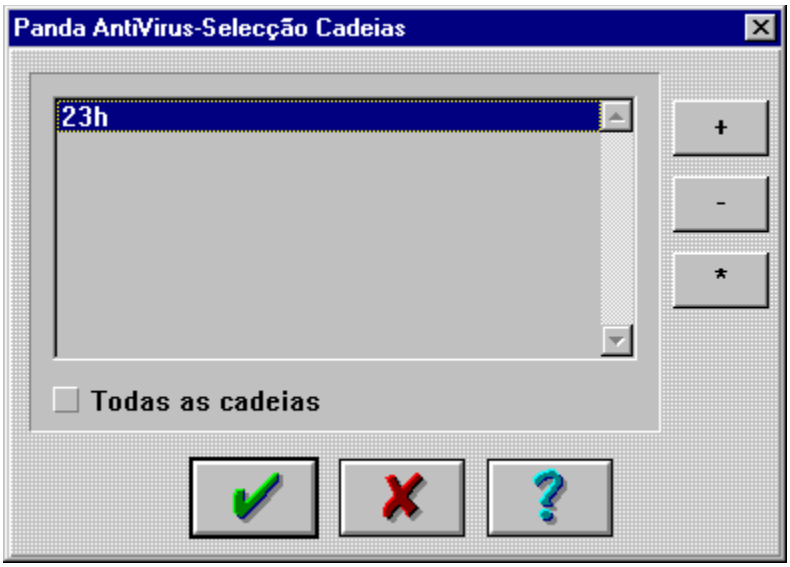
Tal e como se mencionou, em uma procura de cadeias deve indicar-se:

- Que área se quer analisar mediante este método.
- Que cadeias se devem procurar.

A configuração de uma procura de cadeias consiste nas cadeias que se devem procurar.

Cadeias

Premindo o botão *Cadeias* aparece uma janela que permite escolher as cadeias que se procurarão.



Na referida janela se vê uma lista de cadeias introduzidas. Mediante uns botões para tal efeito, pode acrescentar-se uma cadeia a dita lista, modificar uma das cadeias já introduzidas ou eliminar uma cadeia da lista.

Não se procurarão todas as cadeias indicadas na lista a não ser que se marque a opção *Todas as cadeias*. Se a referida opção não está marcada, somente se procurarão as cadeias seleccionadas na lista.

Como desinfectar com o Panda Antivirus

Não existe um item específico de desinfecção no **Panda Antivirus**. A desinfecção vai associada à análise sob solicitação ou à protecção permanente. Se a análise sob solicitação ou a protecção permanente encontram um vírus, tentarão desinfectá-lo (se se configurou assim nas opções destes dois itens).

A configuração da desinfecção permite indicar que se apaguem ou renomeiem todos aqueles ficheiros contaminados que não se possam desinfectar.

Um vírus pode encontrar-se no boot de um disco ou em ficheiros. Em cada caso, há que proceder de uma maneira ligeiramente diferente. Consulte os itens correspondentes para obter um procedimento de desinfecção detalhado.

Desinfecção de um vírus de boot

Partição FAT

Para desinfectar um vírus de boot da unidade C, deve realizar-se os seguintes passos:

1. Apague o seu computador. Introduza uma disquete de arranque limpa de vírus (se vai realizar a desinfecção desde o CD-ROM, a disquete deverá carregar os drivers do CD) e reinicie a sua máquina.
2. Uma vez que tenha arrancado, execute o nosso antivírus em linha de comandos (PAVCL) de acordo às seguintes indicações:

   - Se deseja executar o **Pavcl** desde uma disquete, introduza o disco 1 do **Panda Antivirus** para DOS/Windows 3.1x e tecle o seguinte:

     ```
     PAVCL C: /CLV
     ```

   - Se deseja executar o **Pavcl** desde o nosso CD-ROM, introduza-o na unidade leitora, situe-se no directório DOSWIN3X e no idioma desejado e tecle o seguinte:

     ```
     PAVCL C: /CLV
     ```

     Se em qualquer uma das duas situações lhe aparece uma mensagem indicando que a unidade escolhida não é válida, tecle o seguinte:

     ```
     PAVCL /HD0 /CLV
     ```

Partição NTFS

Para desinfectar um vírus de boot contando com uma partição NTFS, é importante saber se o vírus afecta ao master boot, ao boot ou a ambos. No caso de que o vírus afecte unicamente ao master boot, o procedimento indicado para partições FAT é igualmente válido neste caso.

Se o vírus afecta ao boot, a maneira de eliminar o vírus é substituir o boot por um boot genérico mediante qualquer uma das ferramentas que o Windows NT fornece para tal efeito.

Desinfecção de um vírus presente em ficheiros

Se encontrou vírus em ficheiros, proceda a limpar o seu sistema configurando o antivírus da seguinte maneira:

- Em *Opções de análise* active *Todas as extensões*, *Desinfectar* e *Análise automática*.
- Vá ao item de análise e escolha a opção correspondente a analisar todo o sistema (todas as unidades). Segundo vai-se realizando a análise, ir-se-ão limpando os ficheiros infectados.

Desinfecção mediante a protecção permanente

O **Sentinel** é capaz de desinfectar os vírus que encontra. Se o **Sentinel** detecta um vírus e está configurado para o desinfectar, desinfecta-lo-á antes de que se realize a operação em curso e, uma vez desinfectado, continuará com a operação na que se detectou o vírus. O **Sentinel** sempre mostra uma janela indicando a detecção do vírus.

Análise em linha de comandos

A **Panda Antivirus** conta com um programa chamado **Pavcl** que se executa desde a linha de comandos de MS-DOS. O nosso analisador desde a linha de comandos detecta e desinfecta os mesmos vírus que qualquer outra versão do **Panda Antivirus**.

O Pavcl é um analisador rápido e que ocupa pouca memória porém, para o manejar, é necessário ter um certo conhecimento dos parâmetros que admite. O **Pavcl** está disponível na disquete número 1 da versão DOS/Windows 3.1x ou no directório do idioma correspondente dentro do directório DOSWIN3X no CD-ROM.

Parâmetros de Pavcl

Tarefas

`/NOM` Não analisar a memória.

`/NOB` Não analisar o sistema de arranque BOOT.

`/NOF` Não analisar ficheiros.

`/ALL` Analisar todas as unidades do sistema.

`/INVx` Investigar na unidade "x" à procura de vírus desconhecidos.
Exemplo: `/INVA` investiga na unidade A:.

`/CLV` Eliminar os vírus que se tenham detectado.

`/LIS` Listar os vírus contemplados nesta versão.

`/HEU` Activar método de detecção Heurístico.

`/CMP` Analisar comprimidos.

`/CDR` Mostra os códigos de retorno do **Pavcl**.

`/SAV` Guardar os parâmetros em um ficheiro. Nas execuções seguintes acrescentará estes parâmetros aos introduzidos em cada sessão.

`/IB+` Acrescentar vacina Interna ao BOOT.
`/IB-` Tirar vacina Interna ao BOOT.
`/IB*` Verificar vacina Interna do BOOT.

`/EB+` Acrescentar vacina Externa ao BOOT.

`/EB-` Tirar vacina Externa ao BOOT.
`/EB*` Verificar vacina Externa do BOOT.

`/IF+` Acrescentar vacina Interna a um Ficheiro.
`/IF-` Tirar vacina Interna a um Ficheiro.
`/IF*` Verificar vacina Interna de um Ficheiro.

`/EF+` Acrescentar vacina Externa a um Ficheiro.
`/EF-` Tirar vacina Externa a um Ficheiro.
`/EF*` Verificar vacina Externa de um Ficheiro.

`/B+` Acrescentar vacina Interna e Externa ao BOOT.
`/B-` Tirar vacina Interna e Externa ao BOOT.
`/B*` Verificar vacina Interna e Externa do BOOT.

`/F+` Acrescentar vacina Interna e Externa a um Ficheiro.
`/F-` Tirar vacina Interna e Externa de um Ficheiro.
`/F*` Verificar vacina Interna e Externa de um Ficheiro.

Modificadores

`/NSB` Não analisar os subdirectórios de nível inferior.

`/PTH` Analisar os directórios contidos na variável PATH do DOS.

`/ISO` Activar o método de isolamento.

`/NOS` Desactivar o som.

`/AEX` Analisar todos os ficheiros, independentemente da sua extensão.

`/AUT` Exploração sem a intervenção do utilizador.

`/OVR` Sobrescrever antes de apagar.

`/NOR` Não gerar ficheiro de resultados.

`/DEL` Apaga os ficheiros infectados ainda que se possam desinfectar.

`/LOC` Analisa todas as unidades locais.

`/NBR` Não permite cancelar o processo de análise.

`/ITW` O **Pavcl** só analisará à procura dos vírus *In The Wild*. Este parâmetro só se deve usar em

condições especiais.

Adicionalmente dispõe do switch “/?” estandardizado no DOS, para ter acesso a uma lista dos switches disponíveis. Nesta também se incluem aqueles correspondentes aos idiomas suportados pela versão do **Pavcl**.

As tarefas por defeito são:

- Analisar Memória.
- Analisar Boot.
- Analisar Ficheiros.

e os modificadores por defeito são:

- Analisar subdirectórios.
- Não desinfectar.
- Efeitos de som activados.
- Analisar somente extensões executáveis.
- Gerar ficheiro de resultados.

As tarefas /?, /LIS, /INVx são exclusivas, ou seja, quando são seleccionadas nenhuma das outras tarefas se realiza. Depois de finalizadas se regressa ao DOS. O caminho ou caminhos que se quer analisar se especifica como é habitual no DOS:

[Unidade:][Caminho][NomeFicheiro]

Relatório de resultados

O relatório de resultados vai guardando as diferentes operações que se vão realizando com o antivírus assim como as diferentes incidências que se produzam.

A informação contida no relatório de resultados se conserva de sessão em sessão. Portanto, é útil para consultar, em qualquer momento, a actividade que se levou a cabo com o antivírus.

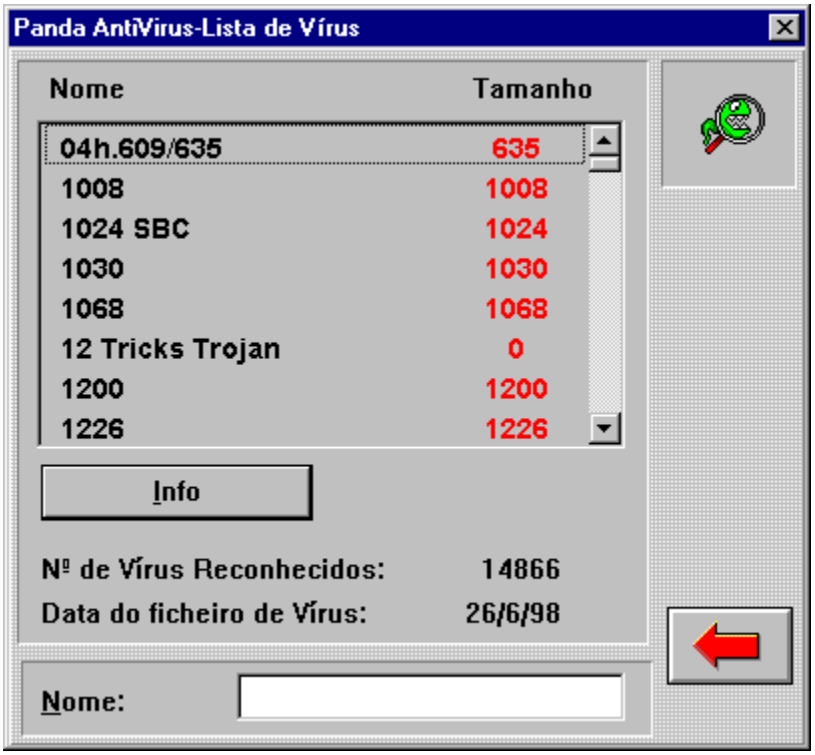
Por cada operação realizada, guardam-se os seguintes dados:

- Data e hora.
- Tipo de operação.
- Área sobre a que se levou a cabo a operação.
- Número de ficheiros revisados.
- Todas as incidências havidas relacionadas com os vírus.

Para se ir armazenando os dados no relatório de resultados, é necessário activar a opção *Gravar resultados* dentro da janela de *Opções de Análise*.

O conteúdo do relatório de resultados pode imprimir-se para facilitar a sua consulta. Também se pode apagar o conteúdo do relatório de resultados em qualquer momento para evitar que adquira um tamanho demasiado grande.

Lista de vírus



A lista de vírus apresenta uma lista com os vírus que o **Panda Antivirus** é capaz de detectar. Na lista de vírus se indica o nome e o tamanho de cada vírus.

Junto à lista, indica-se o número de vírus reconhecidos nessa versão do **Panda Antivirus**. Também se indica a data do ficheiro de vírus para saber, dessa maneira, o actualizado ou desactualizado que se encontra o antivírus.

Pode-se indicar o nome de um vírus no espaço destinado para tal efeito para encontrar assim um vírus concreto com maior facilidade. Com esse mesmo fim, a lista de vírus se apresenta ordenada alfabeticamente.

Uma vez escolhido um vírus, se se prime o botão *Info*, aparece uma janela com uma série de dados de interesse como são:

- Nome.
- Origem.
- Tamanho.
- Alcunha.
- Data na que se detectou pela primeira vez.
- Se se pode desinfectar ou não.
- Áreas da máquina que se podem ver afectadas pelo vírus.
- Características de comportamento do vírus.

A seguir, detalha-se uma explicação sobre as diferentes características com que pode contar um vírus:

- **Residente:** quando se executa, o vírus reserva uma pequena parte da memória e se instala nela para ir contagiando-se desde aí.
- **Stealth:** é uma técnica que usam alguns dos vírus residentes. Esta técnica consiste em camuflar as mudanças que o vírus faz sobre os ficheiros que infecta. Quando alguém tenta olhar uma das características do ficheiro que o vírus modificou, o vírus, que está residente em memória, intercepta a consulta e oferece os dados anteriores à modificação.
- **Encriptado:** os vírus que possuem esta característica são capazes de se encriptar de maneira diferente cada vez que infectam um ficheiro. Desta forma, não se pode tentar procurar o vírus mediante uma cadeia.
- **Sobreescritura:** os vírus de sobreescritura, que podem ser residentes ou não, sobrescrevem o ficheiro que infectam. O referido ficheiro fica, portanto, inservível. O tamanho do ficheiro não varia a não ser que o tamanho do vírus seja maior que o do ficheiro. A única maneira de eliminar estes vírus é apagando o ficheiro infectado e pondo no seu lugar uma cópia sem infectar.
- **Polimórfico:** os vírus polimórficos são versões avançadas dos vírus encriptados. Os polimórficos são capazes de mudar o método de encriptação de geração em geração. Desta forma, não há nenhuma parte do vírus que permaneça inalterada.

Funcionamento geral

O Panda Antivirus para Windows NT apresenta uma cómoda interface fácil de usar. Na janela principal do programa, as opções mais comuns estão disponíveis através de uns botões de grande tamanho.

Premindo sobre esses botões se acede às diferentes partes do programa. Refira-se ao item correspondente para obter uma explicação de funcionamento detalhada.