avast! antivirus
Home Edition **4**.8

Manual de utilizador

ÍNDICE

Introdução

Bem-vindo ao avast! antivírus Home Edition versão 4.8.

O avast! antivírus é a colecção de produtos antivírus de tecnologia de ponta multi-premiada, que trabalham em perfeita sinergia, tendo como único objectivo comum proteger o seu sistema, e informação, livre de vírus. O avast! Representa a melhor solução na sua classe para computadores baseados na plataforma Windows.

O avast! antivírus tem incorporado tecnologia anti-spyware, certificada pelo processo West Coast Lab's Checkmark, assim como anti-rootkit e uma forte capacidade de auto-protecção, garantindo, deste modo, que todos os seus programas e informação valiosa estejam sempre protegidos.

Sobre a ALWIL Software a.s.

Desde 1988, a ALWIL Software tem produzido produtos antivírus que têm sido desenvolvidos até atingirem a linha de produtos multi-premiada avast! antivírus, tornando o avast! um dos antivírus mais amadurecidos e testados do mercado.

Sediada em Praga, na República Checa, a ALWIL Software desenvolve e vende os produtos antivírus avast! que protegem as principais plataformas de sistemas operativos e os principais tipos de dispositivos mais vulneráveis. Mais detalhes sobre a empresa podem ser encontrados no nosso website, www.avast.com.

Para mais ajuda

Caso tenha alguma dificuldade com o seu programa avast! antivírus, que você é incapaz de resolver depois de ler o manual, você pode encontrar a sua resposta no Centro de Apoio do nosso site em **http://support.avast.com**

- Na secção da **Base de Dados** pode rapidamente encontrar as respostas às perguntas mais frequentes

- Como alternativa, pode também tirar vantagem do Fórum de Apoio do avast!. Aqui poderá interagir com outros usuários do avast! que podem ter experimentado o mesmo problema e já ter descoberto a solução. Você precisará registar-se para usar o fórum, mas este é um processo muito rápido e simples. Para se registar e usar o fórum, vá a **http://forum.avast.com/**

Se continua com a sua questão por resolver, poderá "**Submeter uma dúvida**" à nossa equipa de apoio. Mais uma vez, terá de se registar para o fazer e quando nos escrever, por favor inclua o máximo de informação possível.

Ameaças ao seu computador

Viroses, spyware, rootkits e todas as formas de software malicioso são conhecidas colectivamente por malware (abreviação de software malicioso); malware pode também ser referido como “badware”.

O que é um vírus?

Um vírus de computador é um software, normalmente de natureza maliciosa, que é utilizado para se propagar a si mesmo, ou programas semelhantes, para outros computadores. As viroses em si podem causar danos no sistema, perda de informação importante, ou pode ser usado para instalar spyware, rootkits ou outro malware num sistema vulnerável.

A forma essencial para prevenir a infecção é ter uma solução actualizada de antivírus instalada em todos os computadores numa rede, e para ter certeza de que todos os últimos patchs de segurança para o sistema operativo de computador estão instalados. Os usuários também se devem certificar de que podem confiar na origem do software que baixam da internet, pois muitos tipos de malware são instalados junto com outros com aparência de software legítimo.

O que é spyware?

Spyware é um software instalado num sistema de computador que foi projectado para reunir informações sobre o usuário do computador muitas vezes sem o seu consentimento ou conhecimento. Esta informação pode resultar no chamado "roubo de identidade”, ou roubo de informações valiosas (como dados bancários ou do cartão de crédito) ou de dados empresariais.

Hoje em dia, muito do spyware actual é desenvolvido em círculos de crime organizado, em vez de indivíduos oportunistas solitários, e é instalado por um vírus ou outro tipo de malware.

O que são rootkits?

Rootkits são programas que se instalam no seu sistema, mantendo simultaneamente a si próprios, os seus processos, serviços e chaves de registo ocultos, de modo a ficar invisíveis ao usuário. Representam um risco substancial de segurança em casa e em redes de empresas, sendo notoriamente difíceis de encontrar e remover.

Os Rootkits em si são normalmente implantados através de outra infecção de malware (tais como um Cavalo de Tróia, por exemplo), e, por isso, é altamente recomendável que os usuários tenham instalado e a funcionar no seu computador um sistema actualizado de antivírus / anti-spyware. Tal sistema é o avast! antivírus 4.8.

Características chave do avast! antivírus

O avast é a linha de produtos antivírus multi-premiada da ALWIL Software a.s., que é certificada pelos ICSA Labs e Checkmark (tanto para antivírus como anti-malware). O avast! antivírus recebe regularmente o prémio Virus Bulletin 100%, para detecção de 100% de viroses "in-the-wild", além de ser um produto repetidamente vencedor dos Secure Computing Awards.

O avast! antivírus é utilizado em mais de 60 milhões de residências e escritórios no mundo inteiro, e foi desenhado especificamente de modo a ter baixos requisitos de sistema e para se actualizar tanto a ele próprio como às definições de vírus automaticamente.

O avast! antivírus representa uma colecção de tecnologias topo de gama criada para dar-lhe uma protecção sem rivais contra todas as formas de malware. As principais características do avast! antivírus Home Edition e Professional Edition são comparadas e descritas abaixo.

Características chave	Home Edition	Professional Edition
Motor antivírus baseado em tecnologia de alta performance	**Sim**	**Sim**
Forte protecção residente	**Sim**	**Sim**
Anti-spyware	**Sim**	**Sim**
Detecção de rootkits	**Sim**	**Sim**
Forte auto-protecção	**Sim**	**Sim**
Actualizações incrementais automáticas	**Sim**	**Sim**
Quarentena de vírus para armazenamento de ficheiros suspeitos	**Sim**	**Sim**
Integração no Sistema	**Sim**	**Sim**
Limpa Vírus integrado	**Sim**	**Sim**
Verificador com linha de Comandos	**Não**	**Sim**
Bloqueador de Scripts	**Não**	**Sim**
Actualizações PUSH	**Não**	**Sim**
Interface Avançada que lhe dá a capacidade de criar e agendar e definir certas tarefas	**Não**	**Sim**

Núcleo antivírus

O núcleo antivírus é o motor básico do programa. A última versão do avast! antivírus combina uma habilidade de detecção fora de série com uma alta performance. Pode contar com uma detecção de 100% dos vírus "in-the-wild" (vírus já difundidos entre utilizadores) e uma excelente detecção de Cavalos de Tróia.

O Núcleo é certificado pelos **ICSA Labs**; frequentemente participa nos testes da revista Virus Bulletin, muitas vezes ganhando o prémio VB100.

Protecção residente

A protecção residente (a protecção em tempo real do sistema do computador) é uma das características mais importantes de um programa antivírus hoje em dia. A protecção residente do avast! é uma combinação de várias partes ou "módulos residentes", que são capazes de detectar o vírus antes de este ter a oportunidade de infectar o seu computador.

Tecnologia anti-spyware embutida

O avast! antivírus agora vem com tecnologia anti-spyware, que é certificada pelo processo de selecção da West Coast Labs Checkmark oferecendo uma maior protecção dos seus valiosos dados e programas.

Tecnologia anti-rootkit embutida

A tecnologia anti-rootkit é baseada na tecnologia GMER, líder na sua classe, e está também integrada no programa como padrão. Se um rootkit for descoberto, ele será desactivado inicialmente e depois, se ele poder ser removido com segurança sem afectar o desempenho do computador, ele é removido. O avast! antivírus inclui uma base de dados de vírus que pode ser actualizada automaticamente para fornecer protecção contínua contra rootkits.

Forte auto-protecção

Alguns vírus podem tentar desligar o software antivírus dum computador. Para proteger o seu computador, mesmo contra as ameaças mais recentes que podem tentar desactivar a sua protecção de segurança, o avast! tem incluído uma forte auto-protecção, a melhor da sua classe. Esta baseia-se na multi-premiada tecnologia avast! antivírus e oferece uma camada extra de segurança para garantir que os seus dados e programas estão sempre protegidos.

Actualizações automáticas

As actualizações automáticas são uma outra necessidade chave na protecção contra vírus. Tanto a base de dados de vírus e o próprio programa podem ser actualizados automaticamente. As actualizações são incrementais, apenas baixando os novos dados em falta, reduzindo significativamente o tempo de transferência. O tamanho típico de uma actualização da base de dados de vírus é de dezenas de KB, enquanto que as actualizações do programa são tipicamente não mais do que algumas centenas de KB.

Se sua conexão à Internet é contínua (como uma conexão de banda larga sempre ligada), então as actualizações são completamente automáticos em intervalos de tempo fixos. Se estiver ligado à internet apenas ocasionalmente, o avast! monitoriza a sua ligação e tenta efectuar a actualização quando se encontra online. Este recurso é descrito em pormenor na **página 40**.

Quarentena

Quarentena pode ser vista como uma pasta no seu disco, com características especiais que a tornam segura e isolada, concebida para armazenar ficheiros potencialmente nocivos. Pode trabalhar com ficheiros dentro da Quarentena mas com algumas restrições de segurança.

As principais características da Quarentena são um isolamento completo do resto do sistema operacional. Nenhum processo exterior, como um vírus, pode aceder aos ficheiros no seu interior, e o facto de os ficheiros dentro dela não poderem ser executados significa que não há perigo em aí armazenar vírus. Para mais informações, consulte a **página 52**.

Integração no Sistema

O avast! antivírus está plenamente integrado no seu sistema. A Extensão do Explorer permite que seja iniciada uma verificação clicando directamente numa pasta ou num ficheiro com o botão direito do rato e seleccionando a respectiva opção do menu de lista pendente.

Um protector de ecrã especial é também fornecido, que quando activado, também executa uma verificação. O avast! antivírus também funciona com qualquer protector de ecrã, assim não precisa mudar as configurações pessoais para utilizá-lo. Para configurar o protector de ecrã do avast! antivírus consulte a **página 77**.

Nas versões 32-bit do Windows NT/2000/XP/Vista, também é possível executar uma verificação no arranque, o que lhe permite efectuar uma verificação enquanto o sistema está a ser iniciado e antes que um vírus seja activado. O que é útil caso suspeite que o seu computador pode já ter sido infectado por um vírus.

Limpa-Vírus integrado

O avast! antivírus é concebido essencialmente para proteger o computador contra infecção por um vírus ou outro tipo de malware. A sua função principal é a prevenção e não a remediação. Porém, ele agora inclui um Limpa Vírus especial que é capaz de remover alguns dos vírus mais comuns a partir de computadores infectados. Infelizmente, o número de vírus em circulação está a crescer constantemente e, caso o seu computador seja infectado por um vírus que não possa ser removido pelo Limpa Vírus, poderá ser necessário procurar assistência especializada.

Mais informações sobre o limpa-vírus podem ser encontradas no nosso web site, **www.avast.com**.

Verificador de Linha de Comandos (Apenas na Professional Edition)

Para utilizadores experientes, a Professional Edition apresenta uma linha de comandos para fazer verificações. O programa ashCmd usa exactamente o mesmo núcleo de verificação que o avast! portanto, os resultados são exactamente os mesmos. A varredura é realizada na linha de comando usando uma série de parâmetros e opções, e está disponível modo especial STDIN / STDOUT. Este módulo é destinado a ser usado em programas BATCH e a sua saída é a mesma que a saída das tarefas do Interface de Utilizador Avançado (incluindo os ficheiros do relatório).

Bloqueador de Scripts (Apenas na Professional Edition)

Este é um módulo que protege o computador contra vírus script escondidos dentro de páginas Web. Tais scripts são normalmente inofensivos pois os programas que os executam impedem-nos de aceder a ficheiros. No entanto, pode haver uma falha de segurança num navegador de internet que pode ser explorada por um vírus, o que poderá resultar na infecção do seu computador. O avast! verifica, portanto, quaisquer scripts que possam ser potencialmente perigosos mas páginas Web que forem visitadas.

Actualizações PUSH

Uma característica especial da Professional Edition é a actualização PUSH. É uma mudança radical na filosofia de actualizações. Normalmente, cada programa instalado verifica ocasionalmente a disponibilidade de uma nova versão. As Actualizações PUSH são inicializadas pelo nosso servidor; deste modo o seu computador responde com rapidez na realização da necessária actualização. Este sistema é baseado no protocolo SMTP (utilizado para mensagens de e-mail). A actualização em si é controlada pelos clientes de email do avast! residente (MS Outlook e Correio de Internet). Todo o sistema é protegido por cifras assimétricas e é resistente ao uso não autorizado.

Interface Avançada (Apenas na Professional Edition)

O avast! antivírus Professional Edition inclui uma interface de utilizador Avançada, onde é possível criar "tarefas" especiais que podem ser programadas para serem executadas num determinado momento no futuro ou, numa base regular, por exemplo, diária, semanal ou mensal. Quando uma tarefa é executada, uma nova "sessão" é criada, em que os resultados da verificação são armazenados, podendo depois ser visualizados. Diferentemente do interface simples padrão, quando trabalhar na Interface Avançada, é possível indicar com antecedência qual acção que deve ser tomada se um vírus for detectado. Por exemplo, pode mandar que o programa tente reparar imediatamente quaisquer ficheiros infectados. Também é possível especificar uma acção alternativa se

a primeira acção for infrutífera. Por exemplo, se um ficheiro não pode ser reparado, ele pode ser automaticamente transferido para Quarentena.

Requisitos do Sistema

As configurações de hardware descritas abaixo representam a especificação **mínima** recomendada para o sistema operativo.

Para um computador com o Windows® 95/98/Me:
Processador 486, 32MB de RAM e 100 MB de espaço livre no disco rígido.

Para um computador com o Windows® NT® 4.0:
Processador 486, 24MB de RAM e 100 MB de espaço livre no disco rígido e Service Pack 3 (ou superior) instalado

Para um computador com o Windows® 2000/XP® Workstation (Não o Servidor):
Processador de classe Pentium, 64MB de RAM (128MB recomendado) e 100 MB de espaço livre no disco rígido

Para um computador com o Windows® XP® 64-bit Edition:
Um AMD Athlon64, Opteron ou Intel EM64T Pentium 4 / processador Xeon, 128MB de RAM (256MB recomendado) e 100 MB de espaço livre no disco rígido

Para um computador com o Windows® Vista:
Processador Pentium 4, 512MB de RAM e 100 MB de espaço livre no disco rígido
O próprio programa requer cerca de 60 MB de espaço no disco rígido; o restante do espaço é reservado para o ficheiro da base de dados de recuperação de vírus e a sua lista, e os ficheiros de instalação.

Um MS Internet Explorer 4 funcional, ou superior, é necessário para que o programa funcione.

Este produto **não pode ser instalado num sistema operacional dum servidor** (famílias Windows Server NT/2000/2003).

Nota : diversos problemas podem surgir como resultado da instalação de mais de um produto de segurança no mesmo computador. Caso tenha instalado outro software de segurança, recomenda-se que este seja desinstalado antes de tentar instalar o avast!

Como instalar o avast! antivírus Home Edition

Esta secção descreve como baixar e instalar o avast! Home Edition antivírus no seu computador e como instalar a sua chave de licença do software após o download e o processo de instalação forem concluídos. Os ecrãs mostrados nas páginas seguintes são como elas aparecem no Windows XP podendo ser ligeiramente diferentes noutras versões do Windows.

Pode fazer o download do avast! antivírus Professional Edition em **www.avast.com**.

Recomenda-se vivamente que todos os outros programas do Windows sejam fechados antes de começar o download.

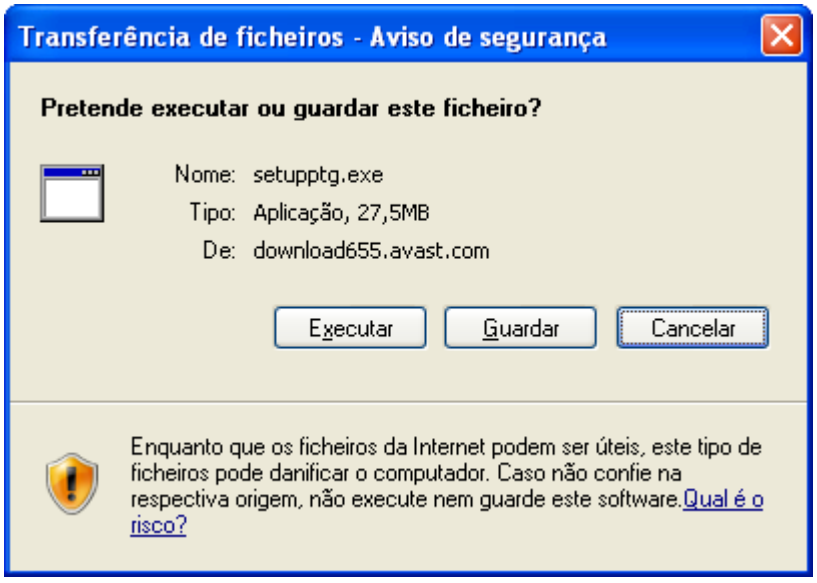
Clique em "Descarregar" e depois em "programas" e, em seguida, seleccione a versão a ser baixada.

A partir da lista de idiomas disponíveis, seleccione a versão na língua que preferir - veja abaixo - e clique no botão "Download".

Download avast! 4 Home Edition

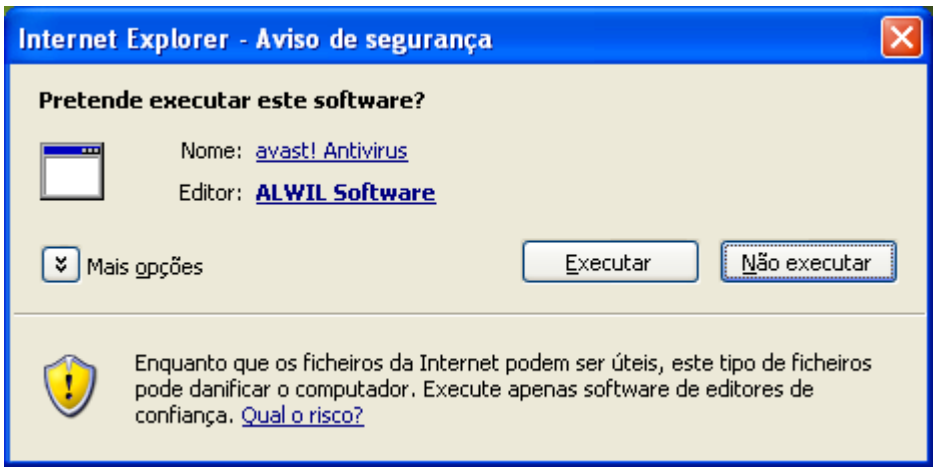
Download avast! 4 Home - versão **Polaca** (length 27.80 MB)
Download avast! 4 Home - versão **Portuguesa (Brasil)** (length 27.52 MB)
Download avast! 4 Home - versão **Portuguesa (Portugal)** (length 27.53 MB)
Download avast! 4 Home - versão **Romena** (length 27.52 MB)

Se utilizar o Internet Explorer como navegador da Web, a caixa mostrada abaixo será apresentada:



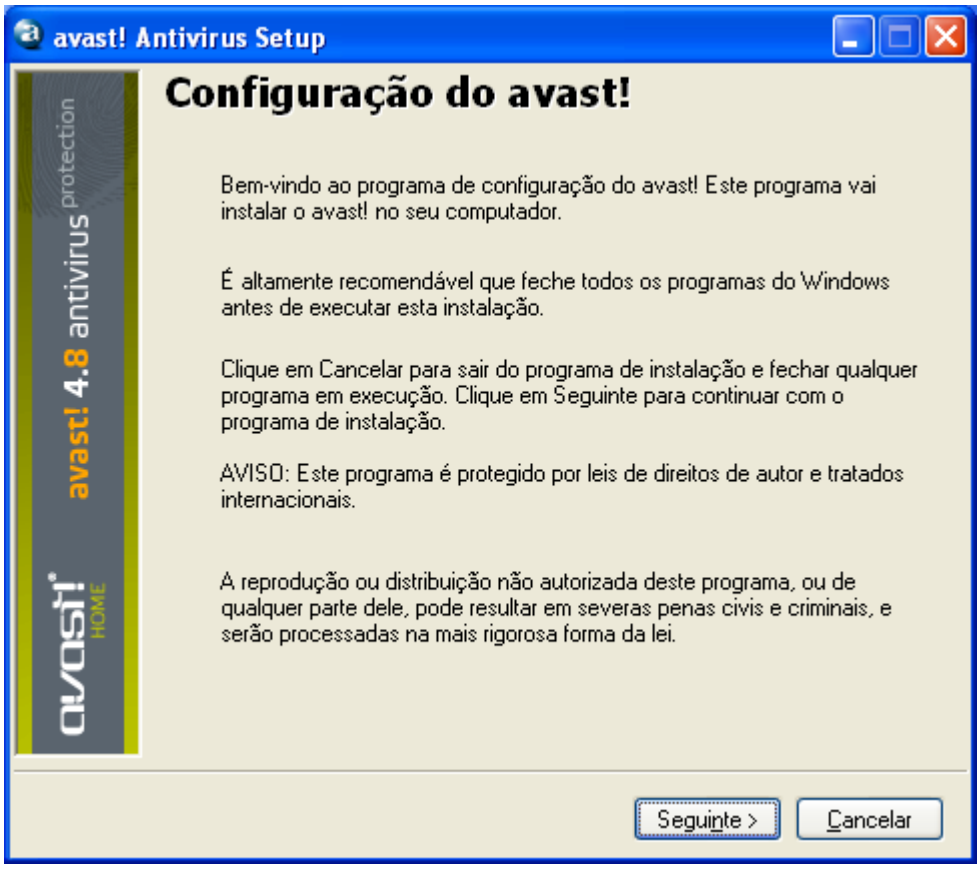
Clicando em "Executar" ou "Guardar" vai iniciar o download do ficheiro de instalação "Setupeng.exe" no seu computador.

Se preferir que o avast! antivírus seja instalado no seu computador imediatamente após o download do ficheiro de instalação, clique em "Executar". Assim que o ficheiro de instalação tenha sido baixado, aparecerá a seguinte imagem:



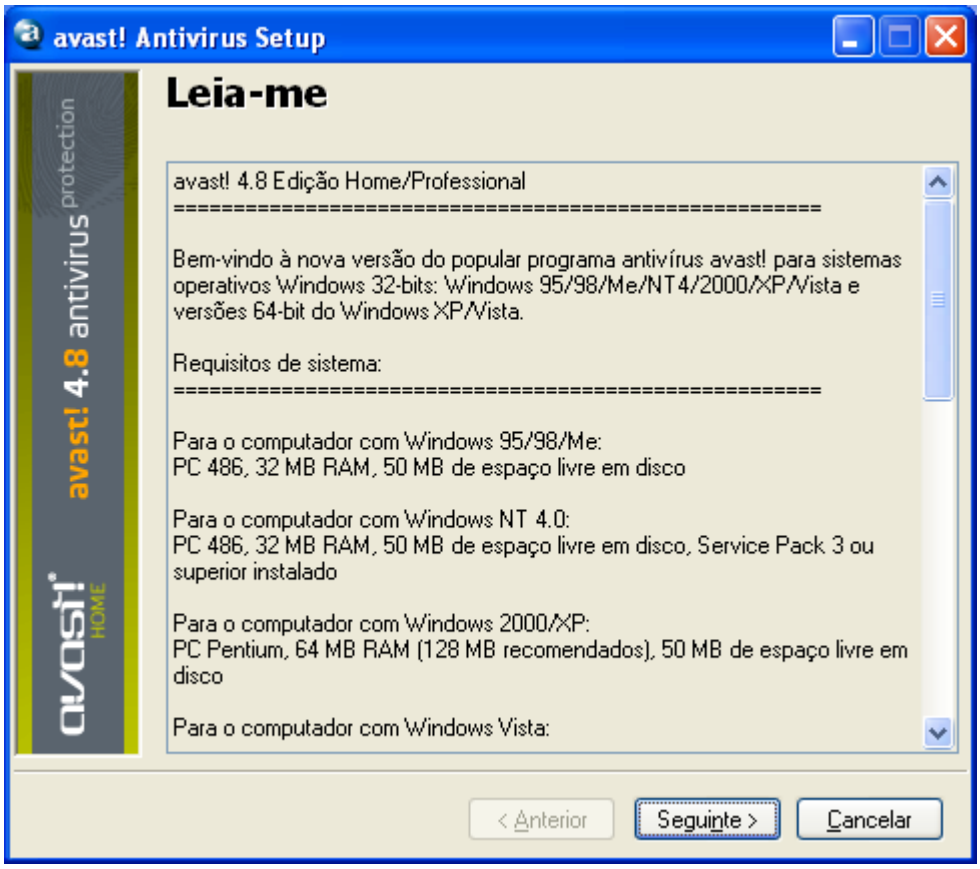
Noutros navegadores da Web, poderá ter apenas a opção "Guardar" o ficheiro. Clicando em "Guardar" irá fazer o download do software no computador, mas ele não será instalado nesse momento. Para concluir o processo de instalação, será necessário executar o ficheiro de instalação "Setupeng.exe", por isso tenha em mente onde o guarda! Dê um duplo clique no ficheiro para executá-lo.

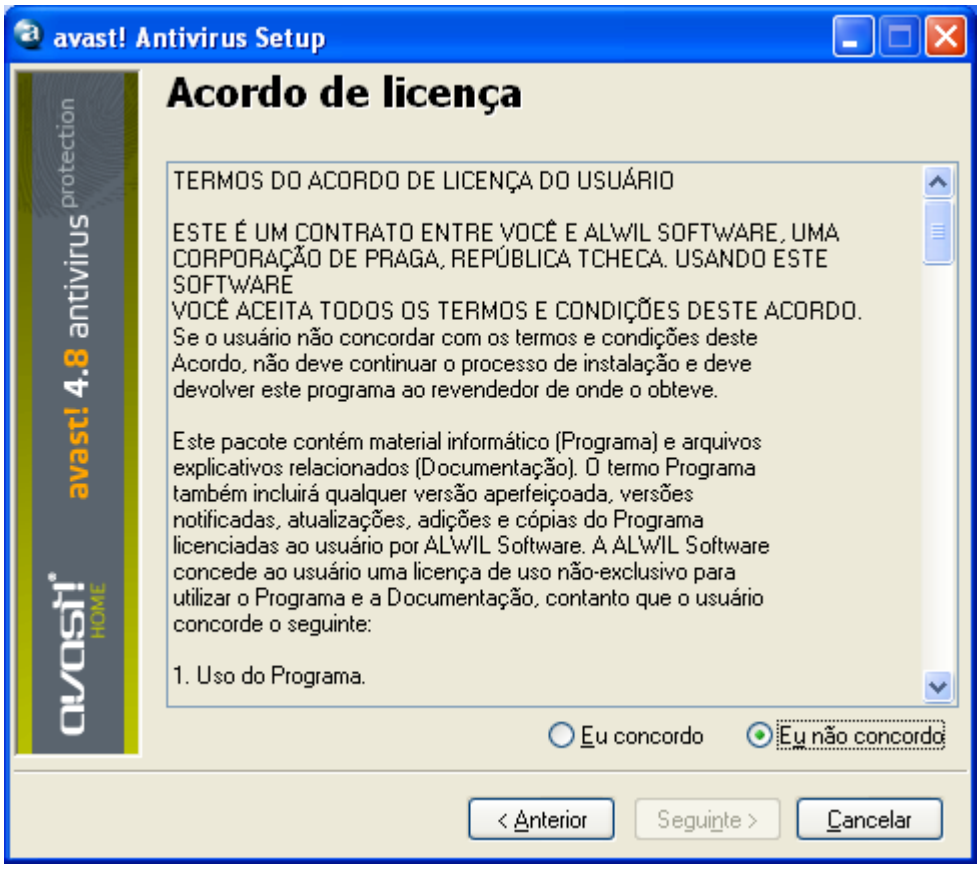
Clicando em "Executar", será levado novamente para a tela de setup do avast!:



Clique em "Seguinte" e, em seguida, o assistente de instalação guiá-lo-á durante o resto do processo de instalação.

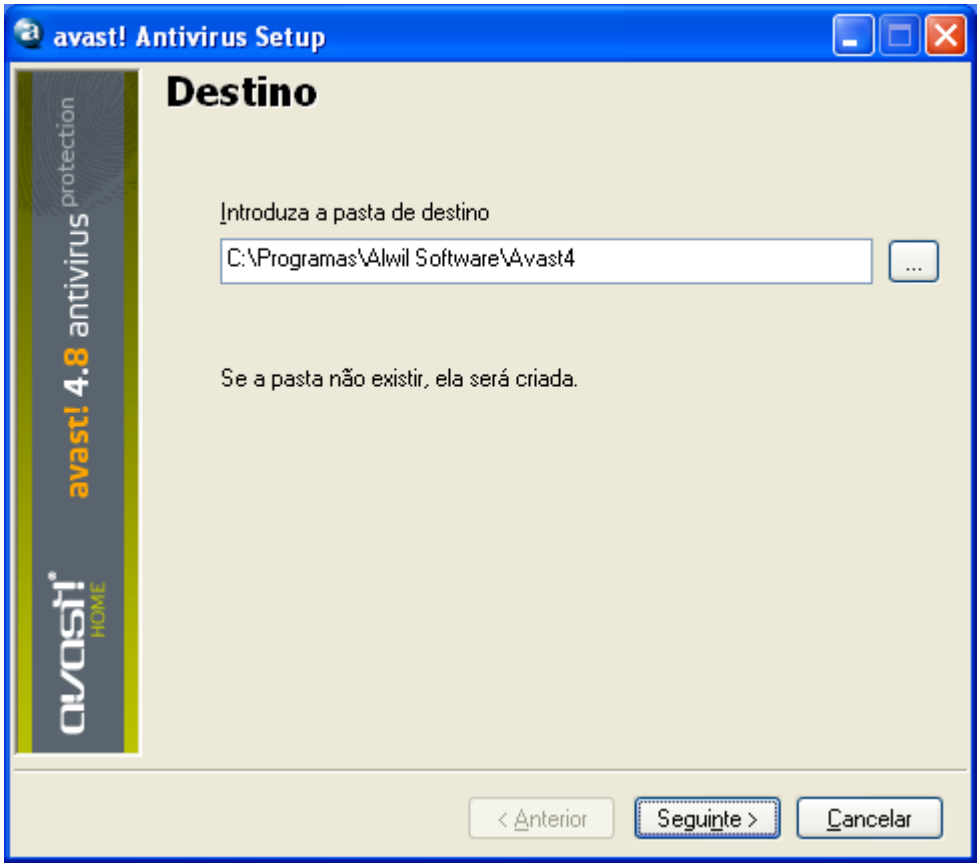
Primeiro, será pedido que leia sobre os requisitos mínimos do sistema e, em seguida, para confirmar que concorda com as condições de licença de utilizador final - ver as seguintes imagens abaixo.


avast! Antivirus Setup
Leia-me
avast! 4.8 antivirus protection
avast! 4.8 Edição Home/Professional
==========
Bem-vindo à nova versão do popular programa antivírus avast! para sistemas operativos Windows 32-bits: Windows 95/98/Me/NT4/2000/XP/Vista e versões 64-bit do Windows XP/Vista.
Requisitos de sistema:
==========
Para o computador com Windows 95/98/Me:
PC 486, 32 MB RAM, 50 MB de espaço livre em disco
Para o computador com Windows NT 4.0:
PC 486, 32 MB RAM, 50 MB de espaço livre em disco, Service Pack 3 ou superior instalado
Para o computador com Windows 2000/XP:
PC Pentium, 64 MB RAM (128 MB recomendados), 50 MB de espaço livre em disco
Para o computador com Windows Vista:
< Anterior
Seguinte >
Cancelar



Para continuar, é necessário clicar em "Eu Concordo", e depois, "Seguinte".

Ser-lhe-á solicitado para confirmar o directório destino, ou seja, onde os ficheiros do programa devem ser guardados. O programa fará isto automaticamente ou criará um novo directório se ele ainda não existir. Recomenda-se a aceitar o directório padrão de destino e simplesmente clicar em "Seguinte" para continuar.



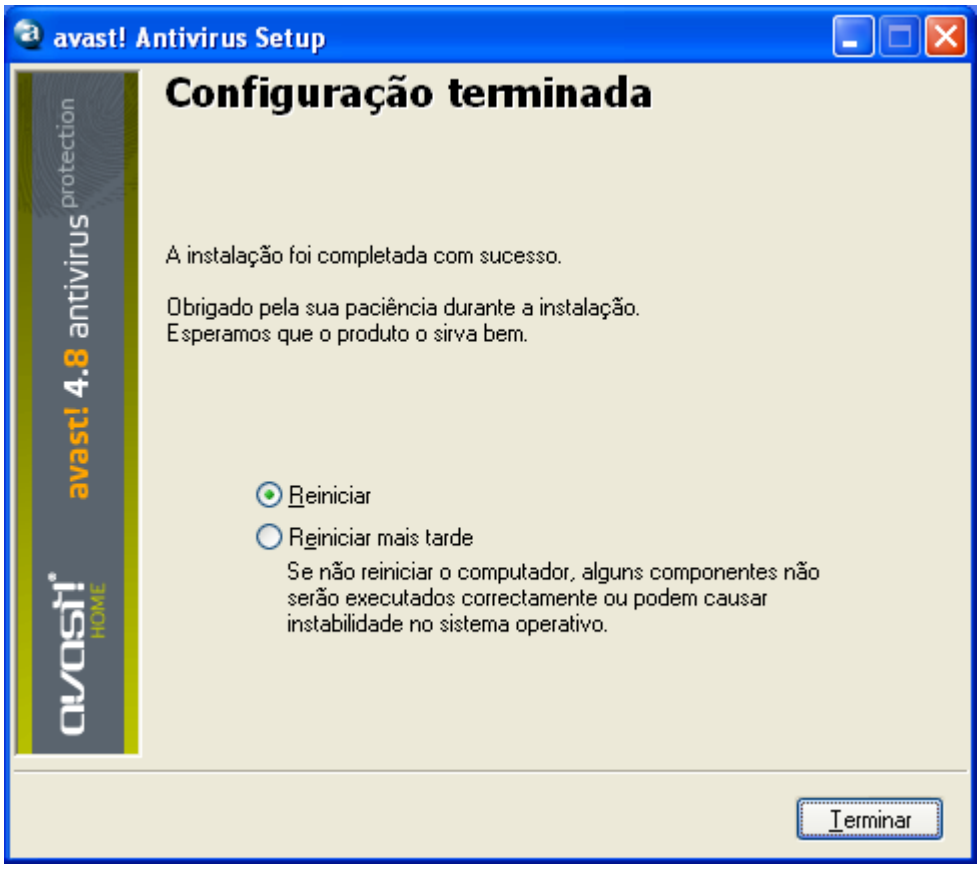
Na próxima imagem será solicitada a confirmação da configuração. As opções mais adequadas para os utilizadores são automaticamente seleccionadas. A menos que deseje alterar qualquer uma das configurações padrão, por exemplo, selecção do idioma, só precisa clicar em "Seguinte" para continuar.

O programa irá então confirmar o que está a ser instalado, onde e a quantidade de espaço de disco disponível e exigida. Clique em "Seguinte" para continuar.

De seguida será perguntado se quer agendar uma verificação durante o arranque – ver **página 42**.

A imagem final deverá confirmar que a instalação foi concluída com êxito, no entanto, para completar o processo, será necessário reiniciar o seu computador.

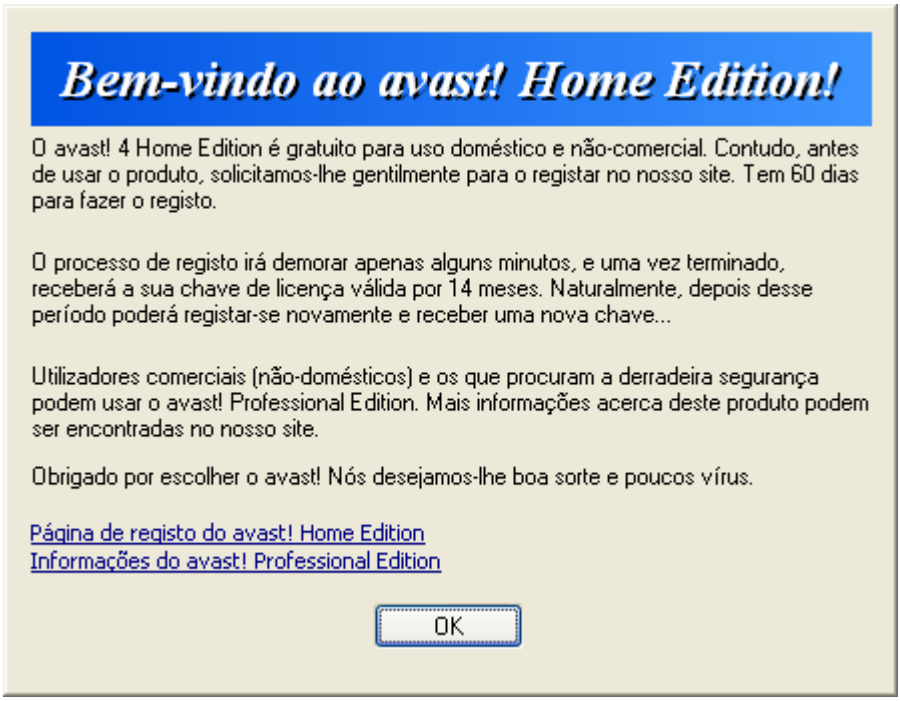
Com "Reiniciar" seleccionado, clique em "Terminar" e o computador será automaticamente reiniciado.



A instalação está agora completa.

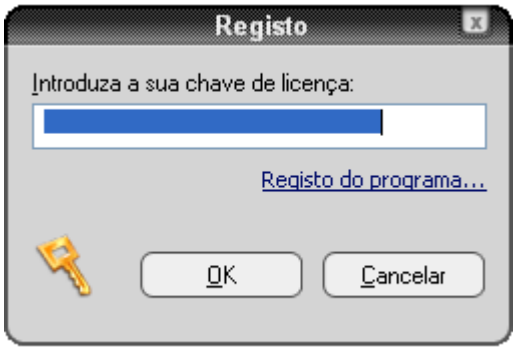
Primeiros Passos

Após reiniciar o computador aparecerá a seguinte imagem e deve ver um ícone de uma bola azul com um "a" branco, no canto inferior direito da imagem do seu ecrã, ao lado do relógio:



O avast! antivírus Home Edition é gratuito para uso doméstico não-comercial. Depois de instalado na versão demonstração, o avast! 4 Home Edition funcionará por 60 dias. Pode obter por e-mail a sua chave de registo GRATUITA depois de preencher um formulário. A chave de registo é válida por 1 ano e tem de ser inserida no programa. Depois de um ano, terá de registar-se novamente.

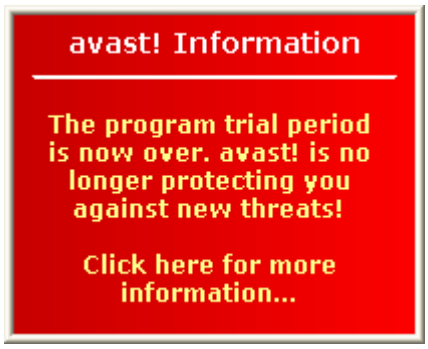
Portanto, a primeira vez que executar o programa irá aparecer-lhe a seguinte janela:



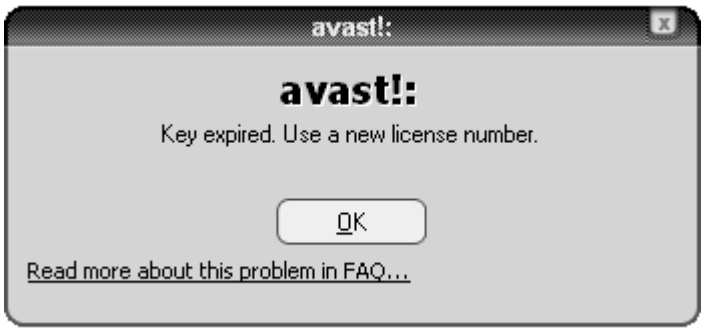
Não é necessário inserir uma chave de licença de imediato. Se deseja executar o programa, até 60 dias sem a aplicação de uma chave de licença, basta clicar em "Cancelar". No entanto, pode solicitar uma chave de licença agora clicando em "Registo do programa…" e seguir o procedimento descrito na próxima secção.

Uma vez seleccionada a versão Demo, esta caixa não irá aparecer na próxima vez que executar o programa. No entanto, pode registar-se para uma chave de licença a qualquer momento - veja a próxima página "Como registar-se para uma chave de licença"

Após 60 dias, se a chave de licença não for inserida, o seguinte aviso aparecerá no canto inferior direito da imagem do computador:



Será exibida a seguinte mensagem sempre que iniciar o programa:



Ao clicar em "OK" aparecerá a caixa registo. O processo para obter uma chave de licença é descrito nas páginas seguintes.

Palavra-chave

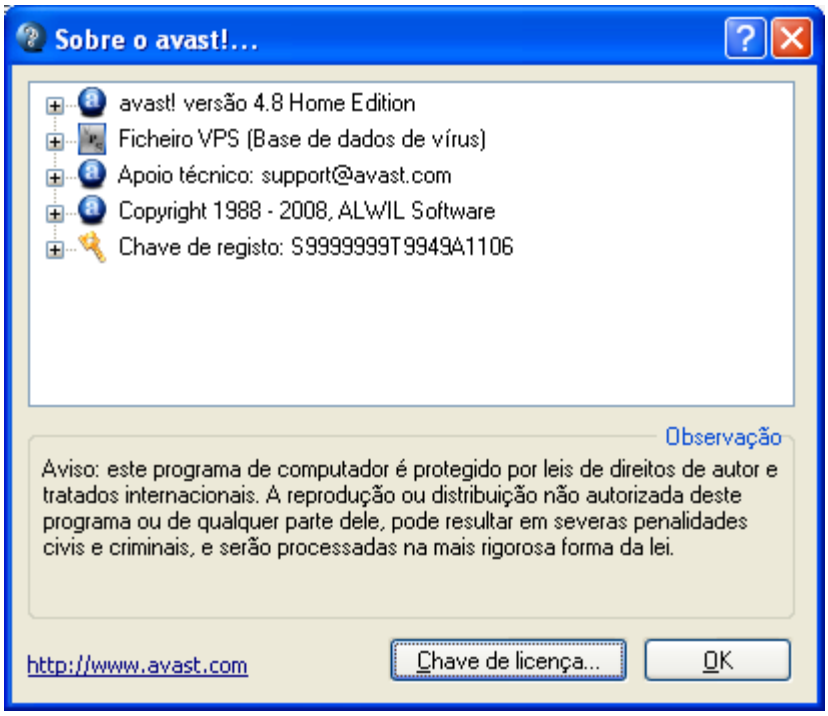
Clicando com o botão direito na bola azul no canto inferior direito da imagem e seleccionar "Definir / alterar senha" pode criar uma senha para proteger o seu programa antivírus contra alterações não autorizadas.

Como se registar para uma chave de licença

Se quiser continuar a utilizar o programa após o período experimental gratuito de 60 dias, será necessário registar-se e obter uma chave de licença válida e inseri-la no programa.

Para tal vá a **www.avast.com** e clique em "Apoio" no topo do ecrã. Depois clique em "Registo no avast! Home GRATUITO". Como alternativa, caso já tenha o programa, clique com o botão direito do rato no ícone avast no canto inferior do seu ecrã, ao lado do relógio. No menu que aparece clique em "Acerca do avast! …"

Clique em "chave de licença...".



Aparecerá a caixa de Inscrição - clique em "Registo do programa…".

Isto irá levá-lo para o site da avast! onde poderá fazer o seu registo online. Quando terminar e clicar em "Registar" a chave de licença será enviada para o email, que introduziu no registo, em menos de 24 horas.

Inserir a chave de licença

Depois de receber a sua chave de licença (enviada por e-mail para o endereço especificado durante o processo de registo), ela deve então ser inserida no programa. Isso permitirá que o programa seja actualizado automaticamente e irá impedir mais avisos sobre a chave de licença.

Nota – o programa avast! tem de estar instalado no seu computador antes de tentar inserir a chave de licença.

Para ver um filme a mostrar como inserir a chave de licença sem iniciar o programa, clique **aqui** ou vá a **www.avast.com** e clique em "Apoio", na parte superior da tela. A partir do menu abaixo, clique em "Apoio Técnico". De seguida, localize "Filme de Instruções" no canto inferior esquerdo da tela e clique em "Como inserir a chave de activação".

Em alternativa, siga os passos descritos abaixo.

1. Seleccione a chave de registo no e-mail recebido da avast! Para fazer isso, mover o cursor do rato de modo q que este fique colocado imediatamente à esquerda da primeira letra da chave de registo. Clique no botão esquerdo do rato e com o botão esquerdo ainda premido, mova o rato para a direita até que toda a chave esteja destacada. Depois liberte o botão esquerdo do rato, mova o rato para posicionar o cursor sobre a chave de licença que destacou. Clique no botão direito do rato e, a partir do menu, seleccione "Copiar".

2. Clique com o botão direito no ícone da bola azul com um “a” no canto inferior direito da tela e depois à esquerda clique em "Sobre avast!..."

3. Clique no botão "Licença" no canto inferior direito.

4. Posicione o cursor na caixa de chave de licença, clique no botão direito do rato e na lista de opções de menu seleccione "Colar". A chave de licença foi agora inserida.

5. Clique em "OK". O programa pode agora continuar a ser utilizada por 12, 24, ou 36 meses, a contar da data da compra, dependendo da licença adquirida. Ao fim desse tempo, será necessário apenas comprar e inserir uma nova chave de licença.

Noções básicas para a utilização do antivírus avast!

O avast! antivírus oferece protecção contra todos os tipos de malware e contém uma poderosa "protecção residente", também vulgarmente designada por protecção "on-access" que ela verifica ficheiros no momento em que eles são acedidos.

Normalmente a protecção residente presta toda a protecção necessária para evitar que o seu computador seja infectado por um vírus. Depois que o programa tenha sido instalado, a protecção residente é executada continuamente em segundo plano e monitoriza todas as partes da actividade do seu computador. No entanto, se a protecção residente é desligado por algum motivo, ou se tiver estado inactiva por algum período de tempo, é possível realizar uma verificação manual (também conhecida como uma verificação "on-demand") de todos os ficheiros no seu computador.

O avast! antivírus também inclui um protector de ecrã especial que constantemente varre o computador em busca de vírus quando é ligado.

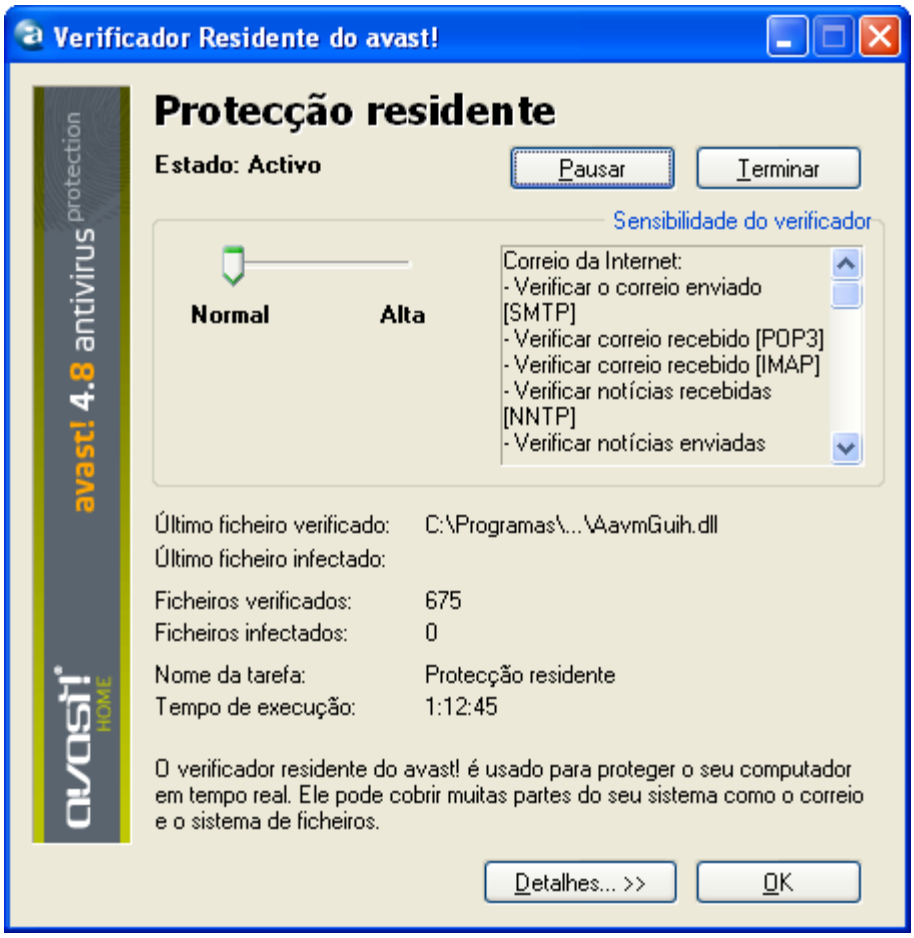
Protecção Residente

Esta parte do programa monitoriza continuamente o computador todo e todos os programas em execução, para detectar eventuais actividades suspeitas (por exemplo, um vírus), evitando assim qualquer dano nos ficheiros do seu computador. Esta aplicação é executada de um modo totalmente independente (é activa automaticamente quando se inicia o computador) e se tudo estiver OK, nem sequer reparará que está em funcionamento.

O ícone da bola azul com um “a” no canto inferior direito do ecrã do computador, ao lado do relógio, mostra o estado actual da protecção residente. Normalmente a presença do ícone azul indica que a protecção residente está instalado e está activamente a proteger o seu computador. Se o ícone tem uma linha vermelha através dele, a protecção está desactivada e o seu computador não está protegido. Se ele tem uma aparência cinza, isso significa que a protecção foi pausado - ver página seguinte.

As configurações da protecção residente podem ser acedidas com um clique com o botão esquerdo do rato no ícone do canto inferior direito do ecrã, ou clique directamente e seleccione "Protecção Residente".

Aparecerá a seguinte imagem:



Nesta janela, pode suspender temporariamente a protecção residente clicando em "Pausar", ou "Terminar". Aqui, ambas as opções têm o mesmo efeito. No entanto, a protecção residente será reactivada automaticamente na próxima vez que o computador seja reiniciado. Isto é simplesmente uma salvaguarda para se certificar de que o seu computador não é deixado acidentalmente desprotegido.

Pode também ajustar a sensibilidade da protecção residente clicando sobre a linha de cada lado do cursor para mudar a sensibilidade para "Normal" ou "Alta". No entanto, a protecção residente na verdade é composta por diferentes módulos ou "Provedores", cada um dos quais é destinado a proteger uma parte diferente do seu computador - veja a próxima página. Todas as alterações que forem feitas nesta janela serão aplicáveis a todos os módulos da protecção residente em conjunto.

A protecção residente é composta pelos seguintes módulos ou "Provedores":

Mensagens Instantâneas verifica os ficheiros descarregados através de mensagens instantâneas ou programas de "chat" como o ICQ e o MSN Messenger e muitos outros. Embora as mensagens instantâneas em si não representem um sério risco de segurança em termos de vírus, hoje em dia as aplicações MI estão longe de ser apenas ferramentas de conversa: a maioria delas também permitem o compartilhamento de ficheiros – o que pode muito facilmente levar a infecções por vírus, se não forem devidamente vigiadas.

Correio da Internet verifica a entrada e saída de mensagens electrónicas de clientes que não o MS Outlook e o MS Exchange, como o Outlook Express, Eudora, etc.

Escudo da Rede fornece protecção de worms da internet, tais como Blaster, Sasser, etc. Este provedor só está disponível para sistemas baseados em NT (Windows NT/2000/XP/Vista).

Outlook/Exchange verifica a entrada e saída de mensagens de correio electrónico processadas pelo MS Outlook ou pelo MS Exchange e bloqueia qualquer mensagem com um potencial vírus de ser aceite ou enviada.

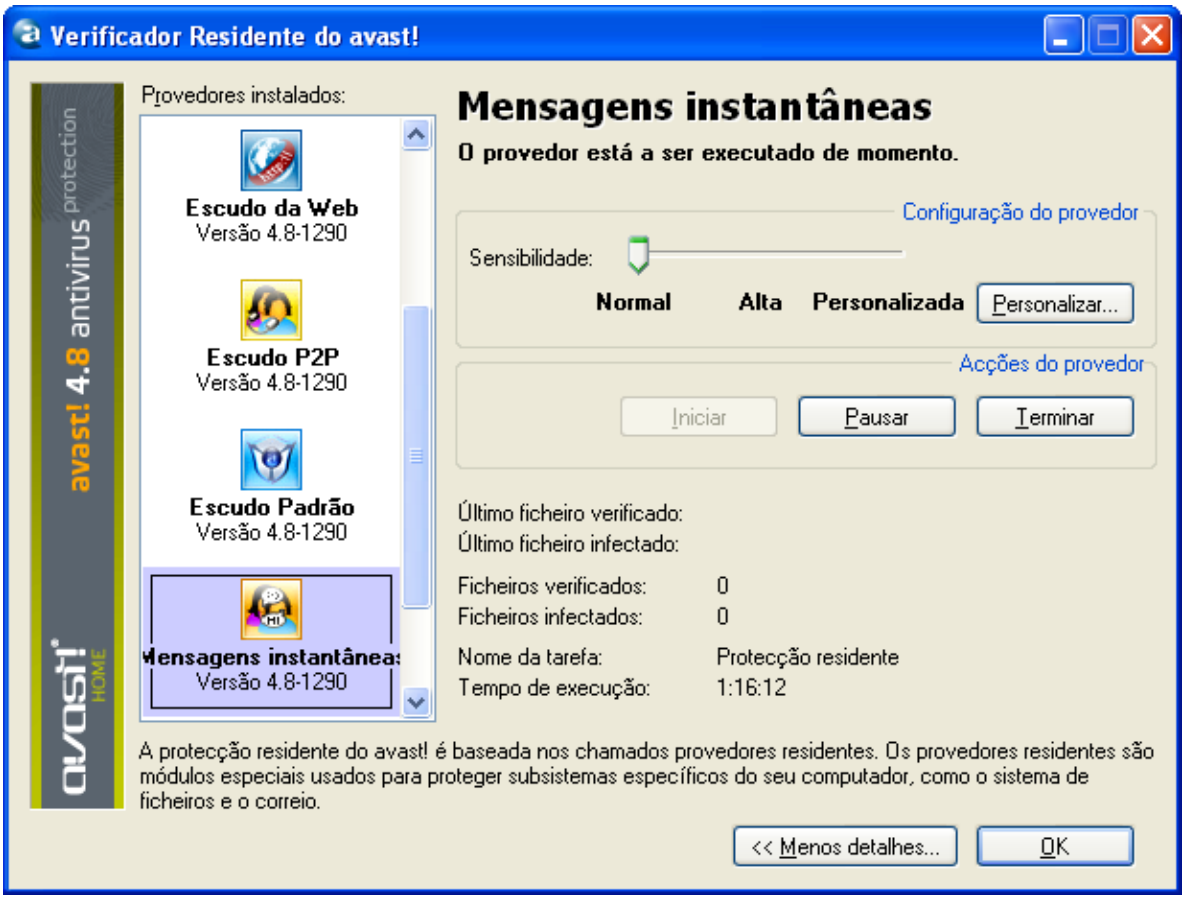
Escudo P2P verifica os ficheiros baixados por programas P2P comuns (partilha de ficheiros), programas como o Kazaa, etc.

Bloqueador de Scripts (apenas na Professional Edition) verifica os scripts de todas as páginas da Web que visitar de modo a evitar qualquer infecção devido a vulnerabilidades do navegador.

Escudo Padrão verifica os programas que estão a ser executados e os documentos que estão abertos. Previne que um programa infectado seja iniciado ou um documento infectado de ser aberto, impedindo assim que um vírus seja activado e provoque quaisquer danos.

Escudo da Web protege o computador contra vírus durante a utilização da internet (navegação, download de ficheiros etc.) e também pode bloquear o acesso a páginas da Web específicas. Se descarregar um ficheiro infectado, a Protecção da Internet irá prevenir que este seja iniciado e cause quaisquer danos. No entanto, a Protecção da Internet irá detectar o vírus até mesmo antes - durante o download do arquivo, proporcionando uma protecção ainda maior. A Protecção da Internet é compatível com os principais navegadores da rede, incluindo o Microsoft Internet Explorer, o FireFox, o Opera e o Mozilla. Devido a uma característica especial chamada "Intelligent Stream Scanning", que permite que os ficheiros descarregados sejam verificados quase em tempo real, o seu impacto na velocidade de navegação é praticamente desprezível.

É possível ajustar a sensibilidade de cada módulo separadamente. Para definir a sensibilidade individual para cada módulo, ou para fazer uma pausa ou encerrar um módulo específico, clique em "Detalhes ...". A janela será, então, expandida como a que se segue:



Na caixa expandida, os provedores são mostrados individualmente no painel do lado esquerdo. A sensibilidade de cada módulo pode ser definida clicando sobre o respectivo módulo do lado esquerdo, de seguida, clique sobre a linha da sensibilidade para a esquerda ou para a direita. Nesta caixa, também é possível parar os diferentes provedores da protecção residente individualmente, tanto temporária como definitivamente, clicando em "Pausar" ou "Terminar". Se clicar em "Pausar", o módulo relevante será reactivado automaticamente na próxima vez que o computador for reiniciado. Se seleccionar " Terminar", o programa perguntará se deseja que o módulo permaneça desligado indefinidamente, ou se deve retomar depois de reiniciar o computador - ver **página 70**. Se clicar “Sim”, esse provedor irá continuar desactivado, mesmo depois de reiniciar o seu computador, até que o reactive manualmente.

Há uma gama de opções adicionais que podem ser seleccionadas para cada provedor, por exemplo, é possível especificar os tipos de ficheiros que devem ser verificados. Pode ter acesso a estas opções adicionais clicando em "Personalizar...". Estas opções são descritas em maior pormenor na **página 56** – Definições da Protecção Residente.

Como iniciar uma verificação manual – Interface Simples de Utilizador

Quando executar o programa a primeira vez, ser-lhe-á apresentada uma imagem de um rádio leitor de CD cinzento-prateado que contém todos os botões para definir, executar e processar os resultados de uma verificação de vírus - veja abaixo. Esta é a aparência padrão ou "pele" (skin) do programa (esta aparência pode ser alterada seleccionando outra "skin" - ver **página 33**).

Inicialmente, o rádio aparece por trás de uma caixa contendo os 5 pontos-chave para iniciar. Clique em "Mais informação" para ler mais e, em seguida, "Página inicial" para regressar ao ecrã principal. A informação mais relevante está resumida nas páginas seguintes. Poderá sempre voltar a estes pontos-chave em qualquer altura clicando no **menu** (botão eject – ver a página seguinte) e seleccionar "Ajuda introdutória".

No centro do rádio, ligeiramente do lado direito, está um ecrã que mostra a informação do estado actual:

Versão actual da BD de vírus – a base de dados de vírus contém informações detalhadas sobre todos os vírus conhecidos e actualmente é utilizada pelo programa para identificar quaisquer ficheiros suspeitos.

Protecção Residente – aqui pode ver o actual nível de sensibilidade.

Data da última verificação – a data de quando foi executada a última verificação manual.

Base de dados de Vírus (VRDB) – contém detalhes dos ficheiros instalados no seu computador e é usado para repará-los, caso sejam danificadas por um vírus. A data indicada é a data em que a base de dados de vírus foi actualizado pela última vez.

Actualizações Automáticas – mostra o estado da actualização de ambos a base de dados de vírus e do próprio programa - para alterar o estado da actualização, clique sobre o actual estado do lado direito da janela – ver **página 40**.

Em ambos os lados do ecrã podem ser vistos três botões de comando:

Em cima no lado esquerdo – este botão abre a **Quarentena**. Para informação sobre como trabalhar com os ficheiros da Quarentena ver a **página 52**.

No meio do lado esquerdo – Ao clicar neste botão poderá alterar a sensibilidade da Protecção Residente deslizando a barra de controle. Clique sobre o controle deslizante e mova-o para a esquerda ou para a direita para diminuir ou aumentar a sensibilidade. Nota – ao alterar o nível da sensibilidade aqui vai afectar todos os provedores da protecção residente. Para ajustar os módulos individualmente ver a **página 23**

Em baixo do lado esquerdo – clicar neste botão ou clicando sobre o estado actual no visor irá actualizar a base de dados de Vírus.

Para actualizar a base de dados com informações sobre quaisquer novos ficheiros que foram instalados ou executados no seu computador, clique com o botão direito do rato sobre a bola azul com um "i" no canto inferior direito do ecrã do computador, e escolha a opção “Criar a VRDB agora”.

Os três botões do lado direito são utilizados para definir as áreas a serem verificadas – qualquer combinação de discos rígidos locais, de media amovível (disquetes, CDs, etc.) e pastas seleccionadas – ver próxima página.

botão **Iniciar** – clique neste botão para iniciar ou retomar a verificação da(s) área(s) seleccionada(s). Este botão passa depois a ser o botão **Pausa**.

botão **Pausar** – clicar neste botão pára momentaneamente a verificação.

botão **Terminar –** Clicar neste botão pára a verificação.

Menu (ejectar) – Clicar no botão com a forma de uma seta a apontar para cima no lado superior esquerdo do rádio irá revelar o **Menu do programa**. Este menu também pode ser acedido se clicar com o botão direito do rato em qualquer posição em cima do rádio.

Quando usar o programa sem uma "skin" (ver **página 33**), as opções do menu são acedidas clicando em "Ferramentas" ou "Definições" na parte superior da imagem.

Algumas opções do menu podem ser acedidas sem iniciar o programa, bastando clicar com o botão direito no ícone da bola azul com um "a" no canto inferior direito do ambiente de trabalho computador.

Todas as opções do menu estão descritas mais à frente neste manual de utilizador.

Selecção das áreas a serem verificadas manualmente

Antes de iniciar a verificação, tem que escolher os ficheiros que pretende verificar.

- ***Verificar Discos Locais***

  Se quer simplesmente verificar tudo no seu computador (todos os ficheiros em todos os discos rígidos), clique no botão superior direito. A imagem no visor com a informação de estado é agora substituída por um novo ecrã - veja abaixo. Para retornar à imagem da informação de estado, clique com o botão direito do rato sobre o rádio e seleccione a opção "Informação de estado".

  Na imagem pode agora ver a linha “Verificar discos locais” e o estado mudou “Desligado” para “Ligado”.

  Pode também ver que apareceu uma outra caixa do rádio. Esta caixa pode ser usada para definir a sensibilidade do verificador. Se deslizar a barra horizontal para a esquerda diminui a sensibilidade, se o fizer para a direita aumentará a sensibilidade. Nesta caixa, poderá também escolher se deseja arquivar ficheiros para serem verificados. Estas opções são descritas na próxima secção.

- ***Verificar media amovível***

  Se deseja verificar o conteúdo de certas medias amovíveis, como por exemplo disquetes ou CD / DVDs, clique no botão direito central.

  Ao clicar neste botão irá mudar o estado de "Verificar media amovível" de "Desligado" para "Ligado".

  Irão também ser exibidas duas caixas à direita do rádio, que podem ser desmarcadas ou marcadas para indicar que tipo de media amovível deve ser verificado (alguns media magnéticos ou magneto-ópticos, tais como discos ZIP, também contam como disquetes).

  Na caixa exibida acima pode especificar a sensibilidade de verificação e decidir se arquivos também devem ser verificados.

- ***Verificar as pastas seleccionadas***

  A última opção é o botão inferior direito. Este botão é usado se pretender definir apenas determinadas pastas para serem verificadas. Depois de clicar neste botão, será exibida uma lista com todas as pastas do seu computador, a partir da qual poderá seleccionar as pastas que deseja serem verificadas. Esta definição oferece mais flexibilidade, mas exige que o utilizador defina exactamente o que é para ser verificado.

  Pode ajustar a sensibilidade da verificação e especificar se ficheiros de arquivos devem ou não ser verificados da mesma maneira que as outras áreas.

É possível combinar mais de um tipo de verificação, por exemplo, é perfeitamente possível iniciar a verificação de todo o seu disco rígido e medias amovíveis, clicando em ambos os botões dos discos rígidos locais e da media amovível.

Ajustar a sensibilidade e executar a verificação

Ao definir a(s) área(s) a ser(em) verificada(s) poderá também configurar a sensibilidade do exame e se o programa irá ou não verificar o conteúdo dos arquivos, ou seja, ficheiros com nomes que terminem em .zip, .rar, .ace, .acj, etc. . Para incluir estes ficheiros seleccione primeiro que áreas que pretende verificar (ver acima), em seguida, clique na caixa de selecção na secção "verificar ficheiros" que aparece acima do rádio. A sensibilidade da verificação determina o nível da minuciosidade do exame. A sensibilidade é definida pelo botão deslizante para a esquerda ou para a direita. Pode escolher entre três níveis pré-definidos.

- **Verificação Rápida**. Esta pesquisa, tal como o nome sugere, é muito mais rápida pois os ficheiros são analisados de acordo com seus nomes, e somente aqueles que são considerados potencialmente perigosos são realmente verificados. Este tipo de verificação por vezes pode levar a que alguns ficheiros que contenham vírus não sejam verificados, no entanto, é geralmente o suficiente.

- **Verificação Padrão**. Neste tipo de verificação, os ficheiros são analisados com base nos seus conteúdos (e não nos seus nomes, como é na Verificação Rápida). No entanto, apenas as partes "perigosas" dos ficheiros são testadas, e não o ficheiro completo. Este tipo de verificação pode também levar a que um vírus não seja detectado, no entanto, é muito mais eficaz do que a Verificação Rápida.

- **Verificação Exaustiva**. Neste tipo de teste todos os ficheiros são verificados na íntegra, e verifica todas as infecções listadas na base de dados. Este tipo de verificação tem a mais alta confiança, mas leva muito mais tempo que uma verificação Rápida ou Padrão.

Após seleccionar as opções de verificação, tudo que tem a fazer é iniciar o teste. Para o fazer clique no botão Play/Iniciar (seta que aponta para direita) do lado esquerdo do leitor.

Método Alternativo

Pode também definir as áreas a serem verificadas indo ao **menu** e clicar em “Iniciar verificação” e depois em “Seleccionar área para verificação”. Depois de escolher a área a ser verificada, poderá também especificar se arquivos devem ser incluídos, seleccionando "Verificar ficheiros de arquivo".

Ao clicar em "Seleccionar nível de verificação" pode também especificar se a verificação deve ser uma Verificação Rápida, Verificação Padrão ou uma Verificação Exaustiva, conforme descrito acima.

Executar e processar os resultados de uma Verificação

Depois de clicar no botão Iniciar (Play) ou seleccionar "Iniciar verificação" no **menu**, o programa começa a verificar as áreas seleccionadas. Este processo pode demorar bastante tempo, dependendo do número e tamanho dos ficheiros a serem testados e da velocidade do seu computador. Lembre-se que embora a Verificação Exaustiva seja a opção que demora mais tempo, é a mais eficaz.

Depois de o programa ter iniciado, pode trabalhar com outros ficheiros ou programas do seu computador, mesmo que o exame esteja a ser executado. Para tal é recomendado minimizar o avast! para que ele seja executado em segundo plano. Caso contrário, pode acontecer que o computador se torne muito lento (a verificação de vírus é uma tarefa bastante exigente). Para enviar a verificação para o segundo plano basta clicar no botão Minimizar (_) no canto superior direito do rádio enquanto o teste está a ser executado e ele desaparecerá da imagem. Para o trazer de volta, basta clicar sobre a "caixa" do avast! que pode ser encontrada na barra horizontal na parte inferior do ecrã.

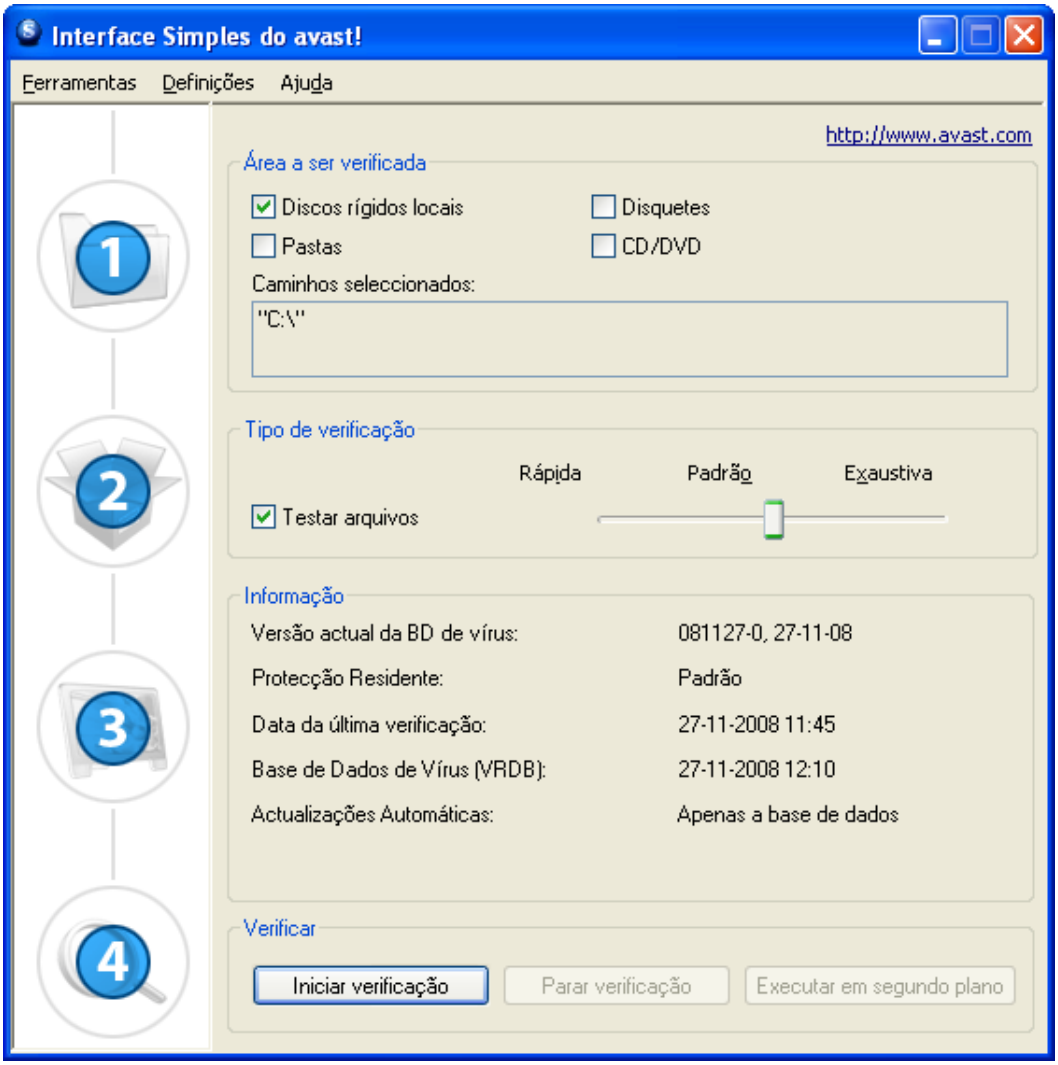
Quando a verificação tiver terminado, e se nenhum vírus foi detectado, a janela do rádio mostrará as informações básicas, tais como o número de pastas e ficheiros verificados, o tempo de execução, etc.

Se forem encontrados quaisquer vírus, o programa irá perguntar-lhe o que fazer com o(s) ficheiro(s) infectado(s). Há várias opções: mover o ficheiro para a **Quarentena**, apagá-lo, alterar-lhe o nome ou movê-lo, ou até, se possível, repará-lo. Além disso, pode simplesmente manter o ficheiro intacto, no entanto, esta opção pode resultar em maior propagação do vírus provocando danos. Estas opções são descritas em mais pormenor na secção "**O que fazer se um vírus for encontrado**".

Alterar a aparência da Interface Simples de Utilizador

Se utilizar a interface simples de utilizador, é possível seleccionar diferentes peles ("skins") do programa. Três skins (aparências) diferentes são oferecidos como padrão e outros podem ser transferidos da Internet caso o deseje – para tal clique com o botão direito do rato sobre o rádio avast! e do **menu**, clique em "Seleccionar Skin..." e depois no link "Obtenha mais skins do nosso servidor". Em alternativa, se quiser usar o programa sem qualquer skin, seleccione "Definições" nas opções do menu, em seguida, desmarque a opção "Activar skins para a Interface Simples de Utilizador". Da próxima vez que iniciar o programa, as opções serão exibidas no seu formato básico. Para restaurar a skin, clique em "Definições", de seguida, clique em"Definições" novamente e, por último, volte a preencher a caixa da opção " Activar skins para a Interface Simples de Utilizador". A skin será restaurada na próxima vez que o programa for iniciado.

Aparência da Interface Simples de Utilizador sem nenhuma skin:



A(s) área(s) a ser verificada(s) e o tipo de verificação são definida(s) marcando as respectivas caixas. Se quer verificar apenas pastas específicas, marcando a caixa "Pastas" irá abrir uma janela com a lista de todas as pastas do seu computador. Para escolher uma pasta, basta marcar a caixa apropriada e ela aparecerá no campo "Caminhos Seleccionados".

Pode ajustar a sensibilidade da verificação movendo o botão deslizante para a posição que desejar em “Tipo de verificação”, caso queira incluir arquivos na verificação, clique em “Testar arquivos”.

Depois de ter iniciado a verificação pode continuar a usar o computador para outras tarefas, basta clicar em "Executar em segundo plano".

A sensibilidade da protecção residente pode ser ajustada se clicar em "Definições" e depois em "Protecção Residente". Utilize o botão deslizante para alterar a sensibilidade para "Padrão" ou "Alta" ou pode até desactivar a protecção residente completamente, para tal arraste o botão para "Desactivar". No entanto, como descrito anteriormente, todas as mudanças que fizer aqui serão aplicadas igualmente a todos os provedores da protecção residente. Para ajustar a sensibilidade destes módulos individualmente veja a **página 23**.

Pode aceder a outras funcionalidades, tais como a Quarentena e a Base de Dados de Vírus, clique em "Ferramentas" e escolha a opção pretendida a partir das opções disponíveis. Estas, e todas as outras características, são descritas em detalhe mais adiante neste manual de utilizador.

A informação do estado actual é apresentada na metade inferior da janela, tal como descrito na secção anterior.

O que fazer se um vírus for encontrado

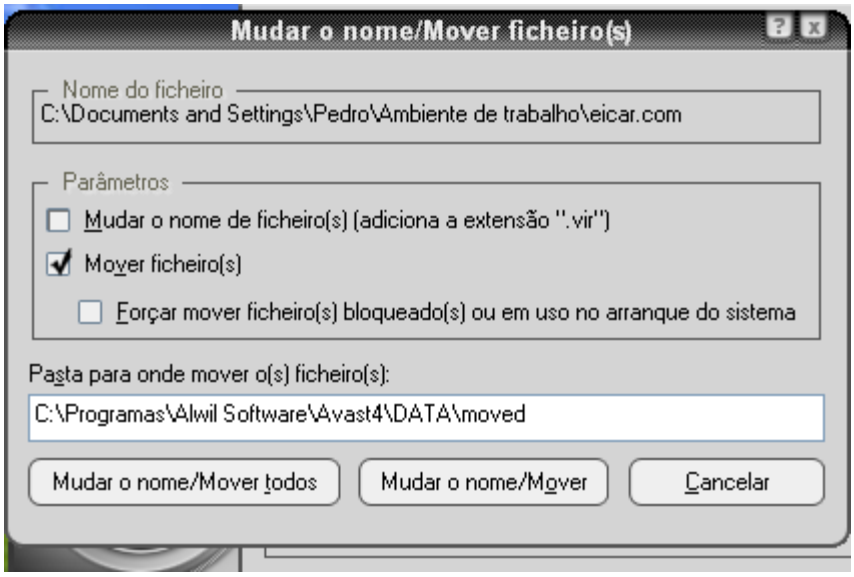
Se o programa detectar um ficheiro suspeito, a verificação será interrompida neste ponto e será exibida uma janela a perguntar como deseja prosseguir:

Se clicar em "Continuar" nenhuma acção será tomada agora e o ficheiro identificado aparecerá na lista dos resultados, no fim da verificação - ver **página 39**. Se clicar em "Parar" parará a verificação neste ponto.

Se um vírus for detectado por um dos provedores de protecção residente, por exemplo ao tentar abrir um ficheiro infectado, ou pelo protector de ecrã, a janela será um pouco diferente – os botões "Continuar" e "Parar" serão substituídos por um único botão a dizer "Nenhuma acção". Se clicar neste botão, para que nenhuma providência seja tomada, o ficheiro infectado permanecerá onde está, mas o vírus não será activado.

No entanto pode também tomar uma das possíveis quatro acções.

Opção 1: Mover o ficheiro infectado para outra pasta no seu computador. Ao mesmo tempo, também terá a oportunidade de mudar o nome. Se clicar em "Mover / MudarNome" será assinalado na caixa de verificação "Mover ficheiro(s)".



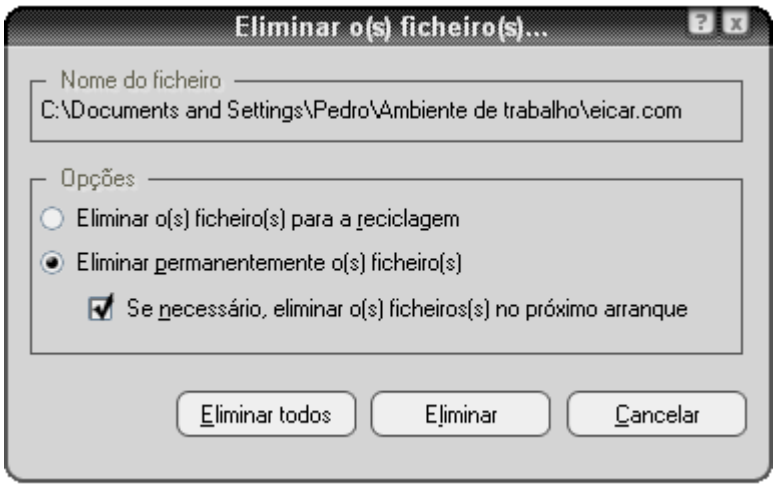
Na parte branca da imagem, é possível especificar para onde deseja mudar o ficheiro suspeito. O programa selecciona automaticamente a pasta de destino adequada, mas pode também definir outra à sua escolha.

Se também clicar na caixa de verificação "Mudar o nome do ficheiro(s)….", isto irá adicionar a extensão ".vir" no fim do nome do ficheiro de modo a este ficar identificado como um ficheiro potencialmente perigoso de modo a que utilizador não o execute acidentalmente, evitando uma infecção que possa danificar o computador.

Se não for possível mover o ficheiro neste momento, por exemplo porque ele está a ser usado por outro programa, se marcar a caixa "Forçar mover ficheiro(s) bloqueado(s) ou em uso no arranque do sistema" irá fazer com que o ficheiro seja movido para o destino seleccionado na próxima vez que o computador for reiniciado.

Nota – no caso de um ***ficheiro de sistema*** ser infectado, por exemplo, um ficheiro que é utilizado para executar um programa fundamental, ao mover o ficheiro poderá resultar num erro na próxima vez o seu computador tente executar o programa. No entanto, se o ficheiro é movido para a Quarentena, ele ficará numa área protegida onde não pode causar danos aos seus outros ficheiros e em que podem eventualmente ser reparados antes de os mover de volta ao seu local inicial – ver **página 8**

Opção 2: Eliminar o ficheiro – se clicar em "Eliminar" irá aparecer a seguinte janela:



Dependendo de qual versão do Windows que utiliza, existem duas maneiras de um ficheiro ser eliminado.

- ***Eliminar o(s) ficheiro(s) para a reciclagem***

Irá mover o(s) ficheiro(s) para a reciclagem mas não o(s) apagará definitivamente. Eles podem, portanto, ser mais tarde restabelecidos. Esta opção pode não estar disponível em algumas versões do Windows.

- ***Eliminar permanentemente o(s) ficheiro(s)***

isto irá remover o(s) ficheiro(s) do seu computador permanentemente, sem qualquer possibilidade de restaurá-lo(s) posteriormente. No entanto, isto só irá excluir o ficheiro infectado. Alguns vírus instalam novos ficheiros no seu computador e se estes ficheiros em si não são eles próprios o vírus, eles não serão detectados como suspeitos. Embora estes ficheiros ocupem espaço no seu computador, eles não devem apresentar qualquer risco de segurança.

Se um vírus for detectado e que possa ser completamente removido pelo limpa vírus embutido no avast, incluindo a remoção de novos ficheiros criados pelo vírus, aparecerá um botão adicional – ***"Eliminar completamente o vírus do sistema"*** – na janela de aviso da presença de vírus. Se esta opção surgir recomenda-se o seu uso.

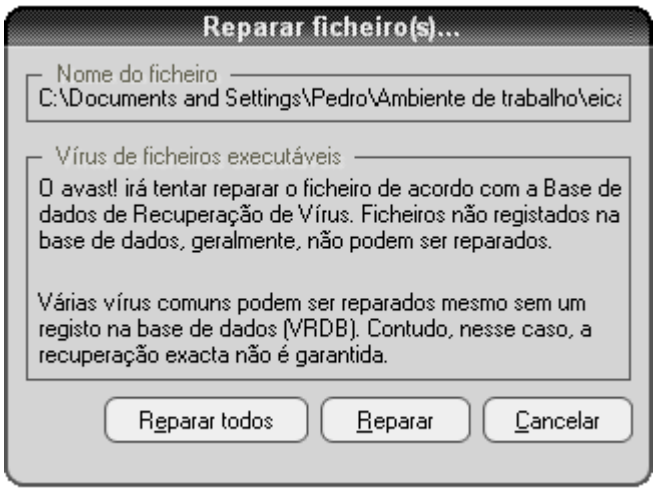
Se não for possível eliminar o ficheiro nesse momento, por exemplo porque ele estar a ser usado por outro programa, se marcar a caixa "Se necessário, eliminar o(s) ficheiro(s) no próximo arranque" irá eliminar o ficheiro automaticamente da próxima vez que o computador seja reiniciado. Em seguida, clique em "Eliminar" novamente para confirmar a exclusão.

Nota – caso um ***ficheiro de sistema*** seja infectado, por exemplo, um ficheiro que é utilizado para executar um programa fundamental, ao ser apagado poderá resultar num erro na próxima vez que o seu computador tente executar o programa. Antes de eliminar o ficheiro, portanto, ter a certeza que o ficheiro infectado não é um ficheiro de sistema, ou que seja possível substituí-lo por um ficheiro limpo, por exemplo, a partir de

uma cópia de segurança.
Caso não tenha a certeza, é recomendado mover o ficheiro para a Quarentena. Aqui ele estará numa área protegida onde não pode provocar quaisquer danos aos outros ficheiros do seu computador e onde poderá eventualmente ser reparado antes de ser restabelecido ao seu local original – ver **página 8**

Opção 3: Reparar o ficheiro.

Se clicar em "Reparar" irá aparecer a seguinte janela:



Se clicar em "Reparar" novamente, o programa irá tentar restaurar o ficheiro infectado ao seu estado original.

De modo a reparar o ficheiro, o programa irá recorrer à ***Base de Dados de Recuperação de Vírus***. Se houver informação suficiente sobre o programa na Base de Dados, tem uma grande probabilidade de poder reparar o ficheiro. Nota – apenas ficheiros que tenham sido fisicamente alterados por um vírus podem ser reparados. Se novos ficheiros foram criados, estes continuarão no sistema a menos que eles possam ser removidos pelo limpa vírus – ver Opção 2.

Se não existirem informações na Base de Dados, a reparação poderá ser possível mas uma recuperação total é menos provável. Por isso é muito importante que Base de Dados esteja continuamente actualizada - para actualizar Base de Dados de Recuperação de Vírus clique com o botão direito do rato sobre a bola azul com um "i" no canto inferior direito do ambiente de trabalho do computador, e escolha a opção "Criar a VRDB agora". A Base de Dados será, então, actualizada com detalhes de quaisquer novos programas instalados no computador desde a última actualização.

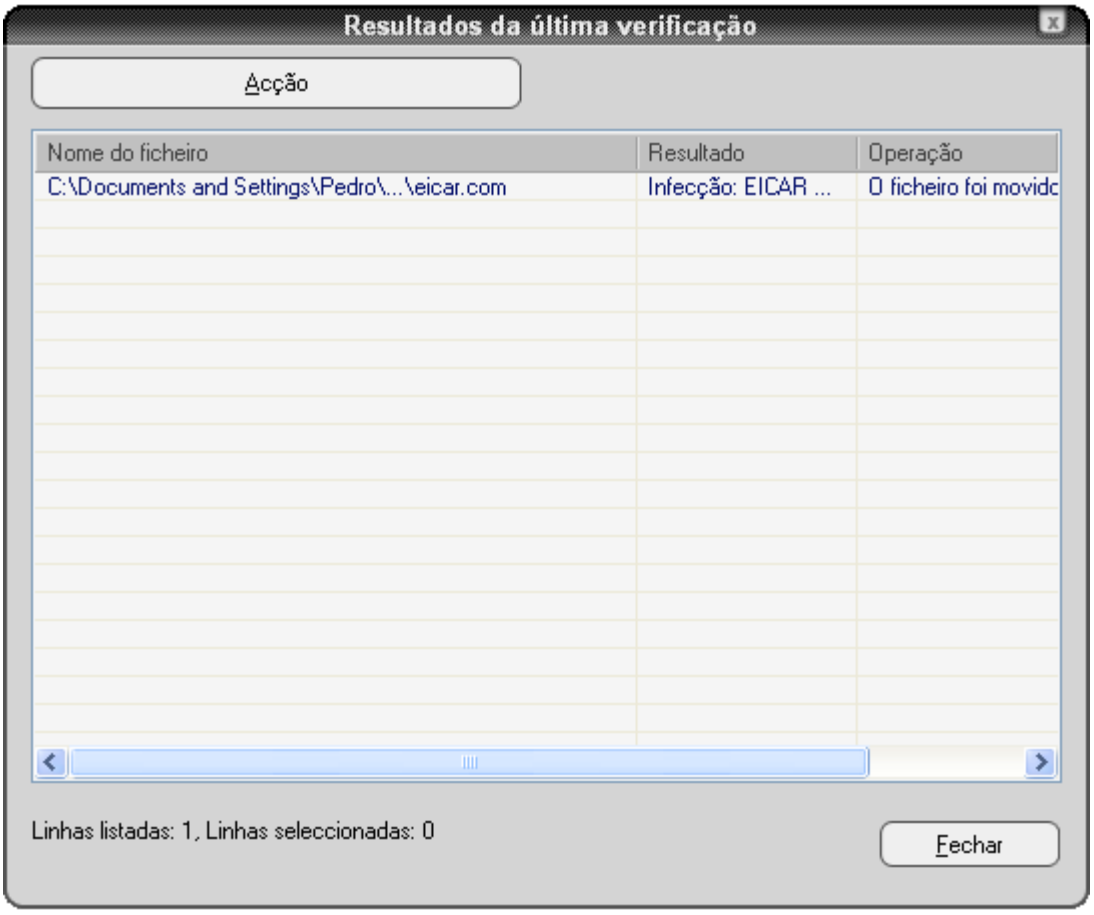
Opção 4: A **Opção RECOMENDADA** é mover o ficheiro para a **Quarentena**.

Nota – caso um ***ficheiro de sistema*** seja infectado, por exemplo, um ficheiro que é utilizado para executar um programa fundamental, ao ser movido poderá resultar num erro na próxima vez que o seu computador tente executar o programa. No entanto, se o

ficheiro for movido para a Quarentena ele estará numa área protegida onde não pode provocar quaisquer danos aos outros ficheiros do seu computador e onde poderá eventualmente ser reparado antes de ser restabelecido ao seu local original – ver **página 8**

Resultados da última verificação

Uma vez que tenha especificado como pretende lidar com o ficheiro seleccionado, a verificação é retomada automaticamente. Se mais alguns ficheiros forem identificados como suspeitos, a verificação será novamente parada e o processo é repetido (a não ser que tenha escolhido a opção “Eliminar todos”. Quando a verificação for concluída, os resultados da verificação são mostrados juntamente com os detalhes das medidas tomadas em relação a cada ficheiro identificado como suspeito - veja abaixo.



Se optou por não tomar qualquer acção durante o processo de verificação em relação a um determinado ficheiro, esse ficheiro será listado na verificação dos resultados, no entanto, a coluna "Operação" estará vazia.

Para lidar com o ficheiro, primeiro clique sobre o nome do ficheiro na tabela, de seguida, clique em "Acção" no canto superior esquerdo e poderá ver a lista de opções como descrito nas páginas anteriores. A acção tomada será então exibida na coluna

"Operação".

Quando acabar este último processo, e se der por satisfeito com as acções tomadas com todos os ficheiros suspeitos, clique em "Fechar" para encerrar o processo de verificação. Para ver novamente os resultados da verificação basta simplesmente abrir o **menu** e seleccionar a opção “Resultados da última verificação”.

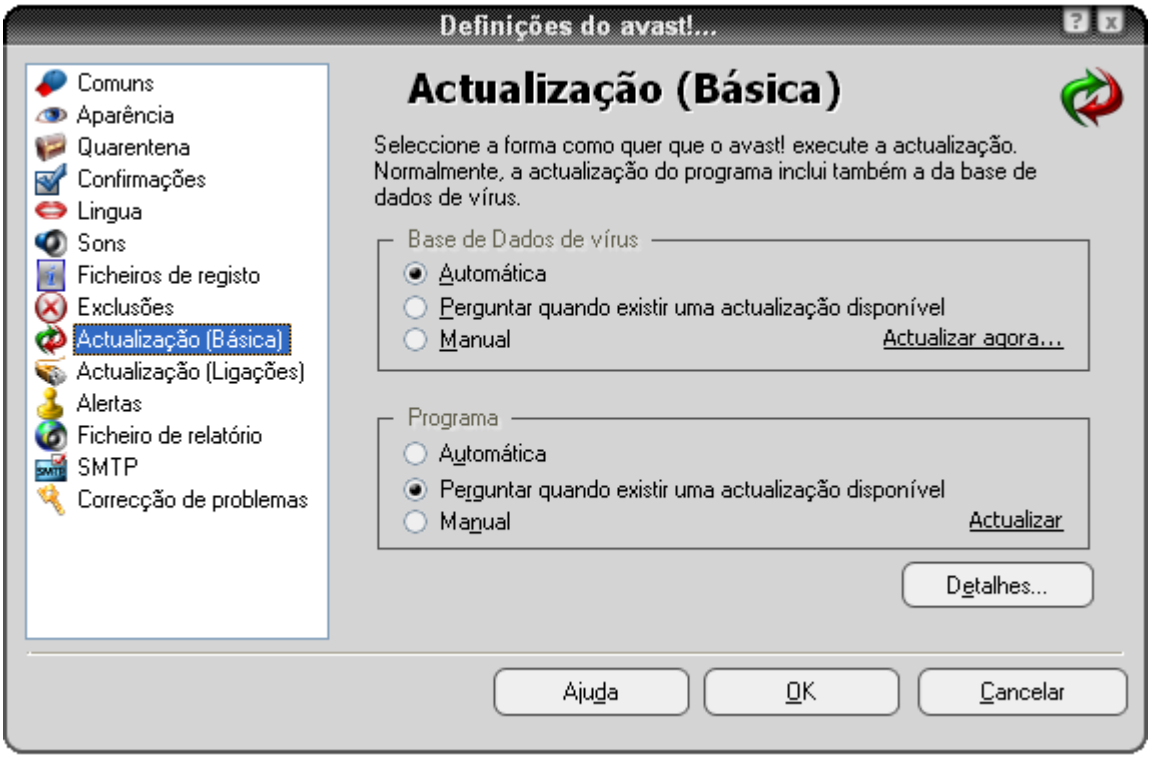
Nota: Se fechar o programa avast!, a opção “Resultados da última verificação”não estará mais disponível e não poderá ver os resultados desta última verificação na próxima vez que iniciar o programa. Esta opção estará apenas disponível novamente caso faça uma nova verificação. No entanto, os detalhes de quaisquer vírus ou erros que tenham sido detectados são guardados e podem ser vistos no Visualizador de Registo – ver **página 54**.

Funcionalidades Avançadas

Configuração das actualizações automáticas

Um programa antivírus é bom apenas se a sua base de dados de vírus conhecidos estiver actualizada, é por isso que é importante actualizar regularmente tanto o programa como a base de dados de vírus.

Pode escolher se o programa e a base de dados de vírus são actualizados automaticamente ou manualmente, ou apenas após uma notificação de que uma actualização está disponível a partir do avast!. Para alterar o estado, tanto pode clicar sobre o estado actual (por exemplo: "Apenas Base de Dados") na janela de rádio do avast, ou simplesmente abrir o **menu** (ver **página 28**), seleccionar “Definições do avast!...”, depois “Actualização (Básica)”. De seguida basta clicar no estado desejado para as actualizações da Base de Dados de Vírus e do Programa (ver abaixo).



Clique em "OK" e o estado na janela do rádio será actualizado do seguinte modo:

- **Ligado** se estiver seleccionada a opção "Automática" em ambos a Base de Dados de Vírus e no Programa
- **Apenas o Programa** se estiver seleccionada a opção "Automática" apenas para o programa
- **Apenas a Base de Dados** se estiver seleccionada a opção "Automática" apenas para a Base de Dados de vírus
- **Desligado** se estiver desligada a opção "Automática" para ambos

Para actualizar **manualmente**, tanto o programa como a base de dados de vírus, vá ao **menu** (ver **página 28**) e seleccione a opção "Actualização".

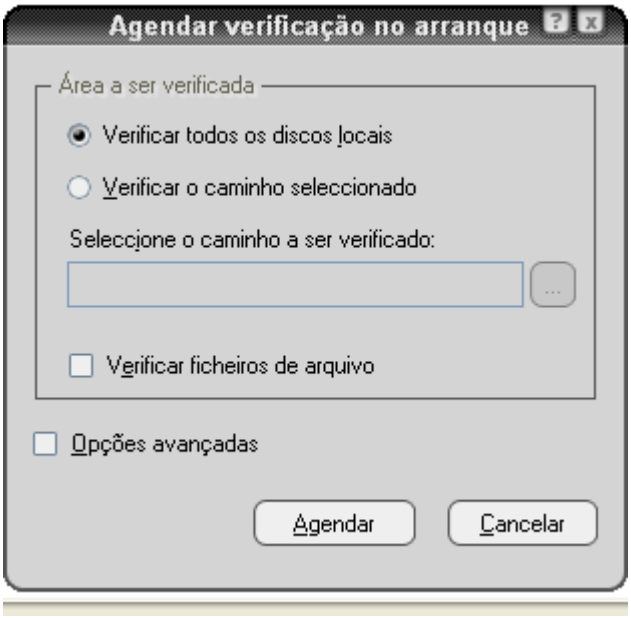
- Para actualizar a Base de Dados de vírus seleccione **Actualização da iAVS**
- Para actualizar o programa avast! seleccione **Actualização do programa**

Como agendar uma verificação durante o arranque

(apenas para versões 32 bits do Windows NT/2000/XP/Vista)

É possível agendar uma verificação a ser efectuada automaticamente quando o computador é reiniciado, ou seja, quando ele "arranca", antes do sistema operacional estar activo. O que é útil se suspeitar que um vírus possa estar instalado no seu computador, uma vez que irá permitir que o vírus seja detectado antes que ele seja activado e, portanto, antes de ter a oportunidade de fazer qualquer dano.

Para agenda uma verificação durante o arranque vá ao **menu** (ver **página 28**) e clique em “Agendar verificação durante o arranque...”. Aparecerá a seguinte janela:



Aqui pode escolher se pretende verificar todos os discos ou apenas áreas seleccionadas. Para verificar apenas áreas seleccionadas, clique em "Verificar o caminho seleccionado" e digite o nome do caminho na caixa fornecida ou clique na caixa quadrada à direita para procurar a área a ser verificada. Quando encontrara área que deseja verificar clique-a e o nome do caminho será copiado automaticamente para a caixa fornecida.

Se deseja incluir a verificação de ficheiros de arquivo basta seleccionar “Verificar ficheiros de arquivo”.

Se seleccionar a caixa “Opções avançadas”, poderá especificar o que deve ser feito com os ficheiros detectados como perigosos. Pode escolher qualquer uma das seguintes opções:

- Eliminar o ficheiro infectado
- Mover o ficheiro infectado
- Mover o ficheiro infectado para a Quarentena

- Ignorar o ficheiro infectado e
- Reparar o ficheiro infectado

Seleccionar "Mover o ficheiro infectado" irá fazer com que todos os ficheiros suspeitos sejam movidos para a pasta C:\Programas\Alwil Software\Avast4\DATA\moved. A extensão ".vir" será também adicionada no fim do nome do ficheiro de modo a indicá-lo como suspeito de modo a que não o execute acidentalmente, infectando assim o seu computador.

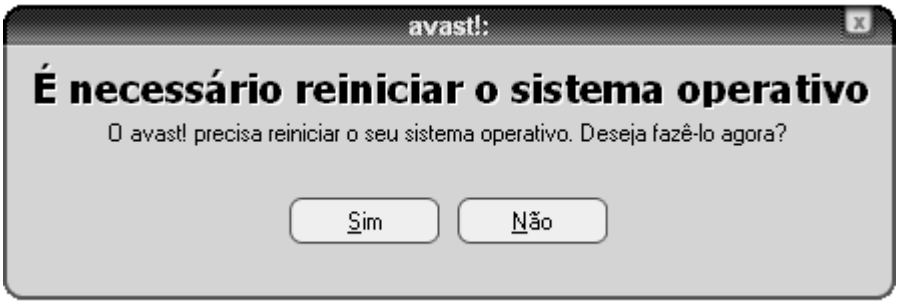
Se escolher qualquer uma das opções para excluir ou mover os ficheiros infectados, será solicitado a confirmar o que fazer se acusar infecção nalgum **ficheiro de sistema**.

Os ficheiros de sistema são usados pelo seu computador para executar programas e ao apagá-los ou movê-los poderá ter consequências graves. Por isso será perguntado se deseja:

- Permitir eliminar ou mover, ou
- Ignorar excluir/mover para ficheiros de sistema

Se escolher "Ignorar excluir/mover" irá prevenir problemas operacionais mas, no entanto, o seu computador ainda poderá estar em risco de uma potencial infecção. A acção recomendada é mover todos os ficheiros suspeitos para a Quarentena. Depois de movidos para a Quarentena, eles não podem causar danos aos seus outros ficheiros. Pode depois lidar com estes ficheiros tal como descrito na **página 52**, por exemplo, eles podem ser eliminado, se tiver a certeza que é seguro fazê-lo, eles podem ser movidos de volta para seu local original, ou podem simplesmente ser armazenados até que decida o que fazer com eles.

Depois de ter confirmado como quaisquer ficheiros infectados devem ser tratados, clique em "Agendar" e aparecerá a seguinte mensagem:



Clique em "Sim" para reiniciar o seu computador e executar a verificação durante o arranque agora, ou escolha "Não" e a verificação será feita automaticamente a próxima vez que executar o seu computador.

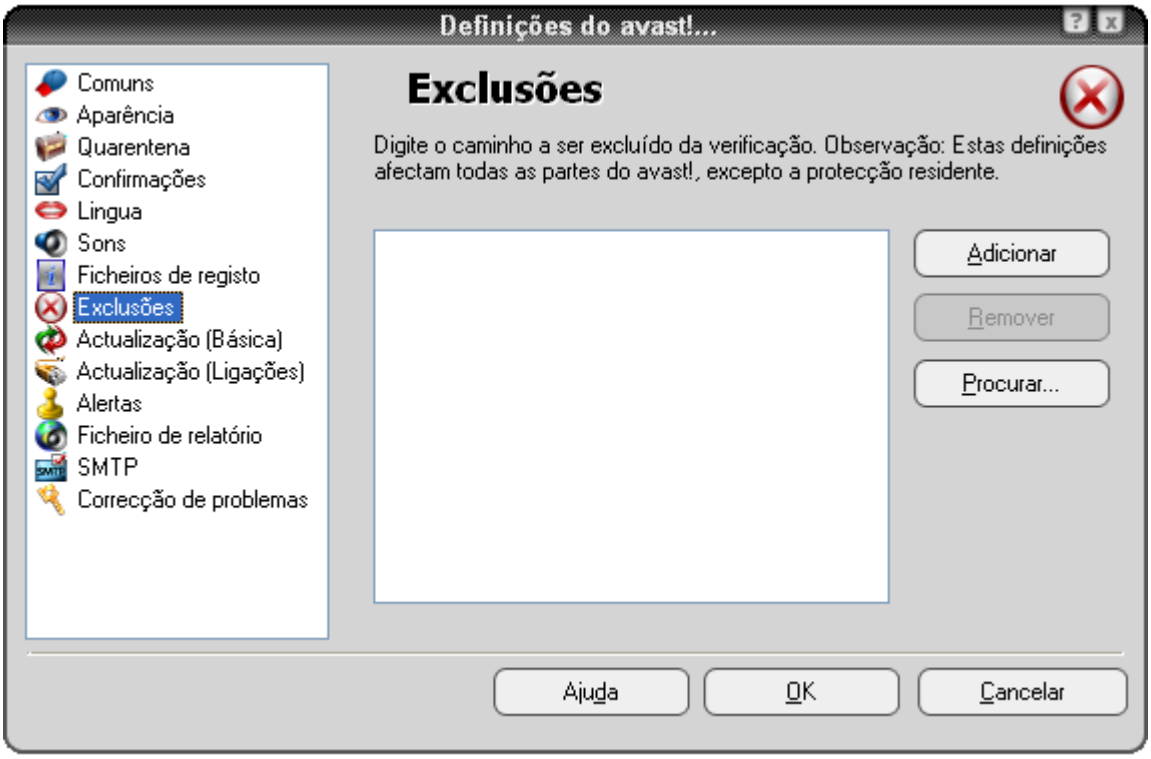
Excluir ficheiros da verificação

É possível excluir alguns locais, ou mesmo ficheiros em particular, de ser verificados, o que significa que eles não serão verificados durante a qualquer exame. Isto pode ser útil em vários casos:

- **Para evitar falsos alarmes**. Se o programa relata uma infecção num ficheiro e tiver a certeza de que se trata de um falso alarme, poderá excluir o ficheiro do teste e evitar mais falsos alarmes. Por favor, informe a avast sobre qualquer um destes ficheiros de modo a que o problema seja corrigido.

- **Para acelerar o processamento**. Se tiver uma pasta no disco rígido que contém apenas imagens, por exemplo, é possível excluí-la do teste adicionando-a à lista de exclusões, o que reduzirá o tempo gasto na verificação.

Tenha em atenção que estas exclusões irão afectar todas as futuras verificações, excepto para a protecção residente. Para excluir certos ficheiros ou pastas de serem verificados, simplesmente clique em "Exclusões" nas "Definições..." no **menu** (ver **página 28**) e aparecerá a seguinte janela:

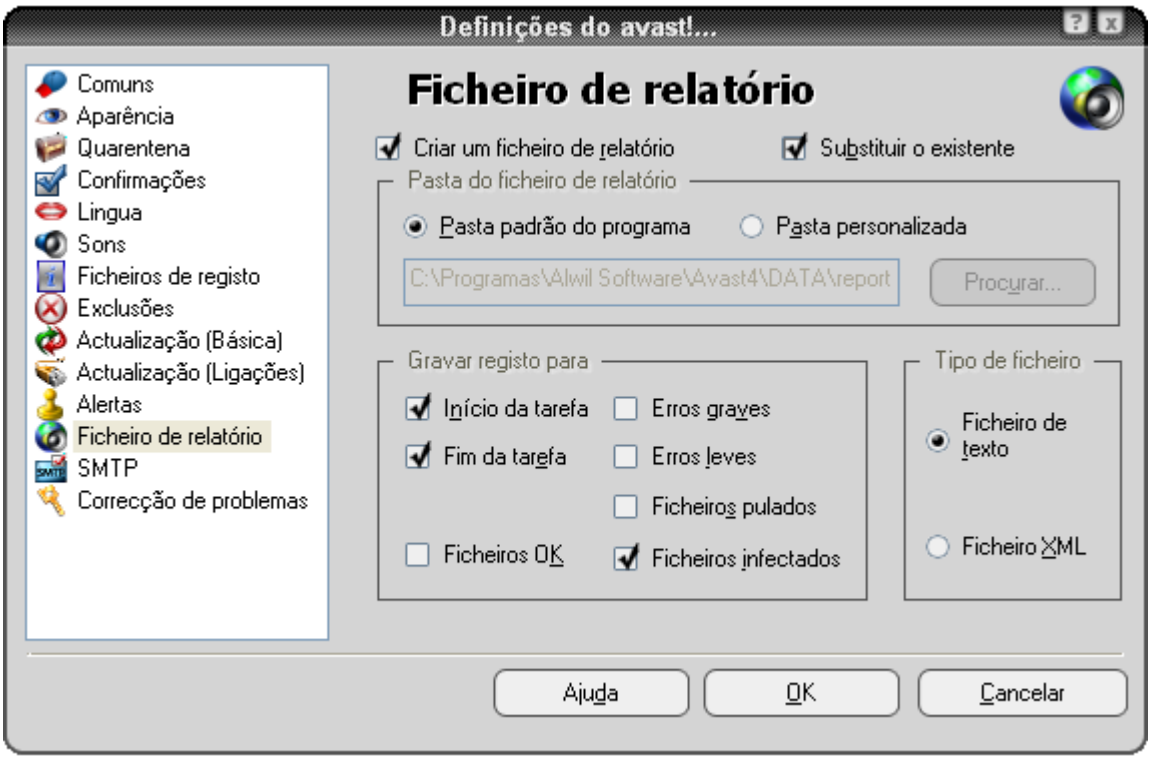


Para excluir uma pasta ou ficheiro clique em "Procurar" e depois escolha a pasta ou ficheiro a ser excluído. Como alternativa pode clicar em "Adicionar" e manualmente digitar o local da pasta ou ficheiro relevante para a caixa de exclusões. Caso deseje excluir uma pasta e todas as suas subpastas é necessário adicionar "*****" no fim do nome

da pasta, por exemplo C:\Windows*. Para remover uma pasta ou um ficheiro da lista de exclusões, clique nele uma vez para realçá-lo e, em seguida, clique em "Remover".

Como criar um ficheiro de relatório da verificação

Pode criar um registo permanente do resultado de cada verificação, criando um relatório que poderá visualizar mais tarde. Para criar um relatório comece por ir ao **menu** como descrito na **página 28** e seleccione "Definições". Depois clique em "Ficheiro de relatório" e no ecrã seguinte clique na caixa "Criar um ficheiro de relatório" como mostrado na imagem abaixo.



Se quer criar um novo relatório depois de cada verificação e não deseja guardar todos os relatórios das suas verificações, preencha a caixa "Substituir o existente". Se esta caixa não for preenchida os resultados de cada verificação serão adicionados ao fim do último relatório.

Pode também escolher onde quer que o relatório seja guardado – na pasta padrão do programa, que o programa atribui automaticamente, ou num novo local especificado por si se clicar em "Pasta personalizada" e inserir a localização da pasta.

De seguida pode especificar que informação deseja incluída no relatório:

- Inicio da tarefa – a data e hora do inicio da verificação
- Fim da tarefa – a data e hora do fim da verificação
- Ficheiros OK – ficheiros verificados em que não foi detectado nada suspeito. Se todas as unidades forem verificadas, ao escolher esta opção irá produzir

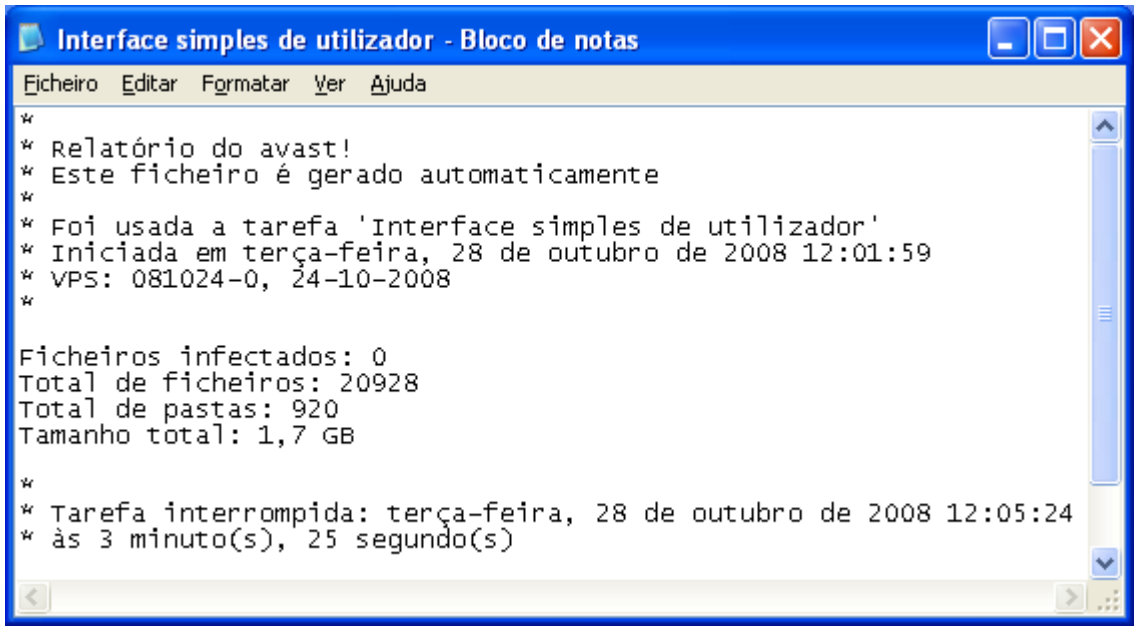
um relatório bastante longo, possivelmente com milhares de linhas. Por isso recomenda-se que active esta opção apenas se for verificar uma verificação limitada ou desejar mesmo ver a lista de ficheiros limpos, para além dos problemáticos.

- Erros graves aparecem quando o programa detecta algo que não seria de esperar. Estes erros normalmente requerem uma investigação mais profunda.
- Erros leves são menos sérios que os últimos e, geralmente, estão relacionados com ficheiros que não puderam ser verificados por estarem abertos e a ser usados por outras aplicações.
- Ficheiros pulados são aqueles que não são verificados devido às definições de verificação. Por exemplo, numa verificação rápida a verificação dos ficheiros é baseada nas extensões dos mesmos. Ficheiros com extensões que não são consideradas perigosas não são verificados. Quaisquer ficheiros excluídos da verificação podem também aparecer como pulados.
- Ficheiros infectados – estes são ficheiros que potencialmente contêm um vírus.

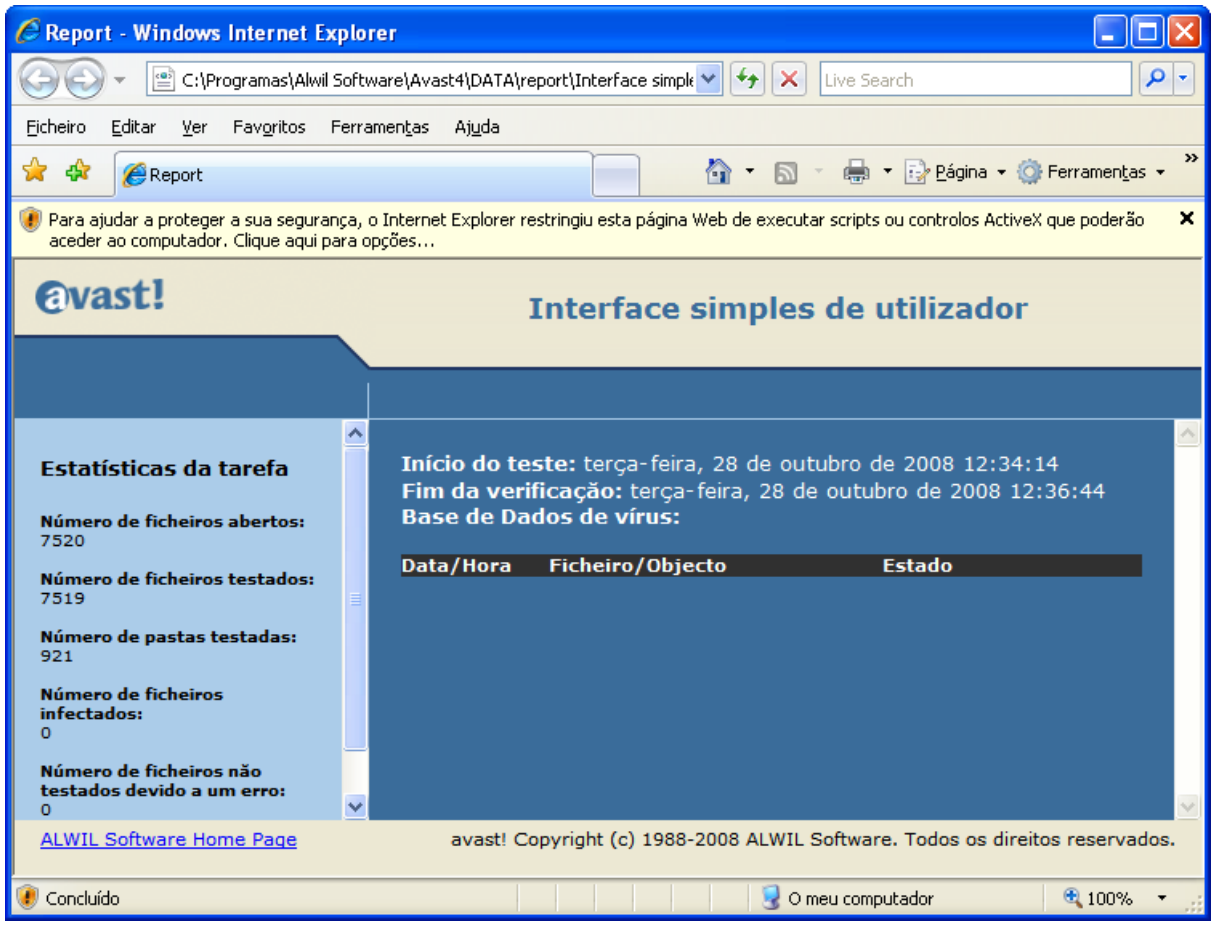
Finalmente, pode especificar se o relatório deve ter a forma de um ficheiro de texto ou de XML. Depois de executar a verificação aparecerá uma nova linha na janela com a informação de estado – "Ver o relatório da última verificação" tal como pode ver na imagem abaixo.

Ao clicar "Ver o relatório da última verificação" aparecerá o relatório no formato previamente especificado. Como alternativa, abra o **menu** (ver **página 28**) e clique em "Visualizar relatórios de verificação..."

Relatório em formato de texto:



Relatório em formato XML:



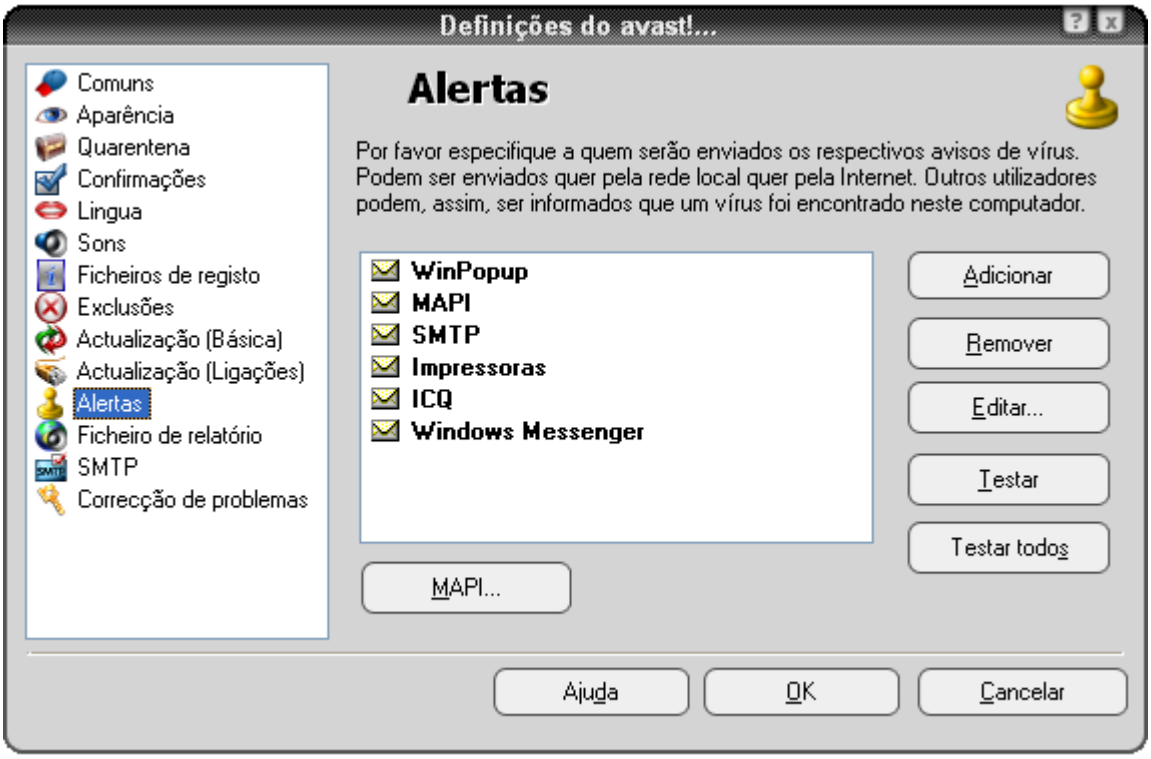
Os relatórios de verificações antigas são armazenados numa pasta escolhida pelo programa ou numa pasta criada por si – ver a página anterior.

Se especificou o formato de texto e não escolheu a opção de "Substituir o existente", poderá também visualizar os relatórios antigos sempre que ver o relatório depois da verificação.

Se não deseja que sejam criados mais nenhuns relatórios basta ir a "Ficheiro de relatório" no **menu** (ver **página 28**) e esvaziar a caixa "Criar um ficheiro de relatório".

Alertas

O avast! pode enviar uma mensagem de aviso sobre a ocorrência de vírus. Do **menu**, seleccione "Definições" e depois "Alertas" Este recurso é útil para administradores de rede que serão notificado sobre a presença de um vírus em qualquer computador na sua rede, para que eles possam reagir rapidamente.



O alerta pode ser enviado das seguintes formas:

- **WinPopup.**
  Clique em "Adicionar" e seleccione WinPopup. Depois insira a morada IP ou o nome do computador na rede onde quer receber o aviso, ou clique em "Procurar" e seleccione uma morada da lista de opções disponível.

- **MAPI.**
  O alerta será enviado por email, utilizando o protocolo MAPI. Insira a morada de email onde quer receber o aviso, depois clique no botão MAPI no fundo da janela e insira o nome do perfil MAPI e a respectiva senha.

- **SMTP.**
  O será enviado por email utilizando o protocolo SMTP. Para criar um novo alerta clique em "Adicionar" e depois SMTP. Na janela que aparece insira a morada de email da pessoa que quer que receba o alerta. Também é necessário especificar certas definições – veja a próxima secção "SMTP".

- **Impressoras.**
  O alerta será enviado para uma impressora. Clique em "Adicionar" e depois "Impressora", depois clique em "Procurar" e seleccione uma impressora da lista apresentada.

- **ICQ.**
  O alerta será enviado como uma mensagem ICQ. Insira o número do ICQ da pessoa que deve receber o aviso.

- **Windows Messenger.**
  Alerta numa mensagem do Messenger. Insira a morada de email utilizada no serviço Windows Messenger.

Para criar um novo alerta, clique em "Adicionar" e seleccione o tipo de alerta requerido, em seguida, digite as informações pedidas, como descrito acima. Depois de criado um alerta, uma mensagem será enviada para o destinatário definido quando for detectado um ficheiro suspeito.

Para editar ou remover um alerta criado, clique nele para o realçar, depois em "Editar" ou "Remover".

Se clicar em "Teste" será enviada uma mensagem de teste para o endereço seleccionado, se clicar em "Testar todos" irá enviar uma mensagem de teste para todos os destinatários da lista.

SMTP

Na lista do lado esquerdo da janela pode especificar os parâmetros do servidor SMTP. O avast! usa estas definições para enviar mensagens de email, especialmente quando:

- Envia Alertas quando um vírus é encontrado.
- Envia ficheiros da Quarentena para a ALWIL Software.
- Envia relatórios de falha de sistema do avast! para a ALWIL Software.

Deve inserir a seguinte informação:

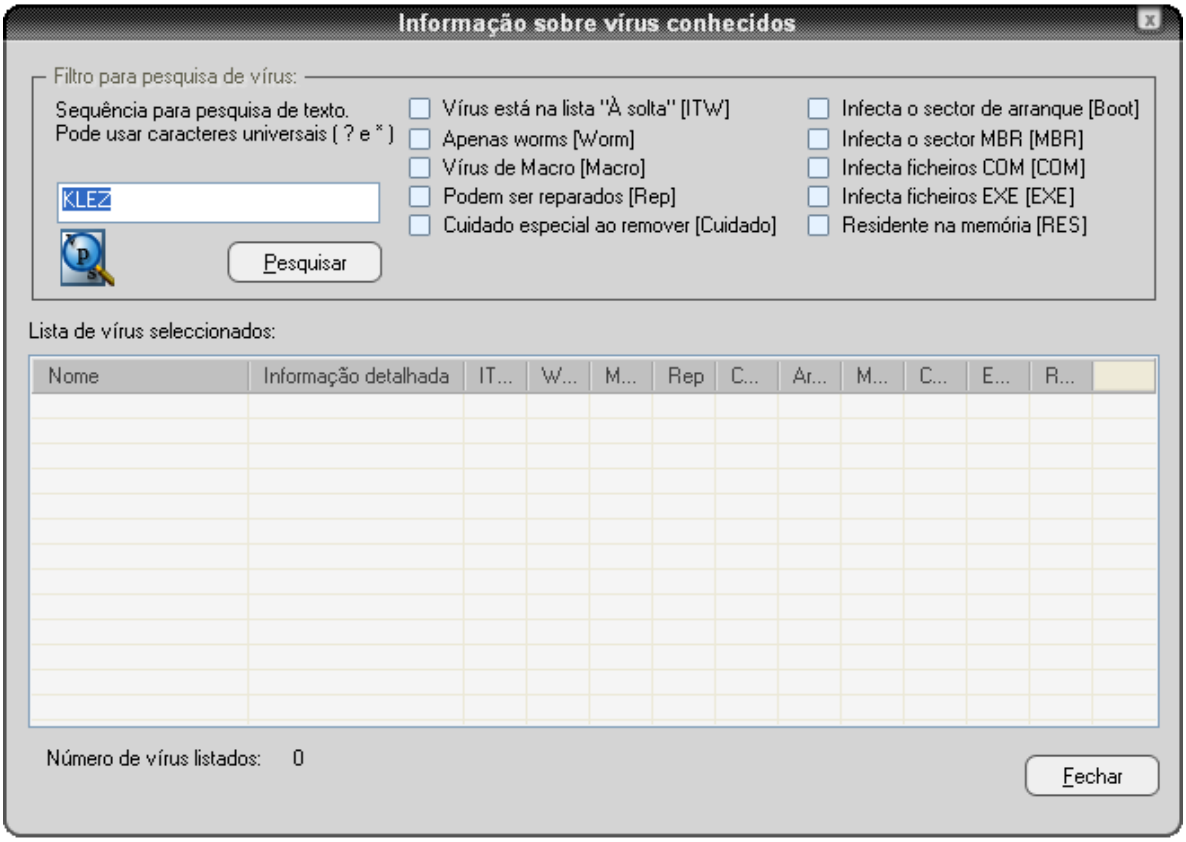
- Morada do Servidor – a morada do servidor de saída de emails (por exemplo smtp.server.com ou 192.168.1.25).
- Porta – número da porta (o padrão é 25).
- De (email) – morada do emissor ("De").

Se o servidor SMTP requer autenticação ao entrar, deve também preencher a respectiva caixa e digitar o nome de utilizador e a senha.

Procurar na Base de Dados de Vírus

A base de dados de vírus contém informação detalhada sobre todos os vírus conhecidos e é utilizada pelo programa para identificar qualquer potencial infecção.

Para aceder a base de dados de vírus abra o **menu** (ver **página 28**) e clique em "Base de dados de vírus...". Aparecerá a seguinte janela:



Os vírus na lista podem ser pesquisados por vários parâmetros. Se souber o nome do vírus, digite-o na caixa e clique no botão "Pesquisar". Se sabe apenas parte do nome pode digitar "?" em vez de cada letra ou número que não souber ou "*" em vez de um grupo de caracteres.

Exemplo: Suponha que procura o vírus “Klez”. Na verdade o seu nome na base de dados é Win32:Klez-H [Wrm]. Deve portanto digitar: *klez*. Deste modo todos os vírus que contenham a palavra “klez" serão encontrados.
Para estrangular a pesquisa, pode também usar as caixas de selecção ao lado de cada característica do vírus. Para a pesquisa sobre um determinado recurso, faça um duplo clique na respectiva caixa. Se clicar uma só vez em qualquer caixa e esta transforme numa caixa cinzenta significa que não tem esse recurso. Se nenhuma caixa é deixada desmarcada, mas de cor azul / verde, significa que não importa se o vírus tem esse recurso ou não.

Propriedades dos vírus utilizadas na sua pesquisa:

- ***Vírus está na lista “À solta” (ITW)***
  O vírus está na lista de vírus espalhados entre utilizadores em todo o mundo.

- ***Apenas Worm (Worm)***
  É um tipo especial de vírus que não infecta os ficheiros directamente, mas executa outras acções indesejáveis como se propagar por email, rouba palavras-chave, etc.

- ***Vírus de Macro (Macro)***
  Este tipo de vírus usa linguagem de macro de produtos Microsoft (por exemplo Word, Excel).

- ***Podem ser reparados (Rep)***
  Ficheiros infectados por estes vírus podem ser reparados pelo avast e restaurados ao seu estado original como antes da infecção.

- ***Cuidado especial ao remover (Cuidado)***
  Para estes vírus é necessário seguir certas instruções caso contrário a sua remoção pode ser mais danosa que o vírus em si.

- ***Infecta o sector de arranque (Boot)***
  Este tipo de vírus infecta o arranque de um disco rígido ou de uma disquete.

- ***Infecta o sector MBR (MBR)***
  Este tipo de vírus infecta o arranque principal de um disco rígido.

- ***Infecta ficheiros COM (COM)***
  Este tipo de vírus infecta ficheiros executáveis de extensão “.com”.

- ***Infecta ficheiros EXE (EXE)***
  Este tipo de vírus infecta ficheiros executáveis de extensão “.exe”.

- ***Residente na memória (RES)***

Estes vírus ficam na memória RAM e infectam ficheiros quando estes são iniciados.

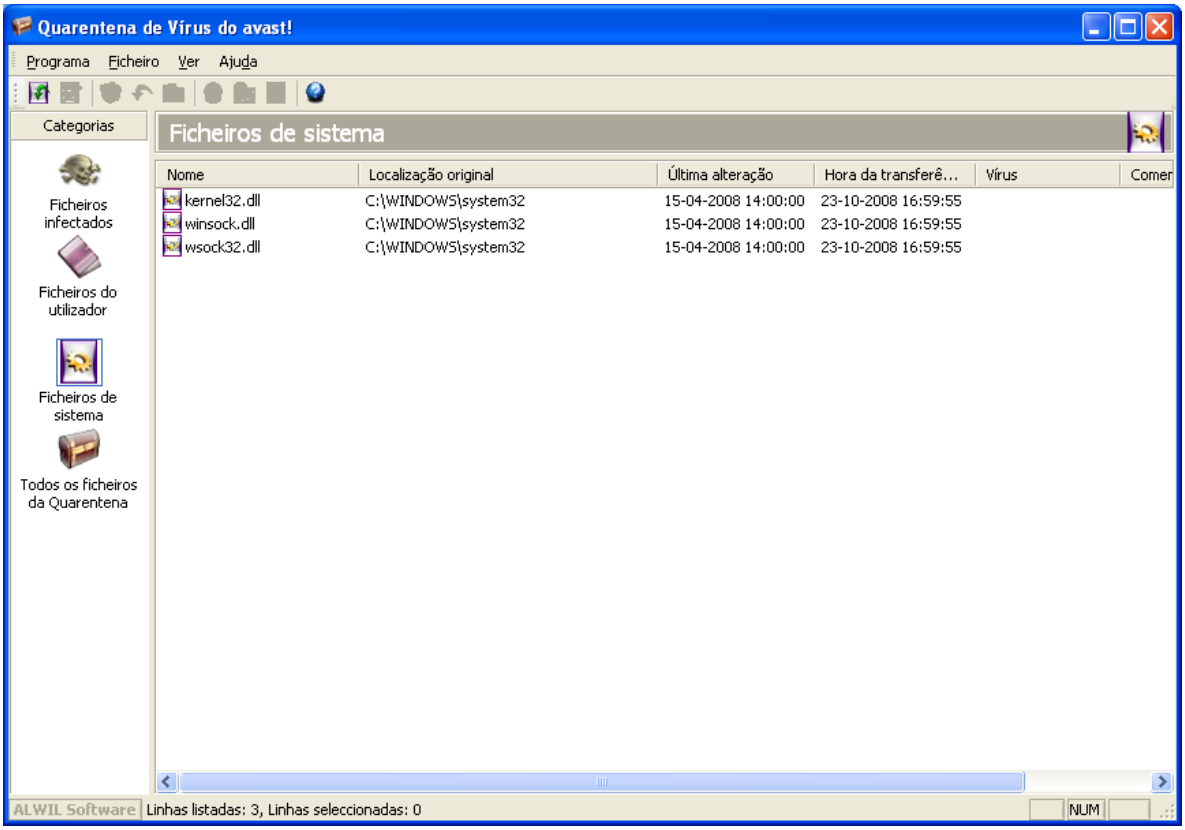
Trabalhar com ficheiros na Quarentena

Pode entrar na Quarentena através do **menu**. Como resultado das suas propriedades únicas, é efectivamente uma área "quarentena", que poderá ser utilizada para as seguintes finalidades:

- ***Armazenar vírus.***
  Se o avast! encontrar um vírus e decidir não excluí-lo por algum motivo, será oferecida a opção de movê-lo para a Quarentena. Com o vírus na Quarentena pode ter certeza que ele não será executado por acidente nem fará qualquer mal ao seu sistema.

- ***Armazenar ficheiros suspeitos.***
  A Quarentena é útil para armazenar quaisquer ficheiros suspeitos para posterior análise.

- ***Cópias de segurança dos seus ficheiros de sistema.***
  Durante a instalação, cópias de alguns ficheiros do sistema críticos são armazenados na Quarentena, na categoria "Ficheiros de Sistema" (veja abaixo). Se o sistema de ficheiros principal ser infectado por um vírus, as cópias podem ser restauradas a partir da Quarentena à sua localização original.



Clique com o botão direito do rato em qualquer ficheiro e aparecerão as seguintes opções. Em alternativa clique com o botão esquerdo num ficheiro para realçá-lo, depois clique no ícone correspondente na parte superior da janela ou clique em "Ficheiro" e seleccione a opção pretendida *(Nota: Se fizer um **duplo-clique** num ficheiro não irá executá-lo mas sim mostrar as suas propriedades. Esta é uma medida de segurança para proteger melhor o seu sistema de infecções acidentais a partir da Quarentena.):*

- ***Actualizar todos os ficheiros***
  Seleccione esta opção se quiser ter a certeza que está a visualizar a lista completa de ficheiros. O programa actualiza a lista automaticamente, mas pode usar esta opção caso não queira esperar.

- ***Adicionar ficheiros.***
  Pode adicionar ficheiros apenas na categoria "Ficheiros do utilizador".

- ***Eliminar os ficheiros.***
  Se seleccionar esta opção o ficheiro será excluído irreversivelmente, ou seja, os ficheiros não serão simplesmente movidos para a lixeira! Antes de eliminar qualquer ficheiro, assegure-se que não é um ficheiro do sistema. Eliminar um ficheiro do sistema pode ter consequências muito graves.

- ***Restaurar ficheiros.***
  O ficheiro seleccionado será restaurado ao seu local original e ao mesmo tempo removido da Quarentena.

- ***Extrair os ficheiros*.**
  O ficheiro será copiado para uma pasta seleccionada.

- ***Verificar ficheiro*.**
  O ficheiro será verificado em relação a vírus.

- ***Propriedades do ficheiro*.**
  As propriedades do ficheiro são mostradas; é também possível adicionar um comentário ao ficheiro.

- ***Email para a ALWIL Software*.**
  O ficheiro seleccionado será enviado (por email) para ALWIL Software. Deve utilizar esta opção apenas em casos especiais - por exemplo, se suspeitar que o programa tem um ficheiro incorrectamente identificado como um vírus. Não se esqueça de incluir o máximo de informação possível - por exemplo, o motivo pelo qual está a enviar o ficheiro, a versão da sua base de dados de vírus, etc. Com isto pode melhorar o nosso serviço.

Ao clicar em “Programa”, “Definições” e depois em “Quarentena” pode ajustar o tamanho máximo permitido da Quarentena e, assim, a quantidade máxima de espaço que ocupa no seu computador. Pode também especificar o tamanho máximo de qualquer ficheiro individual que deva ser mandado para a Quarentena.

Visualizador de registos

Depois de qualquer verificação, o avast! antivírus cria vários ficheiros de registo onde as informações sobre quaisquer erros ou ficheiros suspeitos são armazenadas. Informações sobre instalações e actualizações do programa e os vírus da base de dados também podem aqui ser encontradas. Para ver estes registos seleccione "Visualizador de registos" do **menu** (ver **página 28**).

A informação armazenada nos ficheiros de registo está dividida nas seguintes categorias:

Informação	Apenas informação, tudo está OK.
Observação	Informação importante, tudo está OK. Inclui informação sobre o programa e actualizações da base de dados.
Aviso	Ocorreu um erro ou um vírus foi identificado, mas o programa pode reparar ou trabalhar no problema.
Erro	Ocorreu um erro, o programa não pode trabalhar.
Critico	Ocorreu um erro critico num programa, o programa será terminado.
Alerta	Há a possibilidade de risco para todo o computador.
Emergência	Perigoso para todo o computador (segurança, a apagar ficheiros do sistema).

Se clicar em "Definições" e depois em "Ficheiros de registo", poderá ajustar o tamanho máximo de cada ficheiro de registo.

Dentro do Visualizador de registos é possível procurar registos específicos, filtrar registos de acordo com certos critérios, ou exportar os registos para outro local.

Encontrar um registo

1. Prima "CTRL" e "F" simultaneamente, ou
2. clique em "Editar" no topo esquerdo da janela e depois em "Procurar", ou
3. clique na lupa no topo esquerdo da janela, ou
4. clique com o botão direito do rato na lista de registos e depois em "Procurar" no menu que aparece.

Aparecerá uma caixa onde pode digitar totalmente ou parcialmente o nome do registo que deseja encontrar. Se souber o nome exacto preencha a caixa "Apenas palavras inteiras" de modo a assegurar que apenas sejam listados os registos com esse exacto nome. Do mesmo modo se desejar encontrar nomes com letras maiúsculas ou

minúsculas. Ao clicar em "Cima" ou "Baixo" irá determinar se a lista é apresentada por ordem crescente ou decrescente.

De seguida clique em "Localizar seguinte". O primeiro resultado da pesquisa será mostrado. Os outros resultados da pesquisa que coincidem com o nome inserido podem ser visualizados ao clicar em "Localizar seguinte", até não forem encontrados mais registos.

Filtro para a lista de registos. É utilizado para estrangular os resultados de pesquisa que preencham um certo critério, por exemplo, uma palavra-chave específica ou parte de uma palavra.

1. Pressione simultaneamente "CTRL" e "R", ou
2. Clique em "Editar" no topo esquerdo da imagem e depois em "Filtrar", ou
3. Clique no funil amarelo no topo esquerdo da imagem, ou
4. Clique com o botão direito do rato na lista de registos e depois clique em "Filtrar"

Irá, então, aparecer uma janela onde pode especificar os critérios de filtragem:

Incluir
Insira uma palavra-chave ou parte de uma palavra que deva ser incluída nos resultados mostrados. Pode digitar * em vez de alguma letra que não saiba, por exemplo. Múltiplas palavras-chave têm de ser separadas por ponto e vírgula (;).

Excluir.
Inserir uma palavra-chave ou parte de uma palavra que não deva aparecer nos resultados.

Intervalo de tempo
Aqui pode definir o inicio e o fim do período do registo que quer que seja visualizado.

Seleccione as linhas definidas
Se esta opção for seleccionada, os resultados do critério definido serão simplesmente realçados na lista.

Mostrar as linhas definidas (ocultando as restantes)
Se seleccionar esta opção apenas os resultados do critério definido serão mostrados. Os outros resultados não aparecerão. Esta opção é bastante útil se a lista originar for muito extensa.

Ordenar os registos
Clicar os cabeçalhos das colunas ordena os registos de forma ascendente ou descendente, de acordo com a informação da coluna. Se voltar a clicar no cabeçalho da coluna irá repor a lista na ordem original.

Exportar os registos
Resultados encontrados ou filtrados, ou toda a lista de registos podem ser exportados e guardados como um novo ficheiro. Para exportar registos filtrados

ou encontrados seleccione a opção “Exportar linhas seleccionadas” ou clique na seta verde da esquerda no topo esquerdo da janela. Para exportar uma lista completa seleccione “Exportar a lista actual” ou clique na seta verde do lado direito. Na nova janela que aparecer escolha uma pasta de destino para o ficheiro exportado e digite o novo nome do ficheiro, depois clique em “Guardar”.

Definições da Protecção Residente

1. Mensagens Instantâneas

Programas

Aqui pode especificar que programas devem ser verificados. Se utilizar os Windows 95/98/ME e desejar proteger o programa Trillian terá de introduzir o caminho para o seu ficheiro de configuração - talk.ini (pode utilizar o botão “Procurar...”. Alguns programas só podem ser protegidos se utilizar os Windows NT, 2000, XP, 2003, Vista ou 2008.

2. Correio da Internet

Nas páginas “POP”, “SMTP”, “IMAP” e “NNTP” pode especificar se os emails de entrada e saída são verificados. Caso um vírus seja detectado é colocado um aviso no email em causa. Pode também especificar que uma nota seja inserida nas mensagens limpas assegurando a quem as recebe que estão livres de vírus.

Redireccionar

Esta opção torna possível configurar a verificação transparente do correio. Quaisquer emails que passem nas portas especificadas serão verificados. Opção disponível apenas para os Windows NT/2000/XP/2003/Vista/2008.

- Redireccionar portas.

  As portas padrão são as dos 4 protocolos básicos de email. Caso use outra(s) porta(s) ela(s) deve(m) ser inserida(s) aqui. Múltiplos valores devem ser separados por vírgulas.

- Endereços ignorados.

  Aqui pode inserir os endereços dos servidores de emails ou portas específicas que deseje excluir da verificação. Esta funcionalidade pode ser útil quando quer que o avast verifique apenas mensagens de/para uma certa conta (e ignore as restantes). Por exemplo, se inserir smtp.server.com, o avast! não irá verificar as mensagens de saída (SMTP) para a conta correspondente.

- Ignorar a comunicação local.

Esta opção deve ser seleccionada. Caso não o seja o avast! irá verificar até as comunicações locais (que são geralmente seguras), o que pode provocar uma diminuição da rapidez do seu computador. Nota: Não insira números de portas que não utilize para tráfego de correio. Caso contrário podem ocorrer problemas imprevistos.

Avançado

- Mostra informação detalhada sobre a acção tomada.

  Caso esta caixa seja preenchida a informação sobre os ficheiros a serem verificados nesse momento irá aparecer no canto inferior direito.

- Modo silencioso.

  Se a acção especificada na página de vírus é a padrão, isto é, está seleccionada a opção interactiva, e a opção silenciosa for seleccionada, qualquer ficheiro infectado vai ser tratado automaticamente de acordo com as seguintes regras:

  > Se a opção "com resposta padrão Sim (OK)" for seleccionada qualquer ficheiro infectado anexado a um email será automaticamente apagado.

  > Se a segunda opção "com resposta padrão Não (Cancelar)" for seleccionada qualquer ficheiro infectado anexado a um email será automaticamente movido para a Quarentena.

  Se esta opção quando um vírus for encontrado aparecerá o aviso normal a perguntar o que fazer com o ficheiro infectado.

- Tempo de comunicação com a Internet.

  Este é o tempo, em segundos, de espera pela resposta de um servidor de correio. Pode ainda especificar se a ligação deve ser fechado se não for recebida uma resposta nesse momento ou se lhe deve ser perguntado antes se quer fechar a ligação.

- Mostrar o ícone na área de notificação ao verificar correio.

  Se esta caixa for preenchida aparecerá um pequeno ícone no tabuleiro do sistema, no canto inferior direito do seu ecrã, a indicar que uma verificação está a ser executada.

Heurísticas

O avast! só pode verificar o email de entrada para vírus conhecidos, mas pode também verificar mensagens utilizando a análise heurística e eventualmente revelar um vírus que ainda não se encontre presente na base de dados de vírus. Nesta página pode modificar as configurações da análise heurística.

- Sensibilidade - Baixa.

  > Verificação básica de anexos.
  Anexos são verificados de acordo com o seu nome e caso tenha duas extensões, por exemplo, “Patch.jpg.exe", será tratado como um ficheiro potencialmente perigoso. O avast! também verifica se a extensão do anexo corresponde mesmo ao tipo de ficheiro, por exemplo, verifica se o ficheiro "Pamela.jpg" é mesmo uma foto ou um ficheiro COM cujo nome foi mudado.

  > Verificar sucessão de espaços em branco.
  Alguns vírus adicionam espaços ao fim da extensão, seguidos pela segunda extensão, a verdadeira, que é a perigosa. Devido ao comprimento do nome do ficheiro, o utilizador pode não ver a segunda extensão, no entanto a análise heurística pode desvendar este truque. O número padrão permitido de espaços em branco é cinco consecutivos. Se houver mais de cinco será exibida uma mensagem de aviso.

- Sensibilidade – Média (além do acima mencionado).

  > Verificação exaustiva de anexos.
  Além da verificação básica de anexos será exibida uma advertência se o anexo tiver uma simples extensão executável (EXE, COM, BAT, etc.). Nem todos esses ficheiros são perigosos e, por isso, este nível de sensibilidade irá gerar mais alertas falsos positivos do que a verificação básica de anexos.

- Sensibilidade - Alta (além do acima mencionado)

  > Verificação da parte HTML.
  Alguns vírus podem explorar erros em alguns programas de correio (especialmente MS Outlook e Outlook Express inseguros) que tornem possíveis o inicio de vírus por apenas visualizar a mensagem. O avast! verifica se o código HTML da mensagem contém uma etiqueta que faça tal truque. Se tiver aparecerá uma mensagem de erro.

  > Mensagens enviadas – Verificação do tempo de envio.
  A maioria dos vírus são espalhados por e-mail e enviam-se a si mesmos para os endereços na sua lista de contactos. Num curto período de tempo são enviadas mensagens para um grande número de endereços, com o mesmo assunto e/ou anexo. O avast! verifica o número de mensagens

num certo intervalo de tempo e também o assunto e/ou os anexos. Estes parâmetros podem ser todos ajustados na página Heurísticas (Avançado).

> Mensagens enviadas - Mensagens em massa (SPAM).
Vírus podem também espalhar-se enviando-se em apenas uma mensagem para vário recipientes. O avast! verifica o número total de recipientes da mensagem. O número total de recipientes permitido pode ser definido na página Heurísticas (Avançado).

- Sensibilidade – Personalizada

  Se clicar em "Personalizar…" poderá seleccionar quais dos componentes da análise heurística acima descritos deseja que sejam usados.

  Pode também seleccionar "Verificação da estrutura do assunto". Se o fizer os cabeçalhos dos assuntos de email serão verificados em relação ao número de caracteres sem sentido, por exemplo, se o assunto tiver a sequência "<?*&$(^%#$%*_(", será mostrada uma mensagem de aviso.

- URLs permitidos

  Ao clicar em "URLs permitidos" poderá definir que URLs considera seguras e que podem ser ignoradas na análise heurística. Para adicionar uma URL clique em "Adicionar" e depois insira manualmente o seu nome. Para remover uma URL seleccione-a e depois clique em "Remover".

- Modo silencioso

  Nesta página pode especificar a acção a tomar caso uma mensagem infectada seja detectada.

Heurísticas (Avançado)

Esta página permite-lhe modificar as definições da análise heurística dos emails enviados. As definições são usadas apenas quando a sensibilidade heurística está alta ou em personalizada.

- Tempo de envio.

  O avast! contará as mensagens enviadas no intervalo de tempo especificado. A definição padrão é 5 mensagens em 30 segundos. Se forem enviadas mais de 5 mensagens, com o mesmo assunto e/ou anexo, em meio minuto será mostrado um aviso.

- Alerta de contagem.

Aqui pode definir o número de mensagens que podem ser enviadas sem receber nenhum aviso, mesmo que elas tenham o mesmo assunto e/ou anexo. Quando o número definido for excedido será mostrado um alerta.

- Verificar assunto.

  Se for activado as mensagens em massa serão identificadas de acordo com o assunto.

- Verificar anexos.

  Se for activado as mensagens em massa serão identificadas de acordo com o anexo.

- Contagem absoluta.

  Aqui define o número máximo de recipientes da mensagem, ou seja, o número de moradas nos campos "Para", "CC" e "BCC". Por padrão são 10 e se for excedido este número receberá um aviso.

3. Escudo da rede

O Escudo da rede protege o seu computador de ataques de worms da internet. Tem um funcionamento parecido com o de uma firewall mas não é um substituto para uma.

Definições

- Mostrar mensagens de aviso

  Se esta caixa for preenchida aparecerá no canto inferior direito do ecrã uma mensagem sempre que o ataque de uma worm for detectado.

- Ficheiros de registo

Se activar esta opção o histórico dos ataques de worms será guardado e mostrado na página "Últimos ataques".

Últimos ataques

Nesta página são mostrados os últimos 10 ataques de worm de rede, se a caixa "Ficheiros de registo" da página anterior tiver sido preenchida. Irá incluir a data e hora dos ataques, o tipo de ataque e a morada IP e porta de onde foi originado.

4. Outlook/Exchange

Verificador

Aqui pode especificar que tipos de mensagens devem se verificados, se os corpos das mensagens também devem ser verificados tal como os seus anexos.

Correio recebido

Aqui pode especificar o que deve ser feito caso receba uma mensagem infectada, por exemplo, pode ser entregue, apagada ou dirigida para outra pasta de correio. Pode também especificar se deve ser inserida uma nota nas mensagens limpas e/ou infectadas, além do formato da nota, isto é, TXT ou HTML. Quaisquer ficheiros infectados anexados ou contidos na mensagem serão tratados de acordo com as definições das páginas “Armazenamento de vírus” e “Avançado”.

Correio enviado

Aqui pode especificar se deve ser inserida uma nota nas mensagens limpas e formato da nota, tal como descrito acima. As mensagens infectadas não serão enviadas. Pode também especificar que anexos devem ser verificados no momento em que são anexos em vez do momento em que são enviados.

Assinaturas

Ao utilizar assinaturas é possível reduzir drasticamente o número de mensagens que precisam ser verificadas. Assinaturas são pequenos "selos" anexados às mensagens que não estão infectadas de modo a confirmar que estão livres de vírus. Cada assinatura inclui a data e a hora da verificação.

As assinaturas do provedor MS Outlook/Exchange são completamente compatíveis com as do avast! Exchange Server Edition. Portanto, as mensagens verificadas pelo provedor Exchange Server não serão testadas novamente pelo provedor Outlook/Exchange, obtendo-se uma transferência mais rápida.

- **Inserir assinaturas às mensagens limpas (sem vírus)**.

Deve ser marcada se deseja adicionar assinaturas às mensagens limpas.

- **Confiar sempre nas mensagens assinadas**.

Se esta caixa for preenchida as mensagens assinadas nunca serão verificadas, mesmo que a assinatura seja muito antiga (excepto se a caixa "Ignorar sempre assinaturas mais antigas do que a base de vírus actual” for preenchida).

- **Confiar apenas nas assinaturas até**.

Aqui pode definir a idade de confiança das assinaturas. O valor aqui definido pode ser ignorado devido à opção "Ignorar sempre assinaturas mais antigas do que a base de vírus actual" – ver abaixo.

- **Ignorar todas as assinaturas (não confiar)**.

Se activar esta opção todas as mensagens serão verificadas quer tenham assinatura ou não.

- **Ignorar sempre assinaturas mais antigas do que a base de vírus actual.**

Caso preencha esta casa as assinaturas mais antigas que a base de dados de vírus actual serão ignoradas. Esta opção pode ser útil pois uma mensagem pode conter um novo vírus que pode ter sido adicionado à base de dados desde a última verificação. Se mensagem não fosse verificada o vírus não seria detectado.

Armazenamento de vírus

Nesta janela poderá especificar que uma cópia de um anexo infectado seja gravada numa pasta específica do seu disco rígido. Pode utilizar o botão "Procurar…" para localizar e seleccionar a pasta desejada. Se preencher a caixa "Substituir os ficheiros existentes" qualquer ficheiro com o mesmo nome será substituído pelo novo ficheiro.

Avançado

- Modo Silencioso

  Se preencher esta caixa qualquer ficheiro suspeito será automaticamente movido para a Quarentena. Se deixar esta caixa desmarcada quando for encontrado um ficheiro infectado aparecerá uma janela a perguntar o que deseja fazer com ele.

- Mostrar informações detalhadas da acção realizada

  Se preencher esta caixa a informação sobre os ficheiros a serem verificados em cada momento será mostrada no canto inferior direito do ecrã.

- Montar um ícone na área de notificação ao processar correio

  Caso active esta opção será mostrado um pequeno ícone no tabuleiro do sistema, no canto inferior direito do ecrã, a indicar que a verificação está a ser executada.

- Mostrar ecrã de boas vindas ao iniciar o provedor

  Se activar esta opção será mostrado o ecrã de boas vindas sempre que o provedor de correio for iniciado.

Se inserir o seu perfil MAPI e palavra-chave estes serão utilizados para mostrar a estrutura das suas pastas de email quando clicar no botão de procura na página de correio recebido.

Heurísticas

As definições nesta página são as mesmas que no Correio da Internet.

Heurísticas (Avançado)

As definições nesta página são as mesmas que no Correio da Internet, mas com a adição de mais duas opções:

- Contagem Relativa

  Aqui define o número permitido de recipientes de uma única mensagem, expresso em percentagem do número total de contactos do seu livro de contactos. Caso esta percentagem seja excedida aparecerá um aviso.

- Contagem mínima

  Este é o número mínimo de recipientes, correspondente à contagem relativa, abaixo do qual não aparecerá uma mensagem de aviso. Ou seja, se a contagem relativa for excedida, o aviso não aparecerá se o número real de recipientes for menor que a contagem mínima. Exemplo: Contagem relativa = 20%, Contagem mínima = 10. Se o número de contactos for 40 e a mensagem for enviada a 9 recipientes, a contagem relativa será excedida mas a mensagem de aviso não será exibida pois o número real é menor que o da contagem mínima.

5. Escudo P2P

Programas

Nesta página pode especificar em que programas os ficheiros recebidos devem ser verificados. Alguns programas só podem ser protegidos em Windows NT, 2000, XP, 2003, Vista ou 2008.

6. Escudo Padrão

Verificador (Básico)

Nesta janela pode definir o que deve ser verificado por este provedor. Recomenda-se que todas as opção mostradas estejam activadas, permitindo, assim, a detecção da maior parte dos vírus comuns.

Verificador (Avançado)

Aqui pode especificar outros ficheiros a ser verificados de acordo com a sua extensão, quando forem abertos, criados ou modificados.

- Verificar ficheiros ao serem abertos.

  As extensões dos ficheiros adicionais a serem verificados devem ser separadas por vírgulas. Pode usar o carácter universal "?" (por exemplo, se deseja que todos os ficheiros .htm e .html sejam verificados ao serem abertos, pode inserir "htm", "html" ou usar o carácter universal - "ht?"; neste último caso, todos os ficheiros com extensões a começar por "ht", também "htt", serão verificados).

  > Verificar sempre ficheiros WSH-script.

    Esta opção assegura que todos os ficheiros (Windows Scripting Host) sejam verificados.

  > Não verificar bibliotecas de sistema.

    Bibliotecas de sistema não serão verificadas quando abertas, apenas uma verificação rápida será feita para validar a autenticidade. Esta opção permite que o arranque do sistema seja ligeiramente mais rápido.

- Verificar ficheiros criados/modificados.

  Se activar esta opção os ficheiros serão verificados no momento que forem criados ou modificados. Pode também definir se isto deve ser aplicado a:

  > Todos os ficheiros, ou

  > Apenas ficheiros com as extensões seleccionadas

Se a caixa "Conjunto de extensões padrão (recomendado)" for preenchida apenas os ficheiros com extensões consideradas perigosas serão verificados – clique em "Mostrar..." para ver a lista de extensões padrão. Pode também adicionar extensões a ser verificadas.

Bloqueador

Nesta página pode definir que operações específicas estão bloqueadas aos ficheiros com certas extensões. Isto pode ser aplicado ao "Conjunto de extensões padrão (recomendado)" – clique em "Mostrar…" para ver a lista de extensões padrão. Pode também adicionar extensões para as quais as operações devem ser bloqueadas.

Pode também especificar que operações devem ser bloqueadas para um certo tipo de ficheiros, isto é, abrir, mudar nome, eliminar ou formatar.

Se uma operação tiver que ser bloqueada, mas o avast não puder perguntar o que fazer (por exemplo, por a protecção de ecrã está a ser executada), pode decidir se a acção deve ou não ser bloqueada.

Avançado

- Mostrar informações detalhadas da acção realizada

  Se accionada a informação acerca dos ficheiros a serem verificados nesse momento é mostrada na parte inferior direita do ecrã.

- Modo silencioso

  Se a acção definida na página de Vírus for a padrão – a opção interactiva, e o modo silencioso é activado, quaisquer ficheiros infectados irão ser tratados automaticamente de acordo com as seguintes regras:

  > Se seleccionar "Com resposta padrão Sim (OK)" nenhuma acção será tomada em relação ao ficheiro infectado.

  > Se a segunda opção "Com resposta padrão Não (Cancelar)" for seleccionada quaisquer ficheiros infectados serão movidos automaticamente para a Quarentena.

  Se a acção definida na página de Vírus for a padrão e esta caixa não for a preenchida aparecerá o aviso normal de vírus a perguntar o que deseja fazer com o ficheiro infectado.

  Caso outra acção seja especificada, ou seja, qualquer outra que não a padrão, preencher esta caixa não surtirá qualquer efeito.

Para acabar, pode especificar que localizações não devem ser verificadas por este provedor. Note que localizações que tenham sido excluídas de verificação por todos os provedores não são mostradas nesta lista.

7. Escudo da Web

O Escudo da Web funciona como um servidor proxy local. Em sistemas operativos baseados em NT (Windows NT/2000/XP/2003/Vista/2008) a protecção é completamente transparente e é normalmente não necessário ajustar quaisquer das definições normais. No entanto, caso utilize Windows 95/98/ME, é necessário alterar as definições das Opções da Internet – especialmente a porta da proxy local, tal como se segue:

Se utilizar uma rede local (LAN):	Se utilizar uma ligação de acesso telefónico (modem):
Iniciar o Internet Explorer.	Iniciar o Internet Explorer.
No menu principal seleccionar Ferramentas e depois Opções da Internet.	No menu principal seleccionar Ferramentas e depois Opções da Internet.
Mude para a página Ligações.	Mude para a página Ligações.
Clique em Definições LAN	Seleccione a sua ligação de acesso telefónico da lista e clique em "Definições".
Preencha a opção "Utilizar um servidor proxy para a rede local"	Preencha a opção "Utilizar um servidor proxy para esta ligação"
Campo Endereço escreva "localhost" (como alternativa pode inserir o endereço de IP 127.0.0.1, que é o mesmo que local host). Insira 12080 no campo da porta.	Campo Endereço escreva "localhost" (como alternativa pode inserir o endereço de IP 127.0.0.1, que é o mesmo que local host). Insira 12080 no campo da porta.
Confirme clicando em OK.	Confirme clicando em OK.

Nota: Se utilizar ligações múltiplas é necessário definir o endereço e a porta do servidor proxy local individualmente para cada ligação.

Básico

- Activar a verificação da Web

  Desmarcando esta caixa pode desligar a verificação da Web sem, no entanto, afectar o bloqueio de URLs.

- Utilize a verificação inteligente de stream

  Se activar esta opção os ficheiros transferidos são verificados quase em tempo real. Parte dos dados é verificada assim que chega – e o resto é

transferido apenas quando a primeira parte é assegurada estar livre de vírus. Se a opção não for activada os ficheiros são transferidos para uma pasta temporária e depois verificados.

As outras opções desta página não estão disponíveis para Windows 95, 98, e Millennium:

- Redireccionar porta(s) HTTP.

  Esta opção é importante caso utilize algum tipo de servidor proxy para aceder à Internet e queira verificar a comunicação entre o servidor e o seu computador. Se estiver ligado a um servidor proxy e usar, por exemplo, a porta 3128, insira este número na caixa. Caso contrário, o avast! assumirá que a comunicação é feita pela porta 80 (padrão) e tudo o resto será ignorado. Nota: Não insira mais nenhuma porta além da HTTP (tais como portas para o ICQ, DC++, etc.). Diferentes números de portas devem ser separados por vírgulas.

- Endereços ignorados.

  Aqui deve inserir os nomes de servidores ou endereços de IP que não serão verificados pelo Escudo da Web. Diferentes endereços devem ser separados por vírgulas.

- Ignorar a comunicação local.

  Se preencher esta caixa todas as comunicações - isto é, comunicações entre os programas em execução no seu computados, serão ignoradas.

Verificação da Internet

Aqui pode especificar que ficheiros devem ser verificados quando são transferidos da internet. Pode especificar que todos os ficheiros devem ser verificados ou apenas os que têm certas extensões. Neste segundo caso deve inserir as extensões de ficheiros a serem verificados separadas por vírgulas. Pode também inserir os tipos de MIME dos ficheiros a serem verificados. Em ambos os casos pode utilizar caracteres universais.

Excepções

Nesta página pode definir que objectos não devem ser verificados pelo Escudo da Web. Isto pode ser útil quando transferir um grande número de ficheiros de uma única localização que considere segura.

- URLs excluídos

  Utilize o botão “Adicionar…” para inserir endereços de URLs que podem ser ignorados. Se deseja excluir da verificação uma única página é necessário inserir o seu caminho complete, por exemplo, se adicionar

http://www.yahoo.com/index.html, apenas a página index.html será excluída da verificação. No entanto, se inserir **http://www.yahoo.com/*** nenhuma página a começar por http://www.yahoo.com será verificada. DE um modo semelhante, se deseja que um ficheiro seja excluído da verificação, por exemplo, ficheiros de extensão ".txt", insira simplesmente *.txt.

- Tipos MIME excluídos

  Aqui pode especificar que tipos/subtipos de MIME deseja excluir da verificação.

Bloquear URLs

O Escudo da Web pode também ser usado para bloquear o acesso a certas páginas da Web. Por padrão esta opção está desligada, no entanto pode ser usada para prevenir o acesso a páginas "inconvenientes" (por exemplo, com conteúdos pornográficos, software ilegal, etc.). Se uma página bloqueada for pedida pelo Web browser aparece um aviso do avast! a dizer que o acesso foi evitado pelo avast! antivírus.

Antes de inserir tais URLs tem de preencher a caixa "Activar o bloqueio de URL". Depois utilize o botão "Adicionar…" para inserir as URLs a serem bloqueadas. Podem ser utilizados caracteres padrão (? and *), por exemplo, se inserir http://www.penthouse.com/*, nenhuma página começada por http://www.penthouse.com será aberta.

Os endereços de URL serão completes de acordo com as seguintes regras:

Se o endereço não começa por http:// ou caracteres padrão * ou ?, o avast! adiciona o prefixo http:// ao inicio do endereço e um asterisco ao final. Portanto, se inserir www.yahoo.com, será modificado para http://www.yahoo.com*.

Avançado

- Mostrar informação detalhada da acção realizada

  Se activar esta opção a informação sobre a verificação de ficheiros que estiver nesse momento a ser executada será mostrada no canto inferior direito do seu ecrã.

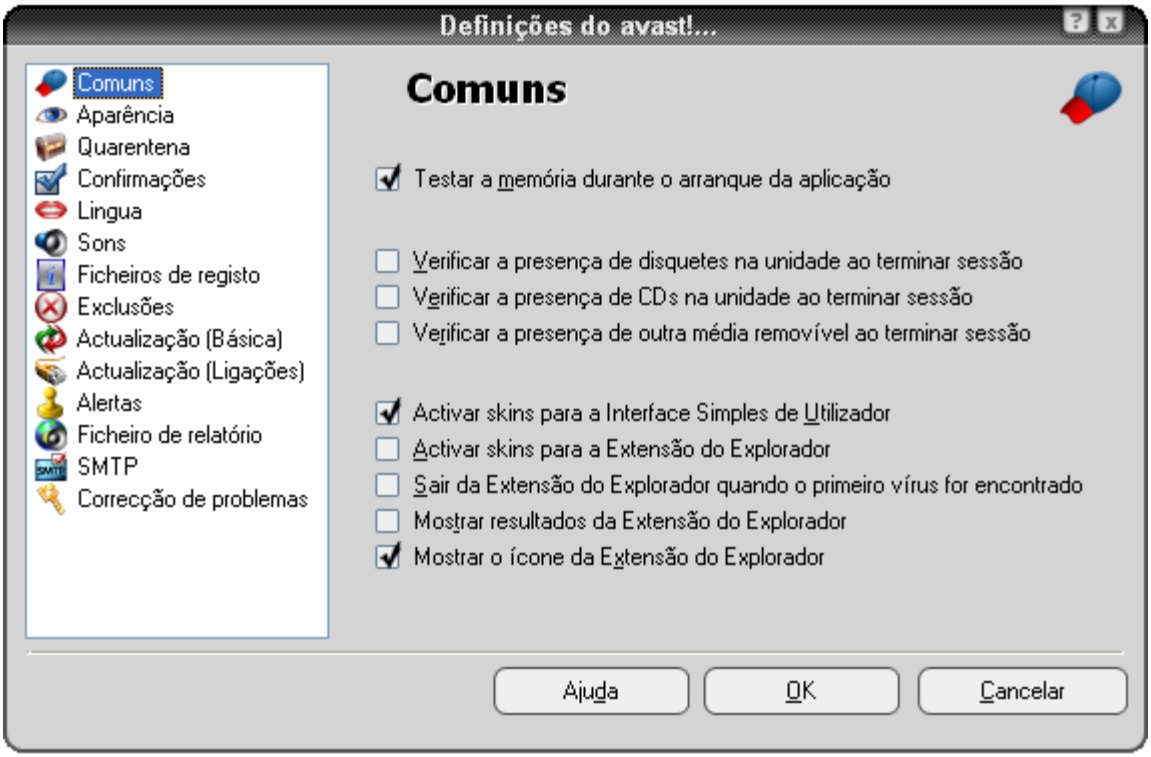
  Modo silencioso

  Caso active esta opção a ligação à internet será interrompida sempre que um vírus for encontrado.

Outras definições do avast!

Muitas outras partes do programa podem ser modificadas de acordo com as suas preferências pessoais. Algumas delas já foram descritas nas secções acima.

Se usar o interface simples e abrir o **menu** (ver **página 28**) e clicar em "Definições" aparece a seguinte janela. Se utilizar o interface avançado precisa apenas de clicar em "Definições" e haverá também uma opção adicional – "Interface Avançado". As diferentes definições podem ser alteradas clicando no título do lado direito:



Comuns

Neste ecrã pode especificar que verificações são feitas quando inicia ou desliga o seu computador. Aqui pode também alterar a aparência do programa ligando/desligando a opção "Activar skins…".

Extensão do Explorador

As últimas quarto opções desta janela estão relacionadas com a "Extensão do Explorador". Esta é a possibilidade de verificar qualquer ficheiro individualmente clicando sobre ele com o botão direito do rato e escolher a opção "Verificar <NomeDoFicheiro>". Se activar a última caixa, aparecerá o ícone do avast! ao lado desta opção.

Aparência

Se clicar neste título pode definir se o ícone do avast! é mostrado no canto inferior do ecrã ou não e se o deseja animar (girar) quando uma verificação é feita.

Pode adicionar um efeito de transparência ao interface simples do avast!. Estas alterações tomam efeito depois de reiniciar o seu computador.

Confirmações

Esta página permite-lhe decidir se lhe são perguntadas confirmações quando escolhe certas acções, e também se deve ou não receber mensagens de confirmação após certas acções terem sido tomadas.

As confirmações são uma funcionalidade da segurança do avast! antivírus que lhe permite cancelar uma acção tomada por engano.

Se não deseja receber nenhuma confirmação em particular, simplesmente desmarque a caixa apropriada. No entanto, se uma confirmação for desligada, a acção relevante será tomada sem lhe dar a possibilidade de cancelar.

As seguintes confirmações estão ligadas (por padrão) mas podem ser desligadas desmarcando a sua caixa:

- ***Perguntar antes de o programa fechar se existirem sessões em progressão***
  Se o programa for fechado durante uma verificação esta parará exactamente nesse ponto.

- ***Perguntar para manter a mudança de estado do provedor residente***
  Esta mensagem aparece se decidir "Terminar" algum dos provedores residentes – ver **página 26**. Se responder "Sim", esse determinado provedor manter-se-á desligado até que o reactive manualmente. Se responder "Não", será reactivado quando reiniciar o seu computador.

- ***Perguntar antes de parar a protecção residente***
  A mensagem aparece se decidir "Terminar" a protecção residente – ver **página 23**. Caso responda "Sim" a protecção residente será desligada mas será reactivada quando reiniciar o seu computador.

- ***Perguntar antes de eliminar ficheiros da Quarentena***
  Se preencher esta caixa o programa irá sempre perguntar-lhe se confirma que quer apagar algum ficheiro. Isto evita que algum ficheiro seja apagado acidentalmente.

- ***Enviar mensagem quando os resultados foram processados com sucesso***
  Com isto confirma qualquer acção tomada em relação a um ficheiro, por exemplo eliminar, mover para a Quarentena, etc., foi concluída.

- ***Enviar mensagem quando ocorrer um erro durante o processamento***
  Esta opção diz-lhe se a acção seleccionada, em relação a um ficheiro, não pôde ser executada.

- ***Enviar mensagem quando um ficheiro VPS antigo foi utilizado***
  Serve para avisar que a base de dados de vírus não está actualizada. Para assegurar que o sistema está completamente protegido esta base de dados deve estar sempre actualizada – ver **página 40**

- ***Aviso da versão BETA do programa***
  Esta mensagem avisa que a versão do programa a ser utilizada ainda está a ser testada.

- ***Mostrar mensagem quando o relatório de erro foi enviado com sucesso***

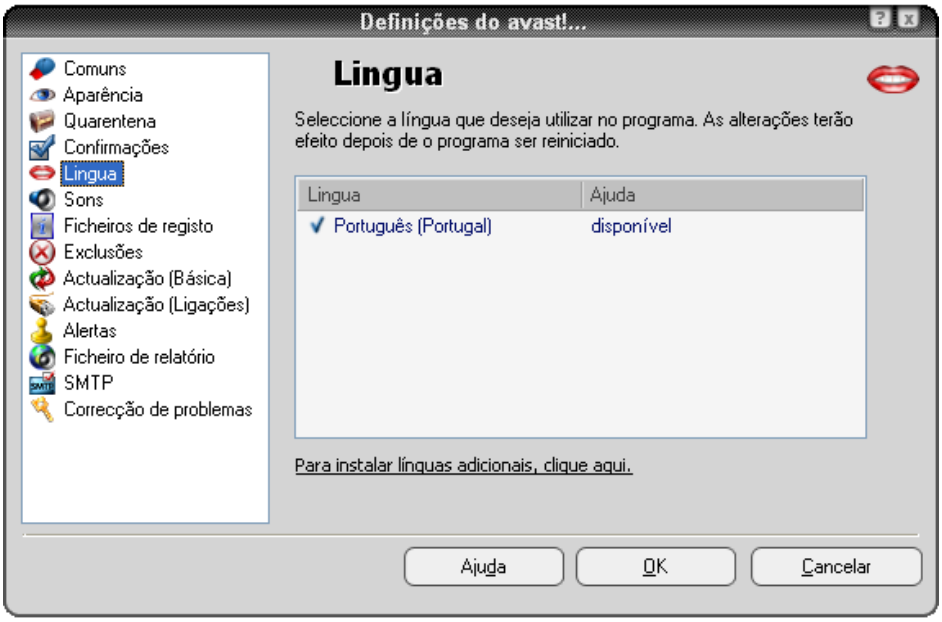
- ***Mostrar a janela de estado na Quarentena mesmo que a acção tenha sido completa sem problemas***
  Caso activada, receberá uma mensagem a confirmar que a acção tomada foi executada com sucesso.

- ***Enviar mensagem quando os resultados ok estiverem activados durante a configuração da tarefa.***
  Recebe um aviso caso escolha que os ficheiros não-infectados também sejam incluídos nos resultados da verificação. Note que isto e aplicado apenas à criação de tarefas no interface avançado.

- ***Eliminação do(s) ficheiro(s) com extensão perigosa***
  Isto é um aviso em como pode não ser seguro apagar um certo ficheiro por ser de um tipo que costuma conter dados importantes.

Alterar a língua do programa

Se deseja alterar o idioma do programa clique em "Língua" e aparecerá a seguinte janela:



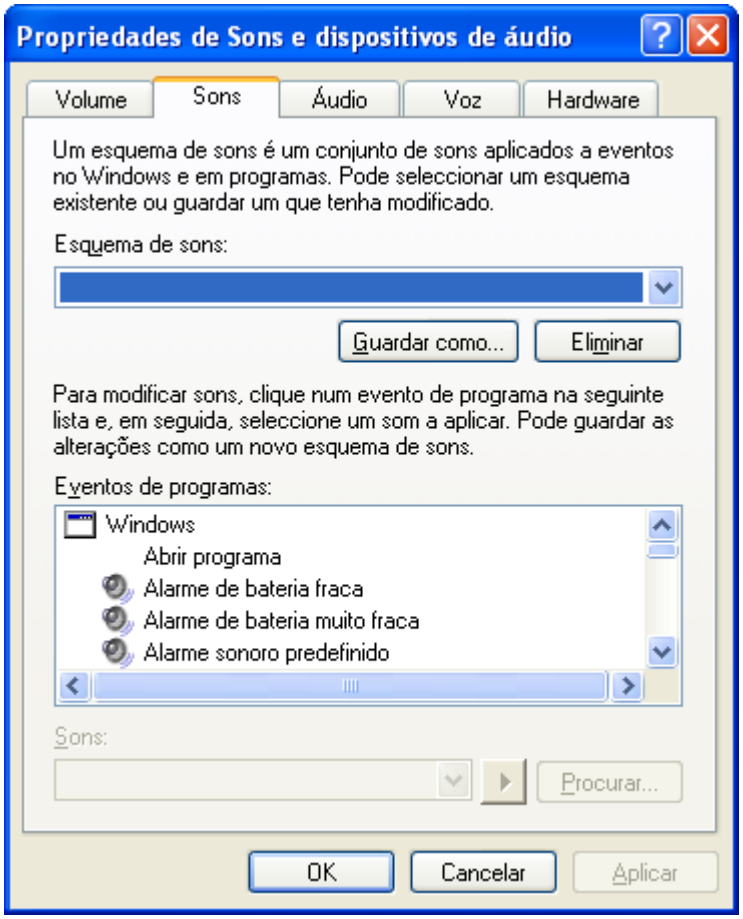
Se o idioma desejado aparece disponível na caixa do lado direito clique-a, e confirme em "OK". Depois necessita fechar o programa e o idioma será alterado na próxima vez que o iniciar.

Se o idioma desejado não estiver disponível clique em "Para instalar línguas adicionais...", depois preencha a caixa da língua pretendida, clique ok e os ficheiros adicionais serão instalados. Quando acabar clique em "Concluir". Poderá então activar a língua desejada tal como descrito acima.

Sons

Nesta janela pode ajustar as definições de som do programa ou simplesmente desligar os sons todos.

Se clicar em "Definições…" aparece uma outra janela onde pode ajustar os sons para todos os programas Windows. Na parte inferior da janela está uma caixa chamada "Eventos de programas" – como pode ver abaixo.



Se deslizar para baixo o botão do lado direito, a meio da lista, poderá encontrar os eventos do avast! antivírus aos quais sons podem ser atribuídos. Se deseja adicionar um novo som a um evento clique no respectivo evento e depois em "Procurar". Da lista disponível seleccione um a seu gosto e clique "OK".

De seguida voltará à janela mostrada acima, clique em "Aplicar" e novamente em "OK".

Isto levar-lhe-á de volta à janela principal dos sons, onde deve clicar em "OK" para acabar.

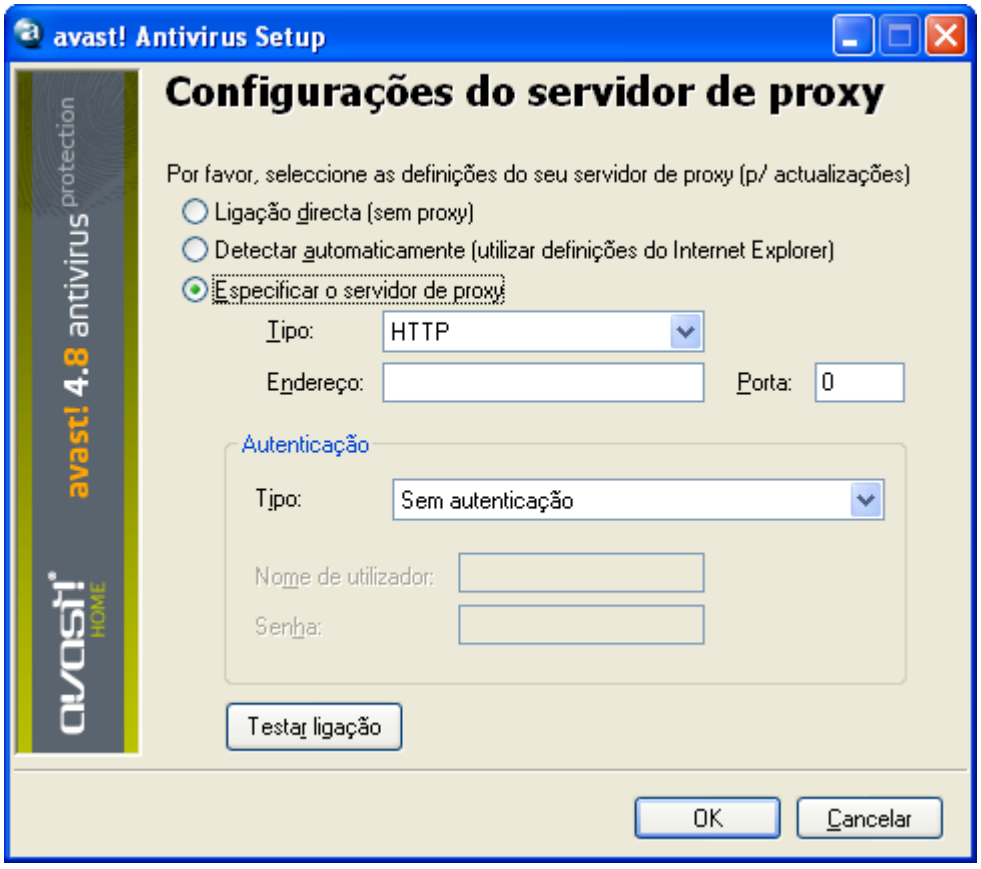
Actualizações (Ligações)

Nesta janela pode especificar o tipo de ligação à internet preenchendo a respectiva caixa, isto é:

- Eu ligo-me à Internet apenas através de um modem (dial-up), ou
- O meu computador está permanentemente ligado à Internet

Isto irá optimizar o modo como o avast! procura novas actualizações e tornará as actualizações automáticas num processo mais fiável.

Depois de especificar o tipo de ligação clique no botão “Proxy...”. Abrirá uma nova janela onde pode inserir as configurações do seu servidor de proxy. Estas configurações são importantes quando o avast! necessita aceder à Internet, por exemplo para actualizar.



Se aceder à internet directamente sem proxy seleccione “Ligação directa (sem proxy)”.

Se não tem a certeza qual o seu tipo de acesso seleccione “Detectar automaticamente (utilizar definições do Internet Explorer)”, ou pergunte ao seu fornecedor de internet ou administrador de rede.

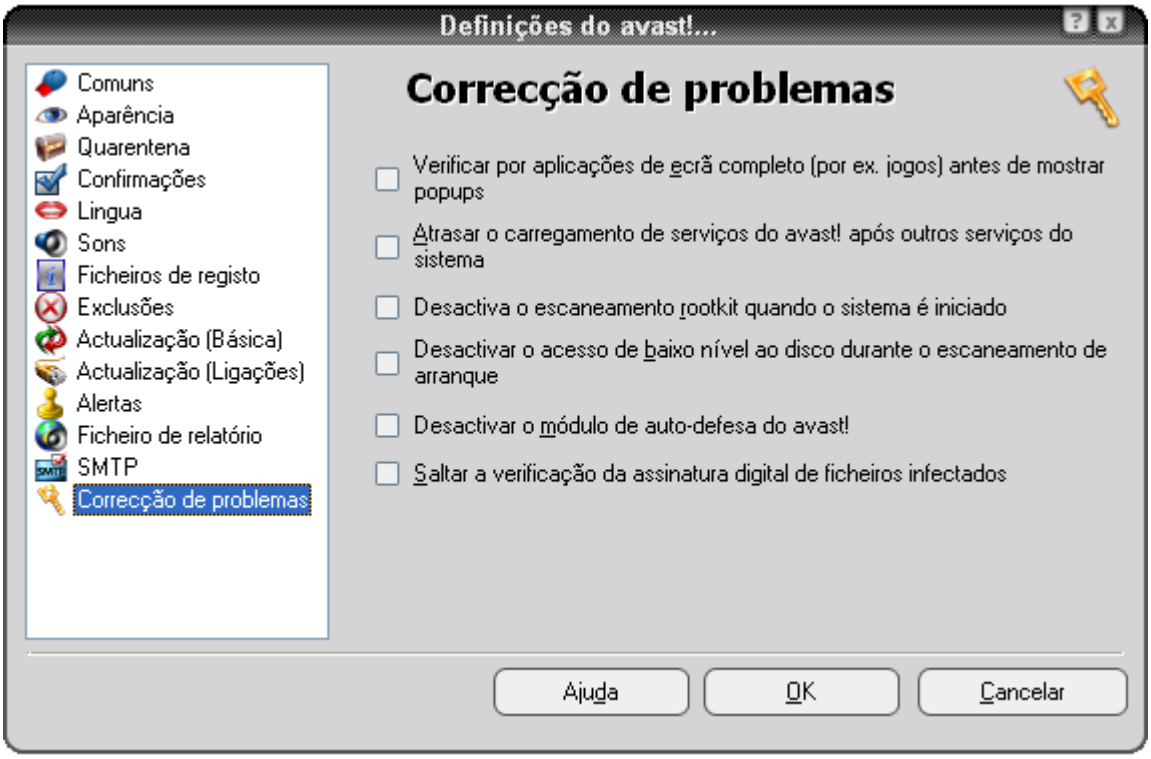
Se sabe o endereço e a porta do seu proxy seleccione “Especificar o servidor de proxy” e

insira os detalhes necessários, tal como se segue:

- **Tipo**: HTTP ou SOCKS4
- **Endereço**. Insira o endereço do seu servidor de proxy.
- **Porta:** Insira a porta que o seu proxy utiliza.
- **Tipo de autentificação:** Especifique aqui se o acesso à internet através do proxy requer o uso de autentificação, e se sim qual.
- **Nome de utilizador e Senha:** Devem ser inseridos caso queira autentificação.

Para acabar, clique em "Testar ligação" para verificar se a ligação baseada nas definições feitas acima funciona.

Correcção de problemas



Alterar as definições nesta página poderá ajudar a resolver alguns problemas específicos com o avast!. No entanto, estas definições não devem ser alteradas sem uma boa razão para tal. Em caso de dúvida contacte-nos antes.

Verificar aplicações de ecrã completo antes de mostrar popups.
De acordo com as configurações do avast! podem aparecer várias mensagens quando o seu computador está a ser executado (por exemplo, a base de dados de vírus foi actualizada, quando emails estão ser verificados, etc.). Normalmente as mensagens são mostradas quando ocorre o evento correspondente. Mas isto pode resultar na interrupção de aplicações de ecrã completo (por exemplo jogos) – o Windows muda do ecrã completo para uma janela mais pequena, caso apareça uma mensagem. Se activar

esta opção o avast! tentará detectar se alguma aplicação de ecrã complete está a ser executada antes de mostrar qualquer mensagem; caso tal aplicação seja encontrada a mensagem não será mostrada.

Atrasar o carregamento de serviços do avast! após outros serviços do sistema

O serviço do avast! antivírus é iniciado bastante cedo durante o processo de arranque do computador. Por vezes isto pode causar problemas quando iniciar outros serviços do sistema – que se pode manifestar através de uma congelação do sistema (por alguns segundos ou minutos) após o seu inicio. Esta opção torna possível atrasar o inicio do avast! antivírus até os outros serviços estarem completamente carregados.

Desactivar a verificação a rootkits quando o sistema é iniciado

O avast! verifica a presença de rootkits sempre que o seu sistema operativo é iniciado. Se deseja desactivar esta verificação preencha a respectiva caixa.

Desactivar o acesso de baixo nível ao disco durante a verificação de arranque.

Durante a verificação de arranque o avast! usa um método especial de acesso ao disco que lhe permite detectar até vírus que escondem os seus próprios ficheiros. Aqui pode desligar esta tarefa e o avast! usará apenas o método normal.

Desactivar o módulo de auto-defesa do avast!

Alguns vírus são capazes de desligar antivírus parando os seus processos, apagando ficheiros críticos ou modificando-os. O avast! contém uma funcionalidade de auto-protecção que previne ataques deste tipo bloqueando as suas operações. Para desactivar esta função preencha a respectiva caixa.

Saltar a verificação da assinatura digital de ficheiros infectados

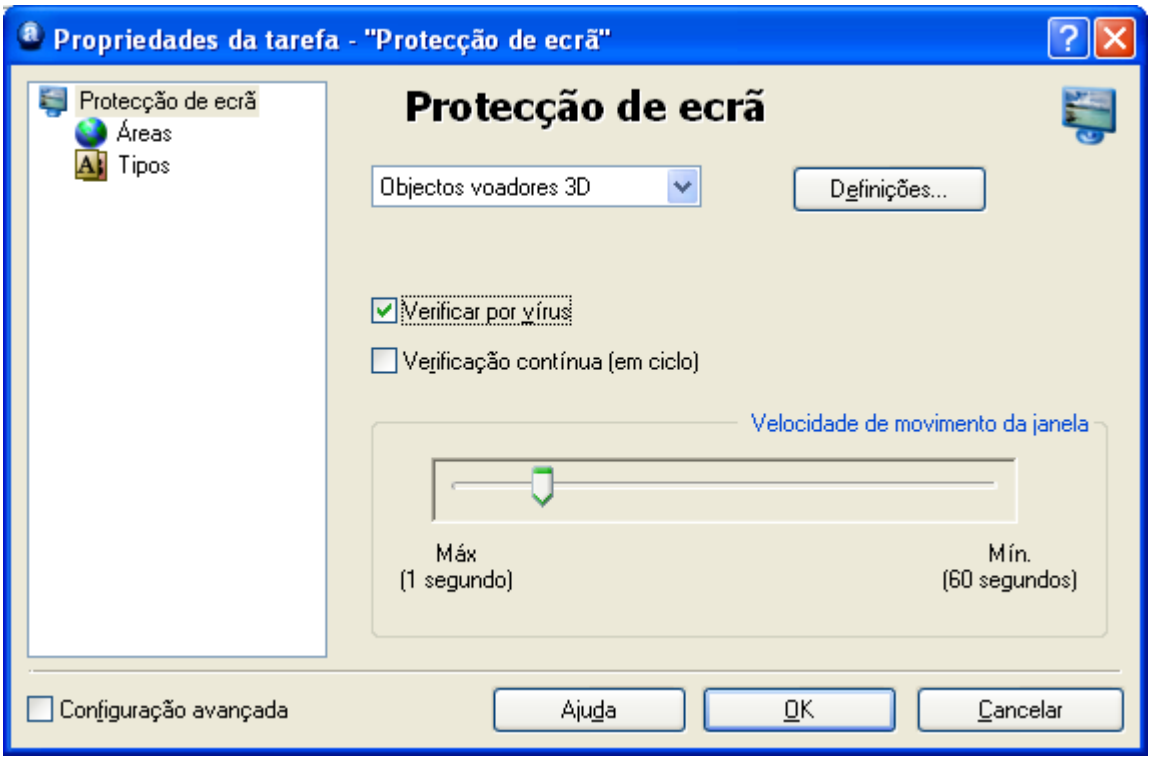
Para evitar avisos falso-positivos o avast! verifica a assinatura digital de ficheiros infectados. Se um ficheiro for detectado como infectado mas conter uma assinatura de confiança (por exemplo Microsoft), é provavelmente um falso-positivo – e o avast! irá ignorar esta detecção. Desactivar esta opção fará com que o avast! não faça esta verificação, alertando para todas as infecções encontradas.

Como activar o protector de ecrã avast! antivírus

O avast! antivírus pode verificar o seu computador quando o seu computador não está a ser usado e a protecção de ecrã é activada. Durante esta verificação aparece no ecrã uma pequena janela com a informação do seu progresso.

Para iniciar o Protector de ecrã do avast! antivírus clique em "Iniciar", depois em "Painel de Controlo". Depois faça um duplo clique em "Visualização" e na janela que aparece escolha "Protecção de Ecrã", de seguida clique no botão com uma seta para baixo e aparecerão várias opções. Clique na opção "avast! antivírus". Na caixa abaixo pode seleccionar o número de minutes a partir dos quais a "Protecção de Ecrã" é activada e se acha necessário ou não uma palavra-chave para continuar.

Ao clicar em "definições" nesta janela poderá escolher a protecção de ecrã na qual a mensagem de progresso do avast! irá aparecer – veja a próxima página.



Se deseja que o seu computador seja verificado seleccione a caixa “Verificar Vírus”. Se esta caixa não for preenchida a protecção de ecrã funcionar apenas como uma protecção de ecrã normal.

Se preencher a caixa “Verificação continua (em ciclo)” será feita outra verificação sempre que a última acabar.

Alterar a “Velocidade de movimento da janela” irá afectar a frequência com que aparece a informação do progresso da verificação.

Se clicar em “Definições” poderá ajustar as definições da protecção de ecrã normal.

Se clicar em “**Áreas**” pode especificar que áreas do seu computador devem ser verificadas. As áreas a serem verificadas automaticamente incluem “Todos os discos rígidos”. Se não deseja que todos os discos rígidos sejam verificados apague esta opção seleccionando-a e premindo depois em “Remover”. Pode depois especificar que áreas devem ser verificadas clicando em “Procurar” e seleccionando as áreas desejadas clicando nas caixas apropriadas. Se clicar em “Adicionar” poderá escolher as áreas de uma lista pré-definida.

Depois de escolher a(s) área(s) a serem verificadas, clique em "**Tipos**" para especificar quais ficheiros devem ser verificados. Os ficheiros podem ser reconhecidos como suspeitos em função do seu conteúdo, o que é mais lento, ou com base no seu nome ou extensão.

Se seleccionar uma verificação baseada no conteúdo, pode especificar que todos os ficheiros devem ser verificados marcando a caixa "Verificar todos os ficheiros". Se marcar

esta caixa, isso significa que, mesmo aqueles ficheiros que não costumam conter vírus, tais como ficheiros de imagem, também serão verificados. Se deixar esta caixa desmarcada, estes ficheiros não serão verificados e aparecerão no relatório como "ficheiros saltados".

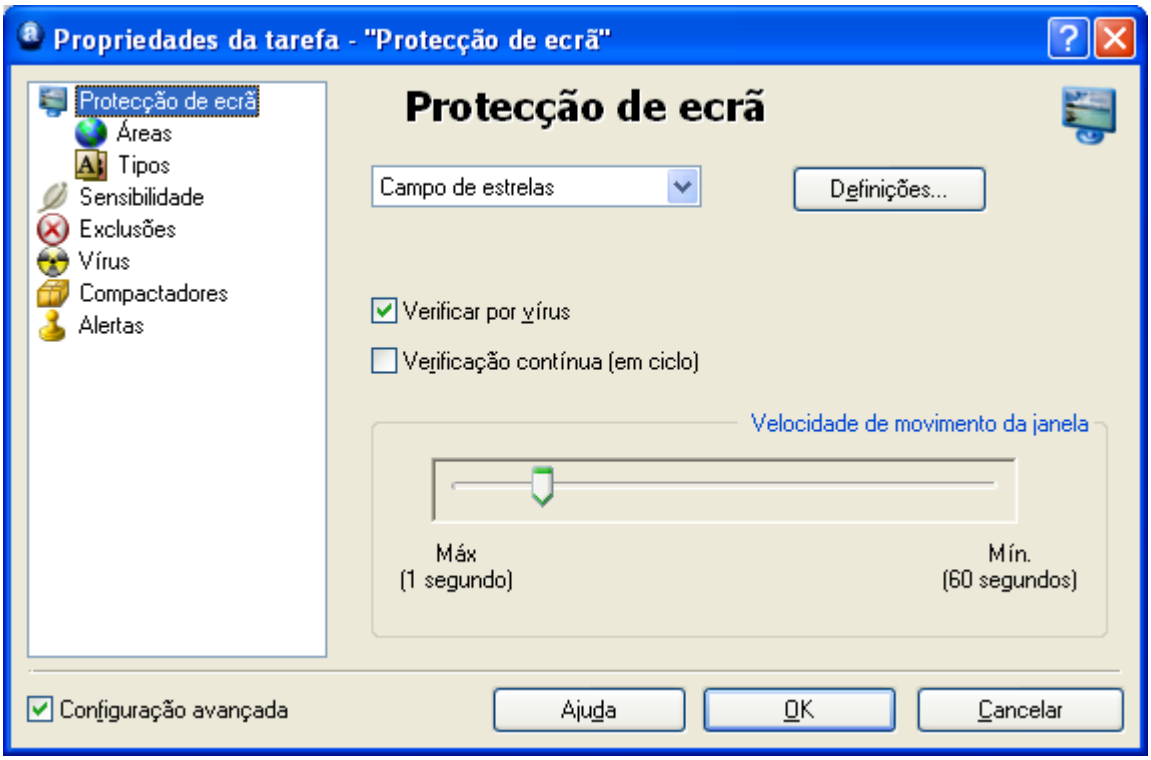
Caso escolha uma verificação baseada na extensão necessita especificar que extensões devem ser reconhecidas como suspeitas.

Para verificar ficheiros com base em uma ou mais extensões específicas, clique em "Procurar..." e será exibida uma lista de extensões de ficheiro. Se puder encontrar a extensão que pretende adicionar, clique sobre ela e, em seguida, clique em "OK" para adicioná-la à lista. Se a extensão que pretende adicionar não estiver na lista, poderá adicioná-la manualmente. Clique em "Adicionar", em seguida, digite a extensão do arquivo que deseja adicionar. Para adicionar uma outra extensão, clique em "Adicionar" novamente. Se quiser remover uma extensão de ficheiro da lista, basta clicar sobre ela para realçá-la e, em seguida, clicar em "Remover".

Se a caixa "Verificar extensões padrão" estiver marcada, isso significa que todas as extensões conhecidas como "perigosas" serão automaticamente verificadas.

Quaisquer ficheiros com extensões diferentes das especificadas não serão verificados.

Se preencher a caixa “Configuração avançada” aparecerão várias opções adicionais – veja abaixo.



- ***Sensibilidade***

Se marcar a caixa "Testar ficheiros inteiros (pode demorar em ficheiros grandes)" os ficheiros serão testados na sua totalidade e não apenas as partes mais frequentemente afectadas por vírus. A maioria dos vírus são encontrados, quer no início dum ficheiro, quer no fim. Ao marcar esta caixa irá fazer uma verificação mais aprofundada, mas também irá tornar a verificação mais lenta.

Se marcar a caixa "Ignorar verificação pela extensão do ficheiro" os ficheiros irão ser verificados contra todos os vírus da base de dados de vírus. Se essa caixa não for marcada, os ficheiros serão testados apenas contra os vírus que afectam determinado tipo de ficheiro. Por exemplo, o programa não vai verificar vírus que infectam ficheiros com uma extensão ".exe" em ficheiros com a extensão ".com".

- ***Exclusões***

Aqui é possível excluir determinados ficheiros ou pastas da verificação. Isto funciona exactamente da mesma maneira descrita na **página 44**, excepto que as exclusões feitas aqui são aplicadas apenas a uma determinada tarefa. Os ficheiros ou pastas que estão excluídos no menu "Definições" serão automaticamente excluídos de todas as verificações.

- ***Vírus***

Ao clicar em “Vírus” aparecerá a seguinte janela:

Neste ecrã pode especificar que acção deve ser tomada quando um vírus é detectado. Por padrão o programa está em “escolha acção”. Esta é a versão interactiva.

Se for deixado assim significa que sempre que um ficheiro suspeito é detectado, ser-lhe-ão apresentadas várias opções das quais uma tem de ser seleccionada. Ou seja, pode especificar a acção a ser efectuada sempre que um ficheiro suspeito for detectado.

Se clicar em “Escolher acção” irão ser apresentadas as opções que aparecem quando um ficheiro suspeito é encontrado, isto é, Eliminar, Reparar, Mover para a Quarentena, Mudar o nome/Mover, ou Parar. Apenas as opções marcadas serão apresentadas como disponíveis. Se alguma destas opções for desmarcada não será apresentada como disponível quando um ficheiro suspeito for encontrado. Estas opções estão descritas na **página 34** na secção “O que fazer quando um vírus é encontrado”.

Ao seleccionar esta acção a verificação é suspensa sempre que um vírus for encontrado, até especificar a acção a ser tomada. Portanto, recomenda-se que escolha mais que uma acção, como Mover para a Quarentena.

Para seleccionar outra acção clique em “Remover a última palavra”. A acção padrão será, então, apagada e as 6 possibilidades aparecerão destacadas no centro do ecrã. Clique em qualquer uma delas e ela aparecerá na caixa acima. Esta será, então, a acção tomada para todos os ficheiros suspeitos encontrados. Para a remover basta clicar novamente em “Remover última palavra”.

As primeiras 4 acções são descritas em detalhe na **página 34**. Se clicar em “Interactiva…” irá reinserir a janela para escolher a acção. Se escolher parar irá simplesmente parar a verificação sempre que um ficheiro suspeito é encontrado.

É possível especificar mais de uma acção a ser tomada utilizando o botão “E”. Por exemplo, pode especificar que quaisquer ficheiros infectados sejam reparados e movidos para outro local, clicando em "Reparar..", depois "E" e, em seguida, "Mover para...".

Também pode especificar quaisquer acções alternativas que devam ser tomadas caso a primeira acção seleccionada falhar. Por exemplo, pode seleccionar "Reparar", como acção preferida, mas se clicar em "Se falhar" e "Mover para a Quarentena", pode garantir que os ficheiros que não possam ser reparados são movidos para a Quarentena – ver **página 52** .

Nota – se seleccionar “Eliminar…” pode especificar se o ficheiro é para ser removido permanentemente (acção padrão), ou simplesmente movido para a Reciclagem. Se escolher “Eliminar permanentemente o(s) ficheiro(s)”, poderá também especificar que ficheiro(s) devem ser apagados na próxima vez que o computador for iniciado se não o poderem ser eliminados agora, para tal preencha a caixa “Se necessário, eliminar o(s) ficheiro(s) no próximo arranque”.

- ***Compactadores***

Nesta página pode especificar que arquivos devem ser testados durante a tarefa. A configuração padrão é apenas executáveis auto-extraíveis. Pode especificar arquivos adicionais que devam ser processados, embora isto irá tornar a verificação mais lenta. Preencha a opção "Todos os arquivos compactados" se desejar verificar todos os arquivos.

- ***Alertas***

Os alertas podem ser de carácter geral, que será enviado quando um vírus é detectado, ou eles podem ser gerados apenas quando um vírus é detectado pelo protector de ecrã. Os alertas que podem ser adicionados ao protector de ecrã são mostrados na caixa "alertas disponíveis".
Os alertas gerais são criados se clicar em “Definições” e “Alertas” como descrito na **página 48**, no entanto, os alertas criados deste modo não podem ser associados ao protector de ecrã.

Se o alerta que deseja adicionar é mostrado aqui, clique nele para o realçar e, em seguida, clique no botão “→”. Isto irá mover o alerta para a caixa de “Alertas usados”, o que significa que está agora associado ao protector de ecrã.

Se o alerta que deseja adicionar não for exibido clique em "Novo..." para criar um novo alerta.

Pode atribuir um nome ao alerta, por exemplo, um nome que o associe ao protector de ecrã e pode também adicionar mais informações na caixa "Comentário". O alerta é então criado exactamente da mesma maneira como descrito na **página 48**

Depois de ter criado o novo alerta, clique em OK e ele será automaticamente colocada na caixa "Alertas usados".

Para remover um alerta da caixa “Alertas usados” clique-o de modo a realçá-lo e depois no botão “←”, o que o moverá de volta para a caixa dos “Alertas disponíveis”.

Para alterar ou apagar um alerta basta realçá-lo e clicar em "Modificar" ou "Eliminar".

Se necessita de um alerta SMTP não se esqueça de inserir os detalhes SMTP, depois de criar a sua tarefa, clicando em “Definições” e em “SMTP”.

Note que alertas ligados ao protector de ecrã só serão enviados de um vírus for detectado pelo protector de ecrã. Eles não serão enviados caso vírus sejam detectados por outros módulos. Se deseja que um alerta seja enviado sempre que um vírus for detectado por qualquer módulo deve criar um alerta geral como descrito na **página 48**.

Para confirmar todas as configurações clique “OK”, depois em “Aplicar” e depois novamente em “OK”.
Agora, sempre que o protector de ecrã for activado executará também verificações de vírus.

Como actualizar para o Professional Edition

Fazer o upgrade do Home Edition para Professional Edition é muito simples.

Não precisa desinstalar a versão presente no seu computador nem nenhum download adicional é necessário. Precisa apenas de comprar o Professional Edition, obter a chave de licença e inseri-la no seu actual programa. Automaticamente o programa fará as alterações necessárias por si mesmo e passará então a ter o Professional Edition na sua máquina.

A chave de licença pode ser comprada para um período de 12, 24, ou 36 meses – basta ir a **www.avast.com** e clicar em "Adquirir".

Como desinstalar o avast! antivírus

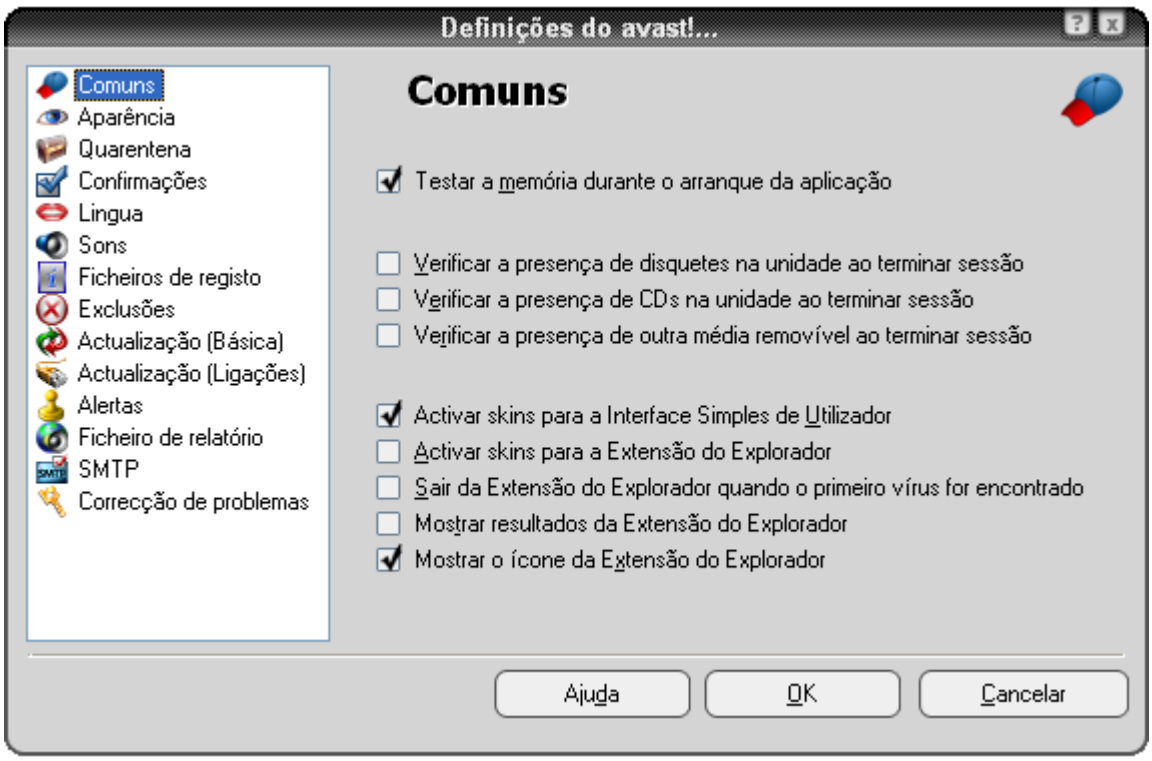
Como alguns vírus são desenhados para desligar ou alterar softwares antivírus de um computador o avast! vem com um forte módulo de auto-defesa (AD) que evita que isso aconteça. Como consequência esta protecção funciona também com outros programas que queiram alterar ou apagar o avast!, tornando-o muito mais difícil de apagar/alterar em comparação com as versões anteriores. De modo a remover completamente o avast! é necessário seguir o seguinte procedimento.

Antes de tentar desinstalar o avast! antivírus recomenda-se que feche todas as outras aplicações do seu computador. Procedimento de desinstalação recomendado:

1. Desligar a AD

- Clique com o botão direito do rato no ícone avast! no canto inferior direito do ecrã do seu computador, e seleccione "Definições do programa...".

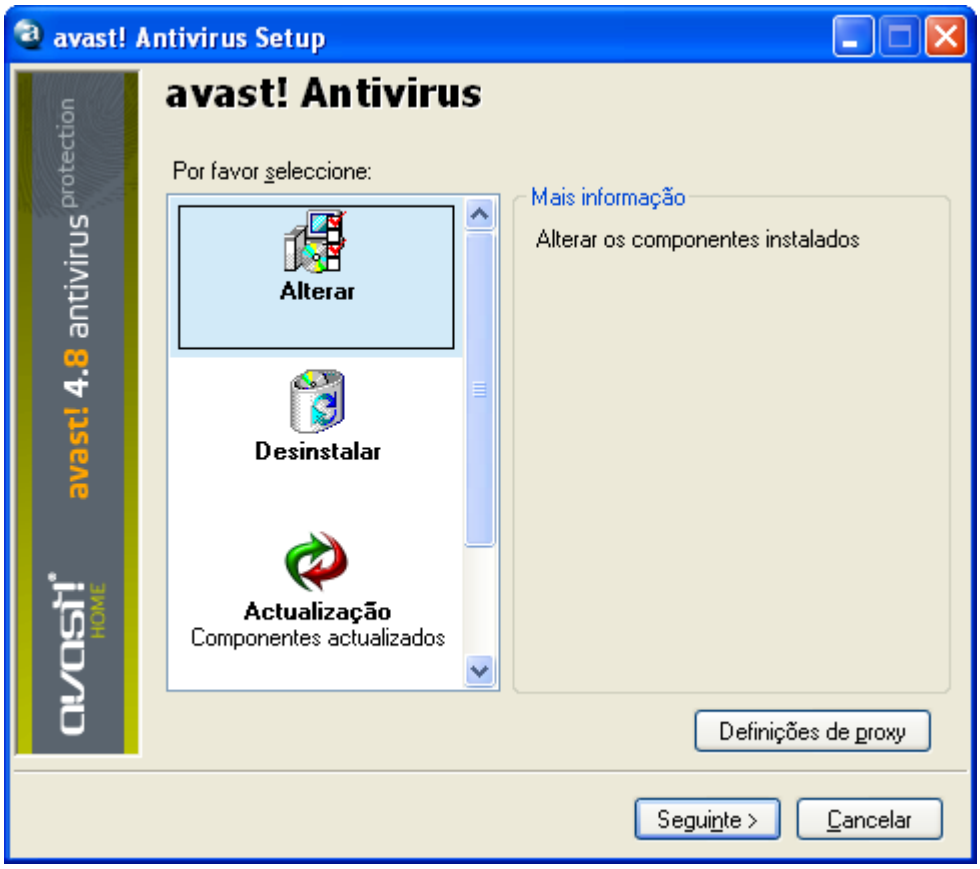
- Clique em "Correcção de problemas" no lado direito e aparecerá a seguinte janela:



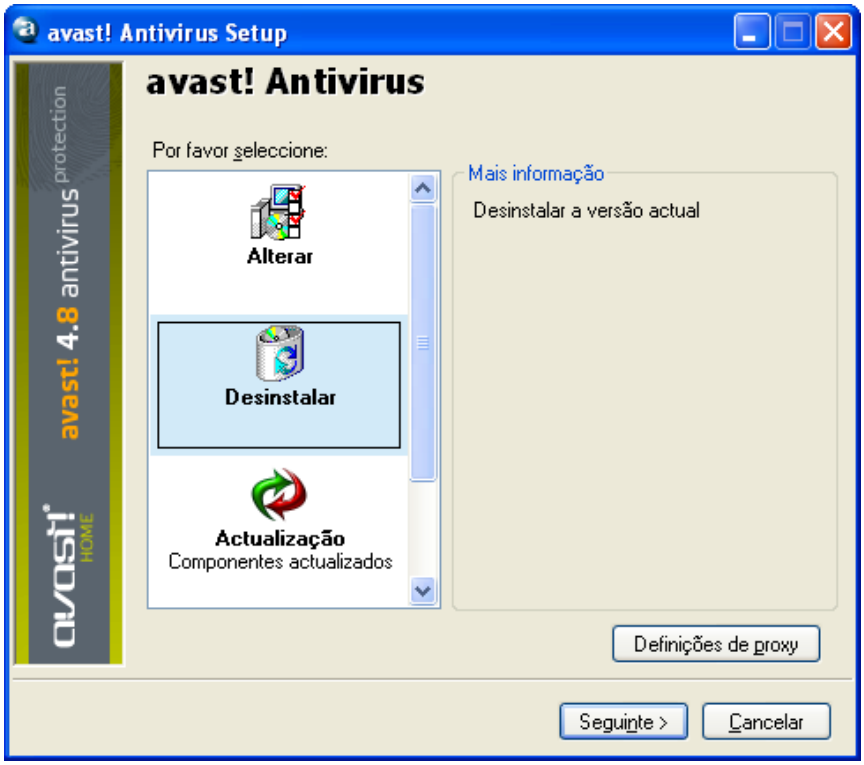
- Preencha a caixa "Desactivar o modulo de auto-defesa do avast!" como mostra a imagem e clique "OK".
- A AD está agora desligada.

2. Remover o programa

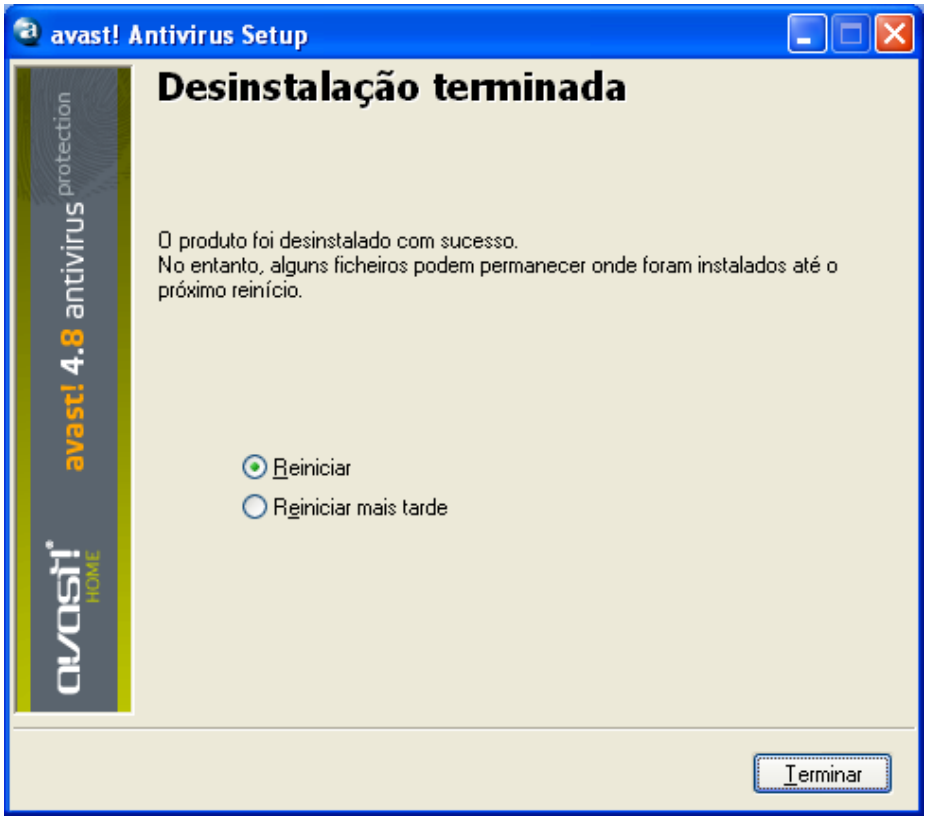
- Clique em "Iniciar" em baixo do lado esquerdo do seu ecrã e abra o seu "Painel de controlo". Caso não o veja clique em definições e ele deve aparecer como uma das opções.
- No Painel de Controlo clique em "Adicionar ou remover programas".
- Aparecerá uma lista de todos os programas instalados no seu computador.
- Seleccione "avast! antivírus" e clique "Alterar/remover"
- Aparecerá a seguinte janela:



Clique em "Desinstalar" e depois em "Seguinte".



O programa será agora desinstalado, aparecendo depois a seguinte janela:



Para completar o processo é necessário reiniciar o seu computador. Seleccione "Reiniciar" e depois clique em "Terminar" e o seu computador reiniciará automaticamente.