

**MANUAL DE UTILIZADOR**

**KASPERSKY  
INTERNET  
SECURITY 2009  
SPECIAL EDITION  
FOR ULTRA-  
PORTABLES**

---

Caro Utilizador do Kaspersky Internet Security 2009!

Obrigado por escolher o nosso produto. Esperamos que esta documentação o ajude no seu trabalho e lhe forneça respostas relativamente a este produto de software.

Aviso! Este documento é propriedade da Kaspersky Lab: todos os direitos deste documento estão reservados pelas leis de direitos de autor da Federação Russa e por tratados internacionais. A reprodução e distribuição ilegal deste documento ou de partes do mesmo resultará em responsabilidade civil, administrativa ou criminal, de acordo com as leis da Federação Russa. Qualquer tipo de reprodução ou distribuição de quaisquer materiais, incluindo na forma traduzida, só é permitida com a autorização escrita da Kaspersky Lab. Este documento e as imagens gráficas contidas no mesmo podem ser utilizados, exclusivamente, para fins informativos, não-comerciais ou pessoais.

Este documento pode ser alterado sem aviso prévio. Para obter a versão mais recente, consulte o site da Kaspersky Lab <http://www.kaspersky.com/docs>. A Kaspersky Lab não assume qualquer responsabilidade pelo conteúdo, qualidade, relevância ou exactidão de quaisquer materiais utilizados neste documento cujos direitos sejam detidos por terceiros ou pelos potenciais danos associados à utilização de tais documentos.

Este documento inclui marcas comerciais registadas e não registadas. Todas as marcas comerciais são propriedade dos respectivos detentores.

© Kaspersky Lab, 1997-2009

+7 (495) 645-7939,  
Tel., fax: +7 (495) 797-8700,  
+7 (495) 956-7000

<http://www.kaspersky.pt/>  
<http://support.kaspersky.pt/>

Data de revisão: 08.04.2009

---

# ÍNDICE

INSTALAÇÃO DO KASPERSKY INTERNET SECURITY .....	6
Obter informação sobre a aplicação.....	6
Fontes de informação para pesquisar por si próprio .....	7
Contactar o Departamento de Vendas .....	7
Contactar o Serviço de Suporte Técnico.....	7
Discutir as aplicações da Kaspersky Lab no Fórum da Internet.....	9
Visão geral da protecção da aplicação .....	9
Assistentes e ferramentas.....	10
Funcionalidades de suporte .....	11
Análise heurística .....	12
Requisitos de hardware e software do sistema.....	13
AMEAÇAS À SEGURANÇA DO COMPUTADOR.....	15
Ameaças contidas em aplicações.....	15
Programas maliciosos .....	16
Vírus e worms.....	16
Trojans.....	20
Utilitários maliciosos .....	26
Programas potencialmente indesejados .....	30
Software com publicidade (Adware) .....	31
Software com pornografia (Pornware) .....	31
Outro software potencialmente perigoso (Riskware) .....	32
Métodos de detecção de objectos infectados, suspeitos e potencialmente perigosos por parte da aplicação .....	36
Ameaças da Internet.....	37
Spam ou e-mails recebidos não solicitados .....	37
Phishing .....	38
Ataques de hackers.....	38
Faixas de publicidade (Banners).....	39
INSTALAÇÃO DA APLICAÇÃO .....	40
Passo 1. Procurar uma versão mais recente da aplicação .....	41
Passo 2. Verificar se o sistema satisfaz os requisitos de instalação.....	42

Passo 3. Janela de Boas-vindas do Assistente .....	42
Passo 4. Visualizar o Contrato de Licença .....	43
Passo 5. Seleccionar o tipo de instalação .....	43
Passo 6. Seleccionar a pasta de instalação .....	44
Passo 7. Seleccionar os componentes da aplicação a instalar .....	44
Passo 8. Procurar outros programas de anti-vírus.....	45
Passo 9. Preparação final para a instalação.....	46
Passo 10. Concluir a instalação.....	46
INTERFACE DA APLICAÇÃO.....	47
Ícone da área de notificação.....	47
Menu de atalho .....	48
Janela principal da aplicação .....	50
Notificações .....	53
Janela de configuração da aplicação.....	53
COMEÇAR.....	55
Seleccionar o tipo de rede .....	56
Actualizar a aplicação .....	57
Análise de segurança .....	57
Verificação de vírus no computador.....	58
Gerir a licença.....	59
Subscrição para a renovação automática da licença.....	60
Participar no Kaspersky Security Network .....	62
Gestão de segurança.....	64
Pausar a protecção.....	66
VALIDAR A CONFIGURAÇÃO DA APLICAÇÃO .....	68
Testar o "vírus" EICAR e suas variantes .....	68
Testar a protecção do tráfego de HTTP.....	72
Testar a protecção do tráfego de SMTP .....	72
Validar a configuração do Anti-vírus de Ficheiros.....	73
Validar a configuração das tarefas de verificação de vírus.....	74
Validar a configuração do Anti-Spam.....	74

---

DECLARAÇÃO DE RECOLHA DE DADOS DO KASPERSKY SECURITY NETWORK .....	76
KASPERSKY LAB .....	83
CRYPTOEX LLC .....	86
MOZILLA FOUNDATION .....	87
CONTRATO DE LICENÇA .....	88

---

# INSTALAÇÃO DO KASPERSKY INTERNET SECURITY

O Kaspersky Internet Security pode ser instalado utilizando um de dois modos:

- modo interactivo, através do Assistente de Instalação da Aplicação. Este modo requer a participação do utilizador ao instalar;
- modo não-interactivo, no qual a instalação da aplicação é executada a partir da linha de comandos e não requer qualquer participação do utilizador.

Antes de instalar o Kaspersky Internet Security, recomenda-se que feche todas as aplicações activas.

## NESTA SECÇÃO:

---

Obter informação sobre a aplicação.....	6
Visão geral da protecção da aplicação.....	9
Requisitos de hardware e software do sistema.....	13

## OBTER INFORMAÇÃO SOBRE A APLICAÇÃO

Se tem alguma questão relativamente à aquisição, instalação ou utilização da aplicação, as respostas estão facilmente disponíveis.

A Kaspersky Lab tem muitas fontes de informação, a partir das quais pode seleccionar as mais convenientes, dependendo da urgência e importância das suas questões.

## **FONTES DE INFORMAÇÃO PARA PESQUISAR POR SI PRÓPRIO**

Pode utilizar o sistema de **Ajuda**.

O sistema de Ajuda contém informação sobre a gestão da protecção do computador: como visualizar o estado de protecção, verificar várias áreas do computador e executar outras tarefas.

Para abrir a Ajuda, clique na ligação **Ajuda** na janela principal da aplicação ou prima <F1>.

## **CONTACTAR O DEPARTAMENTO DE VENDAS**

Se tem questões relativamente à selecção ou aquisição da aplicação ou sobre como prolongar o período de utilização da mesma, pode contactar os especialistas do Departamento de Vendas no nosso Escritório Central em Moscovo, através dos telefones:

**+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00.**

O serviço é prestado em Russo ou Inglês.

Pode enviar as suas questões para o Departamento de Vendas através do endereço de e-mail [ventas@kaspersky.es](mailto:ventas@kaspersky.es).

## **CONTACTAR O SERVIÇO DE SUPORTE TÉCNICO**

Se já comprou a aplicação, pode obter informação sobre a mesma a partir do serviço de Suporte Técnico por telefone ou pela Internet.

Os especialistas do serviço de Suporte Técnico irão responder às suas questões sobre a instalação e utilização da aplicação e, caso o seu computador tenha sido infectado, eles ajudá-lo-ão a eliminar as consequências das actividades do software malicioso.

Antes de contactar o serviço de Suporte Técnico, por favor leia as regras relativas ao suporte (<http://support.kaspersky.com/support/rules>).

### Suporte Técnico por e-mail (apenas para utilizadores registados)

Pode colocar a sua questão aos especialistas do Serviço de Suporte Técnico, preenchendo um formulário on-line do Help Desk (<http://support.kaspersky.pt>).

Pode enviar as suas questões em Russo, Inglês, Alemão, Francês ou Espanhol.

Para enviar um e-mail com a sua questão, tem de indicar o **número de cliente** obtido durante o registo no site do serviço de Suporte Técnico, juntamente com a sua **password**.

#### Nota

Se ainda não é um utilizador registado das aplicações da Kaspersky Lab, pode preencher um formulário de registo na página (<https://support.kaspersky.com/en/PersonalCabinet/Registration/Form/>).

Durante o registo terá de fornecer o código de activação ou o nome do ficheiro de chave.

O serviço de Suporte Técnico irá responder ao seu pedido no seu **Arquivo Pessoal** na página <https://support.kaspersky.com/en/PersonalCabinet> e para o endereço de e-mail que especificou no seu pedido.

No formulário on-line do pedido, descreva o problema que encontrou o mais detalhadamente possível. Especifique as seguintes informações nos campos obrigatórios:

- **Tipo de pedido.** As questões mais frequentes colocadas pelos utilizadores estão agrupadas em tópicos especiais, por exemplo “Problema de instalação/remoção do produto” ou “Problema de remoção/verificação de vírus”. Se não existir nenhum tópico adequado à sua questão, seleccione o tópico “Questão Geral”.
- **Nome e número da versão da aplicação.**
- **Texto do pedido.** Descreva o problema que encontrou o mais detalhadamente possível.

- **Número de cliente e password.** Insira o número de cliente e a password que recebeu durante o registo no site do serviço de Suporte Técnico.
- **Endereço de e-mail.** O serviço de Suporte Técnico irá enviar a resposta para este endereço de e-mail.

### **Suporte Técnico por telefone**

Se tem um problema que requer ajuda urgente, pode telefonar para o departamento de Suporte Técnico mais próximo. Precisarás de fornecer informações de identificação (<http://support.kaspersky.com/support/details>) quando contactar o Suporte Técnico local ([http://support.kaspersky.com/support/support local](http://support.kaspersky.com/support/support%20local)) ou Internacional (<http://support.kaspersky.com/support/international>). Isto ajudará os nossos especialistas a processar o seu pedido o mais rapidamente possível.

## **DISCUTIR AS APLICAÇÕES DA KASPERSKY LAB NO FÓRUM DA INTERNET**

Se a sua questão não requer uma resposta urgente, pode discuti-la com os especialistas da Kaspersky Lab e outros utilizadores do software Kaspersky no nosso fórum na Internet, através do endereço <http://forum.kaspersky.com/>.

Neste fórum pode visualizar os tópicos existentes, deixar as suas respostas, criar novos tópicos e utilizar o motor de pesquisa.

## **VISÃO GERAL DA PROTECÇÃO DA APLICAÇÃO**

O Kaspersky Internet Security protege o seu computador contra ameaças conhecidas e desconhecidas e contra dados indesejados. Cada tipo de ameaça é processado por uma determinada componente da aplicação. 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 Internet Security inclui as seguintes funções de protecção:

- Monitoriza as actividades de sistema executadas por aplicações de utilizador, impedindo quaisquer actividades perigosas por parte das aplicações.
- As componentes de protecção fornecem a protecção em tempo real de todas as transferências de dados e caminhos de entrada através do seu computador.
- As componentes de protecção garantem a protecção do seu computador contra todos os ataques de intrusos e de rede conhecidos, durante as ligações à Internet.
- As componentes de filtragem removem os dados indesejados, poupando tempo, dinheiro e tráfego de Internet.
- As tarefas de verificação de vírus são utilizadas para verificar a existência de vírus em ficheiros individuais, pastas, discos, áreas especificadas ou o computador como um todo. As tarefas de verificação também podem ser configuradas para detectar vulnerabilidades nas aplicações de utilizador instaladas.
- A componente de actualização garante o estado actualizado dos módulos e das bases de dados da aplicação utilizadas para detectar programas maliciosos, ataques de hackers e mensagens de spam.
- Os assistentes e ferramentas facilitam a execução de tarefas durante o funcionamento do Kaspersky Internet Security.
- As funcionalidades de suporte fornecem informação e assistência para trabalhar com a aplicação e expandir as capacidades da mesma.

## **ASSISTENTES E FERRAMENTAS**

Garantir a segurança do computador é uma tarefa complexa que requer o conhecimento das funcionalidades do sistema operativo e dos métodos utilizados para explorar as suas fraquezas. Para além disso, o volume e a diversidade de informações sobre a segurança do sistema dificultam a sua análise e processamento.

Para ajudar a resolver tarefas específicas no fornecimento da segurança do computador, o pacote do Kaspersky Internet Security inclui um conjunto de assistentes e ferramentas:

- O Assistente do Analisador de Segurança realiza diagnósticos ao computador, procurando vulnerabilidades no sistema operativo e nos programas de utilizador instalados no computador.
- O Assistente de Configuração do Navegador analisa as configurações do navegador Microsoft Internet Explorer, avaliando em primeiro lugar a questão da segurança.
- O Assistente de Restauro do Sistema elimina todos os vestígios de ataques de software malicioso no sistema.
- O Assistente de Limpeza de vestígio de actividade procura e elimina rastreios de actividades do utilizador no sistema e nas configurações do sistema operativo, impedindo a recolha de informações sobre as actividades do utilizador.
- A Análise de Pacotes de Rede intercepta pacotes de rede e exhibe detalhes sobre os mesmos.
- O Monitor de Rede exhibe detalhes sobre a actividade de rede no seu computador.
- O Teclado Virtual impede a interceptação dos dados inseridos através do teclado.

## **FUNCIONALIDADES DE SUPORTE**

A aplicação inclui uma série de funcionalidades de suporte que são concebidas para manter a aplicação actualizada, para expandir as capacidades da aplicação e para o assistir enquanto a utiliza.

### **Kaspersky Security Network**

O **Kaspersky Security Network** é um sistema que transfere automaticamente relatórios sobre ameaças detectadas e potenciais para a base de dados central da Kaspersky Lab. Esta base de dados permite à Kaspersky Lab reagir mais rapidamente às ameaças mais espalhadas e notificar os utilizadores sobre surtos de vírus.

### **Licença**

Ao comprar o Kaspersky Internet Security, 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 incluídas no ficheiro de chave de licença.

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

## **Suporte**

Todos os utilizadores registados do Kaspersky Internet Security podem beneficiar do nosso serviço de suporte técnico. Para ver informação sobre como receber suporte técnico, use a função **Suporte**.

Se seguir as ligações, pode aceder ao fórum de utilizadores dos produtos da Kaspersky Lab, enviar um relatório de erro ao Suporte Técnico ou obter informações 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 a aplicação.

## **ANÁLISE HEURÍSTICA**

Os métodos heurísticos são usados por algumas componentes de protecção em tempo real, tais como o Anti-vírus de Ficheiros, Anti-vírus de E-mail, Anti-vírus de Internet, assim como as tarefas de verificação de vírus.

Ao efectuar a verificação dos objectos com o método de assinatura, o qual utiliza uma base de dados com descrições de todas as ameaças conhecidas, isso dar-lhe-á uma resposta precisa sobre se um objecto analisado é malicioso ou não e sobre o perigo que representa. O método heurístico, ao contrário do método de assinatura, tem como objectivo detectar o comportamento típico dos objectos, em vez do seu conteúdo estático, mas não consegue fornecer o mesmo grau de certeza nas suas conclusões.

A vantagem da análise heurística é o facto de detectar software malicioso que não está registado na base de dados, de forma a que não tenha de actualizar as bases de dados antes de efectuar a verificação. Devido a isso, as novas ameaças são detectadas antes dos analistas de vírus as terem detectado.

Contudo, existem métodos para contornar a análise heurística. Uma dessas medidas defensivas consiste em pausar a actividade do código malicioso assim que o objecto detectar a verificação heurística.

**Nota**

Ao utilizar uma combinação de métodos de verificação, isso garante mais segurança.

Ao verificar um objecto, o analisador heurístico simula a execução do objecto num ambiente virtual seguro fornecido pela aplicação. Se for detectada uma actividade suspeita quando o objecto for executado, este será considerado malicioso, não sendo permitida a execução do mesmo no anfitrião, e será apresentada uma mensagem que solicita instruções adicionais ao utilizador:

- Colocar o objecto na Quarentena, permitindo que a nova ameaça seja verificada e processada mais tarde, através das bases de dados actualizadas.
- Apagar o objecto.
- Ignorar (se tiver a certeza de que o objecto não é malicioso).

Para utilizar os métodos heurísticos, assinale a caixa **Análise heurística** e ajuste o indicador de detalhe da verificação para uma das seguintes posições: Nível superficial, Nível médio ou Nível aprofundado. O nível de detalhe da verificação dá o equilíbrio entre o cuidado e qualidade da verificação de novas ameaças e a carga sobre os recursos do sistema operativo, assim como a duração da verificação. Quanto mais elevado for o nível heurístico, maior a quantidade de recursos de sistema que a verificação irá requerer e maior a duração da verificação.

**Aviso!**

As novas ameaças detectadas através da análise heurística são rapidamente analisadas pela Kaspersky Lab e os métodos para desinfectá-las são adicionados às actualizações horárias das bases de dados.

Se actualizar, regularmente, as suas bases de dados, manterá o nível de protecção óptima do seu computador.

## **REQUISITOS DE HARDWARE E SOFTWARE DO SISTEMA**

Para permitir que o programa funcione normalmente, o computador deve obedecer a estes requisitos mínimos:

*Requisitos gerais:*

- 75 MB de espaço livre em disco.
- Um rato.
- Microsoft Internet Explorer 5.5 ou superior (para a actualização das bases da aplicação e dos módulos do software através da Internet).
- Microsoft Windows Installer 2.0.

*Microsoft Windows XP Home Edition (SP2 ou superior), Microsoft Windows XP Professional (SP2 ou superior):*

- Processador Intel Atom, Intel Celeron-M, VIA C7-M.
- 256 MB de RAM livre.

---

# AMEAÇAS À SEGURANÇA DO COMPUTADOR

Existe uma ameaça considerável à segurança do computador que é imposta por ameaças contidas em aplicações. Para além disso, essa ameaça é imposta por spam, ataques de phishing e de hackers e faixas publicitárias de software que contém publicidade (adware). Estas ameaças estão relacionadas com a utilização da Internet.

## NESTA SECÇÃO:

---

Ameaças contidas em aplicações .....	15
Ameaças da Internet .....	37

## AMEAÇAS CONTIDAS EM APLICAÇÕES

O Kaspersky Internet Security consegue detectar milhares de programas maliciosos que possam existir no seu computador. Alguns destes programas representam uma ameaça constante ao seu computador, enquanto outros apenas são perigosos em determinadas condições. Depois da aplicação detectar um programa malicioso, esta classifica-o e atribui-lhe um nível de perigo (elevado ou médio).

Os analistas de vírus da Kaspersky Lab distinguem duas categorias principais de ameaças contidas em aplicações: *programas maliciosos* e *programas potencialmente indesejados*.

Os programas maliciosos (Malware) (ver página 16) são criados para provocar danos ao computador e ao seu utilizador: por exemplo, para roubar, bloquear, alterar ou apagar informação ou para perturbar o funcionamento de um computador ou de uma rede de computadores.

Os programas potencialmente indesejados (PPIs) (ver página 30), ao contrário dos programas maliciosos, não se destinam unicamente a provocar danos, mas podem ajudar a penetrar no sistema de segurança de um computador.

A Enciclopédia de Vírus (<http://www.viruslist.com/en/viruses/encyclopedia>) contém uma descrição detalhada destes programas.

## PROGRAMAS MALICIOSOS

Os **programas maliciosos** (“malware ou software malicioso”) são criados especificamente para provocar danos aos computadores e aos seus utilizadores: para roubar, bloquear, alterar ou apagar informação ou para perturbar o funcionamento de um computador ou de uma rede de computadores.

Os programas maliciosos dividem-se em três subcategorias: *vírus e worms (vermes)*, *programas Trojan (cavalos de tróia)* e *utilitários de software malicioso*.

Os vírus e worms (Vírus\_e\_Worms) (ver página 16) conseguem criar cópias de si próprios, as quais por sua vez se espalham e se reproduzem de novo. Alguns deles são executados sem o conhecimento ou participação do utilizador. Outros requerem acções por parte do utilizador para serem executados. Quando executados, estes programas efectuem as suas acções maliciosas.

Ao contrário dos vírus e worms, os programas Trojan (Programas\_Trojan) (ver página 20) não criam cópias de si próprios. Estes infectam um computador, por exemplo, através do e-mail ou do navegador de Internet, quando o utilizador visita um site “infectado”. Têm de ser iniciados pelo utilizador e efectuem as suas acções maliciosas quando executados.

Utilitários de software malicioso (ferramentas\_maliciosas) (ver página 26) são criados especificamente para provocar danos. Contudo, ao contrário dos outros programas maliciosos, estes não efectuem acções maliciosas quando são executados e podem ser armazenados e executados com segurança no computador do utilizador. Estes têm funções que os hackers usam para criar vírus, worms e programas Trojan, para organizar ataques de rede em servidores remotos, para penetrar em computadores ou efectuar outras acções maliciosas.

## VÍRUS E WORMS

**Subcategoria:** vírus e worms (Vírus\_e\_Worms)

**Nível de gravidade:** elevado

O vírus clássico e os worms executam acções não-autorizadas nos computadores infectados, incluindo a sua própria replicação e disseminação.

## Vírus clássico

Depois de um vírus clássico se infiltrar no sistema, este infecta um ficheiro, activa-se, executa a sua acção maliciosa e adiciona cópias de si próprio a outros ficheiros.

Os vírus clássicos apenas se reproduzem dentro dos recursos locais do computador infectado, mas não conseguem por si só penetrar noutros computadores. A distribuição para outros computadores apenas pode ocorrer se o vírus se adicionar a um ficheiro armazenado numa pasta partilhada ou num CD ou se o utilizador reencaminhar um e-mail com um anexo infectado.

O código de um vírus clássico é normalmente especializado para penetrar numa área específica de um computador, sistema operativo ou aplicação. Dependendo do ambiente, existe uma distinção entre *vírus de ficheiro*, *de inicialização*, *de script* e *de macro*.

Os vírus podem infectar os ficheiros através de vários métodos. Os *vírus de substituição* escrevem o seu próprio código para substituir o código do ficheiro infectado, destruindo os conteúdos originais do ficheiro. O ficheiro infectado deixa de funcionar e não pode ser desinfectado. Os *vírus parasitas* alteram os ficheiros, deixando-os total ou parcialmente funcionais. Os *vírus de companhia* não alteram os ficheiros, mas duplicam-nos de forma a que quando o ficheiro infectado é aberto, o seu duplicado (isto é, o vírus) é que é executado. Outros tipos de vírus incluem os *vírus de link*, vírus OBJ que *infectam módulos de objectos*, vírus LIB que *infectam as bibliotecas do compilador* e vírus que *infectam o texto original dos programas*.

## Worm (Verme)

Depois de penetrar no sistema, o worm de rede, de modo similar ao vírus clássico, fica activado e executa a sua acção maliciosa. O worm de rede é assim denominado devido à sua capacidade para passar secretamente de um computador para outro, para se propagar através de diversos canais de informação.

Os worms são categorizados de acordo com o seu método primário de proliferação, tal como aparece listado na tabela que se segue:

Tabela 1. Worms categorizados segundo o método de proliferação

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIÇÃO</b>
<b>IM-Worm</b>	Worms de MI	<p>Estes worms propagam-se através dos clientes de MI (mensagens instantâneas), tais como o ICQ, o MSN Messenger, o AOL Instant Messenger, o Yahoo Pager e o Skype.</p> <p>Normalmente, estes worms usam as listas de contactos para enviar mensagens com um link para um ficheiro de worm existente num site. Quando um utilizador transfere e abre o ficheiro, o worm é activado.</p>
<b>Email-Worm</b>	Worms de e-mail	<p>Os worms de e-mail infectam os computadores através do e-mail.</p> <p>A mensagem infectada tem um ficheiro anexado que contém uma cópia de um worm ou um link para um ficheiro de worm carregado num site. O site é normalmente um que foi pirateado ou é o próprio site do hacker. Quando o anexo é aberto, o worm é activado. Em alternativa, quando clica no link, transfere e abre o ficheiro, o worm ficará activo. Depois disso, o worm continuará a reproduzir-se, procurando outros endereços de e-mail e enviando mensagens infectadas para os mesmos.</p>
<b>IRC-Worms</b>	Worms de IRC	<p>Os worms deste tipo entram nos computadores através de salas de conversação (IRC), as quais são usadas para comunicar com outras pessoas, em tempo real, através da Internet.</p> <p>Estes worms publicam no canal de conversação da Internet uma cópia do ficheiro de worm ou um link para o ficheiro. Quando o utilizador transfere e abre o ficheiro, o worm será activado.</p>

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIÇÃO</b>
<b>Net-Worms</b>	Worms de rede (worms residentes em redes de computadores)	<p>Estes worms são distribuídos através de redes de computadores.</p> <p>Ao contrário dos outros tipos de worms, os worms de rede propagam-se sem a participação do utilizador. Estes procuram na rede de área local os computadores que contenham programas com vulnerabilidades. Fazem isso, enviando para cada computador um pacote de rede especial (exploração de vulnerabilidades) que contém o código do worm ou uma parte desse código. Se existir um computador vulnerável na rede, esse será infiltrado pelo pacote. Quando o worm penetrar totalmente no computador, este fica activo.</p>
<b>P2P-Worm</b>	Worms de intercâmbio de ficheiros	<p>Os worms de intercâmbio de ficheiros propagam-se através de redes peer-to-peer de intercâmbio de dados, como por exemplo o Kazaa, Grokster, EDonkey, FastTrack ou Gnutella.</p> <p>Para utilizar uma rede de intercâmbio de ficheiros, o worm copia-se a si próprio para a pasta de intercâmbio de ficheiros que, normalmente, está localizada no computador do utilizador. A rede de intercâmbio de ficheiros apresenta informação sobre o ficheiro e o utilizador pode “encontrar” o ficheiro infectado na rede (tal como qualquer outro ficheiro), transferi-lo e abri-lo.</p> <p>Os worms mais complexos imitam os protocolos de rede de uma determinada rede de intercâmbio de ficheiros: estes worms fornecem respostas positivas a pedidos de pesquisa e oferecem cópias de si próprios para transferência.</p>

TIPO	NOME	DESCRIÇÃO
Worm	Outros worms	<p>Os outros worms de rede incluem:</p> <ul style="list-style-type: none"><li>• Worms que distribuem as suas cópias através de recursos de rede. Ao utilizarem as funcionalidades do sistema operativo, estes espalham-se pelas pastas de rede disponíveis, ligam-se a computadores na rede global e tentam abrir as suas unidades de disco para obterem total acesso. Ao contrário dos worms de redes de computadores, neste caso o utilizador tem de abrir um ficheiro que contenha uma cópia do worm, para que o worm seja activado.</li><li>• Worms que utilizam outros métodos de propagação não listados aqui: por exemplo, worms que se propagam através de telemóveis.</li></ul>

## TROJANS

**Subcategoria:** Trojans (Programas\_Trojan)

**Nível de gravidade:** elevado

Ao contrário dos worms e vírus, os programas Trojan não criam cópias de si próprios. Estes infectam um computador, por exemplo, através de um anexo de e-mail infectado ou através de um navegador de Internet, quando o utilizador visita um site "infectado". Os programas Trojan têm de ser iniciados pelo utilizador e começam a efectuar as suas acções maliciosas assim que são executados.

Os programas Trojan podem executar diversas acções maliciosas. As principais funções dos Trojans incluem bloquear, alterar e apagar dados e perturbar o funcionamento de computadores ou de redes de computadores. Para além disso, os programas Trojan conseguem receber e enviar ficheiros, executá-los, exibir mensagens, aceder a páginas de Internet, transferir e instalar programas e reiniciar o computador infectado.

Os intrusos muitas vezes utilizam "conjuntos" que consistem em programas Trojan complementares.

Os diferentes tipos de programas Trojan e o seu comportamento estão descritos na tabela que se segue.

*Tabela 2. Programas trojan categorizados segundo o comportamento no computador infectado*

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIÇÃO</b>
<b>Trojan-ArcBomb</b>	Programas Trojan - arquivos bomba	Arquivos que quando descompactados aumentam para um tamanho que perturba o funcionamento do computador. Quando tenta descompactar o arquivo, o computador pode começar a trabalhar de forma lenta ou "bloquear" e o disco pode ficar cheio de dados "vazios". Os "arquivos bomba" são especialmente perigosos para os servidores de ficheiros e de e-mails. Se no servidor for utilizado um sistema de processamento automático da informação recebida, esse "arquivo bomba" pode parar o servidor.
<b>Backdoor</b>	Programas Trojan de administração remota	Estes programas são considerados os mais perigosos de todos os programas Trojan. Em termos de funcionamento são similares aos programas de administração remota comercializados no mercado. Estes programas instalam-se sem o conhecimento do utilizador e dão ao intruso a gestão remota do computador.

TIPO	NOME	DESCRIÇÃO
Trojans	Trojans	<p>Os Trojans incluem os seguintes programas maliciosos:</p> <ul style="list-style-type: none"><li>• <b>Programas Trojan clássicos</b>, que apenas executam as principais funções dos programas Trojan: bloquear, alterar ou apagar dados, perturbar o funcionamento de computadores ou de redes de computadores. Estes não têm as funções adicionais características de outros tipos de programas Trojan descritos nesta tabela;</li><li>• <b>Programas Trojan para “fins múltiplos”</b>, que têm as funções adicionais características de vários tipos de programas Trojan.</li></ul>
Trojan-Ransoms	Programas Trojan que exigem um resgate	<p>Estes "tomam como refém" a informação existente no computador do utilizador, alterando-a ou bloqueando-a ou perturbam o funcionamento do computador, de forma a que o utilizador não consiga utilizar os dados. Depois o intruso exige um resgate ao utilizador, em troca da promessa de enviar o programa que irá restaurar a funcionalidade do computador.</p>
Trojan-Clickers	Trojan-Clickers	<p>Estes programas acedem a páginas de Internet a partir do computador do utilizador: enviam um comando para o navegador de Internet ou substituem os endereços de Internet armazenados nos ficheiros do sistema.</p> <p>Ao utilizarem estes programas, os intrusos organizam ataques de rede ou aumentam o tráfego de determinados sites, para promoverem as receitas da exibição de faixas de publicidade.</p>

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIÇÃO</b>
<b>Trojan-Downloaders</b>	Programas Trojan - software de transferências	<p>Estes programas acedem à página de Internet do intruso, transferem outros programas maliciosos a partir do mesmo e instalam esses programas no computador do utilizador. Podem armazenar no seu próprio código o nome do ficheiro do programa malicioso transferível ou recebê-lo a partir da página de Internet a que acedem.</p>
<b>Trojan-Droppers</b>	Programas Trojan - droppers	<p>Estes programas guardam programas que contêm outros programas Trojans no disco do computador e depois instalamos.</p> <p>Os intrusos podem usar os Trojans-Droppers de várias formas:</p> <ul style="list-style-type: none"><li>• para instalar programas maliciosos sem o conhecimento do utilizador: os Trojans-droppers não exibem nenhuma mensagem ou exibem mensagens falsas, por exemplo para notificar sobre um erro num arquivo ou sobre a utilização da versão incorrecta do sistema operativo;</li><li>• para impedir que outro programa malicioso conhecido seja detectado: nem todos os programas anti-vírus conseguem detectar um programa malicioso localizado dentro de um Trojan-dropper.</li></ul>

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIÇÃO</b>
<b>Trojan-Notifiers</b>	Trojans-notifiers	<p>Estes notificam o intruso de que o computador infectado está ligado e depois transferem informação sobre o computador para o intruso, incluindo o endereço IP, número de uma porta aberta ou o endereço de e-mail. Estes comunicam com o intruso, utilizando uma série de métodos, incluindo e-mail, FTP e acedendo à página de Internet do intruso.</p> <p>Os Trojan-notifiers são muitas vezes utilizados em conjuntos de programas Trojan complementares. Estes notificam o intruso de que existem outros programas Trojan instalados com sucesso no computador do utilizador.</p>
<b>Trojan-Proxies</b>	Trojans-Proxies	<p>Permitem ao intruso aceder a páginas de Internet de forma anónima, utilizando a identidade do computador do utilizador e são muitas vezes utilizados para enviar spam.</p>
<b>Trojan-PSWs</b>	Trojans que roubam passwords	<p>São trojans que roubam passwords (PSW - Password-Stealing-Ware - Software de Roubo de Passwords). Estes roubam contas de utilizador, como por exemplo, informação de registo de software. Procuram informação confidencial nos ficheiros do sistema e no registo e enviam-na para o seu criador, utilizando uma série de métodos, incluindo e-mail, FTP e acedendo ao site do intruso.</p> <p>Alguns destes programas Trojan enquadram-se em tipos específicos descritos nesta tabela, incluindo Trojan-Bankers, Trojan-MIs e Trojans-GameThieves.</p>

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIÇÃO</b>
<b>Trojan-Spies</b>	Programas Trojan espíões	Estes programas são utilizados para espiar o utilizador. Recolhem informação sobre as acções do utilizador no computador. Por exemplo, interceptam dados inseridos pelo utilizador através do teclado, tiram fotografias do ecrã e recolhem listas de aplicações activas. Depois de receberem esta informação, transferem-na para o intruso, utilizando uma série de métodos, incluindo e-mail, FTP e acedendo ao site do intruso.
<b>Trojans-DoS</b>	Programas Trojan – ataques de rede	Para um ataque de Recusa de Serviço (DoS), o Trojan envia numerosos pedidos a partir do computador do utilizador para um servidor remoto. O servidor irá esgotar os seus recursos ao processar estes pedidos e irá parar de funcionar. Estes programas são muitas vezes utilizados para infectar múltiplos computadores, para fazer um ataque combinado no servidor.
<b>Trojan-MIs</b>	Programas Trojan que roubam dados pessoais de utilizadores de clientes de MI	Estes programas roubam números e passwords de utilizadores de clientes de MI (programas de mensagens instantâneas), tais como o ICQ, o MSN Messenger, o AOL Instant Messenger, o Yahoo Pager ou o Skype. Transferem informação para o intruso, utilizando uma série de métodos, incluindo e-mail, FTP e acedendo ao site do intruso.
<b>Rootkits</b>	Processos ocultos (Rootkits)	Estes programas ocultam outros programas maliciosos e as suas actividades e, assim, prolongam a existência desses programas no sistema. Ocultam ficheiros e processos na memória do computador infectado ou chaves de registo executadas pelos programas maliciosos ou ocultam o intercâmbio de dados entre aplicações instaladas no computador do utilizador e outros computadores da rede.

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIÇÃO</b>
<b>Trojan-SMS</b>	Programas Trojan – Mensagens SMS	Estes programas infectam os telefones móveis e enviam mensagens SMS para números que o utilizador do telefone infectado tem de pagar.
<b>Trojan-GameThieves</b>	Programas Trojan que roubam dados pessoais dos utilizadores de jogos de rede.	Estes programas roubam informações sobre contas de utilizador dos utilizadores de jogos de rede e depois transferem esta informação para o intruso, utilizando uma série de métodos, incluindo e-mail, FTP e acedendo ao site do intruso.
<b>Trojans-Bankers</b>	Programas Trojan que roubam informações de contas bancárias	Estes programas roubam informações de contas bancárias ou informações de contas de dinheiro electrónico/digital. Transferem dados para o intruso, utilizando uma série de métodos, incluindo e-mail, FTP e acedendo ao site do intruso.
<b>Trojan-Mailfinders</b>	Programas Trojan que recolhem endereços de e-mail	Estes programas recolhem endereços de e-mail no computador e transferem esses endereços para o intruso, utilizando uma série de métodos, incluindo e-mail, FTP e acedendo ao site do intruso. O intruso pode utilizar os endereços recolhidos para enviar spam.

## UTILITÁRIOS MALICIOSOS

**Subcategoria:** utilitários maliciosos (Ferramentas\_maliciosas)

**Nível de gravidade:** médio

Estes utilitários são concebidos especificamente para provocar danos. Contudo, ao contrário de outros programas maliciosos, estes são ferramentas utilizadas sobretudo para atacar outros computadores e podem ser armazenados e executados com segurança no computador do utilizador. Estes programas contêm funcionalidades para ajudar a criar vírus, worms e programas Trojan, para organizar ataques de rede em servidores remotos, para penetrar em computadores ou efectuar outras acções maliciosas.

Existem muitos tipos de utilitários maliciosos com diferentes funções, as quais estão descritas na tabela que se segue.

Tabela 3. Utilitários maliciosos agrupados por funções

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIÇÃO</b>
<b>Constructor</b>	Construtores	Os construtores são utilizados para criar novos vírus, worms e programas Trojan. Alguns construtores possuem uma interface padrão com janelas, permitindo ao hacker seleccionar o tipo de programa malicioso a criar, o método que este programa utilizará para resistir à depuração e outras propriedades similares.
<b>Dos</b>	Ataques de rede	Os programas de Recusa de Serviço (DoS) enviam numerosos pedidos a partir do computador do utilizador para um servidor remoto. O servidor irá esgotar os seus recursos ao processar estes pedidos e irá parar de funcionar.
<b>Exploit</b>	Exploração de vulnerabilidades	<p>A exploração de vulnerabilidades (exploit) é um conjunto de dados ou uma parte de código de programa, que utiliza as vulnerabilidades de uma aplicação para executar uma acção maliciosa no computador. Por exemplo, a exploração de vulnerabilidades pode escrever ou ler ficheiros ou aceder a páginas de Internet "infectadas".</p> <p>Os diferentes tipos de exploração de vulnerabilidades utilizam as vulnerabilidades de diferentes aplicações ou serviços de rede. Uma ferramenta de exploração de vulnerabilidades é transferida através da rede para múltiplos computadores sob a forma de um pacote de rede, procurando computadores com serviços de rede vulneráveis. Por exemplo, uma ferramenta de exploração de vulnerabilidades contida num ficheiro DOC procura vulnerabilidades de editores de texto e quando o utilizador abre um ficheiro</p>

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIÇÃO</b>
		<p>infectado, essa exploração de vulnerabilidades pode começar a executar as acções programadas pelo intruso. Uma ferramenta de exploração de vulnerabilidades contida num e-mail procura vulnerabilidades nos clientes de e-mail. Pode começar a executar a sua acção maliciosa, assim que o utilizador abrir uma mensagem infectada através do cliente de e-mail.</p> <p>A exploração de vulnerabilidades também é utilizada para distribuir worms de rede (Net-Worm). Os Exploit-Nukers são pacotes de rede que deixam os computadores inoperacionais.</p>
<b>FileCryptors</b>	Encriptadores de Ficheiros	Os encriptadores de ficheiros encriptam outros programas maliciosos, para os esconderem das aplicações anti-vírus.
<b>Flooders</b>	Programas utilizados para inundar redes	<p>Estes enviam um elevado número de mensagens através de canais de rede, incluindo, por exemplo, canais de salas de conversação (IRC).</p> <p>Contudo, esta categoria de software malicioso não inclui programas que inundam o tráfego de e-mail ou canais de MI e SMS, os quais estão classificados em separado na tabela abaixo apresentada (Email-Flooder, MI-Flooder e SMS-Flooder).</p>

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIÇÃO</b>
<b>HackTools</b>	Ferramentas de Hackers	As ferramentas de hackers são utilizadas para penetrar nos computadores onde estão instaladas ou para organizar ataques a outro computador. Esses ataques incluem: a criação de novas contas de utilizador do sistema sem autorização ou a limpeza dos registos do sistema para ocultar quaisquer vestígios da presença do novo utilizador no sistema. Estas ferramentas incluem alguns programas farejadores (sniffers) que executam funções maliciosas, como por exemplo, interceptar passwords. Os programas farejadores são programas que permitem examinar o tráfego de rede.
<b>not-virus:Hoax</b>	Programas de boato (Hoaxes)	Estes programas assustam o utilizador com mensagens parecidas com vírus. Podem "detectar" um vírus num ficheiro limpo ou exibir uma mensagem sobre a formatação do disco, embora na verdade não ocorra nenhuma formatação.
<b>Spoofers</b>	Falsificadores	Estes programas enviam mensagens e pedidos de rede com um endereço de um remetente falso. Os intrusos utilizam os falsificadores, por exemplo, para fingirem ser um remetente legítimo.
<b>VirTools</b>	São ferramentas utilizadas para criar variantes de programas maliciosos	Estas permitem alterar outros programas maliciosos, para os esconderem das aplicações anti-vírus.
<b>Email-Flooders</b>	Programas para inundar endereços de e-mail	Estes programas enviam numerosas mensagens para endereços de e-mail (inundando-os). Devido ao elevado fluxo de mensagens, os utilizadores não conseguem ver as mensagens recebidas que não são spam.

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIÇÃO</b>
<b>MI-Flooders</b>	Programas utilizados para inundar programas de MI	Estes programas enviam numerosas mensagens para utilizadores de clientes de MI (mensagens instantâneas), tais como o ICQ, o MSN Messenger, o AOL Instant Messenger, o Yahoo Pager ou o Skype. Devido ao elevado fluxo de mensagens, os utilizadores não conseguem ver as mensagens recebidas que não são spam.
<b>SMS-Flooders</b>	Programas utilizados para inundar com mensagens SMS	Estes programas enviam numerosos SMS para telemóveis.

## **PROGRAMAS POTENCIALMENTE INDESEJADOS**

Os **programas potencialmente indesejados**, ao contrário dos programas maliciosos, não se destinam unicamente a provocar danos. Contudo, podem ser utilizados para violar a segurança do computador.

Os programas potencialmente indesejados incluem adware, pornware e outros *programas potencialmente indesejados*.

Os programas de Adware ou software com publicidade (ver página 31) apresentam informação publicitária ao utilizador.

Os programas de Pornware ou software com pornografia (ver página 31) apresentam informação pornográfica ao utilizador.

O outro software potencialmente perigoso (Riskware) (ver página 32) inclui, muitas vezes, programas úteis utilizados por muitos utilizadores de computadores. Contudo, se um intruso obtiver acesso a estes programas ou os instalar no computador do utilizador, esse intruso pode utilizá-los para violar a segurança do computador.

Os programas potencialmente indesejados são instalados através de um dos seguintes métodos:

- São instalados pelo utilizador, individualmente ou juntamente com outro programa. Por exemplo, os criadores de software incluem programas de adware em softwares de utilização gratuita (freeware) ou de distribuição livre (shareware).
- Também são instalados por intrusos. Por exemplo, os intrusos incluem esses programas em pacotes com outros programas maliciosos, utilizando "vulnerabilidades" do navegador de Internet ou através de Trojan downloaders e droppers, quando o utilizador visita um site "infectado".

## **SOFTWARE COM PUBLICIDADE (ADWARE)**

**Subcategoria:** Adware

**Nível de gravidade:** médio

Os programas de Adware envolvem a exibição de informação publicitária ao utilizador. Estes apresentam faixas de publicidade (banners) na interface de outro programa e redireccionam os pedidos de pesquisa para sites com publicidade. Alguns programas de Adware recolhem e enviam ao seu criador informação de marketing sobre o utilizador: por exemplo, que sites o utilizador visita ou que pedidos de pesquisa faz. Ao contrário dos Trojan espíões, esta informação é transferida com a permissão do utilizador.

## **SOFTWARE COM PORNOGRAFIA (PORNWARE)**

**Subcategoria:** Pornware

**Nível de gravidade:** médio

Normalmente, são os próprios utilizadores que instalam esses programas para procurar ou transferir informação pornográfica.

Os intrusos também podem instalar estes programas no computador do utilizador, para lhe apresentarem anúncios de sites e serviços de pornografia comercial, sem a permissão do utilizador. Para serem instalados, eles utilizam vulnerabilidades do sistema operativo ou do navegador de Internet e são normalmente distribuídos por Trojan downloaders e Trojan droppers.

Existem três tipos de programas de pornware, tal como está categorizado na tabela que se segue.

*Tabela 4. Tipos de programas de pornware categorizados segundo as suas funções*

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIÇÃO</b>
<b>Porn-Dialers</b>	Programas de ligações telefónicas automáticas	Estes programas contêm os números de telefone de serviços telefónicos pornográficos e ligam automaticamente para esses números. Ao contrário dos Trojan dialers (programas trojan de ligações telefónicas), estes programas notificam os utilizadores sobre as suas acções.
<b>Porn-Downloaders</b>	Programas para transferir ficheiros a partir da Internet	Estes programas transferem informação pornográfica para o computador do utilizador. Ao contrário dos Trojan dialers, estes programas notificam os utilizadores sobre as suas acções.
<b>Porn-Tools</b>	Ferramentas	São utilizadas para procurar e exibir pornografia. Este tipo inclui barras de ferramentas especiais de navegadores de Internet e leitores de vídeo especiais.

## **OUTRO SOFTWARE POTENCIALMENTE PERIGOSO (RISKWARE)**

**Subcategoria:** outro software potencialmente perigoso

**Nível de gravidade:** médio

A maioria destes programas são programas úteis, de uso comum e legítimo. Este incluem clientes de IRC, programas de ligações telefónicas, programas de gestão de transferências de ficheiros, monitores da actividade do sistema do computador, utilitários de gestão de passwords e servidores FTP, HTTP ou Telnet.

Contudo, se um intruso obtiver acesso a estes programas ou os instalar no computador do utilizador, as suas funcionalidades podem ser utilizadas para violar a segurança do computador.

A tabela lista os tipos de software potencialmente perigoso, agrupados por funções:

*Tabela 5. Outros tipos de software potencialmente perigoso, agrupados por funções*

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIÇÃO</b>
<b>Client-IRC</b>	Programas de clientes de conversação na Internet	Os utilizadores instalam programas para comunicarem através de canais de salas de conversação. Os intrusos usam esses programas para espalharem programas maliciosos.
<b>Dialers</b>	Programas de ligações telefónicas automáticas	Estes programas conseguem estabelecer ligações telefónicas "ocultas" através do modem.
<b>Downloaders</b>	Software de Transferências	Estes programas conseguem transferir ficheiros a partir de sites, de forma secreta.
<b>Monitors</b>	Monitores	Estes programas monitorizam as actividades dos computadores onde estão instalados, incluindo a monitorização do desempenho das aplicações e das operações de intercâmbio de dados com aplicações noutros computadores.
<b>PSWTools</b>	Ferramentas de recuperação de passwords	Estes programas são utilizados para visualizar e recuperar as passwords esquecidas. Os intrusos utilizam esses programas exactamente para isso quando os instalam nos computadores dos utilizadores.

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIÇÃO</b>
<b>RemoteAdmin</b>	Programas de administração remota	<p>Estes programas são muitas vezes utilizados por administradores de sistema. Eles fornecem acesso a um computador remoto para o monitorizar e gerir. Os intrusos utilizam esses programas exactamente para isso quando os instalam nos computadores dos utilizadores.</p> <p>Os programas potencialmente perigosos de administração remota são diferentes dos programas Trojan (ou programas backdoor) de administração remota. Os programas Trojan podem infiltrar-se independentemente no sistema e instalar-se. Os programas legítimos não têm esta funcionalidade.</p>
<b>Server-FTP</b>	Servidores FTP	Estes programas executam as funções dos servidores FTP. Os intrusos instalam-nos nos computadores dos utilizadores para obterem acesso remoto através do protocolo FTP.
<b>Server-Proxy</b>	Servidores de Proxy	Estes programas executam as funções dos servidores de proxy. Os intrusos instalam-nos nos computadores dos utilizadores para enviarem spam, utilizando a identidade do utilizador.
<b>Server-Telnet</b>	Servidores Telnet	Estes programas executam as funções dos servidores Telnet. Os intrusos instalam-nos nos computadores dos utilizadores para obterem acesso remoto através do protocolo Telnet.

<b>TIPO</b>	<b>NOME</b>	<b>DESCRIÇÃO</b>
<b>Server-Web</b>	Servidores de Internet	Estes programas executam as funções dos servidores de Internet. Os intrusos instalam-nos nos computadores dos utilizadores para obterem acesso remoto através do protocolo HTTP.
<b>RiskTool</b>	Ferramentas locais de computadores	Estas ferramentas fornecem aos utilizadores funcionalidades adicionais e apenas são utilizadas dentro do computador do utilizador. Elas permitem ao hacker esconder ficheiros, ocultar as janelas de aplicações activas ou fechar processos activos.
<b>NetTool</b>	Ferramentas de rede	Estas ferramentas permitem ao utilizador de um computador gerir os outros computadores da rede de forma remota, por exemplo, para reiniciar esses computadores, encontrar portas abertas ou executar programas instalados nesses computadores.
<b>Client-P2P</b>	Programas de clientes peer-to-peer	Estes programas são utilizados em redes peer-to-peer. Os intrusos podem utilizá-los para espalhar programas maliciosos.
<b>Client-SMTP</b>	Cientes SMTP	Estes programas enviam e-mails e ocultam esta actividade. Os intrusos instalam esses programas nos computadores dos utilizadores e enviam spam utilizando as identidades dos utilizadores.
<b>WebToolbar</b>	Barras de ferramentas para Internet	Estes programas adicionam as suas próprias barras de ferramentas de pesquisa às barras de ferramentas de outras aplicações.

TIPO	NOME	DESCRIÇÃO
FraudTool	Programas de fraude	Estes programas fazem-se passar por outros programas reais. Por exemplo, os programas anti-vírus fraudulentos exibem mensagens sobre a detecção de programas maliciosos, mas não encontram nem desinfectam nada.

## MÉTODOS DE DETECÇÃO DE OBJECTOS INFECTADOS, SUSPEITOS E POTENCIALMENTE PERIGOSOS POR PARTE DA APLICAÇÃO

O Kaspersky Internet Security detecta programas maliciosos em objectos, através de dois métodos: reactivo (utilizando bases de dados) e pró-activo (utilizando a análise heurística).

As bases de dados da aplicação contêm registos que são utilizados para identificar centenas de milhar de ameaças conhecidas em objectos verificados. Estes registos contêm informação sobre as secções de controlo do código dos programas maliciosos e sobre algoritmos para desinfectar os objectos que contêm estes programas. Os analistas anti-vírus da Kaspersky Lab analisam centenas de novos programas maliciosos diariamente, criam registos que os identificam e incluem esses registos nas actualizações dos ficheiros da base de dados.

Se, num objecto verificado, o Kaspersky Internet Security detectar secções de código que correspondem totalmente às secções de controlo do código de um programa malicioso, com base num registo da base de dados, a aplicação define o estado do objecto como *infectado*: se existir uma correspondência parcial, o estado é definido como *suspeito*.

Através do método pró-activo, a aplicação consegue detectar novos programas maliciosos que ainda não estão listados na base de dados.

A aplicação detecta objectos que contenham novos programas maliciosos, com base no seu comportamento. O código de um novo programa malicioso pode não coincidir total ou até mesmo parcialmente com o código de um programa malicioso conhecido, mas irá conter sequências de comando típicas, tais como a abertura de um ficheiro, a escrita num ficheiro ou a intercepção de vectores

interrompidos. A aplicação consegue determinar, por exemplo, se um ficheiro está infectado com um vírus de inicialização desconhecido.

Os objectos detectados através do método pró-activo são classificados com o estado *potencialmente perigoso*.

## **AMEAÇAS DA INTERNET**

A aplicação da Kaspersky Lab utiliza tecnologias especiais para prevenir as seguintes ameaças à segurança do computador:

- Spam ou mensagens de e-mail recebidas não solicitadas (ver secção "Spam ou e-mails recebidos não solicitados" na página 37);
- Phishing (na página 38);
- Ataques de hackers (na página 38);
- Exibição de banners (na página 39).

## **SPAM OU E-MAILS RECEBIDOS NÃO SOLICITADOS**

A aplicação da Kaspersky Lab protege os utilizadores em relação ao spam. O spam são e-mails recebidos não solicitados, que muitas vezes contém publicidade. O spam aumenta a carga sobre a rede e sobre os servidores de e-mail do fornecedor de correio electrónico. O destinatário paga pelo tráfego criado pelo spam e assim os e-mails legítimos não-spam demoram mais tempo a enviar/receber. Como resultado, o spam é ilegal em muitos países.

O Kaspersky Internet Security integra-se nos clientes de e-mail (Microsoft Outlook, Microsoft Outlook Express e The Bat!) e verifica as mensagens recebidas. As mensagens que detecta como sendo spam são processadas de acordo com acções especificadas pelo utilizador: por exemplo, as mensagens podem ser movidas para uma pasta especial ou apagadas.

O Kaspersky Internet Security detecta spam com um elevado grau de precisão. Este aplica várias tecnologias de filtragem de spam, incluindo: a análise do endereço do remetente e das palavras e frases contidas na linha de assunto da mensagem; a detecção de spam gráfico e a utilização de um algoritmo de auto-aprendizagem para detectar spam com base no texto da mensagem.

As bases de dados do Anti-Spam contêm listas "negras" e "brancas" de endereços de remetentes e listas de palavras e frases relacionadas com diversas categorias de spam, tais como publicidade, medicina e saúde, jogo.

## **PHISHING**

O *Phishing* é um tipo de actividade fraudulenta na Internet que se destina a "pescar" informações pessoais dos utilizadores de computadores, tais como números de cartões de crédito e PINs, para lhes roubar dinheiro.

O phishing está muitas vezes relacionado com serviços bancários por Internet. Os intrusos criam uma cópia exacta do site do banco-alvo e depois enviam mensagens aos clientes do banco. Os clientes são notificados de que, devido a alterações ou falha no sistema bancário por Internet, perderam-se as contas de utilizador e o utilizador tem de confirmar ou alterar a sua informação no site do banco. O utilizador acede ao site do intruso e insere os seus dados pessoais nesse site.

As bases de dados do Anti-phishing contêm uma lista de sites conhecidos como sites utilizados para ataques de phishing.

O Kaspersky Internet Security analisa as mensagens recebidas nos clientes de e-mail suportados (Microsoft Office Outlook e Microsoft Outlook Express) e se encontrar um link para um site de phishing listado, a aplicação assinala essa mensagem como spam. Se o utilizador abrir a mensagem e tentar clicar no link, a aplicação bloqueia a ligação ao site.

## **ATAQUES DE HACKERS**

Um *ataque de rede* é uma intrusão no sistema de um computador remoto para obter o controlo do mesmo, normalmente para provocar a falha do sistema ou para obter acesso a informação protegida.

Os ataques de rede são acções de intrusos (por exemplo, pesquisa de portas, tentativas para roubar passwords), ou de programas maliciosos para executar comandos em nome do intruso e, por exemplo, transferir informação para um programa "central" remoto. Os programas utilizados incluem programas Trojan, ataques DoS, scripts maliciosos e determinados tipos de worms de rede.

Os ataques de rede são espalhados nas redes de área local e global, através de vulnerabilidades dos sistemas operativos e das aplicações. Estes ataques

podem ser transferidos sob a forma de pacotes individuais de dados IP durante ligações de rede.

O Kaspersky Internet Security interrompe os ataques de rede sem perturbar as ligações de rede, através de bases de dados de firewall especiais. Estas bases de dados contêm registos que identificam pacotes típicos de dados IP enviados por vários programas de hackers. A aplicação analisa as ligações de rede e bloqueia nessas ligações quaisquer pacotes IP perigosos.

## **FAIXAS DE PUBLICIDADE (BANNERS)**

Os *banners* ou anúncios publicitários são links para o site de um anunciante publicitário, sendo normalmente exibidos como imagens. A exibição de banners num site não representa uma ameaça à segurança do computador, mas mesmo assim é considerada uma interferência no funcionamento normal do computador. Se os banners aparecerem a piscar no ecrã, então afectam as condições de trabalho e reduzem a eficiência. O utilizador também é distraído com informação irrelevante e ao clicar nos links do banner, isso aumenta o tráfego de Internet.

Muitas organizações proibem a exibição de banners em interfaces, como parte das suas políticas de segurança de dados.

O Kaspersky Internet Security bloqueia os banners, com base no URL do site para o qual o banner tem um link. A aplicação utiliza as bases de dados actualizáveis do Bloqueador de Banners, as quais contêm uma lista de URLs de redes de banners russas e estrangeiras. A aplicação processa os links da página de Internet que está a ser carregada, comparando-os com a lista de endereços existente nas bases de dados e, se encontrar uma correspondência, apaga do site o link para este endereço e continua a carregar a página.

---

# INSTALAÇÃO DA APLICAÇÃO

A aplicação é instalada no computador de forma interactiva, através do Assistente de Instalação da Aplicação.

Aviso!

Recomendamos que feche todas as aplicações em execução antes de continuar com a instalação.

Para instalar a aplicação no seu computador, execute o ficheiro de distribuição (ficheiro com a extensão \*.exe).

Depois disso, será procurado o pacote de instalação da aplicação (ficheiro com a extensão \*.msi) e, se for encontrado, será procurada a versão mais recente nos servidores da Kaspersky Lab na Internet. Se não for encontrado nenhum ficheiro do pacote de instalação, ser-lhe-á dada a possibilidade de o transferir. Quando a transferência estiver concluída, iniciar-se-á a instalação do Kaspersky Internet Security. Se a transferência for descartada, a instalação da aplicação irá continuar no modo padrão.

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 processo de instalação.
- **Anterior** – voltar ao passo anterior do processo de instalação.
- **Cancelar** – cancelar a instalação.
- **Concluir** – concluir o procedimento de instalação da aplicação.

De seguida, é apresentada uma descrição detalhada de cada um dos passos da instalação do pacote.

**NESTA SECÇÃO:**

---

Passo 1. Procurar uma versão mais recente da aplicação.....	41
Passo 2. Verificar se o sistema satisfaz os requisitos de instalação .....	42
Passo 3. Janela de Boas-vindas do Assistente .....	42
Passo 4. Visualizar o Contrato de Licença .....	43
Passo 5. Seleccionar o tipo de instalação .....	43
Passo 6. Seleccionar a pasta de instalação .....	44
Passo 7. Seleccionar os componentes da aplicação a instalar .....	44
Passo 8. Procurar outros programas de anti-vírus .....	45
Passo 9. Preparação final para a instalação .....	46
Passo 10. Concluir a instalação .....	46

## **PASSO 1. PROCURAR UMA VERSÃO MAIS RECENTE DA APLICAÇÃO**

Antes de instalar a aplicação no seu computador, o assistente irá aceder aos servidores de actualização da Kaspersky Lab para verificar se existe uma versão mais recente.

Se não for detectada uma versão mais recente nos servidores de actualização da Kaspersky Lab, o assistente de instalação será iniciado e irá instalar a versão actual.

Se for detectada uma versão mais recente nos servidores, ser-lhe-á perguntado se deseja transferi-la. Se cancelar a transferência, o assistente de instalação irá começar a instalar a versão actual. Se decidir instalar a versão mais recente, os ficheiros de instalação serão transferidos para o seu computador e o assistente de instalação será, automaticamente, iniciado para instalar a versão mais

recente. Para mais detalhes sobre a instalação de uma versão mais recente da aplicação, por favor consulte a documentação dessa versão.

## **PASSO 2. VERIFICAR SE O SISTEMA SATISFAZ OS REQUISITOS DE INSTALAÇÃO**

Antes de instalar a aplicação no seu computador, o assistente irá verificar se o computador satisfaz os requisitos mínimos (ver secção "Requisitos de hardware e software do sistema" na página 13). Também irá verificar se tem os direitos necessários para instalar o software.

Se alguns 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 Internet Security.

## **PASSO 3. JANELA DE BOAS-VINDAS DO ASSISTENTE**

Se o seu sistema cumprir todos os requisitos de sistema (ver secção "Requisitos de hardware e software do sistema" na página 13) e se não for detectada nenhuma versão mais recente da aplicação nos servidores de actualização da Kaspersky Lab ou se você tiver cancelado a instalação dessa versão, será iniciado o assistente de instalação para instalar a versão actual da aplicação.

Será apresentada no ecrã a primeira caixa de diálogo do assistente de instalação, a qual indica que vai começar a instalação.

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

## PASSO 4. VISUALIZAR O CONTRATO DE LICENÇA

A próxima caixa de diálogo do assistente 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 **Aceito os termos do Contrato de Licença** e clique no botão **Seguinte**. A instalação continuará.

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

## PASSO 5. SELECIONAR O TIPO DE INSTALAÇÃO

Durante este passo, ser-lhe-á pedido que seleccione o tipo de instalação que melhor se adequa à sua situação:

- **Instalação rápida.** Se seleccionar esta opção, a aplicação será totalmente instalada no seu computador com as configurações de protecção predefinidas recomendadas pela Kaspersky Lab. Depois de concluída a instalação, será iniciado o assistente de Configuração da Aplicação.
- **Instalação personalizada.** Se seleccionar esta opção, ser-lhe-á pedido para: seleccionar os componentes da aplicação que deseja instalar; especificar a pasta onde a aplicação será instalada (ver secção "Passo 6. Seleccionar a pasta de instalação" na página 44); activar a aplicação; e configurá-la através do assistente de Configuração da Aplicação.

Se seleccionar a primeira opção, o assistente de instalação da aplicação irá avançar directamente para o Passo 8 (ver secção "Passo 8. Procurar outros programas de anti-vírus" na página 45). Caso contrário, terá de introduzir ou confirmar determinados dados em cada passo da instalação.

## PASSO 6. SELECIONAR A PASTA DE INSTALAÇÃO

### Nota

Este passo do assistente de instalação só será executado, se tiver seleccionado a opção de instalação personalizada (ver secção "Passo 5. Seleccionar o tipo de instalação" na página 43).

Durante este passo, ser-lhe-á pedido que identifique a pasta no seu computador onde a aplicação será instalada. O caminho predefinido é:

- Para sistemas 32-bit: <Drive> \ Program Files \ Kaspersky Lab \ Kaspersky Internet Security 2009 Special Edition for Ultra-Portables.

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 fornecido.

### Aviso!

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 7. SELECIONAR OS COMPONENTES DA APLICAÇÃO A INSTALAR

Nota. Este passo do assistente de instalação só será executado, se tiver seleccionado a opção de instalação personalizada (ver secção "Passo 5. Seleccionar o tipo de instalação" na página 43).

Durante a instalação personalizada, tem de seleccionar os componentes da aplicação que deseja instalar no seu computador. Por defeito, são seleccionadas todas as componentes da aplicação: componentes de protecção, verificação e actualização.

Para ajudá-lo a decidir quais as componentes que deseja instalar, estão disponíveis algumas informações sobre cada componente: seleccione a componente na lista e leia a informação no campo por baixo. A informação inclui uma breve descrição da componente e o espaço de disco necessário para a sua instalação.

Para impedir a instalação de uma componente, abra o menu de atalho, clicando no ícone junto ao nome da componente, e seleccione o item **O recurso estará indisponível**. Note que se cancelar a instalação de uma componente, não será protegido contra uma série de programas perigosos.

Para seleccionar uma componente a instalar, abra o menu de atalho, clicando no ícone junto ao nome da componente, e seleccione **Este recurso será instalado no disco rígido local**.

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

## **PASSO 8. PROCURAR OUTROS PROGRAMAS DE ANTI-VÍRUS**

Durante este passo, o assistente procura outros programas de anti-vírus, incluindo outros programas da Kaspersky Lab, que podem causar conflitos com esta aplicação.

Se forem detectados programas de anti-vírus no seu computador, estes serão listados no ecrã. Ser-lhe-á pedido que os desinstale antes de continuar com a instalação.

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

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

## PASSO 9. PREPARAÇÃO FINAL PARA A INSTALAÇÃO

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

Durante a instalação inicial e personalizada da aplicação (ver secção "Passo 5. Seleccionar o tipo de instalação" na página 43), recomendamos que não desmarque a caixa **Activar Autodefesa antes da instalação**. Se a opção de protecção dos módulos estiver activada, então se ocorrer um erro durante a instalação, isso assegurará o correcto procedimento de reversão da instalação. Quando voltar a tentar a instalação, recomendamos que desmarque esta caixa.

### Nota

Se a aplicação estiver a ser instalada de forma remota, através do **Remote Desktop**, recomendamos que desmarque a caixa **Activar Autodefesa antes da instalação**. Se esta caixa estiver assinalada, o procedimento de instalação pode ser incorrectamente executado ou pode não ser executado.

Para continuar a instalação, clique no botão **Seguinte**. Os ficheiros de instalação começarão a ser copiados para o seu computador.

### Aviso!

Durante o processo de instalação, a actual ligação de rede será interrompida se o pacote da aplicação incluir componentes para interceptar o tráfego de rede. A maioria das ligações terminadas será restaurada no devido tempo.

## PASSO 10. CONCLUIR A INSTALAÇÃO

A janela **Concluir Instalação** contém informação sobre a conclusão da instalação da aplicação no seu computador.

Por exemplo, esta janela irá indicar se é necessário reiniciar o computador para concluir correctamente a instalação. Depois de reiniciar o sistema, o assistente de configuração será automaticamente iniciado.

Se não precisar de reiniciar o sistema, clique no botão **Seguinte** para iniciar o assistente de configuração da aplicação.

---

# INTERFACE DA APLICAÇÃO

A aplicação possui uma interface simples e fácil de utilizar. Este capítulo discutirá as suas características básicas em detalhe.

Para além da interface principal da aplicação, existem extensões para o Microsoft Outlook, o The Bat! e o Microsoft Windows Explorer. Estas extensões aumentam as funcionalidades destes programas, uma vez que permitem gerir e configurar as componentes do Kaspersky Internet Security a partir da interface do programa cliente.

## NESTA SECÇÃO:



---

Ícone da área de notificação.....	47
Menu de atalho.....	48
Janela principal da aplicação.....	50
Notificações .....	53
Janela de configuração da aplicação .....	53

## ÍCONE DA ÁREA DE NOTIFICAÇÃO

Logo após a instalação da aplicação, o ícone da aplicação aparecerá na área de notificação da barra de tarefas do Microsoft Windows.

Este ícone indica a operação actual da aplicação. Também reflecte o estado de protecção e mostra algumas das funções básicas executadas pelo programa.

Se o ícone estiver activo  (a cores), a protecção completa da aplicação ou algumas das suas componentes estão a funcionar. Se o ícone estiver inactivo  (a preto e branco), todas as componentes de protecção foram desactivadas.

O ícone da aplicação altera-se em função da operação que está a ser executada:



– Está a ser verificado um e-mail.



– As bases de dados da aplicação e os módulos do programa estão a ser actualizados.



– O computador precisa de ser reiniciado para aplicar as actualizações.




– Ocorreu um erro nalguma componente do Kaspersky Internet Security.

O ícone também permite o acesso aos elementos básicos da interface da aplicação, incluindo o menu de atalho (ver secção "Menu de atalho" na página 48) e a janela principal da aplicação (ver secção "Janela principal da aplicação" na página 50).

Para abrir o menu de atalho, clique sobre o ícone da aplicação com o botão direito do rato.

Para abrir a janela principal da aplicação, clique duas vezes sobre o ícone da aplicação. A janela principal abre-se sempre na secção **Protecção**.

Se estiverem disponíveis notícias da Kaspersky Lab, o ícone de notícias aparecerá na área de notificação da barra de tarefas . Clique duas vezes sobre o ícone para ver as notícias na janela que se abre.

## MENU DE ATALHO

Você pode executar tarefas básicas de protecção a partir do menu de contexto, o qual contém estes itens:

- **Actualização** – inicia a actualização dos módulos e das bases de dados da aplicação e instala as actualizações no seu computador.
- **Verificação completa do computador** – Inicia uma verificação completa do computador quanto à existência de objectos perigosos. Serão verificados os objectos existentes em todas as unidades, incluindo meios de armazenamento removíveis.
- **Verificação de vírus** – selecciona objectos e inicia uma verificação de vírus. A lista predefinida para esta verificação contém vários objectos,

tais como a pasta **Os Meus Documentos** e arquivos de e-mail. Pode adicionar objectos a esta lista, seleccionando outros objectos a serem verificados.

- **Monitor de Rede** – permite ver a lista das ligações de rede estabelecidas, portas abertas e o tráfego.
- **Teclado Virtual** – muda para o teclado virtual.
- **Kaspersky Internet Security** – abre a janela principal da aplicação (ver secção "Janela principal da aplicação" na página 50).
- **Configuração** – Permite ver e alterar as definições da aplicação.
- **Activar** – activa o programa. Para se tornar num utilizador registado, tem de activar a sua aplicação. Este item do menu apenas está disponível se a aplicação não tiver sido activada.
- **Sobre** – apresenta informação sobre a aplicação.
- **Pausar protecção / Retomar protecção** – activa ou desactiva temporariamente as componentes de protecção em tempo real. Esta opção do menu não afecta a execução das actualizações da aplicação ou das tarefas de verificação de vírus.
- **Bloquear tráfego de rede** – bloqueia, temporariamente, todas as ligações de rede do computador. Se deseja permitir que o computador interaja com a rede, clique novamente neste item no menu de contexto.
- **Sair** – fecha a aplicação e descarrega a aplicação da memória do computador.



Figura 1: Menu de atalho

Se estiver a decorrer uma tarefa de verificação de vírus, quando abre o menu de atalho, o respectivo nome e o estado de avanço (percentagem de conclusão) serão apresentados no menu de atalho. Ao seleccionar a tarefa, abrirá a janela principal da aplicação que contém um relatório sobre os resultados actuais da execução da tarefa.

## JANELA PRINCIPAL DA APLICAÇÃO

A janela principal da aplicação pode ser dividida em três partes:

- A parte superior da janela indica o estado actual da protecção do seu computador.



*Figura 2: Estado actual da protecção do computador*

Existem três estados de protecção possíveis: cada estado é indicado por uma determinada cor, semelhante aos semáforos do trânsito. A cor verde indica que a protecção do seu computador está no nível adequado, enquanto as cores amarelo e vermelho indicam que existem ameaças de segurança na configuração do sistema ou no funcionamento da aplicação. Para além dos programas maliciosos, as ameaças incluem bases de dados da aplicação obsoletas, componentes de protecção desactivadas e selecção de configurações de protecção mínimas.

As ameaças de segurança tem de ser eliminadas assim que aparecem. Para obter informação detalhada sobre as ameaças e para as eliminar rapidamente, use a ligação **Corrigir agora** (ver figura acima).

- A parte esquerda da janela, a barra de navegação, permite um acesso rápido às funções da aplicação, incluindo as tarefas de verificação de vírus e de actualização.



Figura 3: Parte esquerda da janela principal

- A parte direita da janela contém informação sobre a função da aplicação seleccionada na parte esquerda, é utilizada para configurar essas funções e apresenta ferramentas para executar tarefas de verificação de vírus, transferir actualizações, etc.



Figura 4: Parte informativa da janela principal

Também pode utilizar estes botões:

- **Configuração** – para abrir a janela de configuração da aplicação.
- **Ajuda** – para abrir o sistema de Ajuda da aplicação.
- **Detectadas** – para abrir uma lista de objectos prejudiciais detectados por qualquer componente ou por uma tarefa de verificação anti-vírus e para ver estatísticas detalhadas das operações da aplicação.
- **Relatórios** – para abrir a lista de eventos que ocorreram durante o funcionamento da aplicação.
- **Suporte** – para exibir informação sobre o sistema e links para os recursos de informação da Kaspersky Lab, incluindo o site do serviço de Suporte Técnico e o fórum.

Nota

Pode mudar a aparência da aplicação, criando e utilizando os seus próprios gráficos e esquemas de cores.

## NOTIFICAÇÕES

Se ocorrerem eventos no decurso do funcionamento da aplicação, serão apresentadas notificações especiais no ecrã, sob a forma mensagens de popup, por cima do ícone da aplicação na barra de tarefas do Microsoft Windows.

Dependendo do nível de criticalidade do evento, no que respeita à segurança do computador, você pode receber os seguintes tipos de notificações:

- **Alerta.** Ocorreu um evento crítico. Por exemplo, foi detectado um vírus ou uma actividade perigosa no seu sistema. Deve decidir de imediato sobre como lidar com esta ameaça. Este tipo de notificação aparece a vermelho.
- **Aviso!** Ocorreu um evento potencialmente perigoso. Por exemplo, foram detectados no seu sistema ficheiros potencialmente infectados ou actividades suspeitas. Deve dar instruções ao programa, dependendo do nível de perigo que atribui a este evento. Este tipo de notificação aparece a amarelo.
- **Nota:** Esta notificação fornece informação sobre eventos não críticos. Por exemplo, este tipo inclui notificações relacionadas com o funcionamento da componente **Filtragem de Conteúdos**. As notificações de informação aparecem a verde.

## JANELA DE CONFIGURAÇÃO DA APLICAÇÃO

Pode abrir a janela de configuração da aplicação a partir da janela principal da aplicação (ver secção "Janela principal da aplicação" na página 50) ou do menu de atalho (ver secção "Menu de atalho" na página 48). Para abrir esta janela, clique na ligação **Configuração** na parte superior da janela principal da aplicação ou seleccione a opção adequada no menu de atalho da aplicação.

A janela de configuração consiste em duas partes:

- A parte esquerda da janela permite o acesso às componentes da aplicação, como por exemplo, as tarefas de verificação de vírus e as tarefas de actualização;

- A parte direita da janela contém uma lista de configurações para a componente ou tarefa seleccionada na parte esquerda da janela.

---

# COMEÇAR

Um dos principais objectivos da Kaspersky Lab, ao conceber o Kaspersky Internet Security, foi o de fornecer a configuração óptima para todas as opções da aplicação. Isso permite que até um utilizador com poucos conhecimentos informáticos possa proteger o seu computador logo após a instalação, sem necessitar de despender horas a alterar as definições.

Para a conveniência do utilizador, reunimos as etapas de configuração preliminar num Assistente de Configuração Inicial unificado, que se inicia assim que a aplicação é instalada. Ao seguir as instruções do Assistente, você pode activar a aplicação, configurar definições para as actualizações, restringir o acesso ao programa com uma password e efectuar outras configurações.

O seu computador pode estar infectado com software malicioso antes da aplicação ser instalada. Para detectar os programas maliciosos existentes, execute uma verificação do computador (ver secção "Verificação de vírus no computador" na página 58).

Como resultado de uma infecção por software malicioso ou de falhas do sistema, as configurações do seu computador podem ser corrompidas. Execute o assistente do Analisador de Segurança para detectar quaisquer vulnerabilidades existentes em software instalado e anomalias nas configurações do sistema.

As bases de dados da aplicação incluídas no pacote de instalação provavelmente estarão desactualizadas. Inicie a actualização da aplicação (ver página 57), caso esta não tenha sido efectuada pelo assistente de configuração ou de forma automática após a instalação da aplicação.

A componente Anti-Spam incluída na estrutura da aplicação utiliza um algoritmo de auto-aprendizagem para detectar mensagens indesejadas. Inicie o assistente de treino do Anti-Spam para configurar a forma como a componente trabalha com a sua correspondência.

Depois de concluir as acções nesta secção, a aplicação estará pronta para proteger o seu computador. Para avaliar a protecção do seu computador, utilize o assistente de Gestão de Segurança (ver secção "Gestão de segurança" na página 64).

## NESTA SECÇÃO:

---

Seleccionar o tipo de rede .....	56
Actualizar a aplicação.....	57
Análise de segurança .....	57
Verificação de vírus no computador .....	58
Gerir a licença .....	59
Subscrição para a renovação automática da licença .....	60
Participar no Kaspersky Security Network.....	62
Gestão de segurança .....	64
Pausar a protecção .....	66

## SELECIONAR O TIPO DE REDE

Depois de concluída a instalação, a componente Firewall analisa as ligações de rede activas no seu computador. Será atribuído um estado a cada ligação de rede, determinando as actividades de rede permitidas.

Se tiver seleccionado o modo interactivo da Kaspersky Internet Security, será apresentada uma notificação sempre que for estabelecida uma ligação de rede. Pode seleccionar o estado para as novas redes na janela de notificação:

- **Redes públicas** – o acesso externo ao seu computador está bloqueado e o acesso a pastas públicas e impressoras também está bloqueado. Este estado é recomendado para ligações à Internet.
- **Redes locais** – o acesso a pastas públicas e impressoras de rede é permitido. Recomenda-se que atribua este estado a redes locais protegidas, por exemplo, uma rede empresarial.
- **Redes confiáveis** – são permitidas todas as actividades. Recomenda-se que atribua este estado somente a redes absolutamente seguras.

Para cada estado de rede, o Kaspersky Internet Security inclui um conjunto de regras para gerir as actividades de rede. Por conseguinte, você pode alterar o estado de rede especificado para cada ligação depois desta ser detectada pela primeira vez.

## ACTUALIZAR A APLICAÇÃO

Aviso!

Precisa de ter ligação à Internet para actualizar o Kaspersky Internet Security.

O Kaspersky Internet Security inclui bases de dados que contêm assinaturas de ameaças, exemplos de frases típicas de spam e descrições de ataques de rede. Contudo, quando a aplicação é instalada, as bases de dados podem já estar obsoletas, uma vez que a Kaspersky Lab actualiza regularmente as bases de dados e os módulos da aplicação.

Você pode especificar a forma como a tarefa de actualização será iniciada quando o assistente de configuração da aplicação for executado. Por defeito, o Kaspersky Internet Security verifica, automaticamente, a existência de actualizações nos servidores da Kaspersky Lab. Se o servidor tiver novas actualizações, a aplicação irá transferi-las e instalá-las em modo silencioso.

Para manter a protecção do seu computador actualizada, recomenda-se que actualize o Kaspersky Internet Security imediatamente após a instalação.

► *Para actualizar, manualmente, o Kaspersky Internet Security,*

1. Abra a janela principal da aplicação.
2. Selecciona a secção **Actualizações** na parte esquerda da janela.
3. Clique no botão **Iniciar actualização**.

## ANÁLISE DE SEGURANÇA

O sistema operativo do seu computador pode ser danificado por falhas do sistema e por actividades de programas maliciosos. Para além disso, as aplicações de utilizador instaladas no seu computador podem conter vulnerabilidades que os intrusos podem explorar para danificar o seu computador.

Para detectar e eliminar esses problemas de segurança, recomenda-se que inicie o *Assistente do Analisador de Segurança* imediatamente depois de instalar a aplicação. O assistente do analisador de segurança procura vulnerabilidades em aplicações instaladas e danos e anomalias nas configurações do sistema operativo e do navegador de Internet.

▶ *Para iniciar o assistente:*

1. Abra a janela principal da aplicação.
2. Na parte esquerda da janela, seleccione **Controlo das Aplicações**.
3. Inicie a tarefa **Analisador de Segurança**.

## VERIFICAÇÃO DE VÍRUS NO COMPUTADOR

Os criadores de software malicioso fazem todos os esforços para esconderem as acções dos seus programas e, por isso, você pode não detectar a presença de programas maliciosos no seu computador.

Depois do Kaspersky Internet Security ser instalado no seu computador, este executa automaticamente uma tarefa de **Verificação Rápida** no seu computador. Esta tarefa procura e neutraliza programas prejudiciais existentes nos objectos que são carregados quando o sistema operativo é iniciado.

Os especialistas da Kaspersky Lab também recomendam que execute a tarefa de **Verificação Completa**.

▶ *Para iniciar / parar uma verificação de vírus:*

1. Abra a janela principal da aplicação.
2. Na parte esquerda da janela, seleccione a secção **Verificar (Verificação Completa, Verificação Rápida)**.
3. Clique no botão **Iniciar verificação** para iniciar a verificação. Se precisar de parar a execução da tarefa, clique no botão **Parar verificação** enquanto a tarefa estiver a decorrer.

## GERIR A LICENÇA

A aplicação precisa de uma chave de licença para funcionar. Ser-lhe-á fornecida uma chave quando adquirir o programa. Esta chave dá-lhe o direito de utilizar o programa a partir do dia em que o comprar e instalar a chave.

Sem uma chave de licença, a não ser que tenha activado uma versão de avaliação da aplicação, esta funcionará no modo que permite apenas uma actualização. A aplicação não transferirá actualizações novas.

Se tiver activado uma versão de avaliação do programa, após terminar o período de avaliação, a aplicação deixará de funcionar.

Quando a chave de licença expirar, o programa continuará a funcionar, mas não conseguirá actualizar as bases de dados. Tal como anteriormente, poderá analisar o seu computador em termos de vírus e utilizar as componentes de protecção, mas só utilizando as bases de dados que possuía quando a licença expirou. Não podemos garantir que fique protegido dos vírus depois da licença do programa expirar.

Para proteger o seu computador da infecção por novos vírus, recomendamos que renove a sua chave da aplicação. A aplicação notificá-lo-á duas semanas antes da chave da aplicação expirar. Durante algum tempo, será exibida uma mensagem adequada sempre que iniciar a aplicação.

A informação acerca da actual chave é apresentada na secção **Licença** na janela principal da aplicação: identificação da chave, tipo (comercial, comercial com subscrição, comercial com subscrição de protecção, avaliação, teste beta), número de anfitriões onde esta chave pode ser instalada, data de validade da chave e número de dias restantes até ao final da validade. A informação sobre a validade da chave não será apresentada se estiver instalada uma licença comercial com subscrição ou uma licença comercial com subscrição de protecção (ver secção "Subscrição para a renovação automática da licença" na página 60).

Para ver o contrato de licença da aplicação, clique no botão **Ler Contrato de Licença**. Para remover uma chave da lista, clique no botão **Adicionar/Apagar**.

Para comprar ou renovar uma chave:

1. Compre uma chave nova. Para o fazer, clique no botão **Comprar licença** (se a aplicação ainda não foi activada) ou **Renovar licença**. A página de Internet que se abre conterá todas as informações sobre como comprar uma chave através da loja online da Kaspersky Lab ou

dos seus parceiros empresariais. Se comprou a licença online, depois do pagamento ser efectuado, ser-lhe-á enviado por e-mail um ficheiro de chave ou um código de activação para o endereço especificado no formulário de encomenda.

2. Instale a chave. Para o fazer, use o botão **Instalar chave** na secção **Licença** na janela principal da aplicação ou use o comando **Activar** no menu principal da aplicação. Isto iniciará o Assistente de Activação.

Nota. A Kaspersky Lab tem regularmente ofertas com preços especiais para prolongar as licenças dos nossos produtos. Procure ofertas especiais no site da Kaspersky Lab em **Products → Sales and special offers**.

## SUBSCRIÇÃO PARA A RENOVAÇÃO AUTOMÁTICA DA LICENÇA

Ao utilizar uma licença com subscrição, a aplicação irá contactar automaticamente o servidor de activação em determinados intervalos de tempo para manter a validade da sua licença durante todo o período de subscrição.

Se a actual chave tiver expirado, o Kaspersky Internet Security irá verificar se existe uma chave actualizada no servidor, através do modo em segundo plano, e se encontrar essa chave, a aplicação irá transferi-la e instalá-la no modo de substituição da chave anterior. Desta forma, a licença será renovada sem a sua participação. Se o período durante o qual a aplicação renova a licença também tiver expirado, a licença pode ser renovada manualmente. Durante o período que permite a renovação manual da licença, a funcionalidade da aplicação será mantida. Depois deste período expirar, se a licença não tiver sido renovada, esta deixará de carregar as actualizações das bases (para a licença comercial com subscrição), assim com deixará de assegurar a protecção do seu computador (para a licença comercial com subscrição de protecção). Para rejeitar a subscrição para a renovação automática da licença, contacte a nossa loja online onde comprou a aplicação.

### Aviso!

Se na altura da activação a aplicação já estiver activada através de uma chave comercial, essa chave comercial será substituída por uma chave de subscrição (uma chave de subscrição de protecção). Se desejar começar a utilizar de novo a chave comercial, tem de apagar a chave de subscrição e active novamente a aplicação com o código de activação com o qual obteve antes a chave comercial.

A condição de subscrição é caracterizada pelos seguintes estados:

1. *Corrompida*. O seu pedido para activar a subscrição ainda não foi processado (é necessário algum tempo para processar o pedido no servidor). O Kaspersky Internet Security funciona em modo de total funcionalidade. Se após um determinado período de tempo o pedido de subscrição não tiver sido processado, você receberá uma notificação de que a subscrição não foi processada. Neste caso, as bases da aplicação deixarão de ser actualizadas (para a licença comercial com subscrição), assim como a protecção do computador deixará de ser executada (para a licença comercial com subscrição de protecção).
2. *Activação*. A subscrição para a renovação automática da licença foi activada para um período de tempo ilimitado (sem data especificada) ou para um determinado período de tempo (data de validade de subscrição especificada).
3. *Renovada*. A subscrição foi renovada, manual ou automaticamente, para um período de tempo ilimitado (sem data especificada) ou para um determinado período de tempo (data de validade de subscrição especificada).
4. *Erro*: A renovação da subscrição resultou em erro.
5. *Expirou*. O período de subscrição terminou. Você pode usar outro código de activação ou renovar a sua subscrição, contactando a loja online onde comprou a aplicação.
6. *Subscrição cancelada*. Você cancela a subscrição para a renovação automática da licença.
7. *A renovação é necessária*. Por alguma razão, a chave para a renovação da subscrição não foi recebida a tempo. Use o botão **Renovar o estado de subscrição** para renovar a subscrição.

Para a licença comercial com subscrição de protecção, a subscrição é caracterizada por dois estados adicionais:

- *Suspensa*. A subscrição para a renovação automática da licença está suspensa (data de validade da subscrição: data de suspensão da validade da subscrição).
- *Retomada*. A subscrição para a renovação automática da licença foi retomada (a data de validade da subscrição não está limitada).

Se o período de validade da subscrição tiver terminado, assim como o período adicional durante o qual a licença pode ser renovada (estado de subscrição – *Expirou*), a aplicação irá notificá-lo sobre isso e deixará de tentar obter uma chave actualizada a partir do servidor. Para a licença comercial com subscrição, a funcionalidade da aplicação será mantida, com excepção da função de actualização das bases da aplicação. Para a licença comercial com subscrição de protecção, as bases da aplicação não serão actualizadas e a protecção do computador não será executada.

Se, por alguma razão, a licença não tiver sido renovada (estado de subscrição – *A renovação é necessária*) a tempo (por exemplo, o computador estava desligado durante todo o tempo em que a renovação da licença estava disponível), você pode renovar o estado manualmente. Para isso, pode usar o botão **Renovar o estado de subscrição**. Até ao momento da renovação da subscrição o Kaspersky Internet Security deixa de actualizar as bases de dados da aplicação (para a licença comercial com subscrição), assim como deixa de executar a protecção do computador (para a licença comercial com subscrição de protecção).

Enquanto estiver a utilizar a subscrição, não pode instalar chaves de outro tipo ou utilizar outro código de activação para renovar a licença. Só poderá utilizar outro código de activação depois do período de subscrição ter terminado (estado de subscrição - *Expirou*).

Aviso!

Note que quando utiliza a subscrição para a renovação automática da licença, se reinstalar a aplicação no seu computador, precisará de voltar a activar o produto manualmente, através do código de activação que obteve quando comprou a aplicação.

## **PARTICIPAR NO KASPERSKY SECURITY NETWORK**

Todos os dias surgem inúmeras ameaças novas a nível mundial. Para facilitar a recolha de estatísticas sobre novos tipos de ameaças, a sua origem e sobre como eliminá-las, a Kaspersky Lab convida-o a utilizar o serviço Kaspersky Security Network.

A utilização do Kaspersky Security Network envolve o envio das seguintes informações à Kaspersky Lab:

- Um identificador único atribuído ao seu computador pela aplicação. Este identificador caracteriza as configurações de hardware do seu computador e não contém nenhuma outra informação.
- Informação sobre ameaças detectadas pela aplicação. A estrutura e conteúdos da informação depende do tipo de ameaça detectada.
- Informação do sistema: a versão do sistema operativo, pacotes de serviço instalados, serviços e controladores transferíveis, versões do cliente de e-mail e do navegador, extensões do navegador, número da versão instalada do Kaspersky Internet Security.

O Kaspersky Security Network também recolhe estatísticas alargadas, incluindo informação sobre:

- Ficheiros executáveis e aplicações assinadas transferidas para o seu computador;
- Aplicações em execução no seu computador.

Esta informação estatística é enviada assim que for concluída a actualização da aplicação.

**Aviso!**

A Kaspersky Lab garante que não é efectuada qualquer recolha ou distribuição de dados pessoais dos utilizadores no âmbito do Kaspersky Security Network.

- ▶ Para configurar o envio de estatísticas:
  1. Abra a janela de configuração da aplicação.
  2. Seleccione a secção **Informação de Retorno** na parte esquerda da janela.
  3. Assinale a opção **Aceito participar no Kaspersky Security Network**, para confirmar a sua participação no Kaspersky Security Network. Assinale a opção **Aceito enviar estatísticas alargadas no âmbito do Kaspersky Security Network**, para confirmar o seu consentimento para enviar estatísticas alargadas.

## GESTÃO DE SEGURANÇA

Os problemas detectados na protecção do computador são indicados na janela principal da aplicação, através de uma alteração da cor do ícone do estado de protecção e do painel onde este ícone se encontra. Quando surgem problemas no sistema de protecção, recomenda-se que os resolva imediatamente.



*Figura 5: Estado actual da protecção do computador*

Pode ver a lista dos actuais problemas, a sua descrição e as soluções possíveis no separador **Estado** (ver figura abaixo), que se abre quando clica na ligação **Corrigir agora** (ver figura abaixo).

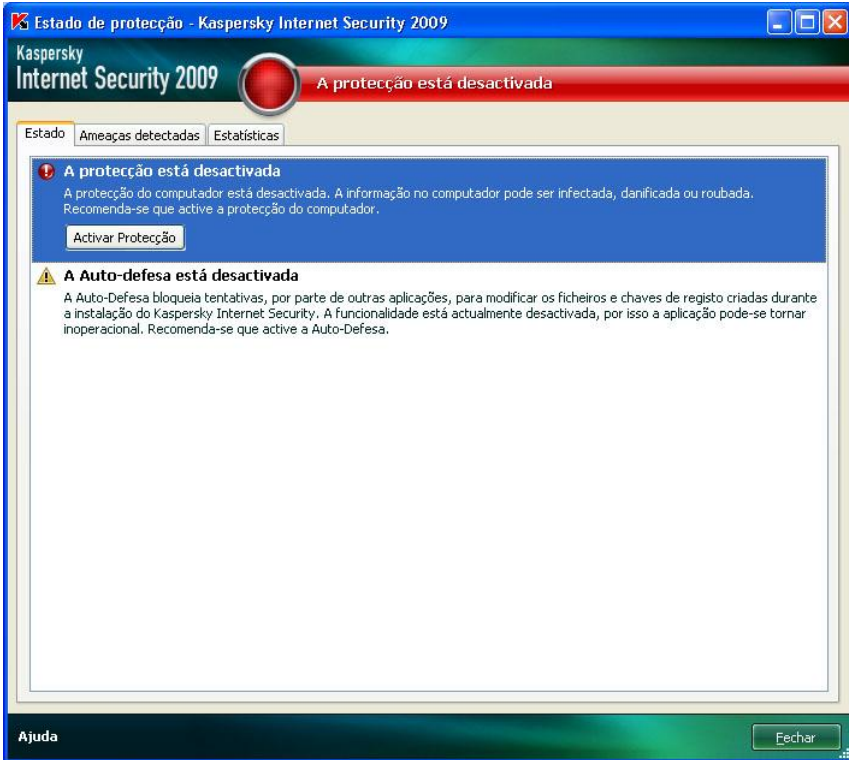


Figura 6: Resolver problemas de segurança

O separador apresenta a lista dos actuais problemas. Os problemas estão listados por ordem de importância: em primeiro, os problemas mais críticos, assinalados com o ícone de estado vermelho; em segundo, os problemas menos importantes, assinalados com o ícone de estado amarelo e, por último, as mensagens de informação, assinaladas com o ícone verde. Para cada problema é fornecida uma descrição detalhada e estão disponíveis as seguintes acções:

- *Eliminar imediatamente.* Através dos respectivos botões, você pode começar a corrigir o problema, que é a acção recomendada.

- **Adiar a eliminação.** Se, por alguma razão, não puder eliminar o problema imediatamente, você pode adiar esta acção e voltar à mesma mais tarde. Para adiar a eliminação, utilize o botão **Ocultar mensagem**.

Note que esta opção não está disponível para os problemas graves. Esses problemas incluem, por exemplo, objectos maliciosos que foram detectados mas não desinfectados, falhas de uma ou várias componentes ou a corrupção dos ficheiros da aplicação.

Para que as mensagens ocultadas voltem a aparecer na lista geral, assinale a opção **Mostrar mensagens ocultadas**.

## PAUSAR A PROTECÇÃO

Pausar a protecção significa desactivar, temporariamente, todas as componentes de protecção durante um determinado período de tempo.

► *Para pausar a protecção do seu computador:*

1. Selecciono o item **Pausar protecção** no **menu de atalho** da aplicação (ver secção "Menu de atalho" na página 48).
2. Na janela **Pausar protecção** que se abre, selecciono o período de tempo durante o qual você pretende que a protecção esteja pausada:
  - **Retomar protecção dentro de <intervalo de tempo>** – a protecção será activada após este período de tempo. Para seleccionar um intervalo de tempo, use o menu suspenso.
  - **Retomar após reinicialização do computador** – a protecção será activada depois do sistema ser reiniciado, desde que a aplicação também esteja configurada para se iniciar automaticamente quando o computador for reiniciado.
  - **Retomar manualmente** – a protecção será retomada somente depois de você a iniciar manualmente. Para activar a protecção, selecciono **Retomar protecção** a partir do menu de atalho da aplicação.

Como resultado da desactivação temporária da protecção, todas as componentes de protecção serão pausadas. Isto é indicado por:

- Nomes inactivos (a cinzento) das componentes desactivadas na secção **Protecção** da janela principal.
- Ícone da aplicação inactivo (a cinzento) (ver secção "Ícone da área de notificação" na página 47) no painel do sistema.
- Cor vermelha para o ícone de estado e para o painel da janela principal da aplicação.

Se as novas ligações de rede estavam a ser estabelecidas ao mesmo tempo que a protecção foi pausada, será apresentada uma notificação sobre a interrupção dessas ligações.

---

# VALIDAR A CONFIGURAÇÃO DA APLICAÇÃO

Depois de instalar e configurar a aplicação, deve verificar se a aplicação está correctamente configurada, usando um "vírus" de teste e variantes do mesmo. É necessário um teste separado para cada componente de protecção / protocolo.

## NESTA SECÇÃO:

---

Testar o "vírus" EICAR e suas variantes .....	68
Testar a protecção do tráfego de HTTP .....	72
Testar a protecção do tráfego de SMTP.....	72
Validar a configuração do Anti-vírus de Ficheiros .....	73
Validar a configuração das tarefas de verificação de vírus .....	74
Validar a configuração do Anti-Spam .....	74

## TESTAR O "VÍRUS" EICAR E SUAS VARIANTES

Este "vírus" de teste foi, especialmente, desenvolvido pelo **eicar** (O Instituto Europeu para Pesquisa de Antivírus de Computador) para testar os produtos anti-vírus.

O "vírus" de teste NÃO É UM VÍRUS porque não contém código que possa danificar o seu computador. Contudo, a maioria dos fabricantes de produtos anti-vírus identifica este ficheiro como um vírus.

Aviso!

Nunca use vírus reais para testar o funcionamento de um produto anti-vírus!

Pode transferir um "vírus" de teste a partir do site oficial do **EICAR**: [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).

#### Nota

Antes de transferir o ficheiro, tem de desactivar a protecção anti-vírus do computador, caso contrário a aplicação iria identificar e processar o ficheiro *anti\_virus\_test\_file.htm* como um objecto infectado transferido através do protocolo HTTP.

Não se esqueça de activar a protecção anti-vírus imediatamente depois de transferir o "vírus" de teste.

A aplicação identifica os ficheiros transferidos do site do **EICAR** como um objecto infectado que contém um vírus que **não pode ser desinfectado** e executa as acções especificadas para esse objecto.

Também pode alterar o "vírus" de teste padrão para verificar o funcionamento da aplicação contra outros tipos de ficheiros. Para alterar o "vírus", altere os conteúdos do "vírus" padrão, adicionando-lhe um dos prefixos (ver tabela que se segue). Para criar os ficheiros do "vírus" alterado, pode utilizar qualquer editor de texto ou hipertexto, como por exemplo o **Microsoft Notepad**, **UltraEdit32**, etc.

#### Aviso!

Só pode testar a adequação do funcionamento da aplicação (através do "vírus" alterado do EICAR) caso as suas bases anti-vírus tenham sido actualizadas em ou depois de 24 de Outubro de 2003 (actualizações acumuladas de Outubro, 2003).

Na tabela que se segue, a primeira coluna contém os prefixos que é necessário adicionar ao início do "vírus" de teste padrão. A segunda coluna lista os possíveis valores de estado que a aplicação pode atribuir ao objecto, com base nos resultados da verificação. A terceira coluna indica a forma como a aplicação processa os objectos com o estado especificado. Por favor, note que as acções efectivamente executadas sobre os objectos são determinadas pelas configurações da aplicação.

Depois de adicionar o prefixo ao "vírus" de teste, guarde o novo ficheiro com um nome diferente, por exemplo: *eicar\_dele.com*. Atribua nomes similares a todos os "vírus" alterados.

Tabela 6. Alterações do "vírus" de teste

Prefixo	Estado do objecto	Informação de processamento do objecto
Sem prefixo, vírus de teste padrão	<b>Infectado.</b> O objecto infectado contém código de um vírus conhecido. A desinfecção não é possível.	A aplicação identifica o objecto como um vírus não desinfectável.  Ocorre um erro ao tentar desinfetar o objecto; será aplicada a acção atribuída para execução com objectos não desinfectáveis.
CORR-	<b>Corrompido.</b>	A aplicação conseguia aceder ao objecto, mas não conseguiu verificá-lo, uma vez que o objecto está corrompido (por exemplo, a estrutura de ficheiro está corrompida ou o formato de ficheiro é inválido). Pode encontrar informação sobre a forma como o objecto foi processado no relatório de funcionamento da aplicação.
WARN-	<b>Suspeito.</b> O objecto suspeito contém código de um vírus desconhecido. A desinfecção não é possível.	O objecto foi considerado suspeito pelo analisador de código heurístico. Na altura da detecção, as bases de dados da aplicação não contêm uma descrição do procedimento para tratar este objecto. Você será notificado quando um objecto deste tipo for detectado.
SUSP-	<b>Suspeito.</b> O objecto suspeito contém código alterado de um vírus conhecido. A desinfecção não é possível.	A aplicação detectou uma correspondência parcial entre uma secção do código do objecto e uma secção de código de um vírus conhecido. Na altura da detecção, as bases de dados da aplicação não contêm uma descrição do procedimento para tratar este objecto. Você será notificado quando um objecto deste tipo for detectado.

Prefixo	Estado do objecto	Informação de processamento do objecto
ERRO-	<b>Erro de verificação.</b>	Ocorreu um erro ao verificar o objecto. A aplicação não conseguiu aceder ao objecto: ou a integridade do objecto foi violada (por exemplo, não há fim para um arquivo multi-volume) ou não existe ligação para o mesmo (se o que objecto que está a ser verificado está localizado numa unidade de rede). Pode encontrar informação sobre o processamento do objecto no relatório de funcionamento da aplicação.
CURE-	<b>Infectado.</b> O objecto infectado contém código de um vírus conhecido. Desinfectável.	O objecto contém um vírus que pode ser desinfectado. A aplicação irá desinfectar o objecto; o texto do corpo do “vírus” será substituído pela palavra CURE. Você será notificado quando um objecto deste tipo for detectado.
DELE-	<b>Infectado.</b> O objecto infectado contém código de um vírus conhecido. A desinfectação não é possível.	A aplicação identifica o objecto como um vírus não desinfectável.  Ocorre um erro ao tentar desinfectar o objecto; a acção executada será a especificada para objectos não desinfectáveis.  Você será notificado quando um objecto deste tipo for detectado.

## TESTAR A PROTECÇÃO DO TRÁFEGO DE HTTP

- ▶ *Para verificar que os vírus são detectados com sucesso em fluxos de dados transferidos através do protocolo HTTP:*

Tente transferir um "vírus" de teste a partir do site oficial do EICAR:  
[http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).

Ao tentar transferir o "vírus" de teste, o Kaspersky Internet Security irá detectar este objecto, identificá-lo como um objecto infectado que não pode ser desinfectado e irá executar a acção especificada nas configurações do tráfego HTTP para objectos com este estado. Por defeito, quando tenta transferir o "vírus" de teste, a ligação com o site será terminada e o navegador irá apresentar uma mensagem a informar o utilizador de que este objecto está infectado com o vírus EICAR-Test-File.

## TESTAR A PROTECÇÃO DO TRÁFEGO DE SMTP

Para detectar vírus em fluxos de dados transferidos através do protocolo SMTP , tem de transferir dados através de um sistema de e-mail que utiliza este protocolo.

### Nota

Recomendamos que teste a forma como o Kaspersky Internet Security processa os e-mails recebidos e enviados, incluindo quer o corpo da mensagem, quer os anexos. Para testar a detecção de vírus no corpo de mensagens, copie o texto do "vírus" de teste padrão ou do "vírus" alterado para o corpo da mensagem.

- ▶ *Para testar a detecção de vírus em fluxos de dados através de SMTP:*

1. Crie uma mensagem de formato **Texto simples**, utilizando um cliente de e-mail instalado no seu computador.

**Nota**

Uma mensagem que contenha um vírus de teste não será verificada se for criada em formato RTF ou HTML!

2. Copie o texto do “vírus” padrão ou alterado no início da mensagem ou anexe um ficheiro com o “vírus” de teste à mensagem.
3. Envie a mensagem para o administrador.

A aplicação irá detectar o objecto, identificá-lo como infectado e bloquear a mensagem.

## **VALIDAR A CONFIGURAÇÃO DO ANTI-VÍRUS DE FICHEIROS**

► *Para verificar se a componente Anti-vírus de Ficheiros está correctamente configurada:*

1. Crie uma pasta num disco e copie para essa pasta o “vírus” de teste do EICAR que transferiu e os “vírus” de teste alterados que criou.
2. Verifique que todos os eventos serão registados, para que o ficheiro de relatório retenha dados sobre objectos corrompidos e objectos não verificados devido a erros.
3. Execute o “vírus” de teste ou uma das suas versões alteradas.

O Anti-vírus de Ficheiros irá interceptar a chamada ao ficheiro, irá verificá-lo e irá executar a acção especificada nas configurações para objectos com esse estado. Ao seleccionar diferentes acções a executar sobre o objecto detectado, pode executar uma verificação completa do funcionamento da componente.

Pode ver informação sobre os resultados do funcionamento do Anti-vírus de Ficheiros no relatório da componente.

## **VALIDAR A CONFIGURAÇÃO DAS TAREFAS DE VERIFICAÇÃO DE VÍRUS**

- ▶ *Para verificar se a tarefa de verificação anti-vírus está correctamente configurada:*
  1. Crie uma pasta num disco e copie para essa pasta o “vírus” de teste do EICAR que transferiu e os “vírus” de teste alterados que criou.
  2. Crie uma nova tarefa de verificação de vírus e seleccione a pasta que contém o conjunto de “vírus” de teste como o objecto a verificar.
  3. Verifique que todos os eventos estão registados, para que o ficheiro de relatório retenha dados sobre objectos corrompidos e objectos não verificados devido a erros.
  4. Execute a tarefa de verificação de vírus.

Quando a tarefa de verificação estiver em execução, as acções especificadas na configuração da tarefa serão executadas à medida que forem detectados objectos suspeitos ou infectados. Ao seleccionar várias acções a executar sobre os objectos detectados, poderá executar uma verificação completa do funcionamento da componente.

Pode ver informação detalhada sobre as acções da tarefa no relatório de funcionamento da componente.

## **VALIDAR A CONFIGURAÇÃO DO ANTI- SPAM**

Pode usar uma mensagem de teste identificada como SPAM para testar a protecção anti-spam.

O corpo da mensagem de teste tem de conter a seguinte linha:

Spam é mau, não o envie

Quando esta mensagem é recebida no computador, a aplicação irá verificá-la, atribuir o estado “spam” à mensagem e irá executar a acção especificada para objectos deste tipo.

---

# DECLARAÇÃO DE RECOLHA DE DADOS DO KASPERSKY SECURITY NETWORK

## INTRODUÇÃO

POR FAVOR, LEIA ESTE DOCUMENTO COM ATENÇÃO. ESTE CONTÉM INFORMAÇÃO IMPORTANTE QUE DEVERÁ SABER ANTES DE CONTINUAR A UTILIZAR OS NOSSOS SERVIÇOS OU SOFTWARE. CASO CONTINUE A UTILIZAR OS SERVIÇOS E SOFTWARE DA KASPERSKY LAB, CONSIDERAR-SE-Á QUE ACEITA ESTA DECLARAÇÃO DE RECOLHA DE DADOS DA KASPERSKY LAB. Reservamos o direito de alterar esta Declaração de Recolha de Dados a qualquer altura, divulgando as alterações nesta página. Por favor, verifique a data de revisão abaixo indicada para determinar se a política foi alterada desde a última vez que a reviu. A utilização continua de qualquer parte dos Serviços da Kaspersky Lab, após terem sido divulgadas as alterações da Declaração de Recolha de Dados, será considerada como constituindo a sua aceitação das alterações.

A Kaspersky Lab e suas afiliadas (colectivamente, "**Kaspersky Lab**") criaram esta Declaração de Recolha de Dados para informar e divulgar as suas práticas de disseminação e recolha de dados para o Kaspersky Anti-Virus e Kaspersky Internet Security.

## Algumas palavras da Kaspersky Lab

A Kaspersky Lab deposita grande empenho no fornecimento de serviços de qualidade superior a todos os nossos clientes e, em especial, no respeito pelas suas preocupações relativas à Recolha de Dados. Compreendemos que poderá ter dúvidas sobre a forma como o Kaspersky Security Network recolhe e utiliza informações e dados. Por isso, preparámos esta declaração para o informar sobre os princípios da Recolha de Dados que regulam o Kaspersky Security Network (a "**Declaração de Recolha de Dados**" ou "**Declaração**").

Esta Declaração de Recolha de Dados contém inúmeros detalhes gerais e técnicos sobre as medidas que tomamos para respeitar as suas preocupações relativas à Recolha de Dados. Organizámos esta Declaração de Recolha de Dados de acordo com os principais processos e áreas, de forma a que possa rapidamente rever as informações que mais lhe interessam. A questão central é que a satisfação das suas necessidades e expectativas constitui a base de tudo o que fazemos - incluindo a protecção na Recolha dos seus Dados.

Os dados e informações são recolhidos pela Kaspersky Lab. Depois de ter revisto esta Declaração de Recolha de Dados, se tiver dúvidas ou preocupações sobre a Recolha de Dados, por favor envie um e-mail para [support@kaspersky.com](mailto:support@kaspersky.com).

### **O que é o Kaspersky Security Network?**

O serviço Kaspersky Security Network permite que os utilizadores dos produtos de segurança da Kaspersky Lab, em todo o mundo, ajudem a facilitar a identificação e a reduzir o tempo que demora a fornecer protecção contra novos riscos de segurança ("que estão à solta") direccionados ao seu computador. Para identificar as novas ameaças e suas origens e para ajudar a melhorar a segurança do utilizador e a funcionalidade do produto, o Kaspersky Security Network recolhe determinados dados de segurança e da aplicação sobre potenciais riscos de segurança direccionados ao seu computador e envia esses dados à Kaspersky Lab para análise. **Essas informações não contêm quaisquer informações pessoalmente identificáveis sobre o utilizador e são utilizadas pela Kaspersky Lab com o único propósito de melhorar os seus produtos de segurança e para fazer progredir as soluções contra ameaças e vírus maliciosos. No caso da transmissão accidental de quaisquer dados pessoais do utilizador, a Kaspersky Lab manterá e protegerá esses dados de acordo com esta Declaração de Recolha de Dados.**

Ao participar no Kaspersky Security Network, você e os outros utilizadores dos produtos de segurança da Kaspersky Lab, em todo mundo, contribuem significativamente para ambiente mais seguro na Internet.

### **Questões Legais**

O Kaspersky Security Network pode estar sujeito às leis de diversas jurisdições, uma vez que os seus serviços podem ser utilizados em diferentes jurisdições, incluindo os Estados Unidos da América. A Kaspersky Lab revelará informações pessoalmente identificáveis sem a sua autorização, quando exigido por lei ou quando acreditar, de boa-fé, que tal acção seja necessária para investigar ou proteger contra actividades danosas os hóspedes, visitantes, associados ou propriedades da Kaspersky Lab ou de outros. Tal como acima mencionado, as leis relacionadas com os dados e informações recolhidos pelo Kaspersky Security Network podem variar entre países. Por exemplo, algumas informações pessoalmente identificáveis recolhidas na União Europeia e nos seus Estados-Membros estão sujeitas às Directivas da UE relativas a dados pessoais, privacidade e comunicações electrónicas incluindo, mas não exclusivamente, a Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas e a Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à

livre circulação desses dados e as leis posteriormente adoptadas nos Estados-Membros da UE, a Decisão 2001/497/CE da Comissão Europeia relativa às cláusulas contratuais-tipo (transferência de dados pessoais para países terceiros) e as leis posteriormente adoptadas nos Estados-Membros da UE.

O Kaspersky Security Network deverá informar devidamente os utilizadores em questão, quando começar a recolher as informações acima mencionadas, sobre qualquer partilha dessas informações, nomeadamente para uso no desenvolvimento de negócios, e deverá permitir que estes utilizadores da Internet comuniquem via on-line a **opção de inclusão** (nos Estados-Membros da UE e outros países que requeiram o procedimento de inclusão) ou de exclusão (para todos os outros países) da utilização comercial destes dados e/ou da transmissão destes dados a terceiros.

A Kaspersky Lab pode ser obrigada, pelas autoridades de aplicação da lei ou judiciais, a fornecer informações pessoalmente identificáveis às autoridades governamentais adequadas. Se exigido pelas autoridades de aplicação da lei ou judiciais, forneceremos estas informações após recepção da documentação adequada. A Kaspersky Lab também pode fornecer informações às autoridades de aplicação da lei para proteger as suas propriedades e a saúde e segurança dos indivíduos, tal como permitido pelos estatutos.

As declarações às autoridades dos Estados-Membros em matéria de Protecção de Dados Pessoais serão feitas de acordo com as leis posteriormente em vigor nos Estados-Membros da UE. A informação sobre essas declarações estará acessível nos serviços do Kaspersky Security Network.

## **INFORMAÇÕES RECOLHIDAS**

### **Dados Que Recolhemos**

O serviço Kaspersky Security Network irá recolher e enviar dados centrais e alargados à Kaspersky Lab sobre potenciais riscos de segurança direccionados ao seu computador. Os dados recolhidos incluem:

#### Dados Centrais

- informação sobre o hardware e software do seu computador, incluindo o sistema operativo e service packs instalados, objectos do núcleo, controladores, serviços, extensões do Internet Explorer, extensões de impressão, extensões do Windows Explorer, ficheiros de programa transferidos, elementos de configuração activa, aplicativos do painel de controlo, registos do ficheiro anfitriões e do registo, endereços IP, tipos de navegador, clientes de e-mail e o número da versão do produto da Kaspersky Lab, que normalmente não é pessoalmente identificável;

- uma ID única que é gerada pelo produto da Kaspersky Lab para identificar máquinas individuais sem identificar o utilizador e que não contém quaisquer informações pessoais;
- informação sobre o estado da protecção anti-vírus do seu computador e dados sobre quaisquer ficheiros ou actividades suspeitos de serem maliciosos (por exemplo, nome do vírus, data/hora da detecção, nomes/caminhos e tamanho dos ficheiros infectados, endereço IP e porta do ataque de rede, nome da aplicação suspeita de ser maliciosa). Por favor, tenha em atenção que os dados recolhidos acima indicados não contêm informações pessoalmente identificáveis.

### Dados Alargados

- informação sobre aplicações digitalmente assinadas transferidas pelo utilizador (URL, tamanho do ficheiro, nome do signatário)
- Informação sobre aplicações executáveis (tamanho, atributos, data de criação, informação sobre cabeçalhos PE, região, nome, localização e utilitário de compressão utilizado).

### **Proteger a Transmissão e Armazenamento de Dados**

A Kaspersky Lab está empenhada em proteger a segurança das informações que recolhe. As informações recolhidas são armazenadas em servidores de computador com acesso limitado e controlado. A Kaspersky Lab opera redes de dados seguras protegidas por firewalls normalizadas e sistemas de protecção por password. A Kaspersky Lab utiliza uma ampla gama de tecnologias e procedimentos de segurança para proteger as informações recolhidas contra ameaças como o acesso, utilização ou divulgação não-autorizados. As nossas políticas de segurança são regularmente revistas e, se necessário, melhoradas e apenas os indivíduos autorizados têm acesso aos dados que recolhemos. A Kaspersky Lab toma medidas para garantir que as suas informações são tratadas de forma segura e de acordo com esta Declaração. Infelizmente, não é possível garantir a segurança total de qualquer transmissão de dados. Como resultado, embora nos esforcemos por proteger os seus dados, não podemos garantir a segurança de quaisquer dados que nos transmita ou a partir dos nossos produtos ou serviços, incluindo sem limitação o Kaspersky Security Network e você utiliza todos esses serviços por sua conta e risco.

Os dados que são recolhidos podem ser transferidos para os servidores da Kaspersky Lab e a Kaspersky Lab tomou as precauções necessárias para garantir que as informações recolhidas, se transferidas, recebem o nível adequado de protecção. Tratamos os dados que recolhemos como informações confidenciais. Estes são adequadamente sujeitos aos nossos procedimentos de

segurança e políticas empresariais relativas à protecção e utilização de informações confidenciais. Depois dos dados recolhidos chegarem à Kaspersky Lab, estes são armazenados num servidor com funcionalidades de segurança física e electrónica normalizadas, incluindo a utilização de procedimentos de início de sessão/password e firewalls electrónicas concebidas para bloquear o acesso não-autorizado a partir do exterior da Kaspersky Lab. Os dados recolhidos pelo Kaspersky Security Network abrangidos por esta Declaração são processados e armazenados nos Estados Unidos e possivelmente noutras jurisdições e também noutros países onde a Kaspersky Lab exerce actividade. Todos os funcionários da Kaspersky Lab estão conscientes das nossas políticas de segurança. Os seus dados só estão acessíveis aos funcionários que deles necessitam para desempenharem as suas funções. Todos os dados armazenados não serão associados a quaisquer informações pessoalmente identificáveis. A Kaspersky Lab não combina os dados armazenados pelo Kaspersky Security Network com quaisquer dados, listas de contacto ou informações de subscrição recolhidas pela Kaspersky Lab para fins promocionais ou outros.

## **UTILIZAÇÃO DOS DADOS RECOLHIDOS**

### **Como São Utilizadas As Suas Informações Pessoais**

A Kaspersky Lab recolhe os dados por forma a analisar e identificar as fontes de potenciais riscos de segurança e para melhorar a capacidade dos produtos da Kaspersky Lab na detecção de comportamentos maliciosos, sites fraudulentos, softwares criminosos e outros tipos de ameaças de segurança na Internet para fornecer o melhor nível de protecção possível aos clientes da Kaspersky Lab no futuro.

### **Divulgação de Informações a Terceiros**

A Kaspersky Lab pode revelar quaisquer informações recolhidas se tal for solicitado por um oficial responsável pela aplicação da lei, tal como exigido ou permitido por lei, ou em resposta a uma intimação ou outro processo legal ou se acreditarmos de boa-fé que o devemos fazer para cumprir com a lei, regulamento, uma intimação ou outro processo legal aplicável ou um pedido executório governamental. A Kaspersky Lab também pode revelar informações pessoalmente identificáveis quando tiver razões para acreditar que a divulgação dessa informação é necessária para identificar, contactar ou actuar legalmente contra alguém que possa estar a violar esta Declaração, os termos dos seus acordos com a Empresa ou para proteger a segurança dos nossos utilizadores e do público ou ao abrigo de acordos de confidencialidade e licenciamento com determinados terceiros que nos dão assistência no desenvolvimento, operação e manutenção do Kaspersky Security Network. Para promover o conhecimento, detecção e prevenção dos riscos de segurança na Internet, a Kaspersky Lab pode partilhar determinadas informações com organizações de investigação e outros fornecedores de software de segurança. A Kaspersky Lab também pode

utilizar as estatísticas derivadas das informações recolhidas para controlar e publicar relatórios sobre a evolução dos riscos de segurança.

### **As escolhas à sua disposição**

A participação no Kaspersky Security Network é opcional. Você pode activar e desactivar o serviço Kaspersky Security Network em qualquer altura, acedendo às configurações da Informação de Retorno na página de opções do seu produto da Kaspersky Lab. Contudo, por favor tenha em atenção que se escolher ocultar as informações ou dados solicitados, poderemos não ser capazes de lhe fornecer alguns dos serviços dependentes da recolha desses dados.

Depois de terminar o período de serviço do seu produto da Kaspersky Lab, algumas das funções do software da Kaspersky Lab podem continuar a funcionar, mas as informações deixarão de ser, automaticamente, enviadas para a Kaspersky Lab.

Também reservamos o direito de enviar mensagens de alerta esporádicas aos utilizadores para os informar sobre alterações específicas que possam afectar a sua capacidade para utilizar os nossos serviços que subscreveram previamente. Também reservamos o direito de o contactar se a tal formos obrigados como parte de um procedimento legal ou se tiver ocorrido uma violação de quaisquer acordos aplicáveis de licenciamento, garantia e compra.

A Kaspersky Lab conserva estes direitos porque, em casos limitados, sentimos que poderemos necessitar do direito de contactá-lo por questões legais ou em relação a assuntos que podem ser importantes para si. Estes direitos não nos permitem contactá-lo para comercializar serviços novos ou já existentes, caso nos tenha solicitado para não o fazermos, e a emissão destes tipos de comunicação é rara.

### **RECOLHA DE DADOS – PEDIDOS E RECLAMAÇÕES RELACIONADAS**

A Kaspersky Lab recebe e trata, com o máximo respeito e atenção, as preocupações dos seus utilizadores sobre a Recolha de Dados. Se detectar alguma situação de incumprimento desta Declaração, no que respeita aos seus dados e informações, ou se tiver outros pedidos ou preocupações relacionadas, pode escrever ou contactar a Kaspersky Lab através do e-mail: [support@kaspersky.com](mailto:support@kaspersky.com).

Na sua mensagem, por favor descreva, o mais detalhadamente possível, a natureza do seu pedido. Investigaremos o seu pedido ou reclamação com a maior rapidez possível.

O fornecimento de informações é voluntário. Uma opção de recolha de dados pode ser desactivada pelo utilizador, a qualquer altura, na secção "**Informação**

**de Retorno**" na página "**Configuração**" de qualquer produto Kaspersky adequado.

Direitos de Autor © 2008 Kaspersky Lab. Todos os direitos reservados.

---

# KASPERSKY LAB

Fundada em 1997, a Kaspersky Lab tornou-se num líder reconhecido nas tecnologias de segurança de informação. Produz uma ampla gama de software de alta performance para segurança de dados, incluindo sistemas anti-vírus, anti-spam e anti-hackers.

A Kaspersky Lab é uma empresa internacional. Centralizada na Federação Russa, a empresa tem filiais no Reino Unido, França, Alemanha, Japão, Benelux, China, Polónia, Roménia e EUA (Califórnia). Um novo escritório da empresa, o Centro Europeu de Pesquisa Anti-vírus, 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 450 especialistas altamente qualificados, dos quais 10 têm graduações M.B.A. e 16 têm doutoramentos. Vários especialistas 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. Uma análise detalhada das actividades dos vírus de computador permite aos especialistas da empresa prever as tendências de desenvolvimento de software malicioso e fornecer aos nossos utilizadores uma protecção atempada contra novos tipos de ataques. A resistência a ataques futuros é a política de base implementada em todos os produtos da Kaspersky Lab. Em qualquer altura, os produtos da empresa permanecem um passo à frente de muitos outros vendedores no fornecimento de uma cobertura anti-vírus extensiva aos nossos clientes.

Anos de árduo trabalho tornaram a empresa num dos melhores fabricantes de software anti-vírus. A Kaspersky Lab foi uma das primeiras companhias do seu género a desenvolver inúmeras normas modernas de software anti-vírus. O produto emblemático da empresa, o Kaspersky Internet Security, fornece uma protecção total para todos os níveis da rede: estações de trabalho, servidores de ficheiros, sistemas de correio electrónico, firewalls, gateways de Internet e computadores portáteis. As suas ferramentas de gestão adequadas e intuitivas maximizam o nível de automação da protecção anti-vírus para computadores e redes empresariais. Muitos fabricantes conhecidos usam o núcleo do Kaspersky Internet Security, incluindo a Nokia ICG (EUA), F-Secure (Finlândia), 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, como a conformidade com as necessidades de negócio específicas dos clientes. Concebemos, implementamos e apoiamos sistemas anti-vírus empresariais. A base de dados anti-vírus da Kaspersky Lab é actualizada a cada hora. A empresa fornece aos seus clientes um serviço de suporte técnico de 24 horas, que está disponível em várias línguas.

Se tiver quaisquer questões, pode contactar os nossos distribuidores ou contactar, directamente, a Kaspersky Lab. São fornecidas consultas detalhadas por telefone ou e-mail. Receberá respostas completas e abrangentes a qualquer questão.

Morada:	Rússia, 123060, Moscovo, 1-st Volokolamsky Proezd, 10, Building 1
Tel., Fax:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00
Suporte de Emergência (24 horas por dia, 365 dias por ano):	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08
Suporte para utilizadores de produtos empresariais:	+7 (495) 797-87-07, +7 (495) 645-79-29, +7 (495) 956-87-08 (das 10 às 19h)  <a href="http://support.kaspersky.pt">http://support.kaspersky.pt</a>
Suporte para utilizadores empresariais:	Ser-lhe-á fornecida a informação de contacto depois de adquirir um produto de software empresarial, dependendo do seu pacote de suporte.
Fórum na Internet da Kaspersky Lab:	<a href="http://forum.kaspersky.com">http://forum.kaspersky.com</a>
Laboratório Anti-vírus:	<a href="mailto:newvirus@kaspersky.com">newvirus@kaspersky.com</a>  (apenas para enviar novos vírus em arquivos)
Grupo de desenvolvimento de documentação para o utilizador:	<a href="mailto:docfeedback@kaspersky.com">docfeedback@kaspersky.com</a>  (apenas para enviar informação de retorno sobre a documentação e o sistema de Ajuda)

Departamento de Vendas:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00  <a href="mailto:ventas@kaspersky.es">ventas@kaspersky.es</a>
Informação Geral:	+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00  <a href="mailto:info@kaspersky.com">info@kaspersky.com</a>
WWW:	<a href="http://www.kaspersky.pt/">http://www.kaspersky.pt/</a>  <a href="http://www.viruslist.com">http://www.viruslist.com</a>

---

# CRYPTOEX LLC

Para criar e verificar as assinaturas digitais, o Kaspersky Internet Security utiliza a biblioteca de software de segurança de dados Crypto C desenvolvida pela Crypto Ex LLC.

A Crypto Ex detém uma licença da Agência Federal de Informações e Comunicações Governamentais (FSB - Serviço Federal de Segurança) para desenvolver, produzir e distribuir software de encriptação para a protecção de dados que não constituam segredo de estado.

A biblioteca Crypto C foi concebida para proteger informação confidencial de classe KS1 e obteve o certificado de conformidade do FSB n.º SF/114-0901 de 1 de Julho de 2006.

A biblioteca permite a encriptação e desencriptação de pacotes de dados e/ou fluxos de dados de tamanho fixo, através das seguintes tecnologias:

- um algoritmo criptográfico (GOST 28147-89);
- algoritmos para gerar e verificar assinaturas digitais electrónicas (GOST R 34.10-94 and GOST 34.10-2001);
- funções hash (GOST 34.11-94);
- geração de informações-chave através de um transmissor de números pseudo-aleatórios;
- um sistema de geração de informações-chave e de vectores de simulação (GOST 28147-89).

Os módulos da biblioteca foram implementados através da linguagem de programação ANSI-C e podem ser integrados em aplicações, como um código estática e dinamicamente carregado. Podem ser executados numa série de plataformas, incluindo x86, x86-64, Ultra SPARC II e plataformas compatíveis.

É possível executar a migração dos módulos da biblioteca para os seguintes sistemas operativos: Microsoft Windows NT/XP/98/2000/2003, Unix (Linux, FreeBSD, SCO Open Unix 8.0, SUN Solaris, SUN Solaris for Ultra SPARC II).

Para mais informação, consulte o site empresarial da CryptoEx LLC:  
<http://www.cryptoex.ru>, ou contacte a empresa através do e-mail:  
[info@cryptoex.ru](mailto:info@cryptoex.ru)

---

# MOZILLA FOUNDATION

A biblioteca **Gecko SDK ver. 1.8** foi utilizada para o desenvolvimento das componentes desta aplicação.

Este software é utilizado segundo os termos e condições da licença MPL 1.1 Licença Pública da Mozilla Foundation <http://www.mozilla.org/MPL>.

Para mais detalhes sobre a biblioteca Gecko SDK, consulte: [http://developer.mozilla.org/en/docs/Gecko\\_SDK](http://developer.mozilla.org/en/docs/Gecko_SDK).

© Mozilla Foundation

Site da Mozilla Foundation: <http://www.mozilla.org>.

---

# CONTRATO DE LICENÇA

Contrato Padrão de Licença de Utilizador Final

AVISO A TODOS OS UTILIZADORES: LEIA CUIDADOSAMENTE O SEGUINTE CONTRATO LEGAL ("CONTRATO") PARA A LICENÇA DO KASPERSKY INTERNET SECURITY ("SOFTWARE") PRODUZIDO PELA KASPERSKY LAB ("KASPERSKY LAB").

SE COMPROU ESTE SOFTWARE PELA INTERNET CLICANDO NO BOTÃO PARA ACEITAR, VOCÊ (TANTO COMO INDIVÍDUO OU COMO ENTIDADE LEGAL ÚNICA) CONSENTE EM ACEITAR E A SER PARTE DESTE CONTRATO. SE NÃO CONCORDAR COM TODOS OS TERMOS DESTE CONTRATO, CLIQUE NO BOTÃO QUE INDICA QUE NÃO ACEITA OS TERMOS DESTE CONTRATO E NÃO INSTALE O SOFTWARE.

SE TIVER COMPRADO ESTE SOFTWARE NUM MEIO FÍSICO, TIVER ROMPIDO O ENVELOPE DO CD VOCÊ (TANTO COMO INDIVÍDUO OU COMO ENTIDADE LEGAL ÚNICA) CONSENTE EM ACEITAR ESTE CONTRATO. SE NÃO CONCORDAR COM TODOS OS TERMOS DESTE CONTRATO NÃO ROMPA O ENVELOPE DO CD, NEM TRANSFIRA, INSTALE OU USE ESTE SOFTWARE.

SEGUNDO A LEGISLAÇÃO, REFERENTE AO SOFTWARE KASPERSKY DESTINADO A UTILIZADORES INDIVIDUAIS E ADQUIRIDO NO SITE DA KASPERSKY LAB OU DO SEU PARCEIRO, O CLIENTE TERÁ UM PERÍODO DE CATORZE (14) DIAS ÚTEIS DESDE A ENTREGA DO PRODUTO PARA O DEVOLVER AO COMERCIANTE PARA TROCA OU REEMBOLSO, DESDE QUE ESTE SOFTWARE NÃO TENHA O SELO DESTRUÍDO.

RELATIVAMENTE AO SOFTWARE KASPERSKY DESTINADO A CONSUMIDORES INDIVIDUAIS, NÃO ADQUIRIDO ATRAVÉS DA INTERNET, ESTE SOFTWARE NÃO PODE SER DEVOLVIDO NEM TROCADO, EXCEPTO EM CASO DE CONSIDERAÇÕES EM CONTRÁRIO PELO PARCEIRO QUE VENDE O PRODUTO. NESTE CASO, A KASPERSKY LAB NÃO FICA ABRANGIDA PELAS CLÁUSULAS DO PARCEIRO.

O DIREITO A DEVOLUÇÃO E REEMBOLSO ABRANGE APENAS O COMPRADOR ORIGINAL.

Todas as referências a "Software" aqui feitas deverão incluir o código de activação do Software que lhe será fornecida pela Kaspersky Lab como parte do Kaspersky Internet Security.

1. *Concessão de Licença.* Sujeito ao pagamento de taxas de licença aplicáveis, e sujeito aos termos e condições deste Contrato, a Kaspersky Lab concede-lhe por este meio o direito não-exclusivo e intransmissível a usar o Software e a documentação que o acompanha (a "Documentação") para o termo deste Contrato, apenas para os fins internos de negócio. Poderá instalar uma cópia do Software num computador.

1.1 *Utilização.* Se comprou o Software num meio físico, você tem o direito a usar o Software para a protecção desse número de computadores, tal como indicado na caixa. Se comprou o software pela Internet, você tem o direito a usar o Software para a protecção desse número de computadores, tal como encomendou quando comprou o Software.

1.1.1 O Software está "em utilização" num computador quando estiver carregado na memória temporária (ou seja, memória de acesso aleatório ou RAM) ou instalado na memória permanente (por exemplo, disco rígido, CD-ROM, ou outro meio de armazenamento) desse computador. Esta licença autoriza-o a fazer apenas as cópias de segurança necessárias do Software para o seu uso legal e apenas para fins de cópia de segurança, desde que todas essas cópias contenham todos os avisos proprietários do Software. Deverá manter registos do número e localização de todas as cópias do Software e documentação e tomar todas as precauções razoáveis para proteger o Software de cópias ou utilização não-autorizadas.

1.1.2 O Software protege o computador em relação a vírus e ataques de rede cujas assinaturas estão contidas nas bases de dados de assinaturas de ameaças e de ataques de rede que estão disponíveis nos servidores de actualização da Kaspersky Lab.

1.1.3 Se vender o computador onde o Software está instalado, deverá assegurar que todas as cópias do Software foram previamente apagadas.

1.1.4 Não deve descompilar, proceder a engenharia reversa, desmontar ou reduzir de outro modo qualquer parte deste Software numa forma humanamente legível nem permitir que terceiros o façam. A interface de informação necessária para obter interoperacionalidade do Software com programas de computador criados independentemente será fornecida pela Kaspersky Lab a pedido mediante pagamento dos seus custos razoáveis e despesas de obtenção e fornecimento dessa informação. Caso a Kaspersky Lab o notifique de que não pretende tornar essa informação disponível por qualquer razão, incluindo (sem limitação) os custos, ser-lhe-á permitido efectuar esses passos para obter interoperacionalidade, desde que apenas proceda a engenharia reversa ou descompile o Software na medida permitida por lei.

1.1.5 Não deverá executar correcções de erros, ou modificar de outro modo, adaptar, ou traduzir o Software, nem criar trabalhos derivativos do Software,

nem permitir a terceiros copiar o Software (além do aqui expressamente permitido).

1.1.6 Não deve alugar, ceder em leasing ou emprestar o Software a qualquer outra pessoa, nem transferir ou sublicenciar os seus direitos de licença a qualquer pessoa.

1.1.7 Não deve fornecer o código de activação ou ficheiro da chave de licença a terceiros ou permitir que terceiros tenham acesso ao código de activação ou chave de licença. O código de activação ou chave de licença são dados confidenciais.

1.1.8 A Kaspersky Lab pode pedir-lhe para instalar a última versão do Software (a última versão e o último pacote de manutenção).

1.1.9 Não deve usar o Software em ferramentas automáticas, semi-automáticas ou manuais concebidas para criar assinaturas de vírus, rotinas de detecção de vírus, quaisquer outros dados ou código para detecção de código malicioso ou dados.

1.1.10 A Kaspersky Lab, com o seu consentimento explicitamente confirmado na respectiva Declaração, tem o direito de recolher informações sobre potenciais ameaças e vulnerabilidades a partir do seu computador. As informações assim recolhidas são utilizadas de forma genérica com o único propósito de melhorar os produtos da Kaspersky Lab.

## 2. Suporte <sup>1</sup>.

- (i) A Kaspersky Lab fornecer-lhe-á os serviços de suporte ("Serviços de Suporte"), tal como está definido abaixo, por um período especificado no Ficheiro de Chave de Licença (período de serviço) e indicado na janela "Serviço", a partir do momento da activação:
  - (a) pagamento do montante para suporte (em vigor no momento em questão) e:

---

<sup>1</sup> Quando utilizar o software de demonstração, não tem direito ao Suporte Técnico especificado na Cláusula 2 deste CLUF, nem tem direito a vender a cópia que possui a outras partes.

Tem direito a utilizar o software para efeitos de demonstração pelo período de tempo especificado no ficheiro de chave de licença, a contar do momento de activação (este período pode ser visualizado na janela Serviço da Interface Gráfica do Utilizador do software).

- (b) preenchimento com êxito do Formulário de Subscrição dos Serviços de Suporte, tal como lhe foi fornecido por este Contrato ou como está disponível no site da Kaspersky Lab, o qual implicará o preenchimento do código de activação que também lhe foi fornecido pela Kaspersky Lab com este Contrato. Deverá ser feito com descrição absoluta da Kaspersky Lab, quer tenha ou não satisfeito esta condição para o fornecimento de Serviços de Suporte.

Os Serviços de Suporte estarão disponíveis após a activação do software. O serviço de suporte técnico da Kaspersky Lab também tem o direito de lhe pedir um registo adicional para atribuição de identificação para fornecimento de Serviços de Suporte.

Até à activação do software e/ou obtenção da identificação de utilizador final (Identificação de Cliente), o suporte técnico apenas fornece apoio na activação de software e registo do Utilizador Final.

- (ii) Os Serviços de Suporte terminarão a menos que sejam renovados anualmente através do pagamento do montante anual para suporte (em vigor no momento em questão) e do preenchimento do Formulário de Subscrição dos Serviços de Suporte.

- (iii) "Serviços de Suporte" significa:

- (a) Actualizações regulares da base de dados anti-vírus;
- (b) Actualizações da base dados de ataques de rede;
- (c) Actualizações da base dados do anti-spam;
- (d) Actualizações livres de software, incluindo actualizações de versão;
- (e) Suporte técnico alargado por e-mail e linha telefónica fornecida pelo vendedor e/ou representante;
- (f) Actualizações de detecção de vírus e desinfecção durante 24 horas por dia.

- (iv) Os Serviços de Suporte são fornecidos apenas se e quando possuir a última versão do Software (incluindo pacotes de manutenção) instalada no seu computador, tal como está disponível no site oficial da Kaspersky Lab ([www.kaspersky.com](http://www.kaspersky.com)).

3. *Direitos de Propriedade.* O Software está protegido por direitos de autor. A Kaspersky Lab e seus fornecedores detêm e retêm todos os direitos, títulos e interesses em e para o Software, incluindo todos os direitos de autor, patentes, marcas registadas e outros direitos de propriedade intelectual aqui previstos. A sua posse, instalação, ou utilização do Software não transfere para si qualquer direito à propriedade intelectual do Software, e não adquire quaisquer direitos sobre o Software, excepto os definidos neste Contrato.

4. *Confidencialidade.* Concorde que o software e a documentação, incluindo o design específico e estrutura dos programas individuais, constituem informação confidencial exclusiva da Kaspersky Lab. Não deve revelar, fornecer ou disponibilizar essa informação confidencial sob qualquer forma a terceiros sem o consentimento prévio da Kaspersky Lab. Deverá implementar medidas razoáveis de segurança para proteger essa informação confidencial, mas sem limitação ao exposto deverá adotar as melhores medidas para manter a segurança do código de activação.

5. *Garantia limitada.*

- (i) A Kaspersky Lab garante que, pelos (6) meses desde a primeira transferência ou instalação do Software adquirido num meio físico, este deverá funcionar substancialmente em consonância com a funcionalidade descrita na Documentação quando for adequadamente utilizado e do modo especificado na Documentação.
- (ii) Você aceita toda a responsabilidade pela selecção deste Software para obedecer aos seus requisitos. A Kaspersky Lab não garante que o Software e/ou a Documentação seja apropriada a esses requisitos nem que qualquer uso seja ininterrupto ou livre de erros.
- (iii) A Kaspersky Lab não garante que este software identifique todos os vírus conhecidos e cartas de spam, nem que o Software não aponte eventualmente um vírus erradamente num título não infectado por esse vírus.
- (iv) A sua única solução e toda a responsabilidade da Kaspersky Lab pela quebra da garantia no parágrafo (i) será opção da Kaspersky Lab, para reparar, trocar ou reembolsar o Software se for relatado à Kaspersky Lab ou sua designada durante o período de garantia. Deverá fornecer toda a informação consoante o necessário para ajudar o Fornecedor a resolver o item defeituoso.
- (v) A garantia referida no parágrafo (i) não se aplicará se você tiver (a) feito ou causado quaisquer modificações a este software sem o consentimento da Kaspersky Lab, (b) usar o Software de um modo para o qual não foi destinado, ou (c) usar o Software para além do permitido neste Contrato.
- (vi) As garantias e condições definidas neste Contrato sobrepõem-se a todas as outras condições, garantias ou outros termos respeitantes ao fornecimento ou intenção de fornecimento, falta de fornecimento ou atraso em fornecer o Software ou a documentação que deveria, mas para este parágrafo (vi) tem efeito entre a Kaspersky Lab e o cliente ou seria de outro modo implicado ou incluído neste Contrato ou qualquer contrato colateral, quer por estatuto, lei comum ou de outra forma, todos aqui excluídos (incluindo, sem limitação, as condições implicadas, garantias ou outros termos como qualidade satisfatória, capacidade para o fim adequado ou como utilização de conhecimento e cuidado razoável).

## 6. Limitação de responsabilidade.

- (i) Nada neste Contrato deverá excluir ou limitar a responsabilidade da Kaspersky Lab por (a) prejuízo de fraude, (b) morte ou acidente pessoal causado pela sua quebra de dever comum legal de cuidado ou qualquer quebra negligente de um termo deste Contrato, ou (c) qualquer outra responsabilidade que não possa ser excluída por lei.
- (ii) Sujeito ao parágrafo (i) acima, a Kaspersky Lab não terá nenhuma responsabilidade (seja em contrato, prejuízo, restituição ou de outra forma) por qualquer dos seguintes prejuízos ou danos (quer esses prejuízos ou danos sejam previstos, previsíveis, conhecidos ou em contrário):
  - (a) Perda de rendimento;
  - (b) Perda actual ou antecipada de lucros (incluindo perda de lucros em contratos);
  - (c) Perda da utilidade do dinheiro;
  - (d) Perda de economias antecipadas;
  - (e) Perda de negócio;
  - (f) Perda de oportunidade;
  - (g) Perda de valor da empresa;
  - (h) Perda de reputação;
  - (i) Perda de, danos a ou corrupção de dados, ou:
  - (j) Qualquer perda indirecta ou em consequência ou danos de alguma forma provocados (incluindo, para evitar dúvida, onde tal perda ou dano é do tipo especificado nos parágrafos (ii), (a) a (ii), (i).
- (iii) Sujeito ao parágrafo (i) acima, a responsabilidade da Kaspersky Lab (quer seja em contrato, prejuízo, restituição ou noutra forma) resultante de ou em ligação com o fornecimento do Software não pode em caso algum exceder uma soma igual ao montante pago igualmente por si pelo Software.

7. Este Contrato contém o acordo completo entre as partes no que respeita à matéria de assunto aqui referida e sobrepõe-se a todo e qualquer acordo prévio, compromissos e promessas entre si e a Kaspersky Lab, quer orais ou por escrito, que foram concedidas ou podem estar implicadas por qualquer acto escrito ou dito em negociações entre nós ou o nosso representante antes deste Contrato, e todos os contratos prévios entre as partes relacionadas com os assuntos anteriormente referidos deverão cessar para ter efeito desde a Data Efectiva.