

Kaspersky Small Office Security

GUIA DE INICIAÇÃO



KASPERSKY lab

ÍNDICE

KASPERSKY SMALL OFFICE SECURITY	4
Descrição geral do software	4
Pacotes de software	4
Iniciação.....	5
Suporte para utilizadores registados.....	7
KASPERSKY ANTI-VIRUS 6.0 PARA WINDOWS WORKSTATIONS	8
Descrição geral.....	8
O que há de novo no Kaspersky Anti-Virus 6.0 para Windows Workstations	8
Como é constituída a protecção do Kaspersky Anti-Virus para Windows Workstations	9
Componentes de protecção.....	9
Tarefas de verificação de vírus.....	10
Actualização	11
Funcionalidades de suporte da aplicação	11
Instalação do Kaspersky Anti-Virus 6.0 para Windows Workstations	12
Requisitos de hardware e software de sistema	12
Instalação através do Assistente de Instalação	13
Instalação da aplicação a partir da linha de comandos.....	16
Instalação a partir do Editor de Objectos de Política de Grupo.....	17
Instalar a aplicação.....	17
Descrição das definições do ficheiro setup.ini.....	17
Actualizar a versão da aplicação	18
Remoção da aplicação	19
Assistente de Configuração Inicial	19
Utilizar os objectos guardados da versão anterior.....	19
Activar a aplicação	19
Activação online	20
Activar a versão de avaliação.....	21
Activar através de um ficheiro da chave.....	21
Concluir a activação	21
Modo de protecção.....	21
Configuração das definições de actualização	21
Configurar verificações de vírus agendadas	22
Restringir o acesso à aplicação.....	22
Configurar o Anti-Hacker	23
Finalizar o Assistente de Configuração	24
KASPERSKY ANTI-VIRUS 6.0 PARA WINDOWS SERVERS.....	25
Descrição geral.....	25
O que há de novo no Kaspersky Anti-Virus 6.0 para Windows Servers.....	25
Como é constituída a protecção do Kaspersky Anti-Virus para Windows Servers.....	26
Antivírus de Ficheiros	26
Tarefas de verificação de vírus.....	26
Actualização	27
Funcionalidades de suporte da aplicação	27
Instalação do Kaspersky Anti-Virus 6.0 para Windows Servers	28
Requisitos de hardware e software	28

Instalação através do Assistente de Instalação	29
Instalação da aplicação a partir da linha de comandos.....	32
Instalação a partir do Editor de Objectos de Política de Grupo.....	32
Instalar a aplicação.....	32
Descrição das definições do ficheiro setup.ini	33
Actualizar a versão da aplicação	33
Remoção da aplicação	34
Assistente de Configuração Inicial	34
Utilizar os objectos guardados da versão anterior.....	34
Activar a aplicação	34
Activação online	35
Configuração das definições de actualização	36
Configurar verificações de vírus agendadas	37
Restringir o acesso à aplicação.....	37
Finalizar o Assistente de Configuração	37
KASPERSKY LAB	39
CONTRATO DE LICENÇA DE UTILIZADOR FINAL DA KASPERSKY LAB	40

KASPERSKY SMALL OFFICE SECURITY

O Kaspersky Small Office Security é um pacote de software que tem como objectivo proporcionar uma protecção abrangente contra vírus e outras ameaças a organizações de pequena dimensão.

DESCRIÇÃO GERAL DO SOFTWARE

O Kaspersky Small Office Security é um conjunto de produtos concebidos para proteger as estações de trabalho e os servidores do Windows da sua rede. Estes produtos são o Kaspersky Anti-Virus 6.0 para Windows Workstations (consulte a secção Kaspersky Anti-Virus 6.0 para Windows Workstations, na página [8](#)) e o Kaspersky Anti-Virus 6.0 para Windows Servers (consulte a secção Kaspersky Anti-Virus 6.0 para Windows Servers, na página [25](#)).

PACOTES DE SOFTWARE

Dependendo do tamanho da sua rede, o Kaspersky Small Office Security, sendo uma solução flexível, pode fornecer licenças para os seguintes conjuntos de computadores:

- 5 estações de trabalho
- 5 estações de trabalho e 1 servidor
- 10 estações de trabalho e 1 servidor

Pode adquirir a versão embalada do Kaspersky Small Office Security através dos nossos revendedores, ou descarregá-lo a partir de lojas na internet, incluindo a secção **eLoja** do sítio <http://www.kaspersky.pt>.

Se comprar a versão embalada do programa, o pacote irá incluir:

- Um envelope selado com um CD de instalação contendo os ficheiros do programa
- Um código de activação da aplicação na etiqueta do CD ou numa folha de papel especial
- Um Guia do Utilizador
- O contrato de licença de utilizador final (EULA)

Antes de romper o selo do envelope do disco de instalação, leia atentamente todo o EULA.

Se comprar o Kaspersky Small Office Security numa loja online, irá copiar o produto a partir do sítio de internet da Kaspersky Lab (**Downloads** → **Downloads de produtos**). Pode descarregar o Guia do Utilizador a partir da secção **Downloads** → **Documentação**.

Ser-lhe-á enviado um código de activação por correio electrónico após o seu pagamento ter sido recebido. Ao instalar o software descarregado, estará a aceitar todos os termos do EULA.

O Contrato de Licença de Utilizador Final é um contrato legal entre o utilizador e a Kaspersky Lab que especifica os termos segundo os quais poderá utilizar o software que adquiriu.

Leia atentamente todo o EULA.

Se não concordar com os termos do EULA, pode devolver o seu produto embalado ao revendedor ao qual o adquiriu, sendo reembolsado pelo montante que pagou pelo programa. Se não concordar com todos os termos do EULA, não abra a capa do CD nem descarregue, instale ou utilize este software.

INICIAÇÃO

Para instalar um produto incluído no Kaspersky Small Office Security no seu computador ou servidor, insira o CD de instalação na unidade de CD/DVD-ROM. Será então apresentada uma janela de carregamento (consulte a Figura 1).



Figura 1. Janela de carregamento do Kaspersky Small Office Security

De acordo com o seu objectivo, seleccione um dos itens do menu:

Protecção para PC, se for instalar o Kaspersky Anti-Virus numa estação de trabalho. No lado esquerdo da nova janela (consulte a Figura 2), clique em **Instalar** para iniciar o assistente de instalação e siga as respectivas instruções (consulte a secção Instalação do Kaspersky Anti-Virus 6.0 para Windows Workstations, na página [12](#)).



Figura 2. Janela de carregamento do Kaspersky Small Office Security. Instalação do Kaspersky Anti-Virus for Windows Workstations

- **Protecção para Servidores de Ficheiros**, se for instalar o Kaspersky Anti-Virus num servidor. No lado esquerdo da nova janela (consulte a Figura 3), clique em **Instalar** para iniciar o assistente de instalação e siga as respectivas instruções (consulte a secção Instalação do Kaspersky Anti-Virus 6.0 para Windows Workstations, na página 12).



Figura 3. Janela de carregamento do Kaspersky Small Office Security.
Instalação do Kaspersky Anti-Virus for Windows Servers

- **Documentação**, se pretender obter mais informações sobre os produtos.

Na nova janela (consulte a Figura 4), seleccione:

- **Guia de Início do Kaspersky Small Office Security** para abrir o guia de instalação
- **Guia do Utilizador do Kaspersky Anti-Virus para Windows Workstations** para abrir o documento correspondente
- **Guia do Utilizador do Kaspersky Anti-Virus para Windows Servers** para abrir o guia de utilizador correspondente
- **Instalar o Adobe Acrobat** para instalar software que permite abrir correctamente os guias de utilizador
- **Suporte Técnico** para visitar o sítio de internet da Assistência Técnica da Kaspersky Lab



Figura 4. Janela de carregamento do Kaspersky Small Office Security.
Documentação

A janela de carregamento apenas é apresentada se a execução automática estiver activada. Se a execução automática estiver desactivada, siga directamente as instruções apresentadas na secção Instalação do Kaspersky Anti-Virus 6.0 para Windows Workstations, na página [12](#), para a instalação do Kaspersky Anti-Virus for Workstations e na secção Instalação do Kaspersky Anti-Virus 6.0 para Windows Servers, na página [28](#), para a instalação do Kaspersky Anti-Virus for Servers. É fornecida assistência aos utilizadores registados.

SUPORTE PARA UTILIZADORES REGISTADOS

A Kaspersky Lab fornece aos seus utilizadores registados uma série de serviços para tornar o Kaspersky Anti-Virus for Windows Servers mais eficaz.

Ao activar o programa, torna-se um utilizador registado e terá os seguintes serviços disponíveis até a licença expirar:

- Novas versões do programa, fornecidas de forma gratuita
- A Kaspersky Lab oferece Suporte Técnico telefónico ou online. Para consultas telefónicas, contacte com a iPortalMais pelo número +351 22 510 64 76. Se, por outro lado, preferir realizar uma consulta online, visite a seguinte página Web: http://www.kaspersky.com/pt/tech_support
- Notificações sobre lançamentos de novos produtos da Kaspersky Lab e sobre novos vírus (este serviço é fornecido aos utilizadores que se registem nas listas de envio de novidades da Kaspersky Lab)
- A Kaspersky Lab não fornece assistência técnica relativamente à utilização do sistema operativo ou de quaisquer produtos de terceiros.

KASPERSKY ANTI-VIRUS 6.0 PARA WINDOWS WORKSTATIONS

O Kaspersky Anti-Virus 6.0 para Windows Workstations é o precursor de uma nova geração de produtos de segurança de dados.

O que realmente destaca o Kaspersky Anti-Virus 6.0 para Windows Workstations das outras ofertas de software de segurança, inclusivamente de outros produtos da Kaspersky Lab, é a sua abordagem multifacetada em relação à segurança dos dados.

DESCRIÇÃO GERAL

O Kaspersky Anti-Virus 6.0 para Windows Workstations é uma ferramenta abrangente de protecção de dados. A aplicação garante não só a protecção antivírus, mas também a protecção contra spam e ataques de rede. As componentes da aplicação também ajudam os utilizadores a proteger os seus computadores contra ameaças desconhecidas e phishing e a restringir o acesso dos utilizadores à Internet.

A protecção multi-facetada abrange todos os canais de transferência e intercâmbio de dados. A configuração flexível fornecida para cada uma das componentes permite aos utilizadores adaptar o Kaspersky Anti-Virus para Windows Workstations às suas necessidades específicas.

O QUE HÁ DE NOVO NO KASPERSKY ANTI-VIRUS 6.0 PARA WINDOWS WORKSTATIONS

Vamos analisar em maior detalhe as inovações do Kaspersky Anti-Virus 6.0 Windows Workstations.

Novidades na protecção:

- O novo núcleo antivírus que o Kaspersky Anti-Virus para Windows Workstations utiliza detecta os programas maliciosos de forma mais eficaz. O novo núcleo antivírus também é significativamente mais rápido na verificação do sistema quanto à presença de vírus. Isto resulta do processamento melhorado dos objectos e da utilização otimizada dos recursos do computador (particularmente, para processadores de dois ou quatro núcleos).
- Foi implementado um novo analisador heurístico, que permite uma maior precisão na detecção e bloqueio dos programas maliciosos anteriormente desconhecidos. Se a assinatura de um programa não for encontrada nas bases de dados antivírus, o analisador heurístico simula a execução do programa num ambiente virtual isolado. Este método é seguro e permite analisar todos os efeitos de um programa antes de este ser executado num ambiente real.
- A componente nova Controlo de Acesso monitoriza o acesso dos utilizadores aos dispositivos I/O externos, permitindo aos administradores restringir o acesso a dispositivos USB externos, dispositivos de multimédia e outros dispositivos de armazenamento de dados.
- Foram introduzidas melhorias significativas na componente Firewall (a eficácia global da componente foi melhorada e o suporte IPv6 foi adicionado) e na Defesa Proactiva (a lista de eventos processados pela componente foi alargada).
- O procedimento de actualização da aplicação foi melhorado. Agora o computador raramente precisa de ser reiniciado.

- A capacidade de verificar o tráfego de ICQ e MSN foi adicionada, o que garante a utilização segura dos clientes de mensagens instantâneas.

Novas funcionalidades da interface:

- A interface torna as funcionalidades do programa simples e fáceis de aceder.
- A interface foi remodelada tendo em conta as necessidades dos administradores de redes de pequena e média dimensão, assim como dos administradores de grandes redes empresariais.

Novas funcionalidades no Kaspersky Administration Kit:

- O Kaspersky Administration Kit facilita e simplifica a gestão dos sistemas de protecção antivírus de uma empresa. Os administradores podem usar a aplicação para gerir, de forma centralizada, a protecção de uma rede empresarial de qualquer dimensão, com milhares de nós, incluindo os utilizadores remotos e móveis.
- Foi adicionada uma funcionalidade que permite a instalação remota da aplicação com a última versão das bases de dados da aplicação.
- A gestão da aplicação quando instalada num computador remoto foi melhorada (a estrutura da política foi redesenhada).
- Agora as componentes Anti-Spam e Anti-Spy podem ser geridas de forma remota.
- Foi adicionada uma funcionalidade que permite utilizar o ficheiro de configuração de uma aplicação existente ao criar uma política.
- Uma outra funcionalidade importante é percebida na opção de criação de configurações específicas para utilizadores móveis ao configurar tarefas de actualização de grupo.
- Foi implementada uma outra funcionalidade que permite desactivar, temporariamente, acções da política e tarefas de grupo para computadores cliente com a aplicação instalada (depois de inserir a password correcta).

COMO É CONSTITUÍDA A PROTECÇÃO DO KASPERSKY ANTI-VIRUS PARA WINDOWS WORKSTATIONS

A protecção do Kaspersky Anti-Virus para Windows Workstations é concebida tendo em conta as fontes de ameaças. Por outras palavras, cada componente da aplicação trata de uma dada ameaça, controlando-a e executando os passos necessários para prevenir os impactos maliciosos daquela fonte nos dados do utilizador. Isto torna a configuração flexível com opções de fácil configuração para todas as componentes, as quais podem ser adaptadas às necessidades de um utilizador em específico ou da empresa como um todo.

O Kaspersky Anti-Virus para Windows Workstations inclui:

- Componentes de protecção (na página [9](#)) que permitem uma defesa global em todos os canais de transmissão e intercâmbio de dados no seu computador em tempo real.
- Tarefas de verificação de vírus (na página [10](#)), que verificam a existência de vírus no computador ou em ficheiros individuais, pastas, discos ou áreas.
- Actualização (na página [11](#)), que garante o estado actualizado dos módulos internos da aplicação e das bases de dados utilizadas para detectar programas maliciosos, ataques de rede e mensagens de spam.
- Funcionalidades de suporte (ver secção "Funcionalidades de suporte da aplicação" na página [11](#)) que fornecem informação de suporte para trabalhar com a aplicação e expandir as capacidades da mesma.

COMPONENTES DE PROTECÇÃO

As seguintes componentes de protecção permitem a defesa do seu computador em tempo real:

Antivírus de Ficheiros

O *Antivírus de Ficheiros* monitoriza o sistema de ficheiros do computador. Verifica todos os ficheiros que possam ser abertos, executados ou guardados no seu computador e todas as unidades de disco ligadas. O Kaspersky Anti-Virus para Windows Workstations intercepta todas as tentativas para aceder a um ficheiro e verifica o ficheiro quanto à existência de vírus conhecidos. O ficheiro apenas pode ser alvo de processamento adicional, caso não esteja infectado ou se for desinfectado com sucesso pela aplicação. Se, por qualquer razão, um ficheiro não puder ser desinfectado, este será apagado, sendo guardada uma cópia do ficheiro na Cópia de Segurança ou sendo movido para a Quarentena.

Antivírus de E-mail

O Antivírus de E-mail verifica todos os e-mails recebidos e enviados no seu computador. Analisa os e-mails quando à presença de programas maliciosos. O e-mail apenas é disponibilizado ao destinatário se não contiver objectos perigosos. A componente também analisa os e-mails para detectar phishing.

Antivírus de Internet

O Antivírus de Internet intercepta e bloqueia scripts em sites, caso representem uma ameaça. Todo o tráfego HTTP é sujeito a uma inspeção rigorosa. A componente também analisa as páginas de Internet para detectar phishing.

Defesa Proactiva

A Defesa Proactiva permite detectar um novo programa malicioso antes de este executar a sua actividade maliciosa. A componente foi concebida em torno da monitorização e análise do comportamento de todas as aplicações instaladas no seu computador. Com base nas acções executadas por uma aplicação, o Kaspersky Anti-Virus para Windows Workstations toma uma decisão sobre se a aplicação é ou não potencialmente perigosa. Por isso, o seu computador está protegido não só em relação a vírus conhecidos, mas também relativamente a novos vírus que ainda não foram descobertos.

Anti-Spy

O Anti-Spy controla a publicidade não autorizada (faixas de publicidade, janelas de pop-up), intercepta as tentativas dos programas de marcação telefónica para estabelecerem ligações a sites pagos, e bloqueia-os.

Anti-Hacker

O Anti-Hacker protege o seu computador enquanto trabalha na Internet e noutras redes. Monitoriza as ligações de entrada e de saída e verifica portas e pacotes de dados.

Anti-Spam

O Anti-Spam está integrado no cliente de e-mail instalado no seu computador e monitoriza todos os e-mails recebidos quanto à presença de spam. Todos os e-mails que contenham spam são marcados com um cabeçalho especial. Também é fornecida a opção de configurar o Anti-Spam para o processamento de spam (apagar automaticamente, mover para uma pasta especial, etc.) A componente também analisa os e-mails para detectar phishing.

Controlo de Dispositivos

A componente foi concebida para monitorizar o acesso dos utilizadores aos dispositivos externos instalados no computador. Esta limita o acesso das aplicações aos dispositivos externos (USB, Firewire, Bluetooth, etc.).

TAREFAS DE VERIFICAÇÃO DE VÍRUS

É extremamente importante verificar, periodicamente, a existência de vírus no seu computador. Isto é necessário para eliminar a possibilidade de propagação de programas maliciosos que ainda não foram descobertos pelas componentes de protecção, por exemplo, porque o nível de segurança é baixo ou por outras razões.

O Kaspersky Anti-Virus para Windows Workstations inclui as seguintes tarefas de verificação de vírus:

Verificação

Verifica objectos seleccionados pelo utilizador. Pode verificar qualquer objecto no sistema de ficheiros do computador.

Verificação Completa

Uma verificação minuciosa de todo o sistema. Por defeito, são verificados os seguintes objectos: memória do sistema, programas carregados ao iniciar, cópia de segurança do sistema, bases de dados de e-mail, discos rígidos, meios de armazenamento removíveis e unidades de rede.

Verificação Rápida

Verificação de vírus dos objectos de inicialização do sistema operativo.

ACTUALIZAÇÃO

Para bloquear qualquer ataque de rede, apagar um vírus ou outro programa malicioso, o Kaspersky Anti-Virus para Windows Workstations deve ser regularmente actualizado. A componente **Actualização** foi concebida para esse fim. Esta gere a actualização das bases de dados e dos módulos utilizados pela aplicação.

O serviço de distribuição de actualizações permite guardar numa pasta local as actualizações da base de dados e dos módulos do programa transferidas a partir dos servidores da Kaspersky Lab e depois torná-las acessíveis a outros computadores da rede para poupar no tráfego de Internet.

FUNCIONALIDADES DE SUPORTE DA APLICAÇÃO

O Kaspersky Anti-Virus para Windows Workstations inclui uma série de funcionalidades de suporte. Estas foram concebidas para manter a aplicação actualizada, para expandir as capacidades da aplicação e para o assistir enquanto a utiliza.

Ficheiros de dados e relatórios

Ao utilizar a aplicação, cada componente de protecção, tarefa de verificação ou actualização da aplicação cria um relatório próprio. Os relatórios contêm informação sobre actividades executadas e os resultados. Através destes, poderá obter informação detalhada sobre como funcionam as componentes do Kaspersky Anti-Virus para Windows Workstations. Se surgirem problemas, poderá enviar os relatórios à Kaspersky Lab para os nossos especialistas poderem estudar a situação em maior detalhe e ajudá-lo com a maior rapidez possível.

O Kaspersky Anti-Virus para Windows Workstations move todos os ficheiros suspeitos de serem perigosos para uma área de armazenamento especial denominada de *Quarentena*. Aqui são guardados na forma encriptada para evitar a infecção do computador. Pode fazer uma verificação de vírus nestes objectos, restaurá-los para as suas localizações anteriores, apagá-los ou colocar, por si próprio, os ficheiros na Quarentena. No final da verificação de vírus, todos os ficheiros que se concluir não estarem infectados, são automaticamente restaurados para as suas localizações anteriores.

A *Cópia de Segurança* guarda cópias de objectos desinfectados e apagados pelo Kaspersky Anti-Virus para Windows Workstations. Estas cópias são criadas de forma a que possa restaurar os ficheiros ou obter informação sobre a sua infecção, se necessário. As cópias de segurança dos ficheiros são também guardadas na forma encriptada para evitar mais infecções.

Pode restaurar um ficheiro da cópia de Segurança para a sua localização original e apagar a cópia.

Disco de Recuperação

O Disco de Recuperação foi concebido para verificar e desinfectar computadores compatíveis com x86 que foram infectados. Deve ser utilizado quando a infecção atinge um nível em que se considera ser impossível desinfectar o computador através de aplicações antivírus ou utilitários de remoção de software malicioso.

Licença

Ao comprar o Kaspersky Anti-Virus para Windows Workstations, você entra num contrato de licença com a Kaspersky Lab que regula o uso da aplicação, assim como o seu acesso às actualizações da base de dados da aplicação e ao Suporte Técnico durante um período de tempo especificado. Os termos de uso e outras informações necessárias para a funcionalidade completa da aplicação são fornecidos na licença.

Ao utilizar a função **Licença**, você pode obter informação detalhada sobre a sua licença actual, comprar uma nova licença ou renovar a licença existente.

Suporte

Todos os utilizadores registados do Kaspersky Anti-Virus para Windows Workstations podem beneficiar do nosso Serviço de Suporte Técnico. Para saber onde pode obter suporte técnico, use a função **Suporte**.

Utilizando as ligações que se seguem, pode aceder ao fórum de utilizadores dos produtos da Kaspersky Lab, enviar um relatório de erro ao Suporte Técnico ou fornecer informação de retorno sobre a aplicação, preenchendo um formulário especial on-line.

Também tem acesso ao Suporte Técnico on-line e aos Serviços de Arquivo Pessoal para Utilizadores. Os nossos funcionários terão todo o prazer em prestar-lhe suporte, por telefone, para o Kaspersky Anti-Virus para Windows Workstations.

INSTALAÇÃO DO KASPERSKY ANTI-VIRUS 6.0 PARA WINDOWS WORKSTATIONS

O Kaspersky Anti-Virus 6.0 para Windows Workstations pode ser instalado num computador através de várias formas:

- instalação local – instalação da aplicação num único computador. Para a instalação ser executada e concluída, é necessário ter acesso directo àquele computador. A instalação local pode ser executada através de um dos seguintes modos:
 - modo interactivo, utilizando o assistente de instalação da aplicação (ver secção "Instalação através do Assistente de Instalação" na página [13](#)); este modo requer a participação do utilizador durante a instalação;
 - modo não interactivo, no qual a instalação da aplicação é executada a partir da linha de comandos e não requer a participação do utilizador durante a instalação (ver secção "Instalação da aplicação a partir da linha de comandos" na página [16](#)).
- instalação remota – instalação da aplicação em computadores ligados em rede, geridos de forma remota a partir de uma estação de trabalho do administrador com a utilização do:
 - Solução de software Kaspersky Administration Kit (ver Guia de Implementação do Kaspersky Administration);
 - Políticas de domínios de grupo do Microsoft Windows Server 2000/2003 (ver secção "Instalação a partir do Editor de Objectos de Política de Grupo" na página [17](#)).

Antes de iniciar a instalação do Kaspersky Anti-Virus para Windows Workstations (inclusive numa instalação remota), recomenda-se que encerre todas as aplicações activas.

REQUISITOS DE HARDWARE E SOFTWARE DE SISTEMA

Para o funcionamento adequado do Kaspersky Anti-Virus 6.0 para Windows Workstations, o computador deve obedecer a estes requisitos mínimos:

Requisitos gerais:

- 300 MB de espaço livre em disco.
- Microsoft Internet Explorer 6.0 ou superior (para a actualização das bases da aplicação e dos módulos do programa através da Internet).
- Microsoft Windows Installer 2.0 ou superior.

Microsoft Windows 2000 Professional (Service Pack 4 Rollup1), Microsoft Windows XP Professional (Service Pack 2 ou superior), Microsoft Windows XP Professional x64 (Service Pack 2 ou superior):

- Processador Intel Pentium 300 MHz 32-bit (x86) / 64-bit (x64) ou superior (ou compatível).
- 256 MB de RAM livre.

Microsoft Windows Vista Business / Enterprise / Ultimate (Service Pack 1 ou superior), Microsoft Windows Vista Business / Enterprise / Ultimate x64 (Service Pack 1 ou superior), Microsoft Windows 7 Professional / Enterprise / Ultimate, Microsoft Windows 7 Professional / Enterprise / Ultimate x64:

- Processador Intel Pentium 800 MHz 32-bit (x86) / 64-bit (x64) ou superior (ou compatível).
- 512 MB de RAM livre.

INSTALAÇÃO ATRAVÉS DO ASSISTENTE DE INSTALAÇÃO

Para instalar o Kaspersky Anti-Virus para Windows Workstations no seu computador, execute o ficheiro de instalação a partir do CD do produto.

Instalar a aplicação a partir do ficheiro de instalação transferido da Internet é idêntico a instalar a aplicação a partir do CD.

O programa de instalação é implementado como um assistente padrão do Windows. Cada janela contém um conjunto de botões para controlar o processo de instalação. De seguida, é apresentada uma breve descrição das suas funções:

- **Seguinte** – aceitar a acção e avançar para o próximo passo do procedimento de instalação.
- **Anterior** – voltar ao passo anterior do procedimento de instalação.
- **Cancelar** cancelar a instalação.
- **Concluir** concluir o procedimento de instalação da aplicação.

De seguida, é apresentada uma discussão detalhada de cada passo da instalação do pacote.

Passo 1. Verificar se o sistema satisfaz os requisitos de instalação

Antes de instalar o Kaspersky Anti-Virus para Windows Workstations no computador, o assistente irá verificar se o computador satisfaz os requisitos mínimos. Também irá verificar se tem os direitos necessários para instalar o software.


Se algum destes requisitos não for satisfeito, será apresentada no ecrã a respectiva notificação. Recomendamos que instale as actualizações necessárias, através do serviço **Windows Update** e os programas necessários, antes de voltar a tentar instalar o Kaspersky Anti-Virus para Windows Workstations.

Passo 2. Janela de início da instalação

Se o seu sistema cumprir todos os requisitos impostos, logo depois do ficheiro de instalação ser executado, a janela de início abrir-se-á no ecrã, apresentando a informação sobre o início da instalação do Kaspersky Anti-Virus para Windows Workstations.

Para continuar a instalação, clique no botão **Seguinte**. Para cancelar a instalação, clique no botão **Cancelar**.

Passo 3. Visualizar o Contrato de Licença

A próxima caixa de diálogo da aplicação contém o contrato de licença introduzido entre você e a Kaspersky Lab. Leia-o com atenção e se concordar com todos os termos e condições do contrato, seleccione a opção  **Eu aceito os termos do Contrato de Licença** e clique no botão **Seguinte**. A instalação irá continuar.

Para cancelar a instalação, clique no botão **Cancelar**.

Passo 4. Seleccionar a pasta de instalação

O passo seguinte da instalação do Kaspersky Anti-Virus para Windows Workstations define a pasta onde a aplicação será instalada. O caminho predefinido é o seguinte:

- <Drive> → Program Files → Kaspersky Lab → Kaspersky Anti-Virus 6.0 para Windows Workstations – para sistemas 32-bit.
- <Drive> → Program Files (x86) → Kaspersky Lab → Kaspersky Anti-Virus 6.0 para Windows Workstations – para sistemas 64-bit.

Pode especificar uma pasta diferente, clicando no botão **Procurar** e seleccionando uma pasta na janela padrão de selecção da pasta ou inserindo o caminho da pasta no campo de registo fornecido.

Por favor, note que se inserir, manualmente, o caminho completo para a pasta de instalação, este não deve exceder os 200 caracteres e não deve conter caracteres especiais.

Para continuar a instalação, clique no botão **Seguinte**.

Passo 5. Utilizar configurações da aplicação guardadas numa instalação anterior

Neste passo, ser-lhe-á pedido que especifique se deseja utilizar as definições de protecção, as bases de dados da aplicação e a base de dados do Anti-Spam no funcionamento da aplicação, caso esses objectos tenham sido guardados no seu computador depois de remover a versão anterior do Kaspersky Anti-Virus 6.0 para Windows Workstations.

Vamos analisar em maior detalhe sobre como activar as funcionalidades acima descritas.

Se uma versão anterior (compilação) do Kaspersky Anti-Virus para Windows Workstations esteve instalada no seu computador e você guardou as bases de dados da aplicação depois de remover essa versão, então pode integrá-las na versão que está a instalar. Para o fazer, assinale a caixa **Bases de dados da Aplicação**. As bases de dados da aplicação incluídas no pacote de instalação não serão copiadas para o computador.

Para utilizar as definições de protecção que alterou numa versão anterior e que guardou no seu computador, assinale a caixa **Definições da aplicação**.

Recomenda-se também que utilize a base de dados do Anti-Spam, caso esta tenha sido guardada depois de remover a versão anterior da aplicação. Isto permitir-lhe-á saltar o procedimento de treino do Anti-Spam. Para considerar a base de dados que criou anteriormente, assinale a caixa **Bases de dados do Anti-Spam**.

Passo 6. Seleccionar o tipo de instalação

Neste passo, deve definir a abrangência da instalação da aplicação. Existem duas opções de instalação:

Completa. Neste caso, todas as componentes do Kaspersky Anti-Virus para Windows Workstations serão instaladas no seu computador. Para se familiarizar com os passos adicionais da instalação, consulte o Passo 8.

Personalizada. Neste caso, ser-lhe-á pedido que seleccione as componentes da aplicação que deseja instalar. Para mais detalhes, veja o Passo 7.

Para seleccionar o modo de instalação, clique no botão correspondente.

Passo 7. Seleccionar as componentes da aplicação a instalar

Este passo só será executado, se tiver seleccionado a opção de instalação **Personalizada**.

Antes de iniciar a instalação personalizada, deve seleccionar as componentes do Kaspersky Anti-Virus para Windows Workstations que deseja instalar. Por defeito, estão seleccionados para instalação todas as componentes de protecção, a componente de verificação de vírus e o conector do Agente de Rede para a administração remota da aplicação através do Kaspersky Administration Kit.

Para seleccionar uma componente para instalação adicional, deve abrir o menu, clicando com o botão esquerdo do rato no ícone junto ao nome da componente, e seleccionar o item **Este recurso será instalado no disco rígido local**. Na parte inferior desta janela de instalação do programa, encontrará mais informação sobre o tipo de protecção fornecida pela componente que seleccionou e sobre o espaço de armazenamento necessário para a instalação da mesma.

Para obter informações detalhadas sobre o espaço disponível no disco do seu computador, clique no botão **Volume**. A informação será apresentada na janela que se abre.

Para cancelar a instalação da componente, seleccione a opção **Este recurso ficará indisponível** a partir do menu de contexto. Note que se cancelar a instalação de uma componente, não será protegido contra uma série de programas perigosos.


Depois de terminar de seleccionar as componentes a instalar, clique no botão **Seguinte**. Para regressar à lista predefinida de componentes a instalar, clique no botão **Repor**.

Passo 8. Desactivar a firewall do Microsoft Windows

Este passo só deve ser executado se o Kaspersky Anti-Virus para Windows Workstations estiver a ser instalado num computador com a firewall activada e se o Anti-Hacker for uma das componentes que deseja instalar.

Neste passo da instalação do Kaspersky Anti-Virus para Windows Workstations, ser-lhe-á dada a opção de desactivar a Firewall do Microsoft Windows, já que a componente Anti-Hacker do Kaspersky Anti-Virus para Windows Workstations garante protecção total para as suas actividades de rede e não há necessidade de construir uma protecção adicional dentro do próprio sistema operativo.

Se desejar utilizar a Anti-Hacker como a sua principal ferramenta de protecção das actividades de rede, clique no botão **Seguinte**. A firewall do Microsoft Windows será, automaticamente, desactivada.

Se desejar proteger o seu computador com a firewall do Microsoft Windows, seleccione a opção  **Manter a Firewall do Windows activada**. Neste caso, a componente Anti-Hacker será instalada, mas desactivada para evitar conflitos no funcionamento das aplicações.

Passo 9. Procurar outras aplicações antivírus

Neste passo, o assistente procura outros programas antivírus, incluindo outros programas da Kaspersky Lab, que podem entrar em conflito com o Kaspersky Anti-Virus para Windows Workstations.

Se forem detectadas aplicações antivírus no seu computador, as mesmas serão listadas no ecrã. Ser-lhe-á dada a opção de as desinstalar antes de continuar com a instalação.

Pode escolher removê-las automaticamente ou manualmente, utilizando os controlos existentes por baixo da lista de programas de antivírus detectados.

Para continuar a instalação, clique no botão **Seguinte**.

Passo 10. Preparação final para a instalação

Este passo conclui a preparação para a instalação da aplicação no seu computador.

Na instalação inicial do Kaspersky Anti-Virus 6.0 para Windows Workstations, recomenda-se que não desmarque a caixa **Proteger o processo de instalação**. A activação da protecção permite-lhe efectuar o procedimento correcto de reversão da instalação, caso ocorram erros durante a instalação da aplicação. Quando voltar a tentar a instalação de uma aplicação, recomendamos que desmarque esta caixa.

Se a aplicação estiver a ser instalada de forma remota, através do **Windows Remote Desktop**, recomenda-se que desmarque a caixa

Proteger o processo de instalação. Caso contrário, o procedimento de instalação pode ser incorrectamente executado ou pode não ser executado.

Para continuar a instalação, clique no botão **Instalar**.

Ao instalar as componentes do Kaspersky Anti-Virus para Windows Workstations, as quais interceptam o tráfego de rede, as actuais ligações de rede são interrompidas. A maioria das ligações terminadas é retomada após algum tempo.

Passo 11. Concluir a instalação

A janela **Instalação concluída** contém informação sobre a conclusão da instalação do Kaspersky Anti-Virus para Windows Workstations no seu computador.

Para executar o Assistente de Configuração Inicial, clique no botão **Seguinte**.

Se for necessário reiniciar o computador para concluir a instalação com sucesso, será apresentada no ecrã a notificação especial.

INSTALAÇÃO DA APLICAÇÃO A PARTIR DA LINHA DE COMANDOS

➔ Para instalar o Kaspersky Anti-Virus 6.0 para Windows Workstations, digite o seguinte na linha de comandos:

```
msiexec /i <nome_pacote>
```

O assistente de instalação iniciar-se-á (ver secção "Instalação através do Assistente de Instalação" na página 13). Quando a aplicação estiver instalada, será necessário reiniciar o computador.

➔ Para instalar a aplicação no modo não interativo (sem executar o assistente de instalação), digite o seguinte:

```
msiexec /i <nome_pacote> /qn
```

Neste caso, o computador deve ser manualmente reiniciado depois de a instalação estar concluída. Para reiniciar o computador automaticamente, digite o seguinte na linha de comandos:

```
msiexec /i <nome_pacote> ALLOWREBOOT=1 /qn
```

Note que a reinicialização automática só pode ser efectuada no modo de instalação não interactiva (utilizando a chave /qn).

➔ Para instalar a aplicação com uma password, que confirma o direito de remoção da aplicação, digite o seguinte:

```
msiexec /i <nome_pacote> KLUNINSTPASSWD=***** – quando instalar a aplicação no modo interactivo;
```

```
msiexec /i <nome_pacote> KLUNINSTPASSWD=***** /qn – quando instalar a aplicação no modo não interactivo sem reiniciar o computador;
```

```
msiexec /i <nome_pacote> KLUNINSTPASSWD=***** ALLOWREBOOT=1 /qn – quando instalar a aplicação no modo não interactivo e depois reiniciar o computador.
```

Se instalar o Kaspersky Anti-Virus para Windows Workstations no modo não interactivo, é suportada a leitura do ficheiro `setup.ini` (ver página 17), que contém as definições gerais para a instalação da aplicação, do ficheiro de configuração `install.cfg` e do ficheiro da chave de licença. Tenha em atenção que estes ficheiros devem estar localizados na mesma pasta que o pacote de instalação do Kaspersky Anti-Virus para Windows Workstations.

INSTALAÇÃO A PARTIR DO EDITOR DE OBJECTOS DE POLÍTICA DE GRUPO

Através do **Editor de Objectos de Política de Grupo**, você pode instalar, actualizar e remover o Kaspersky Anti-Virus para Windows Workstations em estações de trabalho empresariais que façam parte do domínio, sem utilizar o Kaspersky Administration Kit.

INSTALAR A APLICAÇÃO

➔ Para instalar o Kaspersky Anti-Virus para Windows Workstations, execute as seguintes acções:

1. Crie uma pasta de rede partilhada no computador que funciona como controlador do domínio e coloque o pacote de instalação do Kaspersky Anti-Virus para Windows Workstations, com o formato `msi`, nessa mesma pasta.

Para além disso, neste directório pode colocar o ficheiro `setup.ini` (ver página 17), que contém a lista de definições para a instalação do Kaspersky Anti-Virus para Windows Workstations, o ficheiro de configuração `install.cfg` e o ficheiro da chave de licença.

2. Abra o **Editor de Objectos de Política de Grupo** a partir da consola MMC padrão (para obter informações detalhadas sobre como trabalhar com este editor, consulte o sistema de ajuda do Microsoft Windows Server).
3. Crie um novo pacote. Para o fazer, a partir da árvore da consola, seleccione **Objecto de Política de Grupo / Configuração do computador / Configuração do programa / Instalação do software** e use o comando **Criar / Pacote** a partir do menu de contexto.

Na janela que se abre, especifique o caminho para a pasta de rede partilhada que contém o pacote de instalação Kaspersky Anti-Virus para Windows Workstations. Na caixa de diálogo **Implementação do programa**, seleccione a configuração **Atribuída** e clique no botão **OK**.

A política de grupo será aplicada em cada estação de trabalho na próxima vez que os computadores forem registados no domínio. Como resultado, o Kaspersky Anti-Virus para Windows Workstations será instalado em todos os computadores.

DESCRIÇÃO DAS DEFINIÇÕES DO FICHEIRO SETUP.INI

O ficheiro `setup.ini`, localizado na pasta do pacote de instalação do Kaspersky Anti-Virus para Windows Workstations, é utilizado quando instala a aplicação no modo não interactivo a partir da linha de comandos ou do Editor de Objectos de Política de Grupo. Este ficheiro inclui as seguintes definições:

[Setup] – definições gerais para a instalação da aplicação.

- **InstallDir**=caminho para a pasta de instalação da aplicação>.
- **Reboot**=sim|não – define se o computador deve ou não ser reiniciado depois de a aplicação ser instalada (por defeito, a reinicialização não é executada).
- **SelfProtection**=sim|não – define se a Autodefesa do Kaspersky Anti-Virus para Windows Workstations deve ser activada durante a instalação (por defeito, a Autodefesa está activada).
- **NoKLIM5**=sim|não – define se a instalação dos controladores de rede do Kaspersky Anti-Virus para Windows Workstations deve ser cancelada durante a instalação da aplicação (por defeito, os controladores são instalados). Os controladores de rede do Kaspersky Anti-Virus para Windows Workstations do tipo NDIS, que interceptam o tráfego da rede para as componentes da aplicação como o Anti-Hacker, o Antivírus de E-mail, o

Antivírus de Internet e o Antispam, podem causar conflitos com outras aplicações ou dispositivos instalados no computador do utilizador. Você pode ignorar a instalação dos controladores de rede nos computadores com o Microsoft Windows XP ou Microsoft Windows 2000 para evitar possíveis conflitos.

Esta opção não está disponível em computadores com o Microsoft Windows XP x64 Edition ou Microsoft Vista.

[Componentes] – selecção das componentes da aplicação a serem instaladas. Se não for especificada nenhuma componente, a aplicação será completamente instalada. Se for especificada pelo menos uma componente, as componentes que não estiverem listadas não serão instaladas.

- **FileMonitor=sim|não** – instalação da componente Antivírus de Ficheiros.
- **MailMonitor=sim|não** – instalação da componente Antivírus de E-mail.
- **WebMonitor=sim|não** – instalação da componente Antivírus de Internet.
- **ProactiveDefence=sim|não** – instalação da componente Defesa Proactiva.
- **AntiSpy=sim|não** – instalação da componente Anti-Spy.
- **AntiHacker=sim|não** – instalação da componente Anti-Hacker.
- **AntiSpam=sim|não** – instalação da componente Anti-Spam.
- **LockControl=sim|não** – instalação da componente Controlo de Dispositivos.

[Tarefas] – activação das tarefas do Kaspersky Anti-Virus para Windows Workstations. Se não for especificada nenhuma tarefa, após a instalação todas as tarefas serão activadas. Se for especificada pelo menos uma tarefa, as tarefas que não estiverem listadas serão desactivadas.

- **ScanMyComputer=sim|não** – tarefa de verificação completa.
- **ScanStartup=sim|não** – tarefa de verificação rápida.
- **Scan=sim|não** – tarefa de verificação.
- **Updater=sim|não** – tarefa de actualização das bases de dados da aplicação e dos módulos do programa.

Em vez do valor **sim** pode utilizar os valores 1, on, activar, activado; em vez do valor **não** pode utilizar os valores 0, off, desactivar, desactivado.

ACTUALIZAR A VERSÃO DA APLICAÇÃO

➔ Para actualizar a versão do Kaspersky Anti-Virus para Windows Workstations, execute as seguintes acções:

1. Coloque o pacote de instalação, que contém as actualizações do Kaspersky Anti-Virus para Windows Workstations no formato MSI, numa pasta de rede partilhada.
2. Abra o **Editor de Objectos de Política de Grupo** e crie um novo pacote utilizando o procedimento acima descrito.
3. Seleccione o novo pacote na lista e use o comando **Propriedades** no menu de contexto. Na janela de propriedades do pacote, seleccione o separador **Actualizações** e especifique o pacote que contém o pacote de instalação da versão anterior do Kaspersky Anti-Virus para Windows Workstations. Para instalar uma versão actualizada do Kaspersky Anti-Virus para Windows Workstations, guardando as definições de protecção, seleccione a opção para instalar em substituição do pacote existente.

A política de grupo será aplicada em cada estação de trabalho na próxima vez que os computadores forem registados no domínio.

REMOÇÃO DA APLICAÇÃO

➤ Para remover o Kaspersky Anti-Virus para Windows Workstations, execute as seguintes acções:

1. Abra o **Editor de Objectos de Política de Grupo**.
2. Seleccione **Objecto_Política_Grupo / Configuração do computador/ Configuração do programa/ Instalação do software** na árvore da consola.

Seleccione o pacote do Kaspersky Anti-Virus para Windows Workstations na lista de pacotes, abra o menu de contexto e execute o comando **Todas as tarefas/ Remover**.

Na caixa de diálogo **Remover aplicações**, seleccione a opção **Remover imediatamente esta aplicação dos computadores de todos os utilizadores** para que o Kaspersky Anti-Virus para Windows Workstations seja removido na próxima reinicialização do computador.

ASSISTENTE DE CONFIGURAÇÃO INICIAL

O Assistente de Configuração do Kaspersky Anti-Virus para Windows Workstations inicia-se no final da instalação da aplicação. Foi concebido para o ajudar a configurar as definições iniciais da aplicação, com base nas características e tarefas do seu computador.

A interface do Assistente de Configuração foi concebida da mesma forma que um assistente típico do Microsoft Windows e consiste numa série de passos entre os quais pode navegar, utilizando os botões **Anterior** e **Seguinte**, ou concluir, utilizando o botão **Concluir**. Para parar o assistente em qualquer altura, utilize o botão **Cancelar**.

Para concluir a instalação da aplicação no computador, devem ser executados todos os passos do assistente. Se o funcionamento do assistente for interrompido, por alguma razão, os valores das configurações, que já tinham sido especificadas, não serão guardados. Na próxima tentativa de execução da aplicação, o Assistente de Configuração Inicial será novamente executado, requerendo que edite novamente as configurações.

UTILIZAR OS OBJECTOS GUARDADOS DA VERSÃO ANTERIOR

Esta janela do assistente aparece quando instala a aplicação em substituição da versão anterior do Kaspersky Anti-Virus para Windows Workstations. Ser-lhe-á pedido para seleccionar quais os dados utilizados pela versão anterior que deseja importar para a nova versão. Estes podem incluir objectos da quarentena ou da cópia de segurança ou ainda definições de protecção.

Para utilizar estes dados na nova versão da aplicação, assinale todas as caixas necessárias.

ACTIVAR A APLICAÇÃO

O procedimento de activação consiste em registar uma licença, instalando um ficheiro da chave. Com base na licença, a aplicação irá determinar os privilégios existentes e calcular o respectivo prazo de utilização.

O ficheiro da chave contém a informação de assistência necessária para que todas as funcionalidades do Kaspersky Anti-Virus para Windows Workstations funcionem, assim como dados adicionais:

- informação de suporte (quem presta o serviço de suporte e onde pode ser obtido);
- nome e número da chave, assim como a data de validade da licença.

Dependendo do caso que se aplicar (se já tem um ficheiro de chave ou se irá receber um a partir do servidor da Kaspersky Lab), você tem as seguintes opções para activar o Kaspersky Anti-Virus para Windows Workstations:

- Activação online (ver página [20](#)). Seleccione esta opção de activação se tiver adquirido uma versão comercial da aplicação e lhe tiver sido fornecido um código de activação. Pode usar este código para obter um ficheiro da chave que lhe dá acesso a todas as funcionalidades da aplicação durante todo o período da licença.

- Activar a versão de avaliação (ver página [21](#)). Use esta opção de activação se desejar instalar a versão de avaliação da aplicação, antes de tomar a decisão de comprar uma versão comercial. Ser-lhe-á fornecido um ficheiro de chave gratuito e válido durante um período especificado no contrato de licença da versão de avaliação.
- Activação com um ficheiro de chave obtido anteriormente (consulte a secção "Activar através de um ficheiro da chave" na página [21](#)). Activar a aplicação, utilizando o ficheiro de chave do Kaspersky Anti-Vírus 6.0 para Windows Workstations obtido anteriormente.
- Activar mais tarde. Se escolher esta opção, irá ignorar a etapa de activação. A aplicação será instalada no seu computador e você terá acesso a todas as funcionalidades da aplicação, excepto as actualizações (imediatamente a seguir à instalação, só estará disponível uma actualização da aplicação). A opção **Activar mais tarde** apenas estará disponível na primeira inicialização do Assistente de Activação. Nas inicializações seguintes, se a aplicação já estiver activada, a opção **Apagar ficheiro de chave** está disponível para executar a eliminação.

Se for seleccionada alguma das primeiras duas opções de activação da aplicação, a aplicação será activada através do servidor de Internet da Kaspersky Lab, o que requer uma ligação à Internet. Antes de iniciar a activação, verifique e altere as definições da ligação de rede, como for necessário, na janela que se abre quando clica no botão **Definições de LAN**. Para mais detalhes sobre as definições de rede, contacte o seu administrador de rede ou o fornecedor de serviços de Internet.

Se na altura da instalação a ligação à Internet não estiver disponível, pode efectuar a activação mais tarde, a partir da interface da aplicação, ou pode aceder à Internet a partir de outro computador e obter uma chave utilizando o código de activação obtido ao registar-se no site do Serviço de Suporte Técnico da Kaspersky Lab.

Também pode activar a aplicação utilizando o Kaspersky Administration Kit. Para o fazer, deve criar uma tarefa de instalação do ficheiro da chave (ver página [21](#)) (para mais detalhes, consulte o manual de ajuda do Kaspersky Administration Kit).

ACTIVAÇÃO ONLINE

A activação online é efectuada, inserindo um código de activação que recebeu por e-mail quando adquiriu o Kaspersky Anti-Vírus para Windows Workstations através da Internet. Se adquiriu a aplicação numa caixa (versão a retalho), o código de activação será impresso no envelope com o disco de instalação.

INSERIR O CÓDIGO DE ACTIVAÇÃO

Neste passo, o código de activação deve ser inserido. O código de activação é uma sequência de números e letras separados por hífenos em quatro grupos de cinco símbolos sem espaços. Por exemplo, 11111-11111-11111-11111. Note que o código de activação tem ser inserido em caracteres latinos.

Insira as suas informações pessoais na parte inferior da janela: nome completo, endereço de e-mail, cidade e país de residência. Esta informação pode ser necessária para identificar um utilizador registado se, por exemplo, os seus dados da licença forem roubados ou perdidos. Neste caso, pode obter outro código de activação, utilizando as suas informações pessoais.

OBTER UM FICHEIRO DA CHAVE

O Assistente de Configuração estabelece ligação com os servidores de Internet da Kaspersky Lab e envia os seus dados de registo, incluindo o código de activação e as suas informações de contacto. Depois de estabelecer a ligação, o código de activação e as informações de contacto serão verificados. Se o código de activação passar na verificação com sucesso, o Assistente receberá um ficheiro da chave que será então automaticamente instalado. No final da activação, abre-se uma janela com informação detalhada sobre a licença obtida.

Se o código de activação não passar na verificação, surgirá uma notificação relevante no ecrã. Se isso acontecer, contacte o fornecedor do software, ao qual você adquiriu a aplicação, para solicitar informação.

Se for excedido o número de activações com o código de activação, surgirá uma notificação relevante no ecrã. O processo de activação será interrompido e aplicação dar-lhe-á a opção de contactar o Serviço de Suporte da Kaspersky Lab.

ACTIVAR A VERSÃO DE AVALIAÇÃO

Use esta opção de activação se desejar instalar a versão de avaliação do Kaspersky Anti-Virus para Windows Workstations, antes de tomar a decisão de comprar uma versão comercial. Ser-lhe-á fornecida uma licença gratuita, que será válida durante o período especificado no contrato de licença da versão de avaliação. Depois de a licença expirar, você não poderá activar novamente a versão de avaliação.

ACTIVAR ATRAVÉS DE UM FICHEIRO DA CHAVE

Se possui um ficheiro da chave, pode utilizá-lo para activar o Kaspersky Anti-Virus para Windows Workstations. Para o fazer, use o botão **Procurar** e seleccione o caminho para o ficheiro, o qual tem a extensão **.key**.

Depois de ter instalado a chave com sucesso, na parte inferior da janela verá a informação sobre a licença: o número da licença, o tipo de licença (comercial, beta, avaliação, etc.), a data de validade da licença e o número de anfitriões.

CONCLUIR A ACTIVAÇÃO

O Assistente de Configuração irá informá-lo de que o Kaspersky Anti-Virus para Windows Workstations foi activado com sucesso. Para além disso, também será fornecida informação sobre a licença: o número da licença, o tipo (comercial, beta, avaliação, etc.), a data de validade e o número de anfitriões.

MODO DE PROTECÇÃO

Nesta janela, o Assistente de Configuração pede-lhe que seleccione o modo de protecção segundo o qual a aplicação será executada:

- **Protecção básica.** Este é o modo predefinido, que foi concebido para utilizadores que não têm uma experiência muito aprofundada com computadores ou software antivírus. Este modo atribui a todas as componentes da aplicação os seus níveis de segurança recomendados e apenas informa o utilizador acerca de eventos perigosos, tais como a detecção de código malicioso ou acções perigosas que estejam a ser executadas.
- **Protecção interactiva.** Comparativamente ao modo Básico, este modo fornece uma protecção mais personalizada dos dados do seu computador. Permite registar tentativas de alteração das definições do sistema, actividades suspeitas no sistema e operações não autorizadas na rede.




Todas estas acções podem ser provocadas pela actividade de um programa malicioso ou podem ser uma característica padrão do funcionamento de algumas das aplicações instaladas no seu computador. Terá que decidir, para cada caso em separado, se essas actividades devem ser permitidas ou bloqueadas.

Se seleccionar este modo, especifique quando é que deve ser usado:

- **Activar Modo de Treino do Anti-Hacker** pede ao utilizador que tome decisões quando as aplicações instaladas no seu computador tentam ligar-se a um recurso de rede. Você pode permitir ou bloquear essa ligação e configurar regras do Anti-Hacker para essa aplicação. Se desactivar o Modo de Treino, o Kaspersky Anti-Virus para Windows Workstations é executado com as definições de protecção mínima, o que significa que permite que todas as aplicações tenham acesso a recursos de rede.
- **Activar Monitorização do Registo** pede ao utilizador que tome uma decisão se forem detectadas tentativas para alterar os objectos do registo do sistema.

CONFIGURAÇÃO DAS DEFINIÇÕES DE ACTUALIZAÇÃO

A qualidade da protecção do seu computador depende directamente da actualização regular das bases de dados e dos módulos da aplicação. Nesta janela, o Assistente de Configuração pede-lhe que seleccione o modo de actualização da aplicação e que edite as definições de agendamento:

-  **Automaticamente.** O Kaspersky Anti-Virus para Windows Workstations verifica, em intervalos especificados, se existem pacotes de actualização na origem de actualização. A frequência dessa verificação pode aumentar durante surtos de vírus e diminuir quanto não existirem surtos. Se existirem novas actualizações, o Kaspersky Anti-Virus para Windows Workstations transfere-as e instala-as no computador. Este é o modo predefinido.
-  **A cada 2 hora(s)** (a frequência pode variar dependendo das definições de agendamento). As actualizações serão automaticamente executadas com base no agendamento criado. Pode alterar as definições de agendamento numa outra janela, clicando no botão **Alterar**.
-  **Manualmente.** Se seleccionar esta opção, você executará as actualizações da aplicação manualmente.

Tenha em atenção que as bases de dados e os módulos da aplicação incluídos no pacote de instalação poderão estar desactualizados na altura em que instalar a aplicação. Por isso, recomendamos que obtenha as últimas actualizações da aplicação. Para o fazer, clique no botão **Actualizar agora**. Neste caso, o Kaspersky Anti-Virus para Windows Workstations irá transferir as actualizações necessárias a partir dos sites de actualização e irá instalá-las no seu computador.

Se desejar aceder à configuração das actualizações (especificar definições de ligação de rede, seleccionar uma origem de actualização, executar uma actualização com uma conta de utilizador específica ou activar a transferência de actualizações para uma origem local), clique no botão **Configuração**.

CONFIGURAR VERIFICAÇÕES DE VÍRUS AGENDADAS

A verificação de áreas seleccionadas, quando à existência de objectos maliciosos, é uma das tarefas-chave na protecção do computador.

Quando instala o Kaspersky Anti-Virus para Windows Workstations, por defeito, são criadas várias tarefas de verificação de vírus. Nesta janela, o Assistente de Configuração pede-lhe que seleccione um modo de execução da tarefa de verificação:

Verificação Completa

Uma verificação minuciosa de todo o sistema. Por defeito, são verificados os seguintes objectos: memória do sistema, programas carregados ao iniciar, cópia de segurança do sistema, bases de dados de e-mail, discos rígidos, meios de armazenamento removíveis e unidades de rede. Você pode alterar as definições de agendamento na janela que se abre quando clica no botão **Configuração**.

Verificação Rápida



Verificação de vírus dos objectos de inicialização do sistema operativo. Você pode alterar as definições de agendamento na janela que se abre quando clica no botão **Configuração**.

RESTRINGIR O ACESSO À APLICAÇÃO

Uma vez que várias pessoas com diferentes níveis de conhecimentos informáticos poderão usar um computador pessoal e uma vez que os programas maliciosos podem desactivar a protecção, você tem a opção de proteger o acesso ao Kaspersky Anti-Virus para Windows Workstations através de uma password. A utilização de uma password pode proteger a aplicação de tentativas não autorizadas para desactivar a protecção, alterar as definições ou desinstalar a aplicação.

Para activar a protecção por password, assinale a caixa **Activar protecção por password** e preencha os campos **Password** e **Confirmar password**.

Por baixo, especifique a área à qual pretende aplicar a protecção por password:

-  **Todas as operações (excepto notificações de objectos perigosos).** A password será solicitada se o utilizador tentar executar alguma acção com a aplicação, excepto nas respostas às notificações sobre a detecção de objectos perigosos.
-  **Operações seleccionadas:**

- **Ao configurar as definições da aplicação** – solicita a password se o utilizador tentar alterar as definições do Kaspersky Anti-Virus para Windows Workstations.
- **Ao fechar a aplicação** – a password será solicitada quando o utilizador tentar sair da aplicação.
- **Ao desactivar componentes de protecção e ao parar tarefas de verificação** – solicita a password quando o utilizador tenta desactivar uma componente de protecção ou parar uma tarefa de verificação de vírus.
- **Ao desactivar a política do Kaspersky Administration Kit** – solicita a password se o utilizador tentar remover o computador do âmbito das políticas e tarefas de grupo (ao trabalhar através do Kaspersky Administration Kit).
- **Ao desinstalar a aplicação** – solicita a password se o utilizador tentar remover a aplicação do computador.

CONFIGURAR O ANTI-HACKER

O Anti-Hacker é a componente do Kaspersky Anti-Virus para Windows Workstations que garante a segurança do seu computador nas redes locais e na Internet. Nesta etapa, o Assistente de Configuração irá pedir-lhe que crie uma lista de regras que guiarão o Anti-Hacker na análise da actividade de rede do seu computador.

DETERMINAR A SITUAÇÃO DE UMA ZONA DE SEGURANÇA

Nesta etapa, o Assistente de Configuração analisa o ambiente de rede do seu computador. Com base nessa análise, o espaço de rede total é desagregado em zonas convencionais:

- *Internet* – a rede mundial. Nesta zona, o Kaspersky Anti-Virus para Windows Workstations funciona como uma firewall pessoal. Ao fazê-lo, existem regras predefinidas para pacotes e aplicações que regulam toda a actividade de rede para garantir o máximo de segurança. Você não pode alterar as definições de protecção quando trabalhar nesta zona, para além de poder activar o Modo Furtivo no seu computador para segurança adicional.
- *Zonas de segurança* – determinadas zonas convencionais que correspondem, sobretudo, a sub-redes às quais o seu computador está adicionado (estas podem ser sub-redes locais em casa ou no trabalho). Por defeito, estas zonas são zonas com um nível de risco médio quando trabalha com elas. Pode alterar a situação destas zonas, com base no seu grau de confiança em relação a uma determinada sub-rede, e pode configurar regras para filtragem de pacotes e para aplicações.

Todas as zonas detectadas serão apresentadas numa lista. Cada uma delas é apresentada com uma descrição, o endereço e a máscara de sub-rede. A lista também contém as situações de acordo com as quais uma qualquer actividade de rede será permitida ou bloqueada no âmbito do funcionamento da componente Anti-Hacker:

- **Internet.** Por defeito, esta é a situação atribuída à Internet, visto que quando você acede à Internet, o seu computador está sujeito a todos os tipos de ameaças possíveis. Recomenda-se que seleccione esta situação para redes que não estão protegidas por nenhuma aplicação antivírus, por nenhuma firewall, filtros, etc. Quando selecciona esta situação, a aplicação garante segurança máxima para esta zona:
 - bloqueia qualquer actividade de rede NetBios no âmbito da sub-rede;
 - bloqueia regras de aplicações e de filtragem de pacotes que permitam actividade NetBios no âmbito desta sub-rede.

Mesmo se tiver criado uma pasta partilhada, a informação na mesma não estará disponível para utilizadores de sub-redes com esta situação. Para além disso, quando esta situação é seleccionada para uma determinada sub-rede, você não poderá aceder a ficheiros e impressoras noutros computadores desta sub-rede.

- **Rede Local.** A aplicação atribui esta situação à maioria das zonas de segurança detectadas na análise do ambiente de rede do computador, com excepção da Internet. Esta situação é recomendada para zonas com um factor de risco médio (por exemplo, Redes de Área Local de empresas). Se seleccionar esta situação, a aplicação dá permissão a:
 - qualquer actividade de rede NetBios no âmbito da sub-rede;

- regras de aplicações e de filtragem de pacotes que permitam actividade NetBios no âmbito desta sub-rede.

Seleccione esta situação se desejar conceder acesso a certas pastas ou impressoras no seu computador, mas bloquear qualquer outra actividade exterior.

- **Rede confiável.** Esta situação é recomendada apenas para zonas que considera absolutamente seguras, onde o seu computador não está sujeito a ataques ou tentativas para obter acesso aos seus dados. Se seleccionar esta situação, será permitida toda a actividade de rede. Mesmo que tenha seleccionado o nível Protecção máxima e forem criadas regras de bloqueio, estas não serão aplicadas a computadores remotos de uma zona confiável.

Você pode utilizar o *Modo Furtivo* para uma segurança acrescida quando utilizar redes classificadas como **Internet**. Esta funcionalidade apenas permite as actividades de rede que sejam iniciadas a partir do seu computador. Na verdade, isso significa que o seu computador se torna invisível em relação ao que o rodeia. Este modo não afecta o desempenho do seu computador na Internet.

Não recomendamos o uso do Modo Furtivo se o computador estiver a ser usado como servidor (por exemplo, um servidor de e-mail ou HTTP). Caso contrário, os computadores que se ligam ao servidor não conseguirão vê-lo na rede.

Para alterar a situação de uma zona ou para activar/desactivar o Modo Furtivo, seleccione-a na lista e utilize as ligações correspondentes na caixa **Descrição da regra**, que surge por baixo da lista. Você pode executar acções similares, assim como editar endereços e máscaras de sub-rede na janela **Propriedades da zona**, janela essa que poderá abrir com o botão **Editar**.

Pode adicionar uma nova zona à lista enquanto a visualiza. Para o fazer, clique no botão **Actualizar**. O Anti-Hacker procurará zonas disponíveis para registo, e se detectar alguma, o programa pedir-lhe-á para seleccionar uma situação para as mesmas. Além disso, poderá adicionar manualmente novas zonas à lista (se ligar o seu computador portátil a uma nova rede, por exemplo). Para o fazer, utilize o botão **Adicionar** e insira a informação necessária na janela **Propriedades da zona**.

Para apagar uma rede da lista, clique no botão **Apagar**.

CRIAR A LISTA DE APLICAÇÕES DE REDE

O Assistente de Configuração analisa o software instalado no seu computador e cria uma lista das aplicações que usam ligações de rede.

O Anti-Hacker cria uma regra para controlar a actividade de rede para cada uma dessas aplicações. As regras são aplicadas, utilizando modelos para aplicações mais comuns que usam ligações de rede, modelos criados na Kaspersky Lab e incluídos no produto.

Você pode visualizar a lista de aplicações de rede e as regras para as mesmas na janela de definições do Anti-Hacker, janela essa que pode abrir, clicando no botão **Aplicações**.

Para segurança acrescida, recomendamos que desactive o armazenamento temporário de DNS quando navegar nos recursos da Internet. Esta funcionalidade reduz, drasticamente, o tempo que o seu computador demora a ligar-se a um recurso de Internet desejado. Contudo, esta funcionalidade constitui, ao mesmo tempo, uma vulnerabilidade perigosa e, ao utilizá-la, os intrusos podem provocar fugas de dados que não é possível detectar através de uma firewall. Por isso, para aumentar o grau de segurança do seu computador, nós recomendamos que desactive de opção de guardar a informação sobre nomes de domínios na memória temporária.

FINALIZAR O ASSISTENTE DE CONFIGURAÇÃO

A última janela do Assistente irá perguntar-lhe se deseja reiniciar o seu computador para concluir a instalação da aplicação. Você deve reiniciar o computador, para que os controladores do Kaspersky Anti-Virus para Windows Workstations sejam registados.

Você pode adiar a reinicialização, mas a aplicação não funcionará, na sua totalidade, até que o computador seja reiniciado.

KASPERSKY ANTI-VIRUS 6.0 PARA WINDOWS SERVERS

O Kaspersky Anti-Virus 6.0 para Windows Servers é o precursor de uma nova geração de produtos de segurança de dados.

DESCRIÇÃO GERAL

O Kaspersky Anti-Virus para Windows Servers protege os dados armazenados em servidores de ficheiros do Windows (incluindo as versões x64 mais recentes) contra todos os tipos de programas maliciosos. Esta solução garante uma elevada fiabilidade, satisfazendo as exigentes necessidades dos servidores empresariais que processam cargas pesadas.

O QUE HÁ DE NOVO NO KASPERSKY ANTI-VIRUS 6.0 PARA WINDOWS SERVERS

O Kaspersky Anti-Virus 6.0 para Windows Servers é uma ferramenta abrangente de protecção de dados. Vamos analisar em maior detalhe as inovações do Kaspersky Anti-Virus 6.0 para Windows Servers.

Novidades na protecção:

- O novo núcleo antivírus que o Kaspersky Anti-Virus para Windows Servers utiliza detecta os programas maliciosos de forma mais eficaz. O novo núcleo antivírus também é significativamente mais rápido na verificação do sistema quanto à presença de vírus. Isto resulta do processamento melhorado dos objectos e da utilização otimizada dos recursos do computador (particularmente, para processadores de dois ou quatro núcleos).
- Foi implementado um novo analisador heurístico, que permite uma maior precisão na detecção e bloqueio dos programas maliciosos anteriormente desconhecidos. Se a assinatura de um programa não for encontrada nas bases de dados antivírus, o analisador heurístico simula a execução do programa num ambiente virtual isolado. Este método é seguro e permite analisar todos os efeitos de um programa antes de este ser executado num ambiente real.
- O procedimento de actualização da aplicação foi melhorado. Agora o computador raramente precisa de ser reiniciado.

Novas funcionalidades da interface:

- A interface torna as funcionalidades do programa simples e fáceis de aceder.
- A interface foi remodelada tendo em conta as necessidades dos administradores de redes de pequena e média dimensão, assim como dos administradores de grandes redes empresariais.

Novas funcionalidades no Kaspersky Administration Kit:

- O Kaspersky Administration Kit facilita e simplifica a gestão dos sistemas de protecção antivírus de uma empresa. Os administradores podem usar a aplicação para gerir, de forma centralizada, a protecção de uma rede empresarial de qualquer dimensão, com milhares de nódulos, incluindo os utilizadores remotos e móveis.
- Foi adicionada uma funcionalidade que permite a instalação remota da aplicação com a última versão das bases de dados da aplicação.
- A gestão da aplicação quando instalada num computador remoto foi melhorada (a estrutura da política foi redesenhada).

- Foi adicionada uma funcionalidade que permite utilizar o ficheiro de configuração de uma aplicação existente ao criar uma política.
- Uma outra funcionalidade importante é percebida na opção de criação de configurações específicas para utilizadores móveis ao configurar tarefas de actualização de grupo.
- Foi implementada uma outra funcionalidade que permite desactivar, temporariamente, acções da política e tarefas de grupo para computadores cliente com a aplicação instalada (depois de inserir a password correcta).

COMO É CONSTITUÍDA A PROTECÇÃO DO KASPERSKY ANTI-VIRUS PARA WINDOWS SERVERS

A protecção do Kaspersky Anti-Virus para Windows Servers inclui:

- Antivírus de Ficheiros (na página [26](#)) que monitoriza o sistema de ficheiros do computador em tempo real.
- Tarefas de verificação de vírus (na página [26](#)) que são utilizadas para verificar a existência de vírus em todo o computador ou em ficheiros individuais, pastas, discos ou áreas.
- Actualização (na página [27](#)) garantindo o estado actualizado dos módulos internos da aplicação e das bases de dados utilizadas para verificar programas maliciosos.
- Funcionalidades de suporte (ver secção "Funcionalidades de suporte da aplicação" na página [27](#)) que fornecem informação de suporte para trabalhar com a aplicação e expandir as capacidades da mesma.

ANTIVÍRUS DE FICHEIROS

O servidor é protegido em tempo real, através do Antivírus de Ficheiros.

Um sistema de ficheiros pode conter vírus e outros programas perigosos. Os programas maliciosos podem ser guardados no seu sistema de ficheiros durante anos, depois de se terem instalado através de um disco removível ou pela Internet, sem se mostrarem. Mas bastará abrir o ficheiro infectado e o vírus é imediatamente activado.

O Antivírus de Ficheiros é a componente que monitoriza o sistema de ficheiros do seu computador. Verifica todos os ficheiros abertos, executados ou guardados no computador e em todas as unidades de disco ligadas. O Kaspersky Anti-Virus para Windows Servers intercepta todas as tentativas para aceder a um ficheiro e verifica o ficheiro quanto à existência de vírus conhecidos. O ficheiro apenas pode ser alvo de processamento adicional, caso não esteja infectado ou se for desinfectado com sucesso pela aplicação. Se, por qualquer razão, um ficheiro não puder ser desinfectado, este será apagado, sendo guardada uma cópia do ficheiro na Cópia de Segurança ou sendo movido para a Quarentena.

TAREFAS DE VERIFICAÇÃO DE VÍRUS

Para além da protecção do Antivírus de Ficheiros, é extremamente importante verificar, periodicamente, a existência de vírus no servidor. Isto é necessário para eliminar a possibilidade de disseminação de programas maliciosos que ainda não foram descobertos pelo Antivírus de Ficheiros, porque o nível de segurança é baixo ou por outras razões.

O Kaspersky Anti-Virus para Windows Servers inclui as seguintes tarefas de verificação de vírus:

Verificação

Verifica objectos seleccionados pelo utilizador. Pode verificar qualquer objecto no sistema de ficheiros do computador.

Verificação Completa

Uma verificação minuciosa de todo o sistema. Por defeito, são verificados os seguintes objectos: memória do sistema, programas carregados ao iniciar, cópia de segurança do sistema, bases de dados de e-mail, discos rígidos, meios de armazenamento removíveis e unidades de rede.

Verificação Rápida

Verificação de vírus dos objectos de inicialização do sistema operativo.

ACTUALIZAÇÃO

Para bloquear qualquer ataque de rede, apagar um vírus ou outro programa malicioso, o Kaspersky Anti-Virus para Windows Servers deve ser regularmente actualizado. A componente **Actualização** foi concebida para esse fim. Esta gere a actualização das bases de dados e dos módulos utilizados pela aplicação.

O serviço de distribuição de actualizações permite guardar numa pasta local as actualizações da base de dados e dos módulos do programa transferidas a partir dos servidores da Kaspersky Lab e depois torná-las acessíveis a outros computadores da rede para poupar no tráfego de Internet.

FUNCIONALIDADES DE SUPORTE DA APLICAÇÃO

O Kaspersky Anti-Virus para Windows Servers inclui uma série de funcionalidades de suporte. Estas foram concebidas para manter a aplicação actualizada, para expandir as capacidades da aplicação e para o assistir enquanto a utiliza.

Ficheiros de dados

Ao utilizar a aplicação, cada componente de protecção, tarefa de verificação ou actualização da aplicação cria um relatório próprio. Os relatórios contêm informação sobre actividades executadas e os resultados. Através destes, poderá obter informação detalhada sobre como funcionam as componentes do Kaspersky Anti-Virus para Windows Servers. Se surgirem problemas, poderá enviar os relatórios à Kaspersky Lab para os nossos especialistas poderem estudar a situação em maior detalhe e ajudá-lo com a maior rapidez possível.

O Kaspersky Anti-Virus para Windows Servers move todos os ficheiros suspeitos de serem perigosos para uma área de armazenamento especial denominada de *Quarentena*. Aqui são guardados na forma encriptada para evitar a infecção do computador. Pode fazer uma verificação de vírus nestes objectos, restaurá-los para as suas localizações anteriores, apagá-los ou colocar, por si próprio, os ficheiros na Quarentena. No final da verificação de vírus, todos os ficheiros que se concluir não estarem infectados, são automaticamente restaurados para as suas localizações anteriores.

A *Cópia de Segurança* guarda cópias de objectos desinfectados e apagados pelo Kaspersky Anti-Virus para Windows Servers. Estas cópias são criadas de forma a que possa restaurar os ficheiros ou obter informação sobre a sua infecção, se necessário. As cópias de segurança dos ficheiros são também guardadas na forma encriptada para evitar mais infecções.

Pode restaurar um ficheiro da cópia de Segurança para a sua localização original e apagar a cópia.

Disco de Recuperação

O Disco de Recuperação foi concebido para verificar e desinfectar computadores compatíveis com x86 que foram infectados. Deve ser utilizado quando a infecção atinge um nível em que se considera ser impossível desinfectar o computador através de aplicações antivírus ou utilitários de remoção de software malicioso.

Licença

Ao comprar o Kaspersky Anti-Virus para Windows Servers, você entra num contrato de licença com a Kaspersky Lab que regula o uso da aplicação, assim como o seu acesso às actualizações da base de dados da aplicação e ao Suporte Técnico durante um período de tempo especificado. Os termos de uso e outras informações necessárias para a funcionalidade completa da aplicação são fornecidos na licença.

Ao utilizar a função **Licença**, você pode obter informação detalhada sobre a sua licença actual, comprar uma nova licença ou renovar a licença existente.

Suporte

Todos os utilizadores registados do Kaspersky Anti-Virus para Windows Servers podem beneficiar do nosso Serviço de Suporte Técnico. Para saber onde pode obter suporte técnico, use a função **Suporte**.

Utilizando as ligações fornecidas, pode aceder ao fórum de utilizadores de produtos da Kaspersky Lab e procurar uma lista de perguntas frequentes com respostas que poderão ajudá-lo a resolver o seu problema. Também pode enviar uma mensagem sobre um erro ou um comentário sobre o funcionamento do programa para o Suporte Técnico, preenchendo um formulário especial no site.

Também poderá aceder ao Serviço de Suporte Técnico on-line, e, é claro, os nossos funcionários estarão sempre prontos a dar-lhe assistência sobre o Kaspersky Anti-Virus para Windows Servers, por telefone.

INSTALAÇÃO DO KASPERSKY ANTI-VIRUS 6.0 PARA WINDOWS SERVERS

O Kaspersky Anti-Virus 6.0 para Windows Servers pode ser instalado num computador através de várias formas:

- instalação local – instalação da aplicação num único computador. Para a instalação ser executada e concluída, é necessário ter acesso directo àquele computador. A instalação local pode ser executada através de um dos seguintes modos:
 - modo interactivo, utilizando o assistente de instalação da aplicação (ver secção "Instalação através do Assistente de Instalação" na página [29](#)); este modo requer a participação do utilizador durante a instalação;
 - modo não interactivo, no qual a instalação da aplicação é executada a partir da linha de comandos e não requer a participação do utilizador durante a instalação (ver secção "Instalação da aplicação a partir da linha de comandos" na página [32](#)).
- instalação remota – instalação da aplicação em computadores ligados em rede, geridos de forma remota a partir de uma estação de trabalho do administrador com a utilização do:
 - Solução de software Kaspersky Administration Kit (ver Guia de Implementação do Kaspersky Administration);
 - Políticas de domínios de grupo do Microsoft Windows Server 2000/2003 (ver secção "Instalação a partir do Editor de Objectos de Política de Grupo" na página [32](#)).

Antes de iniciar a instalação do Kaspersky Anti-Virus para Windows Servers (inclusive numa instalação remota), recomenda-se que encerre todas as aplicações activas.

REQUISITOS DE HARDWARE E SOFTWARE

Para o funcionamento adequado do Kaspersky Anti-Virus 6.0 para Windows Servers, o computador deve obedecer a estes requisitos mínimos:

Requisitos gerais:

- 300 MB de espaço livre em disco.
- Microsoft Internet Explorer 6.0 ou superior (para a actualização das bases da aplicação e dos módulos do programa através da Internet).
- Microsoft Windows Installer 2.0 ou superior.

Windows 2000 Server / Advanced Server (Service Pack 4 Rollup1), Windows Server 2003 Standard / Enterprise (Service Pack 2), Windows Server 2003 x64 Standard / Enterprise (Service Pack 2), Windows Small Business Server 2003:

- Processador Intel Pentium 400 MHz 32-bit (x86) / 64-bit (x64) ou superior (ou compatível).
- 512 MB de RAM livre.

Windows Server 2003 R2 Standard / Enterprise Edition, Windows Server 2003 R2 x64 Standard / Enterprise Edition, Windows Server 2008 Standard / Enterprise (Service Pack 1 ou superior), Windows Server 2008 x64 Standard / Enterprise (Service Pack 1 ou superior), Windows Small Business Server 2008, Windows Essential Business Server 2008, Windows Server 2008 R2 x64 Standard / Enterprise:

- Processador Intel Pentium 1 GHz 32-bit (x86) / 1.4 GHz 64-bit (x64) ou superior (ou compatível).
- 1 GB de RAM livre.

INSTALAÇÃO ATRAVÉS DO ASSISTENTE DE INSTALAÇÃO

Para instalar o Kaspersky Anti-Virus para Windows Servers no seu computador, execute o ficheiro de instalação a partir do CD do produto.

Instalar a aplicação a partir do ficheiro de instalação transferido da Internet é idêntico a instalar a aplicação a partir do CD.

O programa de instalação é implementado como um assistente padrão do Windows. Cada janela contém um conjunto de botões para controlar o processo de instalação. De seguida, é apresentada uma breve descrição das suas funções:

- **Seguinte** – aceitar a acção e avançar para o próximo passo do procedimento de instalação.
- **Anterior** – voltar ao passo anterior do procedimento de instalação.
- **Cancelar** cancelar a instalação.
- **Concluir** concluir o procedimento de instalação da aplicação.

De seguida, é apresentada uma discussão detalhada de cada passo da instalação do pacote.

Passo 1. Verificar se o sistema satisfaz os requisitos de instalação

Antes de instalar o Kaspersky Anti-Virus para Windows Servers no computador, o assistente irá verificar se o computador satisfaz os requisitos mínimos. Também irá verificar se tem os direitos necessários para instalar o software.


Se algum destes requisitos não for satisfeito, será apresentada no ecrã a respectiva notificação. Recomendamos que instale as actualizações necessárias, através do serviço **Windows Update** e os programas necessários, antes de voltar a tentar instalar o Kaspersky Anti-Virus para Windows Servers.

Passo 2. Janela de início da instalação

Se o seu sistema cumprir todos os requisitos impostos, logo depois do ficheiro de instalação ser executado, a janela de início abrir-se-á no ecrã, apresentando a informação sobre o início da instalação do Kaspersky Anti-Virus para Windows Servers.

Para continuar a instalação, clique no botão **Seguinte**. Para cancelar a instalação, clique no botão **Cancelar**.

Passo 3. Visualizar o Contrato de Licença

A próxima caixa de diálogo da aplicação contém o contrato de licença introduzido entre você e a Kaspersky Lab. Leia-o com atenção e se concordar com todos os termos e condições do contrato, seleccione a opção  **Eu aceito os termos do Contrato de Licença** e clique no botão **Seguinte**. A instalação irá continuar.

Para cancelar a instalação, clique no botão **Cancelar**.

Passo 4. Seleccionar a pasta de instalação

O passo seguinte da instalação do Kaspersky Anti-Virus para Windows Servers define a pasta onde a aplicação será instalada. O caminho predefinido é o seguinte:

- <Drive> → Program Files → Kaspersky Lab → Kaspersky Anti-Virus 6.0 para Windows Servers – para sistemas 32-bit.
- <Drive> → Program Files (x86) → Kaspersky Lab → Kaspersky Anti-Virus 6.0 para Windows Servers – para sistemas 64-bit.

Pode especificar uma pasta diferente, clicando no botão **Procurar** e seleccionando uma pasta na janela padrão de selecção da pasta ou inserindo o caminho da pasta no campo de registo fornecido.

Por favor, note que se inserir, manualmente, o caminho completo para a pasta de instalação, este não deve exceder os 200 caracteres e não deve conter caracteres especiais.

Para continuar a instalação, clique no botão **Seguinte**.

Passo 5. Utilizar configurações da aplicação guardadas numa instalação anterior

Neste passo, ser-lhe-á pedido que especifique se deseja utilizar as definições de protecção, as bases de dados da aplicação no funcionamento da aplicação, caso esses objectos tenham sido guardados no seu computador depois de remover a versão anterior do Kaspersky Anti-Virus 6.0 para Windows Servers.

Vamos analisar em maior detalhe sobre como activar as funcionalidades acima descritas.

Se uma versão anterior (compilação) do Kaspersky Anti-Virus para Windows Servers esteve instalada no seu computador e você guardou as bases de dados da aplicação depois de remover essa versão, então pode integrá-las na versão que está a instalar. Para o fazer, assinale a caixa **Bases de dados da Aplicação**. As bases de dados incluídas no pacote de instalação não serão copiadas para o server.

Para utilizar as definições de protecção que alterou numa versão anterior e que guardou no seu computador, assinale a caixa **Definições da aplicação**.

Passo 6. Seleccionar o tipo de instalação

Neste passo, deve definir a abrangência da instalação da aplicação. Existem duas opções de instalação:

Completa. Neste caso, todas as componentes do Kaspersky Anti-Virus para Windows Servers serão instaladas no seu server. Para se familiarizar com os passos adicionais da instalação, consulte o Passo 8.

Personalizada. Neste caso, ser-lhe-á pedido que seleccione as componentes da aplicação que deseja instalar. Para mais detalhes, veja o Passo 7.

Para seleccionar o modo de instalação, clique no botão correspondente.

Passo 7. Seleccionar as componentes da aplicação a instalar

Este passo só será executado, se tiver seleccionado a opção de instalação **Personalizada**.

Antes de iniciar a instalação personalizada, deve seleccionar as componentes do Kaspersky Anti-Virus para Windows Servers que deseja instalar. Por defeito, são seleccionados para a instalação a componente Antivírus de Ficheiros, a componente de verificação de vírus e o conector Agente de Rede para gerir a aplicação remotamente através do Kaspersky Administration Kit.

Para seleccionar uma componente para instalação adicional, deve abrir o menu, clicando com o botão esquerdo do rato no ícone junto ao nome da componente, e seleccionar o item **Este recurso será instalado no disco rígido local**. Na

parte inferior desta janela de instalação do programa, encontrará mais informação sobre o tipo de protecção fornecida pela componente que seleccionou e sobre o espaço de armazenamento necessário para a instalação da mesma.

Para obter informações detalhadas sobre o espaço disponível no disco do seu computador, clique no botão **Volume**. A informação será apresentada na janela que se abre.

Para cancelar a instalação da componente, seleccione a opção **Este recurso ficará indisponível** a partir do menu de contexto. Note que se cancelar a instalação de uma componente, não será protegido contra uma série de programas perigosos.

Depois de terminar de seleccionar as componentes a instalar, clique no botão **Seguinte**. Para regressar à lista predefinida de componentes a instalar, clique no botão **Repor**.

Passo 9. Procurar outras aplicações antivírus

Neste passo, o assistente procura outros programas antivírus, incluindo outros programas da Kaspersky Lab, que podem entrar em conflito com o Kaspersky Anti-Virus para Windows Servers.

Se forem detectadas aplicações antivírus no seu server, as mesmas serão listadas no ecrã. Ser-lhe-á dada a opção de as desinstalar antes de continuar com a instalação.

Pode escolher removê-las automaticamente ou manualmente, usando os controlos localizados abaixo da lista de programas antivírus detectados (apenas serão removidos automaticamente os produtos da Kaspersky Lab).

Para continuar a instalação, clique no botão **Seguinte**.

Passo 10. Preparação final para a instalação

Este passo conclui a preparação para a instalação da aplicação no seu server.

Na instalação inicial do Kaspersky Anti-Virus 6.0 para Windows Servers, recomenda-se que não desmarque a caixa **Proteger o processo de instalação**. A activação da protecção de módulos permite-lhe efectuar o procedimento correcto de reversão da instalação, caso ocorram erros durante a instalação da aplicação. Quando voltar a tentar a instalação de uma aplicação, recomendamos que desmarque esta caixa.

Se a aplicação estiver a ser instalada de forma remota, através do **Windows Remote Desktop**, recomenda-se que desmarque a caixa **Proteger o processo de instalação**. Caso contrário, o procedimento de instalação pode ser incorrectamente executado ou pode não ser executado.

Se deseja que as exclusões recomendadas pela Microsoft sejam automaticamente adicionadas à lista de exclusões, assinale a caixa **Excluir da verificação de vírus as áreas recomendadas pela Microsoft**.

Se pretender que o caminho para o avp.com seja adicionado à variável %Path% do ambiente após a instalação, assinale a caixa **Adicionar caminho para o avp.com à variável %PATH% do sistema**.

Para continuar a instalação, clique no botão **Instalar**.

Ao instalar as componentes do Kaspersky Anti-Virus para Windows Servers, as quais interceptam o tráfego de rede, as actuais ligações de rede são interrompidas. A maioria das ligações terminadas é retomada após algum tempo.

Passo 11. Concluir a instalação

A janela **Instalação concluída** contém informação sobre a conclusão da instalação do Kaspersky Anti-Virus para Windows Servers no computador.

Para executar o Assistente de Configuração Inicial, clique no botão **Seguinte**.

Se for necessário reiniciar o computador para concluir a instalação com sucesso, será apresentada no ecrã a notificação especial.

INSTALAÇÃO DA APLICAÇÃO A PARTIR DA LINHA DE COMANDOS

➤ Para instalar o Kaspersky Anti-Virus 6.0 para Windows Servers, digite o seguinte na linha de comandos:

```
msiexec /i <package_name>
```

O assistente de instalação iniciar-se-á (ver secção "Instalação através do Assistente de Instalação" na página [29](#)). Quando a aplicação estiver instalada, será necessário reiniciar o computador.

➤ Para instalar a aplicação no modo não interactivo (sem executar o assistente de instalação), digite o seguinte:

```
msiexec /i <package_name> /qn
```

Neste caso, o computador deve ser manualmente reiniciado depois de a instalação estar concluída. Para reiniciar o computador automaticamente, digite o seguinte na linha de comandos:

```
msiexec /i <package_name> ALLOWREBOOT=1 /qn
```

Note que a reinicialização automática só pode ser efectuada no modo de instalação não interactiva (utilizando a chave /qn).

➤ Para instalar a aplicação com uma password, que confirma o direito de remoção da aplicação, digite o seguinte:

```
msiexec /i <package_name> KLUNINSTPASSWD=***** – quando instalar a aplicação no modo interactivo;
```

```
msiexec /i <nome_pacote> KLUNINSTPASSWD=***** /qn – quando instalar a aplicação no modo não interactivo sem reiniciar o computador;
```

```
msiexec /i <nome_pacote> KLUNINSTPASSWD=***** ALLOWREBOOT=1 /qn – quando instalar a aplicação no modo não interactivo e depois reiniciar o computador.
```

Se instalar o Kaspersky Anti-Virus para Windows Servers no modo não interactivo, é suportada a leitura do ficheiro setup.ini, que contém as definições gerais para a instalação da aplicação, do ficheiro de configuração *install.cfg* e do ficheiro da chave de licença. Tenha em atenção que estes ficheiros devem estar localizados na mesma pasta que o pacote de instalação do Kaspersky Anti-Virus para Windows Servers.

INSTALAÇÃO A PARTIR DO EDITOR DE OBJECTOS DE POLÍTICA DE GRUPO

Através do **Editor de Objectos de Política de Grupo**, você pode instalar, actualizar e remover o Kaspersky Anti-Virus para Windows Servers em estações de trabalho empresariais que façam parte do domínio, sem utilizar o Kaspersky Administration Kit.

INSTALAR A APLICAÇÃO

➤ Para instalar o Kaspersky Anti-Virus para Windows Servers, execute as seguintes acções:

1. Crie uma pasta de rede partilhada no computador que funciona como controlador de domínios e coloque na mesma o pacote de instalação do Kaspersky Anti-Virus para Windows Servers no formato MSI.

Para além disso, neste directório pode colocar o ficheiro *setup.ini*, que contém a lista de definições para a instalação do Kaspersky Anti-Virus para Windows Servers, o ficheiro de configuração *install.cfg* e o ficheiro da chave de licença.

- Abra o **Editor de Objectos de Política de Grupo** a partir da consola MMC padrão (para obter informações detalhadas sobre como trabalhar com este editor, consulte o sistema de ajuda do Microsoft Windows Server).
- Crie um novo pacote. Para o fazer, a partir da árvore da consola, seleccione **Objecto de Política de Grupo / Configuração do computador/ Configuração do programa / Instalação do software** e use o comando **Criar / Pacote** a partir do menu de contexto.

Na janela que se abre, especifique o caminho para a pasta de rede partilhada que contém o pacote de instalação Kaspersky Anti-Virus para Windows Servers. Na caixa de diálogo **Implementação do programa**, seleccione a configuração **Atribuída** e clique no botão **OK**.

A política de grupo será aplicada em cada estação de trabalho na próxima vez que os computadores forem registados no domínio. Como resultado, o Kaspersky Anti-Virus para Windows Servers será instalado em todos os computadores.

DESCRIÇÃO DAS DEFINIÇÕES DO FICHEIRO SETUP.INI

O ficheiro *setup.ini*, localizado na pasta do pacote de instalação do Kaspersky Anti-Virus para Windows Servers, é utilizado quando instala a aplicação no modo não interactivo a partir da linha de comandos ou do Editor de Objectos de Política de Grupo. Este ficheiro inclui as seguintes definições:

[Setup] – definições gerais para a instalação da aplicação.

- InstallDir**=caminho para a pasta de instalação da aplicação>.
- Reboot**=sim|não – define se o computador deve ou não ser reiniciado depois de a aplicação ser instalada (por defeito, a reinicialização não é executada).
- SelfProtection**=sim|não – define se a Autodefesa do Kaspersky Anti-Virus para Windows Servers deve ser activada durante a instalação (por defeito, a Autodefesa está activada).

[Components] – selecção das componentes da aplicação a serem instaladas. Se este grupo não contiver quaisquer componentes, a aplicação será instalada na sua totalidade.

- FileMonitor**=sim|não – instalação da componente Antivírus de Ficheiros.

[Tugas] – activação das tarefas do Kaspersky Anti-Virus para Windows Servers. Se não for especificada nenhuma tarefa, após a instalação todas as tarefas serão activadas. Se for especificada pelo menos uma tarefa, as tarefas que não estiverem listadas serão desactivadas.

- ScanMyComputer**=sim|não – tarefa de verificação completa.
- ScanStartup**=sim|não – tarefa de verificação rápida.
- Scan**=sim|não – tarefa de verificação.
- Updater**=sim|não – tarefa de actualização das bases de dados da aplicação e dos módulos do programa.

Em vez do valor **sim** pode utilizar os valores 1, on, activar, activado; em vez do valor **não** pode utilizar os valores 0, off, desactivar, desactivado.

ACTUALIZAR A VERSÃO DA APLICAÇÃO

➡ Para actualizar a versão do Kaspersky Anti-Virus para Windows Servers, efectue o seguinte:

- Coloque o pacote de instalação, que contém as actualizações do Kaspersky Anti-Virus para Windows Servers no formato .msi numa pasta de rede partilhada.
- Abra o **Editor de Objectos de Política de Grupo** e crie um novo pacote utilizando o procedimento acima descrito.

3. Seleccione o novo pacote na lista e use o comando **Propriedades** no menu de contexto. Na janela de propriedades do pacote, seleccione o separador **Actualizações** e especifique o pacote que contém o pacote de instalação da versão anterior do Kaspersky Anti-Virus para Windows Servers. Para instalar uma versão actualizada do Kaspersky Anti-Virus para Windows Servers, guardando as definições de protecção, seleccione a opção para instalar em substituição do pacote existente.

A política de grupo será aplicada em cada estação de trabalho na próxima vez que os computadores forem registados no domínio.

Tenha em conta que os computadores que estejam a executar o Microsoft Windows 2000 Server não suportam a actualização do Kaspersky Anti-Virus para Windows Servers através do Editor de Objectos de Política de Grupo.

REMOÇÃO DA APLICAÇÃO

➔ Para remover o Kaspersky Anti-Virus para Windows Servers, execute as seguintes acções:

1. Abra a **Editor de Objectos de Política de Grupo**.
2. Seleccione **Objecto_Política_Grupo / Configuração do computador/ Configuração do programa/ Instalação do software** na árvore da consola.

Seleccione o pacote do Kaspersky Anti-Virus para Windows Servers na lista de pacotes, abra o menu de contexto e execute o comando **Todas as tarefas/ Remover**.

Na caixa de diálogo **Remover aplicações**, seleccione a opção **Remover imediatamente esta aplicação dos computadores de todos os utilizadores** para que o Kaspersky Anti-Virus para Windows Servers seja removido na próxima reinicialização do computador.

ASSISTENTE DE CONFIGURAÇÃO INICIAL

O Assistente de Configuração do Kaspersky Anti-Virus para Windows Servers inicia-se no final da instalação da aplicação. Foi concebido para o ajudar a configurar as definições iniciais da aplicação, com base nas características e tarefas do seu computador.

A interface do Assistente de Configuração foi concebida da mesma forma que um assistente típico do Microsoft Windows e consiste numa série de passos entre os quais pode navegar, utilizando os botões **Anterior** e **Seguinte**, ou concluir, utilizando o botão **Concluir**. Para parar o assistente em qualquer altura, utilize o botão **Cancelar**.

Para concluir a instalação da aplicação no computador, devem ser executados todos os passos do assistente. Se o funcionamento do assistente for interrompido, por alguma razão, os valores das configurações, que já tinham sido especificadas, não serão guardados. Na próxima tentativa de execução da aplicação, o Assistente de Configuração Inicial será novamente executado, requerendo que edite novamente as configurações.

UTILIZAR OS OBJECTOS GUARDADOS DA VERSÃO ANTERIOR

Esta janela do assistente aparece quando instala a aplicação em substituição da versão anterior do Kaspersky Anti-Virus para Windows Servers. Ser-lhe-á pedido para seleccionar quais os dados utilizados pela versão anterior que deseja importar para a nova versão. Estes podem incluir objectos da quarentena ou da cópia de segurança ou ainda definições de protecção.

Para utilizar estes dados na nova versão da aplicação, assinale todas as caixas necessárias.

ACTIVAR A APLICAÇÃO

O procedimento de activação consiste em registar uma licença, instalando um ficheiro da chave. Com base na licença, a aplicação irá determinar os privilégios existentes e calcular o respectivo prazo de utilização.

O ficheiro da chave contém a informação de assistência necessária para que todas as funcionalidades do Kaspersky Anti-Virus para Windows Servers funcionem, assim como dados adicionais:

- informação de suporte (quem presta o serviço de suporte e onde pode ser obtido);
- nome e número da chave, assim como a data de validade da licença.

Dependendo do caso que se aplicar (se já tem um ficheiro de chave ou se irá receber um a partir do servidor da Kaspersky Lab), você tem as seguintes opções para activar o Kaspersky Anti-Virus para Windows Servers:

- Activação online (consulte página [35](#)). Selecciona esta opção de activação se tiver adquirido uma versão comercial da aplicação e lhe tiver sido fornecido um código de activação. Pode usar este código para obter um ficheiro da chave que lhe dá acesso a todas as funcionalidades da aplicação durante todo o período da licença.
- Activar a versão de avaliação (consulte página [36](#)). Use esta opção de activação se desejar instalar a versão de avaliação da aplicação, antes de tomar a decisão de comprar uma versão comercial. Ser-lhe-á fornecido um ficheiro de chave gratuito e válido durante um período especificado no contrato de licença da versão de avaliação.
- Activação com um ficheiro de chave obtido anteriormente (consulte a secção "Activar através de um ficheiro da chave" na página [36](#)). Activar a aplicação, utilizando o ficheiro de chave do Kaspersky Anti-Virus 6.0 para Windows Servers obtido anteriormente.
- Activar mais tarde. Se escolher esta opção, irá ignorar a etapa de activação. A aplicação será instalada no seu computador e você terá acesso a todas as funcionalidades da aplicação, excepto as actualizações (imediatamente a seguir à instalação, só estará disponível uma actualização da aplicação). A opção **Activar mais tarde** apenas estará disponível na primeira inicialização do Assistente de Activação. Nas inicializações seguintes, se a aplicação já estiver activada, a opção **Apagar ficheiro de chave** está disponível para executar a eliminação.

Se for seleccionada alguma das primeiras duas opções de activação da aplicação, a aplicação será activada através do servidor de Internet da Kaspersky Lab, o que requer uma ligação à Internet. Antes de iniciar a activação, verifique e altere as definições da ligação de rede, como for necessário, na janela que se abre quando clica no botão **Definições de LAN**. Para mais detalhes sobre as definições de rede, contacte o seu administrador de rede ou o fornecedor de serviços de Internet.

Se na altura da instalação a ligação à Internet não estiver disponível, pode efectuar a activação mais tarde, a partir da interface da aplicação, ou pode aceder à Internet a partir de outro computador e obter uma chave utilizando o código de activação obtido ao registar-se no site do Serviço de Suporte Técnico da Kaspersky Lab.

Também pode activar a aplicação utilizando o Kaspersky Administration Kit. Para o fazer, deve criar uma tarefa de instalação do ficheiro da chave (consulte página [36](#)) (para mais detalhes, consulte o manual de ajuda do Kaspersky Administration Kit).

ACTIVAÇÃO ONLINE

A activação online é efectuada, inserindo um código de activação que recebeu por e-mail quando adquiriu o Kaspersky Anti-Virus para Windows Servers através da Internet. Se adquiriu a aplicação numa caixa (versão a retalho), o código de activação será impresso no envelope com o disco de instalação.

INSERIR O CÓDIGO DE ACTIVAÇÃO

Neste passo, o código de activação deve ser inserido. O código de activação é uma sequência de números e letras separados por hífenes em quatro grupos de cinco símbolos sem espaços. Por exemplo, 11111-11111-11111-11111. Note que o código de activação tem ser inserido em caracteres latinos.

Insira as suas informações pessoais na parte inferior da janela: nome completo, endereço de e-mail, cidade e país de residência. Esta informação pode ser necessária para identificar um utilizador registado se, por exemplo, os seus dados da licença forem roubados ou perdidos. Neste caso, pode obter outro código de activação, utilizando as suas informações pessoais.

OBTER UM FICHEIRO DA CHAVE

O Assistente de Configuração estabelece ligação com os servidores de Internet da Kaspersky Lab e envia os seus dados de registo, incluindo o código de activação e as suas informações de contacto. Depois de estabelecer a ligação, o código de activação e as informações de contacto serão verificados. Se o código de activação passar na verificação com sucesso, o Assistente receberá um ficheiro da chave que será então automaticamente instalado. No final da activação, abre-se uma janela com informação detalhada sobre a licença obtida.

Se o código de activação não passar na verificação, surgirá uma notificação relevante no ecrã. Se isso acontecer, contacte o fornecedor do software, ao qual você adquiriu a aplicação, para solicitar informação.

Se for excedido o número de activações com o código de activação, surgirá uma notificação relevante no ecrã. O processo de activação será interrompido e aplicação dar-lhe-á a opção de contactar o Serviço de Suporte da Kaspersky Lab.

ACTIVAR A VERSÃO DE AVALIAÇÃO

Use esta opção de activação se desejar instalar a versão de avaliação do Kaspersky Anti-Virus para Windows Servers, antes de tomar a decisão de comprar uma versão comercial. Ser-lhe-á fornecida uma licença gratuita, que será válida durante o período especificado no contrato de licença da versão de avaliação. Depois de a licença expirar, você não poderá activar novamente a versão de avaliação.

ACTIVAR ATRAVÉS DE UM FICHEIRO DA CHAVE

Se possui um ficheiro da chave, pode utilizá-lo para activar o Kaspersky Anti-Virus para Windows Servers. Para o fazer, use o botão **Procurar** e seleccione o caminho para o ficheiro, o qual tem a extensão **.key**.




Depois de ter instalado a chave com sucesso, na parte inferior da janela verá a informação sobre a licença: o número da licença, o tipo de licença (comercial, beta, avaliação, etc.), a data de validade da licença e o número de anfitriões.

CONCLUIR A ACTIVAÇÃO

O Assistente de Configuração irá informá-lo de que o Kaspersky Anti-Virus para Windows Servers foi activado com sucesso. Para além disso, também será fornecida informação sobre a licença: o número da licença, o tipo (comercial, beta, avaliação, etc.), a data de validade e o número de anfitriões.

CONFIGURAÇÃO DAS DEFINIÇÕES DE ACTUALIZAÇÃO

A qualidade da protecção do seu computador depende directamente da actualização regular das bases de dados e dos módulos da aplicação. Nesta janela, o Assistente de Configuração pede-lhe que seleccione o modo de actualização da aplicação e que edite as definições de agendamento:

-  **Automaticamente.** O Kaspersky Anti-Virus para Windows Servers verifica, em intervalos especificados, se existem pacotes de actualização na origem de actualização. A frequência dessa verificação pode aumentar durante surtos de vírus e diminuir quando não existirem surtos. Se existirem novas actualizações, o Kaspersky Anti-Virus para Windows Servers transfere-as e instala-as no computador. Este é o modo predefinido.
-  **A cada 2 hora(s)** (a frequência pode variar dependendo das definições de agendamento). As actualizações serão automaticamente executadas com base no agendamento criado. Pode alterar as definições de agendamento numa outra janela, clicando no botão **Alterar**.
-  **Manualmente.** Se seleccionar esta opção, você executará as actualizações da aplicação manualmente.

Tenha em atenção que as bases de dados e os módulos da aplicação incluídos no pacote de instalação poderão estar desactualizados na altura em que instalar a aplicação. Por isso, recomendamos que obtenha as últimas actualizações da aplicação. Para o fazer, clique no botão **Actualizar agora**. Neste caso, o Kaspersky Anti-Virus para Windows Servers irá transferir as actualizações necessárias a partir dos sites de actualização e irá instalá-las no seu computador.

Se desejar aceder à configuração das actualizações (especificar definições de ligação de rede, seleccionar uma origem de actualização, executar uma actualização com uma conta de utilizador específica ou activar a transferência de actualizações para uma origem local), clique no botão **Configuração**.

CONFIGURAR VERIFICAÇÕES DE VÍRUS AGENDADAS

A verificação de áreas seleccionadas, quando à existência de objectos maliciosos, é uma das tarefas-chave na protecção do computador.

Quando instala o Kaspersky Anti-Virus para Windows Servers, por defeito, são criadas várias tarefas de verificação de vírus. Nesta janela, o Assistente de Configuração pede-lhe que seleccione um modo de execução da tarefa de verificação:

Verificação Completa

Uma verificação minuciosa de todo o sistema. Por defeito, são verificados os seguintes objectos: memória do sistema, programas carregados ao iniciar, cópia de segurança do sistema, bases de dados de e-mail, discos rígidos, meios de armazenamento removíveis e unidades de rede. Você pode alterar as definições de agendamento na janela que se abre quando clica no botão **Configuração**.

Verificação Rápida

Verificação de vírus dos objectos de inicialização do sistema operativo. Você pode alterar as definições de agendamento na janela que se abre quando clica no botão **Configuração**.

RESTRINGIR O ACESSO À APLICAÇÃO

Uma vez que várias pessoas com diferentes níveis de conhecimentos informáticos poderão usar um servidor e uma vez que os programas maliciosos podem desactivar a protecção do computador, você tem a opção de restringir o acesso ao Kaspersky Anti-Virus para Windows Servers através de uma password. A utilização de uma password pode proteger a aplicação de tentativas não autorizadas para desactivar a protecção, alterar as definições ou desinstalar a aplicação.

Para activar a protecção por password, assinale a caixa **Activar protecção por password** e preencha os campos **Password** e **Confirmar password**.

Por baixo, especifique a área à qual pretende aplicar a protecção por password:

- **Todas as operações (excepto notificações de objectos perigosos)**. A password será solicitada se o utilizador tentar executar alguma acção com a aplicação, excepto nas respostas às notificações sobre a detecção de objectos perigosos.
- **Operações seleccionadas:**
 - **Ao configurar as definições da aplicação** – solicita a password se o utilizador tentar alterar as definições do Kaspersky Anti-Virus para Windows Servers.
 - **Ao fechar a aplicação** – a password será solicitada quando o utilizador tentar sair da aplicação.
 - **Ao desactivar componentes de protecção e ao parar tarefas de verificação** – solicita a password quando o utilizador tenta desactivar o Antivírus de Ficheiros ou parar uma tarefa de verificação de vírus.
 - **Ao desactivar a política do Kaspersky Administration Kit** – solicita a password se o utilizador tentar remover o computador do âmbito das políticas e tarefas de grupo (ao trabalhar através do Kaspersky Administration Kit).
 - **Ao desinstalar a aplicação** – solicita a password se o utilizador tentar remover a aplicação do computador.

FINALIZAR O ASSISTENTE DE CONFIGURAÇÃO

Na última janela do Assistente irá ver uma mensagem a dizer que o Kaspersky Anti-Virus para Windows Servers foi instalado e configurado com sucesso. Pode iniciar a aplicação de imediato, assinalando a opção **Iniciar aplicação**.

Se tiver ocorrido algum problema durante a instalação, como por exemplo um problema de incompatibilidade com outras aplicações antivírus, ser-lhe-á pedido para reiniciar o seu computador.

KASPERSKY LAB

A Kaspersky Lab foi fundada em 1997. Actualmente, é a empresa russa líder no desenvolvimento de uma vasta gama de produtos de software de segurança de informação, incluindo sistemas antivírus, anti-spam e anti-hackers.

A Kaspersky Lab é uma empresa internacional. Centralizada na Federação Russa, a empresa tem filiais representantes no Reino Unido, França, Alemanha, Japão, Benelux, China, Polónia, Roménia e EUA (Califórnia). Um novo departamento da empresa, o Centro Europeu de Pesquisa Antivírus, foi recentemente criado em França. A rede de parceiros da Kaspersky Lab inclui mais de 500 empresas em todo o mundo.

Hoje, a Kaspersky Lab emprega mais de 1000 especialistas altamente qualificados, dos quais 10 têm graduações M.B.A. e 16 têm doutoramentos. Todos os especialistas antivírus seniores da Kaspersky Lab são membros da Computer Anti-virus Researchers Organization (CARO).

Os bens mais valiosos da nossa empresa são a experiência e o conhecimento únicos acumulados pelos nossos especialistas ao longo de 14 anos a combater vírus de computador. A análise detalhada das actividades dos vírus de computador permite que os especialistas da empresa consigam prever as tendências no desenvolvimento de software malicioso e forneçam aos nossos utilizadores uma protecção atempada contra novos tipos de ataques. Esta vantagem é a base dos produtos e serviços da Kaspersky Lab. Em qualquer altura, os produtos da empresa permanecem um passo à frente dos outros fornecedores no fornecimento de uma cobertura antivírus abrangente para os nossos clientes.

Anos de árduo trabalho tornaram a empresa num dos melhores fabricantes de software antivírus. A Kaspersky Lab foi a primeira empresa a desenvolver muitos dos padrões modernos de software antivírus. O produto emblemático da empresa, o Kaspersky Anti-Virus®, protege com fiabilidade todos os tipos de sistemas de computadores contra ataques de vírus, incluindo estações de trabalho, servidores de ficheiros, sistemas de correio electrónico, firewalls, gateways de Internet e computadores portáteis. As suas ferramentas de gestão fáceis de utilizar maximizam o nível de automação da protecção antivírus para computadores e redes empresariais. Um grande número fabricantes a nível mundial usam o núcleo do Kaspersky Anti-Virus nos seus produtos, incluindo a Nokia ICG (EUA), Aladdin (Israel), Sybari (EUA), G Data (Alemanha), Deerfield (EUA), Alt-N (EUA), Microworld (Índia) e BorderWare (Canadá).

Os clientes da Kaspersky Lab beneficiam de uma ampla gama de serviços adicionais que asseguram tanto o funcionamento estável dos produtos da empresa, assim como a total conformidade com as necessidades específicas dos clientes. Concebemos, implementamos e damos apoio a sistemas empresariais antivírus. A base de dados antivírus da Kaspersky Lab é actualizada a cada hora. A empresa fornece aos seus clientes um serviço de suporte técnico de 24 horas, disponível em várias línguas.

Se tiver alguma questão, comentário ou sugestão, pode contactar-nos através dos nossos distribuidores ou contactar, directamente, a Kaspersky Lab. Teremos todo o prazer em ajudá-lo por telefone ou por e-mail em qualquer assunto relacionado com nossos produtos. Receberá respostas completas e abrangentes a todas as suas questões.

Site oficial da Kaspersky Lab: <http://www.kaspersky.pt>

Enciclopédia de Vírus: <http://www.viruslist.com>

Laboratório Antivírus: newvirus@kaspersky.com
(apenas para enviar arquivos de objectos suspeitos)
<http://support.kaspersky.ru/virlab/helpdesk.html?LANG=en>
(para consultas a analistas de vírus)

CONTRATO DE LICENÇA DE UTILIZADOR FINAL DA KASPERSKY LAB

AVISO LEGAL IMPORTANTE A TODOS OS UTILIZADORES: LEIA COM ATENÇÃO O SEGUINTE ACORDO LEGAL ANTES DE COMEÇAR A UTILIZAR O SOFTWARE.

AO CLICAR NO BOTÃO “ACEITAR” NA JANELA DO CONTRATO DE LICENÇA OU AO INTRODUIR SÍMBOLO(S) CORRESPONDENTE(S) CONCORDA EM ESTAR VINCULADO PELOS TERMOS E CONDIÇÕES DESTE CONTRATO. **ESSA ACÇÃO SIMBOLIZA A SUA ASSINATURA E ESTÁ A CONCORDAR ESTAR VINCULADO AO CONTRATO, CONSTITUINDO UMA PARTE DO MESMO, E CONCORDA QUE ESTE CONTRATO É EXECUTÓRIO COMO QUALQUER OUTRO CONTRATO NEGOCIADO POR ESCRITO E ASSINADO POR SI.** SE NÃO CONCORDAR COM TODOS OS TERMOS E CONDIÇÕES DESTE CONTRATO, CANCELE A INSTALAÇÃO DO SOFTWARE E NÃO O INSTALE.

SE O CONTRATO DE LICENÇA OU DOCUMENTO IDÊNTICO ACOMPANHAR O SOFTWARE, OS TERMOS DO USO DO SOFTWARE DEFINIDOS NESSE DOCUMENTO PREVALECERÃO SOBRE OS TERMOS DO CONTRATO DE LICENÇA DE UTILIZADOR FINAL ACTUAL.

DEPOIS DE CLICAR NO BOTÃO “ACEITAR” NA JANELA DO CONTRATO DE LICENÇA OU APÓS TER INTRODUIZIDO O(S) SÍMBOLO(S) CORRESPONDENTE(S), TEM O DIREITO DE UTILIZAR O SOFTWARE DE ACORDO COM OS TERMOS E CONDIÇÕES DESTE CONTRATO.

1. Definições

- 1.1. **Software** refere-se ao software, incluindo quaisquer Actualizações e materiais relacionados.
- 1.2. **Detentor dos Direitos** (proprietário de todos os direitos, quer exclusivos ou relativos ao Software) refere-se à Kaspersky Lab ZAO, uma empresa incorporada de acordo com as leis da Federação Russa.
- 1.3. **Computador(es)** refere-se ao(s) hardware(s), incluindo os computadores pessoais, portáteis, estações de trabalho, assistentes digitais pessoais, ‘smart phones’, dispositivos manuais ou outros dispositivos electrónicos para os quais o Software foi concebido e onde o Software será instalado e/ou usado.
- 1.4. **Utilizador Final** refere-se ao(s) indivíduo(s) que instalam ou utilizam o Software a seu favor ou que utilizam legalmente uma cópia do Software; ou, se o Software for transferido ou instalado em nome de uma organização, quando se refere a um funcionário, “*Utilizador Final*” refere-se ainda à organização para a qual o Software foi transferido ou instalado ficando por este meio claramente definido que essa organização autorizou a pessoa que aceitou este contrato a fazê-lo em seu nome. Para fins deste contrato, o termo “*organização*”, sem limitações, inclui quaisquer parcerias, empresas de responsabilidade limitada, corporações, associações, empresas de capitais mistos, empresas de crédito, “joint ventures”, sindicatos de trabalho, empresas não constituídas em sociedade ou autoridades governamentais.
- 1.5. **Parceiro(s)** refere-se a organizações ou indivíduo(s), que distribuem o Software com base num contrato e numa licença do Detentor dos Direitos.
- 1.6. **Actualização(ões)** refere-se a todas as actualizações, revisões, correcções (“patches”), melhorias, “fixes”, modificações, cópias, adições ou pacotes de manutenção, etc.
- 1.7. **Manual do Utilizador** refere-se ao manual do utilizador, guia do administrador, livro de referências e material explicativo ou de outro tipo relacionado.

2. Concessão de licença

- 2.1. O Detentor de Direitos concede, por este meio, uma licença de não exclusividade ao Utilizador Final que lhe permite armazenar, carregar, instalar, executar e visualizar (para “utilizar”) o Software num número específico de Computadores, tendo como finalidade ajudar a proteger o Computador do Utilizador Final no qual o Software está instalado, contra as ameaças descritas no Manual do Utilizador, de acordo com todos os requisitos técnicos descritos no Manual do Utilizador e com os termos e condições deste Contrato (a “Licença”) e o utilizador final aceita esta Licença:

Versão experimental. Se recebeu, transferiu e/ou instalou uma versão experimental do Software sendo-lhe por este meio concedida uma licença de avaliação para o Software, só pode utilizar o Software para fins de avaliação e

apenas durante o período de avaliação único aplicável, a não ser se indicado o contrário, a contar da data da instalação inicial. A utilização do Software para outros fins ou para além do período de avaliação aplicável é estritamente proibida.

Software de vários ambientes; Software de vários idiomas; Software de dualidade de multimédia; várias cópias; pacotes. Se utilizar versões diferentes do Software ou edições do Software em idiomas diferentes, se receber o Software em vários suportes, se receber várias cópias do Software ou se receber o Software num pacote junto com outro software, o número total permitido de Computadores em que as versões do Software estão instaladas devem corresponder ao número total de computadores especificados nas licenças obtidas junto do Detentor dos Direitos e, *a não ser* que os termos da licença indiquem o contrário, cada licença adquirida dá-lhe o direito de instalar e utilizar o Software nessa quantidade de Computador(es), como especificado nas Cláusulas 2.2 e 2.3.

- 2.2. Se o Software foi adquirido num meio físico, o Utilizador Final tem o direito de utilizar o Software para protecção na quantidade de Computador(es) especificada na embalagem do Software.
- 2.3. Se o Software foi adquirido através da Internet, o Utilizador Final tem o direito de utilizar o Software para protecção na quantidade de Computador(es) especificada na Licença do Software quando adquirido.
- 2.4. Tem o direito de fazer uma cópia do Software apenas para fins de cópia de segurança e apenas para substituir a cópia legal caso essa cópia se perca, seja destruída ou fique inutilizada. Esta cópia de segurança não pode ser utilizada para outros fins e tem de ser destruída se perder o direito de utilização do Software ou quando a licença de Utilizador Final expirar ou for rescindida por qualquer outra razão, de acordo com a legislação em vigor no país de residência principal do Utilizador Final ou no país onde o mesmo está a utilizar o Software.
- 2.5. A partir do momento em que o Software foi activado ou que o ficheiro da chave de licença foi instalado (à excepção de uma versão experimental do Software), tem o direito de receber os seguintes serviços pelo período definido especificado na embalagem de Software (se o Software foi adquirido num meio físico) ou especificado durante a aquisição (se o Software foi adquirido através da Internet):
 - Actualizações do Software através da Internet quando e como o Detentor dos Direitos os publicar no seu próprio website ou através de outros serviços online. Quaisquer Actualizações que possa receber passam a fazer parte do Software e os termos e condições deste Contrato aplicam-se às mesmas;
 - Assistência técnica através da Internet e assistência técnica através de uma linha telefónica grátis.

3. Activação e Termo

- 3.1. Se o Utilizador Final modificar o seu Computador ou fizer alterações ao software de outros fabricantes instalado nesse mesmo Computador, o Detentor dos Direitos poderá exigir que repita a activação do Software ou a instalação do ficheiro da chave de licença. O Detentor dos Direitos reserva-se o direito de utilizar quaisquer meios ou procedimentos de verificação para confirmar a validade da Licença e/ou a legalidade de uma cópia instalada do Software e/ou utilizada no Computador do Utilizador Final.
- 3.2. Se o Software foi adquirido num meio físico, o Software pode ser utilizado, mediante a sua aceitação deste Contrato, pelo período especificado na embalagem. Esse período terá início a partir do momento de aceitação deste Contrato.
- 3.3. Se o Software foi adquirido através da Internet, o Software pode ser utilizado, mediante a sua aceitação deste Contrato, pelo período especificado durante a aquisição.
- 3.4. Tem o direito de utilizar uma versão experimental do Software, como disposto na Cláusula 2.1 sem que tenha de pagar nada durante o período de avaliação (30 dias) desde o momento em que o Software é activado, de acordo com este Contrato, *desde que* a versão experimental não de ao Utilizador Final acesso a Actualizações e a assistência técnica através da Internet e da linha telefónica.
- 3.5. A Licença para Utilização do Software está limitada ao período de tempo especificado nas Cláusulas 3.2 ou 3.3 (como aplicável) e o restante período pode ser visto através dos meios descritos no Manual do Utilizador.
- 3.6. Se tiver adquirido o Software que se destina a ser usado em mais do que um Computador, a sua Licença para Usar o Software estará limitada ao período de tempo que tem início com a data de activação do Software ou da instalação do ficheiro da chave de licença no primeiro Computador.
- 3.7. Sem prejuízo de quaisquer recursos legais ou de justiça natural que o Detentor dos Direitos possa ter, caso haja alguma violação de qualquer parte dos termos e condições deste Contrato por parte do Utilizador Final, o Detentor dos Direitos pode, em qualquer altura e sem qualquer aviso prévio ao Utilizador Final, rescindir esta Licença de utilização do Software sem reembolsar o preço de compra ou qualquer outra parte do mesmo.

3.8. Concorde que, ao utilizar o Software e qualquer relatório ou informações derivadas resultantes da utilização deste Software, irá cumprir todas as leis e regulamentos internacionais, nacionais, estatais, regionais e locais aplicáveis, incluindo, mas não se limitando às leis da privacidade, direitos de autor, controlo de exportação e obscenidade.

3.9. Excepto quando especificamente indicado neste documento, não pode transferir nem atribuir a terceiros nenhum dos direitos a si concedidos, ao abrigo deste Contrato, nem nenhuma das suas obrigações em conformidade com o presente.

4. Assistência técnica

4.1. A assistência técnica descrita na Cláusula 2.5 deste Contrato é fornecida ao Utilizador Final depois de ter sido instalada a mais recente Actualização do Software (excepto quando se trata de uma versão experimental do Software).

Serviço de assistência técnica: <http://support.kaspersky.pt>

5. Limitações

5.1. Não deve emular, clonar, alugar, emprestar, arrendar, vender, modificar, descompilar ou inverter a engenharia do Software, nem desmontar ou criar trabalhos dele derivados e baseados no Software ou em qualquer parte do mesmo, sendo que a única excepção é a existência de um direito sem limitações concedido ao Utilizador Final pela legislação aplicável, bem como não pode reduzir qualquer parte do Software a uma forma legível, nem transferir o Software licenciado, ou qualquer outro subconjunto do Software licenciado, nem permitir que terceiros o façam, excepto até ao ponto em que as restrições indicadas sejam expressamente proibidas pela lei aplicável. Não se pode utilizar o código de binários nem a fonte do Software, nem inverter a engenharia, para recriar o algoritmo do programa, que é registado. Todos os direitos que não são aqui expressamente concedidos são reservados pelo Detentor dos Direitos e/ou pelos seus fornecedores, como aplicável. Qualquer utilização não autorizada do Software resultará na rescisão imediata e automática deste Contrato e da Licença concedida pelo mesmo e pode resultar em processos criminais e/ou civis contra o Utilizador Final.

5.2. Não pode transferir os direitos de utilização do Software para terceiros.

5.3. Não pode fornecer o código de activação e/ou a ficheiro com a chave da licença a terceiros nem permitir que terceiros cedam ao código de activação e/ou chave da licença que são considerados dados confidenciais do Detentor dos Direitos.

5.4. Não pode alugar, arrendar ou emprestar o Software a terceiros.

5.5. Não pode utilizar o Software para criação de dados ou de software utilizado para a detecção, bloqueio ou tratamento das ameaças descritas no Manual do Utilizador.

5.6. O Detentor dos Direitos tem o direito de bloquear o ficheiro da chave ou rescindir a Licença de utilização do Software caso haja alguma violação de qualquer parte dos termos e condições deste Contrato por parte do Utilizador Final sem qualquer reembolso.

5.7. Se o Utilizador Final está a utilizar a versão experimental do Software, não tem o direito de receber a Assistência Técnica especificada na Cláusula 4 deste Contrato e o Utilizador Final não tem o direito de transferir a licença ou os direitos de utilização do Software a terceiros.

6. Garantia limitada e Renúncias

6.1. O Detentor dos Direitos garante que o Software irá cumprir substancialmente o que lhe é devido, de acordo com as especificações e descrições indicadas no Manual do Utilizador *desde que, no entanto*, essa garantia limitada não se aplique ao seguinte: (w) As deficiências e violações relacionadas do computador para as quais o Detentor dos Direitos renuncia expressamente todas as responsabilidades da garantia; (x) avarias, defeitos ou falhas resultantes de má utilização; abuso; acidente; negligência; instalação imprópria, operação ou manutenção; roubo; vandalismo; casos fortuitos; actos de terrorismo; falhas de energia ou picos de potência; acidentes; alterações, modificações não permitidas ou reparações por qualquer parte além do Detentor de Direitos; ou as acções do Utilizador Final ou causas que estejam para além do controlo razoável do Detentor dos Direitos; (y) qualquer defeito que o Utilizador Final não tenha dado a conhecer ao Detentor de Direitos logo que possível depois de o defeito aparecer pela primeira vez; e (z) incompatibilidade provocada pelos componentes de hardware e/ou software instalados no Computador do Utilizador Final.

6.2. O Utilizador Final reconhece, aceita e concorda que não existe nenhum software isento de erros e o Utilizador Final é aconselhado a fazer cópias de segurança do Computador, com a frequência e a fiabilidade adequada para o Utilizador Final.

- 6.3. O Detentor dos Direitos não oferece qualquer garantia de que o Software irá funcionar correctamente em caso de violações dos termos descritos no Manual do Utilizador ou neste Contrato.
- 6.4. O Detentor dos Direitos não garante que o Software irá funcionar correctamente se o Utilizador Final não fizer regularmente transferências das Actualizações especificadas na Cláusula 2.5 deste Contrato.
- 6.5. O Detentor dos Direitos não garante protecção das ameaças descritas no Manual do Utilizador após a expiração do período especificado nas Cláusulas 3.2 ou 3.3 deste Contrato ou após a rescisão da Licença de utilização do Software, caso ela seja rescindida por qualquer razão.
- 6.6. O SOFTWARE É ENTREGUE "TAL COMO ESTÁ" E O DETENTOR DOS DIREITOS NÃO FAZ QUALQUER REPRESENTAÇÃO NEM DÁ QUAISQUER GARANTIAS DA SUA UTILIZAÇÃO OU DESEMPENHO. EXCEPTO NO QUE SE REFERE A QUALQUER GARANTIA, CONDIÇÃO, REPRESENTAÇÃO OU TERMO NA MEDIDA EM QUE NÃO POSSA SER EXCLUÍDA OU LIMITADA PELA LEI APLICÁVEL, O DETENTOR DOS DIREITOS E OS SEUS PARCEIROS NÃO CONCEDEM QUALQUER GARANTIA, CONDIÇÃO, REPRESENTAÇÃO OU TERMO (EXPRESSO OU IMPLÍCITO, QUER SEJA POR ESTATUTO, LEI COMUM, PERSONALIZAÇÃO, UTILIZAÇÃO OU QUALQUER OUTRO) QUE, SEM OUTRO ASSUNTO INCLUINDO, MAS NÃO SE LIMITANDO, A NÃO INFRAÇÃO DOS DIREITOS DE TERCEIROS, COMERCIALIZAÇÃO, QUALIDADE SATISFATÓRIA, INTEGRAÇÃO OU APLICABILIDADE A UM FIM ESPECÍFICO. O UTILIZADOR FINAL ASSUME TODAS AS AVARIAS E TODO O RISCO DE DESEMPENHO E RESPONSABILIDADE POR SELECIONAR O SOFTWARE DE MODO A CONSEGUIR OS RESULTADOS PRETENDIDOS, E PELA INSTALAÇÃO, UTILIZAÇÃO E RESULTADOS OBTIDOS DO SOFTWARE. SEM LIMITAR AS DISPOSIÇÕES ANTERIORES, O DETENTOR DOS DIREITOS NÃO CONCEDE QUALQUER REPRESENTAÇÃO E NÃO DÁ GARANTIAS DE QUE O SOFTWARE NÃO CONTÉM ERROS OU NÃO ESTÁ LIVRE DE INTERRUPÇÕES OU OUTRAS FALHAS OU QUE O SOFTWARE VAI AO ENCONTRO DE TODOS E QUAISQUER REQUISITOS DO UTILIZADOR FINAL TENHAM OU NÃO SIDO DIVULGADOS AO DETENTOR DOS DIREITOS.

7. Exclusão e limitação da responsabilidade

- 7.1. NA MEDIDA MÁXIMA PERMITIDA PELA LEI APLICÁVEL, EM CASO ALGUM O DETENTOR DOS DIREITOS OU OS SEUS PARCEIROS SÃO RESPONSÁVEIS POR QUAISQUER DANOS ESPECIAIS, ACIDENTAIS, PUNITIVOS, INDIRECTOS OU CONSEQUENCIAIS, SEJAM ELES QUAIS FOREM, (INCLUINDO, MAS NÃO SE LIMITANDO A DANOS POR PERDA DE LUCROS OU DE INFORMAÇÕES CONFIDENCIAIS, OU OUTRAS, POR INTERRUPÇÃO DO NEGÓCIO, POR PERDA DE PRIVACIDADE, POR CORRUPÇÃO, DANOS E PERDAS DE DADOS OU PROGRAMAS, POR FALHA DE PAGAMENTO DE QUAISQUER DIREITOS INCLUINDO QUAISQUER DIREITOS LEGAIS, DIREITOS DE LEALDADE OU DIREITOS DE CUIDADOS RAZOÁVEIS, POR NEGLIGÊNCIA, POR PERDA ECONÓMICA, E POR QUALQUER PERDA PECUNIÁRIA OU OUTRA, SEJA ELA QUAL FOR) QUE SURJA DE UMA QUALQUER FORMA RELACIONADA COM A UTILIZAÇÃO OU INCAPACIDADE DE UTILIZAÇÃO DO SOFTWARE, A DISPOSIÇÃO OU FALHA DE FORNECIMENTO DE ASSISTÊNCIA OU OUTROS SERVIÇOS, INFORMAÇÕES, SOFTWARE E CONTEÚDOS RELACIONADOS ATRAVÉS DO SOFTWARE OU QUE, POR OUTRO LADO, SURJA DA UTILIZAÇÃO DO SOFTWARE, OU, AO CONTRÁRIO, MEDIANTE OU EM LIGAÇÃO A QUALQUER DISPOSIÇÃO DESTES CONTRATOS, OU QUE SURJA DE QUALQUER VIOLAÇÃO DO CONTRATO OU QUALQUER DELITO (INCLUINDO NEGLIGÊNCIA, MÁ REPRESENTAÇÃO OU QUALQUER OBRIGAÇÃO OU DEVER DE RESPONSABILIDADE LIMITADA), OU QUALQUER VIOLAÇÃO DOS DEVERES LEGAIS, OU QUALQUER VIOLAÇÃO DA GARANTIA DO DETENTOR DOS DIREITOS OU QUALQUER UM DOS SEUS PARCEIROS, MESMO QUE O DETENTOR DOS DIREITOS OU QUALQUER PARCEIRO TENHA SIDO AVISADO DA POSSIBILIDADE DESSES DANOS.

O UTILIZADOR FINAL CONCORDA QUE, CASO O DETENTOR DOS DIREITOS E/OU OS SEUS PARCEIROS SEJAM TIDOS COMO RESPONSÁVEIS, A RESPONSABILIDADE DO DETENTOR DOS DIREITOS E/OU DOS SEUS PARCEIROS DEVE SER LIMITADA PELOS CUSTOS DO SOFTWARE. EM CASO ALGUM DEVE A RESPONSABILIDADE DO DETENTOR DOS DIREITOS E/OU DOS SEUS PARCEIROS EXCEDER AS TAXAS PAGAS PELO SOFTWARE AO DETENTOR DOS DIREITOS OU AO PARCEIRO (COMO SE APLICAR).

NADA NESTE ACORDO EXCLUI OU LIMITA QUAISQUER REIVINDICAÇÕES DE MORTE E FERIMENTOS PESSOAIS. ALÉM DISSO, NO CASO DE ALGUMA RESPONSABILIDADE, EXCLUSÃO OU LIMITAÇÃO NESTE CONTRATO NÃO POSSAM SER EXCLUÍDAS OU LIMITADAS DE ACORDO COM A LEI APLICÁVEL, ENTÃO APENAS ESSA RESPONSABILIDADE, EXCLUSÃO OU LIMITAÇÃO NÃO SE DEVEM APLICAR AO UTILIZADOR FINAL E CONTINUA A FICAR VINCULADO POR TODAS AS RESTANTES RESPONSABILIDADES, EXCLUSÕES E LIMITAÇÃO.

8. GNU e outras licenças de terceiros

- 8.1. O Software pode incluir alguns programas de software licenciados (ou sublicenciados) ao utilizador no âmbito da Licença Pública Geral GNU (General Public License, GPL) ou outras licenças semelhantes de software grátis que, entre outros direitos, permite ao utilizador copiar, modificar e redistribuir determinados programas, ou partes do mesmo, e ter acesso ao código fonte ("Software de Código Aberto"). Se essas licenças necessitarem que, para qualquer software que é distribuído às pessoas num formato de binário executável, que o código fonte também seja tornado disponível a esses utilizadores, então o código fonte deve ser tornado disponível enviando o pedido para

source@kaspersky.com ou é fornecido com o Software. Se quaisquer licenças de Software de Código Aberto precisarem que o Detentor dos Direitos forneça direitos de utilização, cópia ou modificação de um programa de Software de Código Aberto, mais vastos do que os direitos concedidos neste Contrato, então esses direitos devem ter precedência sobre os direitos e restrições aqui indicados.

9. Posse dos direitos de propriedade

- 9.1. Concorde que o Software e a respectiva autoria, os sistemas, ideias, métodos de funcionamento, documentação e outras informações contidas no Software, são propriedade intelectual registada e/ou segredo comercial, de grande valor, do Detentor dos Direitos ou dos seus parceiros e que o Detentor dos Direitos e os seus parceiros, conforme aplicável, estão protegidos pela lei civil e criminal e pelas leis de direitos de autor, segredos comerciais, marcas registadas e patentes da Federação Russa, União Europeia e Estados Unidos e de outros países, bem como pelos tratados internacionais. Este Contrato não concede ao Utilizador Final quaisquer direitos no que se refere à propriedade intelectual, incluindo as marcas comerciais ou as marcas dos serviços do Detentor dos Direitos e/ou dos seus parceiros (“Marcas Comerciais”). Pode utilizar as Marcas Comerciais apenas e até ao ponto de identificar resultados impressos produzidos pelo Software de acordo com a prática das marcas comerciais aceites, incluindo a identificação do nome do proprietário da Marca Comercial. A utilização de qualquer Marca Comercial não dá ao Utilizador Final quaisquer direitos de propriedade sobre essa Marca Comercial. O Detentor dos Direitos e/ou os seus parceiros são proprietários e retêm todos os direitos, títulos e interesse no Software e em relação ao mesmo, incluindo, sem limitações, quaisquer correcções de erros, melhoramentos, Actualizações ou outras modificações ao Software, quer sejam feitas pelo Detentor dos Direitos ou por quaisquer terceiros, e todos os direitos sobre direitos de autor, patentes, segredos comerciais, marcas comerciais e outras propriedades intelectuais contidas neste documento. A posse, instalação ou utilização do Software não lhe transfere qualquer título para a propriedade intelectual no Software e não adquire quaisquer direitos ao Software excepto quando expressamente estipulado neste Contrato. Todas as cópias do Software realizadas nos termos do presente Contrato têm de conter os mesmos avisos de propriedade que aparecem no Software. Excepto como aqui indicado, este Contrato não concede ao Utilizador Final quaisquer direitos de propriedade intelectual sobre o Software e o Utilizador Final reconhece que a Licença, tal como está definida aqui, concedida nos termos deste Contrato, concede apenas o direito de utilização limitada mediante os termos e as condições deste Contrato. O Detentor dos Direitos reserva-se todos os direitos não expressamente concedidos ao Utilizador Final neste Contrato.
- 9.2. Concorde em não modificar nem alterar o Software seja de que forma for. Não pode remover nem alterar quaisquer avisos de direitos de autor ou outros avisos de propriedade em nenhuma cópia do Software.

10. Lei vigente; arbitragem

- 10.1. Este Contrato é regido, e será interpretado, de acordo com as leis da Federação Russa sem referência a conflitos de regras e princípios legais. Este Contrato não será regido pela Convenção das Nações Unidas referente a Contratos para a Venda Internacional de Bens, a aplicação da qual é expressamente excluída. Qualquer litígio que surja no seguimento da interpretação ou aplicação dos termos deste Contrato ou qualquer infracção ao mesmo, a não ser que se resolva por negociação directa, deverá ser resolvido no Tribunal de Arbitragem Comercial Internacional na Câmara do Comércio e Indústria da Federação Russa em Moscovo, na Federação Russa. Qualquer decisão apresentada pelo árbitro deve ser final e obrigatória para as partes e qualquer julgamento sobre essa decisão de arbitragem pode ser feita cumprir em qualquer tribunal da jurisdição competente. Nada nesta Secção 11 deve impedir que uma Parte procure e obtenha qualquer reparação equitativa de um tribunal da jurisdição competente, quer seja antes, durante ou depois dos processos de arbitragem.

11. Período para interpor acções

- 11.1. Nenhuma acção, independentemente da forma, que surja das transacções nos termos deste Contrato, pode ser trazida aqui por qualquer uma das partes mais de um (1) ano depois da causa da acção ter ocorrido, ou de ter sido descoberta a ocorrência, excepto que uma acção por violação dos direitos de propriedade intelectual seja trazida dentro do período legal máximo aplicável.

12. Contrato completo; redução; sem renúncia

- 12.1. Este Contrato constitui todo o contrato entre o Utilizador Final e o Detentor dos Direitos e substitui quaisquer outros acordos prévios, propostas, comunicações ou publicidade, oral ou escrita, referente ao Software ou ao assunto deste Contrato. O Utilizador Final reconhece que leu este Contrato, compreendeu-o e concorda em estar vinculado pelos seus termos. Se qualquer disposição deste Contrato for indicada por um tribunal de jurisdição competente como sendo inválida, nula ou inexecutável por qualquer razão, no todo ou em parte, essa disposição será ainda mais restritamente interpretada de tal forma que será legal e executória, e todo o Contrato não falhará por conta do mesmo e o saldo do Contrato continuará válido e com efeitos até ao máximo permitido por lei ou equidade ao mesmo tempo que preserva, até ao máximo possível, a sua intenção original. Nenhuma renúncia de nenhuma disposição ou condição aqui indicadas será válida a não ser por escrito e assinada pelo Utilizador Final e um representante autorizado do Detentor dos Direitos desde que nenhuma renúncia de nenhuma infracção de nenhuma disposição deste Contrato constitua uma renúncia de qualquer infracção anterior, concorrente ou subsequente. A não insistência por parte do Detentor dos Direitos no que se refere a fazer valer o desempenho

rigoroso de todas as disposições deste Contrato ou nenhum direito deve ser interpretado como sendo uma renúncia de qualquer uma dessas disposições ou direitos.

13. Informações de contacto do Detentor dos Direitos

Se tiver quaisquer dúvidas referentes a este Contrato ou se, por qualquer razão, pretender contactar o Detentor dos Direitos, contacte o nosso Departamento de Apoio ao Cliente em:

Kaspersky Lab ZAO, 10 build. 1 1st Volokolamsky Proezd
Moscovo, 123060
Federação Russa

Tel.: +7-495-797-8700

Fax: +7-495-645-7939

E-mail: info@kaspersky.com

Website: www.kaspersky.com

© 1997-2010 Kaspersky Lab ZAO. Todos os direitos reservados. O Software e toda a documentação que o acompanha têm direitos de autor e estão protegidos pelas leis de direitos de autor e por tratados internacionais de direitos de autor, bem como por outras leis e tratados de propriedade intelectual.