Kaspersky Internet Security

Manual de utilizador

VERSÃO DA APLICAÇÃO: 14.0

Estimado utilizador,

Obrigado por escolher o nosso produto. Esperamos que este documento auxilie o desempenho das suas funções e que forneça respostas relativamente a este produto de software.

Data de revisão do documento: 03-06-2013

http://www.kaspersky.pt
http://www.kaspersky.com/pt/tech_support/

ÍNDICE

SOBRE ESTE MANUAL

Este documento é o Manual do Utilizador do Kaspersky Internet Security.

Para uma utilização adequada do Kaspersky Internet Security, deverá estar familiarizado com a interface do sistema operativo que utiliza, conhecer as principais técnicas específicas desse sistema, saber utilizar o e-mail e a Internet.

Este manual destina-se ao seguinte:

- Ajudá-lo a instalar, activar e utilizar o Kaspersky Internet Security.
- Assegurar uma procura rápida de informações acerca de questões relacionadas com a aplicação.
- Descrever fontes adicionais de informações acerca da aplicação e formas de receber Suporte Técnico.

NESTA SECÇÃO

NESTE MANUAL

Este documento inclui as seguintes secções.

Fontes de informação sobre a aplicação

Esta secção descreve fontes de informação acerca da aplicação e apresenta uma lista de sites que pode utilizar para discutir o funcionamento da aplicação.

Kaspersky Internet Security

Esta secção descreve as funcionalidades da aplicação e fornece informação resumida sobre as funções e componentes da mesma. Ficará a saber quais os itens incluídos no kit de distribuição e quais os serviços que estão disponíveis para os utilizadores registados da aplicação. Esta secção fornece informação acerca dos requisitos de software e hardware que o computador deve cumprir para permitir que o utilizador instale a aplicação no mesmo.

Instalar e remover a aplicação

Esta secção contém instruções detalhadas para a instalação e remoção da aplicação.

Licenciamento da aplicação

Esta secção fornece informação acerca dos termos gerais relacionados com a activação da aplicação. Leia esta secção para saber mais sobre o objectivo do Contrato de Licença do Utilizador Final, as formas de activação da aplicação e a renovação da licença.

Resolver tarefas típicas

Esta secção contém instruções detalhadas para realizar tarefas de utilizador típicas fornecidas pela aplicação.

Contactar o Suporte Técnico

Esta secção fornece informação sobre como contactar o Suporte Técnico da Kaspersky Lab.

Glossário

Esta secção contém uma lista de termos referidos no documento e as suas respectivas definições.

Kaspersky Lab ZAO

Esta secção fornece informação acerca da Kaspersky Lab.

Informação acerca de código de terceiros

Esta secção fornece informação acerca da utilização de código de terceiros na aplicação.

Avisos de marcas comerciais

Esta secção indica as marcas comerciais de terceiros que são utilizadas no documento.

Índice

Esta secção permite-lhe encontrar rapidamente a informação necessária no documento.

CONVENÇÕES DE DOCUMENTOS

O texto do documento é acompanhado por elementos semânticos aos quais é recomendável dar atenção especial: avisos, sugestões e exemplos.

As convenções de documentos são utilizadas para destacar os elementos semânticos. A tabela que se segue apresenta convenções de documentos e exemplos da sua utilização.

Table 1. Convenções de documentos

TEXTO DE AMOSTRA	DESCRIÇÃO DAS CONVENÇÕES DO DOCUMENTO
Note que...	Os avisos são destacados a vermelho e são apresentados dentro de caixas. Os avisos fornecem informações sobre possíveis acções não pretendidas que podem originar perda de dados, falhas na utilização do equipamento ou problemas no sistema operativo.
É recomendado utilizar...	As notas aparecem dentro de caixas. As notas podem conter sugestões úteis, recomendações, valores específicos para as definições ou casos especiais importantes na utilização da aplicação.
Exemplo: ...	Os exemplos são apresentados num fundo amarelo e com o título "Exemplo".

TEXTO DE AMOSTRA	DESCRIÇÃO DAS CONVENÇÕES DO DOCUMENTO
Actualização significa... A ocorrência do evento *Bases de dados estão desactualizadas*.	Os seguintes elementos semânticos aparecem em itálico no texto: • Novos termos • Nomes dos estados das aplicações e eventos
Prima **ENTER**. Prima **ALT**+**F4**.	Os nomes das teclas do teclado são apresentados a negrito e em maiúsculas. Os nomes das teclas que estão ligados por um sinal + (adição) indicam a utilização de uma combinação de teclas. Essas teclas têm de ser premidas em simultâneo.
Clique no botão **Activar**.	Os nomes dos elementos da interface da aplicação, como os campos de registo, os itens de menu e os botões, aparecem a negrito.
➡ *Para configurar um agendamento de tarefas:*	As frases introdutórias das instruções estão em itálico e assinaladas com uma seta.
Na linha de comandos, introduza help. Aparece então a seguinte mensagem: Especifique a data no formato dd/mm/aa.	Os seguintes tipos de conteúdo de texto aparecem com um tipo de letra especial: • Texto na linha de comandos • O texto das mensagens que a aplicação apresenta no ecrã • Dados que o utilizador deve introduzir.
<Nome de utilizador>	As variáveis aparecem entre parênteses angulares. Em alternativa à variável, insira o valor correspondente, não incluindo os parêntesis angulares.

FONTES DE INFORMAÇÃO SOBRE A APLICAÇÃO

Esta secção descreve fontes de informação acerca da aplicação e apresenta uma lista de sites que pode utilizar para discutir o funcionamento da aplicação.

Pode seleccionar a fonte de informação mais adequada, dependendo do nível de importância e urgência da questão.

NESTA SECÇÃO

FONTES DE INFORMAÇÃO PARA PESQUISA INDEPENDENTE

Pode utilizar as seguintes fontes de informação efectuar pesquisas de forma autónoma:

- A página da aplicação no site da Kaspersky Lab
- A página da aplicação no site de Suporte Técnico (Base de Conhecimento)
- Ajuda online
- Documentação

Se não conseguir solucionar o problema, recomendamos contactar o Suporte Técnico da Kaspersky Lab (consulte a secção "Suporte técnico por telefone" na página 76).

É necessária uma ligação à Internet para utilizar as fontes de informação no site da Kaspersky Lab.

A página da aplicação no site da Kaspersky Lab

O site da Kaspersky Lab dispõe de uma página individual para cada aplicação.

Numa página (http://www.kaspersky.com/pt/kaspersky_internet_security), pode visualizar informações gerais acerca de uma aplicação, as suas funções e funcionalidades.

A página inclui uma ligação para a eLoja. Aqui pode adquirir ou renovar a aplicação.

A página da aplicação no site de Suporte Técnico (Base de Conhecimento)

A Base de Conhecimento é uma secção do site do Suporte Técnico que fornece aconselhamento sobre a utilização das aplicações da Kaspersky Lab. A Base de Conhecimento contém artigos de referência agrupados por tópicos.

Na página da aplicação na Base de Conhecimento (http://support.kaspersky.com/kis2013), pode ler artigos que fornecem informações e recomendações úteis, assim como respostas para perguntas frequentes acerca de como adquirir, instalar e utilizar a aplicação.

Os artigos podem fornecer respostas para questões fora do âmbito do Kaspersky Internet Security, as quais estão relacionadas com outras aplicações da Kaspersky Lab. Podem também conter notícias do Suporte Técnico.

Ajuda online

A ajuda online da aplicação inclui ficheiros de ajuda.

A ajuda de contexto fornece informações acerca de cada janela da aplicação, listando e descrevendo as definições correspondentes e uma lista de tarefas.

A Ajuda completa fornece informações sobre a gestão da protecção do computador, a configuração da aplicação e a resolução de tarefas típicas do utilizador.

Documentação

O manual de utilizador da aplicação fornece informações sobre como instalar, activar e configurar a aplicação, assim como dados de funcionamento da aplicação. O documento também descreve a interface da aplicação e fornece formas de resolver as tarefas típicas do utilizador ao trabalhar com a aplicação.

DISCUTIR AS APLICAÇÕES DA KASPERSKY LAB NO FÓRUM

Se a sua questão não requer uma resposta imediata, pode discuti-la com os especialistas da Kaspersky Lab e com outros utilizadores no nosso Fórum (http://forum.kaspersky.com).

Neste fórum, pode visualizar os tópicos existentes, deixar os seus comentários e criar novos tópicos de debate.

CONTACTAR O DEPARTAMENTO DE VENDAS

Se tiver alguma questão sobre como seleccionar, adquirir ou renovar a aplicação, pode contactar os especialistas do nosso Departamento de Vendas através de uma das seguintes formas:

- Por telefone (http://www.kaspersky.com/pt/contacts).
- Enviando uma mensagem com a sua questão para retail@kaspersky.pt.

O serviço é fornecido em russo e em inglês.

CONTACTAR O DEPARTAMENTO DE DOCUMENTAÇÃO TÉCNICA E LOCALIZAÇÃO POR E-MAIL

Para entrar em contacto com o Departamento de Documentação Técnica e Localização, envie um e-mail para docfeedback@kaspersky.com. Utilize "Kaspersky Help Feedback: Kaspersky Internet Security" como a linha de assunto na sua mensagem.

KASPERSKY INTERNET SECURITY

Esta secção descreve as funcionalidades da aplicação e fornece informação resumida sobre as funções e componentes da mesma. Ficará a saber quais os itens incluídos no kit de distribuição e quais os serviços que estão disponíveis para os utilizadores registados da aplicação. Esta secção fornece informação acerca dos requisitos de software e hardware que o computador deve cumprir para permitir que o utilizador instale a aplicação no mesmo.

NESTA SECÇÃO

O QUE HÁ DE NOVO

O Kaspersky Internet Security fornece as seguintes funcionalidades novas:

- Para aumentar a segurança das aplicações, foi adicionado o modo Aplicações confiáveis. Quando o modo Aplicações confiáveis está activado, o Kaspersky Internet Security detecta automaticamente as aplicações seguras e permite executar apenas as aplicações seguras.
- A funcionalidade Pagamento Seguro foi melhorada. Pode agora seleccionar um navegador da Internet para abrir os sites de bancos ou sistemas de pagamentos. A lista de sites populares para operações financeiras com activação automática do modo Pagamento Seguro foi também adicionada.
- A funcionalidade Controlo Parental também foi melhorada: a opção de definir permissões para executar jogos e aplicações foi adicionada. Foram adicionados modelos predefinidos das definições de Controlo Parental adequadas à idade dos utilizadores controlados.
- Agora é mais fácil configurar o Kaspersky Internet Security. Agora, apenas as definições das aplicações utilizadas frequentemente estão disponíveis para configuração.
- São agora suportadas as versões mais recentes dos navegadores mais populares: os componentes de protecção (por exemplo Conselheiro de URLs da Kaspersky, Pagamento Seguro) são compatíveis com Mozilla™ Firefox™ 16.x, 17.x, 18.x, e 19.x; Internet Explorer® 8, 9, e 10; e Google Chrome™ 22.x, 23.x, 24.x, 25.x, e 26.x.
- Foi adicionada protecção contra programas de bloqueio de ecrã. Pode desbloquear o ecrã utilizando o atalho de tecla especificado. A protecção contra programas de bloqueio de ecrã detecta e elimina a ameaça.
- A protecção contra phishing está mais eficaz: a funcionalidade Anti-Phishing foi melhorada e actualizada.
- O desempenho da aplicação foi melhorado e o consumo de recursos do computador foi optimizado.
- Foi adicionado o modo de actividade limitada quando o computador está inactivo. Agora, quando o computador está inactivo, o Kaspersky Internet Security consome menos recursos do computador o que permite poupar energia quando o computador é utilizado com bateria.
- A aplicação inicia mais rapidamente.

- Foi melhorado o desempenho da GUI da aplicação e o tempo de resposta às acções do utilizador foi reduzido.
- Os relatórios da aplicação foram melhorados. Agora, os relatórios são mais simples e mais claros.
- Foi adicionada a opção de participar no programa Protect a Friend. Agora pode partilhar uma ligação para o Kaspersky Internet Security com amigos e receber códigos de activação de bónus.

KIT DE DISTRIBUIÇÃO

Pode adquirir a aplicação através de uma das seguintes formas:

- **Embalado**. Distribuído nas lojas dos nossos parceiros.
- **Na loja online**. Distribuído nas lojas online da Kaspersky Lab (por exemplo, http://www.kaspersky.pt, secção **eLoja**) ou empresas parceiras.

Se adquirir a versão embalada da aplicação, o kit de distribuição contém os seguintes itens:

- envelope selado com o CD de instalação que contém os ficheiros da aplicação e os ficheiros da documentação;
- breve Manual de Utilizador com um código de activação;
- Contrato de licença que especifica os termos mediante os quais pode utilizar a aplicação.

O conteúdo do kit de distribuição pode variar consoante a região onde a aplicação é distribuída.

Se adquirir o Kaspersky Internet Security numa loja online, estará a copiar a aplicação a partir do site da loja. As informações necessárias para activar a aplicação, incluindo um código de activação, serão enviadas por e-mail, após recepção do pagamento.

Para obter mais detalhes sobre as formas de aquisição e sobre o kit de distribuição, contacte o Departamento de Vendas através de retail@kaspersky.pt.

PRINCIPAIS FUNCIONALIDADES DA APLICAÇÃO

O Kaspersky Internet Security fornece ao seu computador protecção abrangente contra ameaças conhecidas e novas, ataques de rede e phishing, spam e outro conteúdo indesejado. Estão disponíveis diferentes funções e componentes de protecção no Kaspersky Internet Security para fornecer uma protecção completa.

Protecção do Computador

Os *Componentes de protecção* foram concebidos para proteger o computador contra ameaças novas e conhecidas, ataques de rede, fraude e spam e outras informações não solicitadas. Todos os tipos de ameaça são processados por um componente de protecção individual (consulte a descrição dos componentes nesta secção). Os componentes podem ser activados ou desactivados de forma independente e as respectivas definições configuradas.

Além da protecção constante fornecida pelos componentes de segurança, é recomendado *verificar* regularmente e presença de vírus no computador. Tal é necessário para excluir a possibilidade de propagação de programas maliciosos que não tenham sido detectados pelos componentes de protecção, por exemplo, devido ao nível de segurança definido ser baixo ou por outras razões.

Para manter o Kaspersky Internet Security actualizado, é necessário *actualizar* as bases de dados e os módulos de software utilizados pela aplicação.

Algumas tarefas específicas que devem ser executadas ocasionalmente (tais como a remoção de vestígios da actividade do utilizador no sistema) são executadas utilizando *assistentes e ferramentas avançadas*.

Os componentes de protecção seguintes protegem o computador em tempo real:

É descrita em seguida a lógica de funcionamento dos componentes de protecção no modo do Kaspersky Internet Security recomendado pelos especialistas da Kaspersky Lab (ou seja, a predefinições da aplicação).

Antivírus de Ficheiros

O Antivírus de Ficheiros previne a infecção do sistema de ficheiros do computador. O componente é iniciado no arranque do sistema operativo, permanece continuamente na RAM do computador e verifica todas os ficheiros abertos, guardados ou iniciados no computador e em todas as unidades ligadas. O Kaspersky Internet Security intercepta todas as tentativas de acesso a um ficheiro e verifica o ficheiro quanto à presença de vírus conhecidos. O ficheiro só poderá continuar a ser processado se não estiver infectado ou se for corrigido com êxito pela aplicação. Se, por algum motivo, não for possível desinfectar um ficheiro, este será eliminado. Nesse caso, uma cópia do ficheiro será movida para a Quarentena.

Antivírus de E-mail

O Antivírus de E-mail verifica as mensagens de e-mail recebidas e enviadas no computador. O e-mail fica disponível apenas se não incluir objectos perigosos.

Antivírus de Internet

O Antivírus de Internet intercepta e bloqueia a execução de scripts em sites da Web se estes constituírem uma ameaça. O Antivírus de Internet também monitoriza todo o tráfego da Web e bloqueia o acesso aos sites perigosos.

Antivírus de MI

O Antivírus de MI garante a utilização segura de pagers da Internet. O componente protege a informação que chega ao computador através de protocolos de MI. O Antivírus de MI garante o funcionamento seguro de várias aplicações para mensagens instantâneas.

Controlo das Aplicações

O Controlo das Aplicações regista as acções efectuadas pelas aplicações no sistema e efectua a gestão das actividades das aplicações, com base no grupo a que o componente as atribui. É especificado um conjunto de regras para cada grupo de aplicações. Estas regras efectuam a gestão do acesso das aplicações a vários recursos do sistema operativo.

Firewall

A Firewall garante a segurança do seu trabalho em redes locais e na Internet. O componente filtra todas as actividades de rede utilizando regras de dois tipos: *regras para aplicações* e *regras de pacotes*.

Monitor de Rede

O Monitor de Rede foi concebido para monitorizar a actividade de rede em tempo real.

Bloqueio de Ataques de Rede

O Bloqueio de Ataques de Rede é carregado no arranque do sistema operativo e monitoriza o tráfego de rede de entrada quanto a actividades características de ataques de rede. Se forem detectadas tentativas de ataque ao computador, o Kaspersky Internet Security bloqueia todas as actividades de rede do computador atacante direccionadas ao seu computador.

Anti-Spam

O Anti-Spam é integrado no cliente de e-mail instalado no computador e verifica todas as mensagens de e-mail recebidas quanto a spam. Todas as mensagens com spam são marcadas com um cabeçalho específico. Pode configurar o componente Anti-Spam para processar as mensagens de spam de uma determinada forma (por exemplo, apagar as mesmas automaticamente ou movê-las para uma pasta especial).

Anti-Phishing

O Anti-Phishing permite verificar se os URLs estão incluídos na lista de URLs de phishing. Este componente está integrado nos componentes Antivírus de Internet, Anti-Spam e Antivírus de MI.

Anti-Banner

O Anti-Banner bloqueia banners de anúncios em sites da Internet e na interface das aplicações.

Pagamento Seguro

O Pagamento Seguro permite proteger os dados confidenciais ao utilizar serviços bancários online e sistemas de pagamento e impede o furto de activos ao efectuar pagamentos online.

Controlo Parental

O Controlo Parental destina-se a proteger crianças e adolescentes de ameaças relacionadas com a utilização do computador e da Internet.

O Controlo Parental permite definir restrições flexíveis ao acesso aos recursos da Web e aplicações, para diferentes utilizadores, com base na respectiva idade. O Controlo Parental permite também a visualização de relatórios estatísticos sobre as actividades realizadas pelos utilizadores controlados.

SERVIÇOS PARA UTILIZADORES

Mediante a aquisição de uma licença para a aplicação, pode beneficiar dos seguintes serviços durante o período da licença:

- Actualizações da base de dados e acesso a novas versões da aplicação.
- Aconselhamento por telefone e por e-mail acerca de questões relacionadas com a instalação, configuração e utilização da aplicação.
- As notificações sobre a disponibilização de novas aplicações da Kaspersky Lab e sobre novos vírus e surtos de vírus. Para utilizar este serviço, pode subscrever o envio de notícias da Kaspersky Lab no site de Suporte Técnico.

Não é prestado aconselhamento acerca de questões relacionadas com o funcionamento de sistemas operativos, software e tecnologias de terceiros.

REQUISITOS DE HARDWARE E DE SOFTWARE

Para garantir o funcionamento do Kaspersky Internet Security, o seu computador deve obedecer aos seguintes requisitos:

Requisitos gerais:

- 480 MB de espaço livre no disco rígido (incluindo 380 MB na unidade do sistema).
- CD-/DVD-ROM (para instalar com o CD de instalação).
- Acesso à Internet (para a activação da aplicação e para actualizar bases de dados e módulos de software).
- Internet Explorer 8.0 ou superior.

- Microsoft® Windows® Installer 3.0 ou posterior.
- Microsoft .NET Framework 4.

Requisitos para Microsoft Windows XP Home Edition (Service Pack 3 ou posterior), Microsoft Windows XP Professional (Service Pack 3 ou posterior) e Microsoft Windows XP Professional x64 Edition (Service Pack 2 ou posterior):

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

Requisitos para Microsoft Windows Vista® Home Basic (Service Pack 1 ou posterior), Microsoft Windows Vista Home Premium (Service Pack 1 ou posterior), Microsoft Windows Vista Business (Service Pack 1 ou posterior), Microsoft Windows Vista Enterprise (Service Pack 1 ou posterior), Microsoft Windows Vista Ultimate (Service Pack 1 ou posterior), Microsoft Windows 7 Starter, Microsoft Windows 7 Home Basic, Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate, Microsoft Windows 8, Microsoft Windows 8 Pro e Microsoft Windows 8 Enterprise:

- Processador Intel Pentium 1 GHz 32-bit (x86) / 64-bit (x64) ou superior (ou um equivalente compatível).
- 1 GB de RAM disponível (para sistemas operativos de 32 bits); 2 GB de RAM disponíveis (para sistemas operativos de 64 bits).

INSTALAR E REMOVER A APLICAÇÃO

Esta secção contém instruções detalhadas para a instalação e remoção da aplicação.

NESTA SECÇÃO

PROCEDIMENTO DE INSTALAÇÃO PADRÃO

O Kaspersky Internet Security será instalado no seu computador, de forma interactiva, utilizando o Assistente de Instalação.

O Assistente consiste numa série de janelas (passos), entre as quais pode navegar utilizando os botões **Anterior** e **Seguinte**. Para fechar o Assistente depois de este concluir a sua tarefa, clique no botão **Concluir**. Para parar a actividade do assistente em qualquer passo da instalação, feche a janela do assistente.

Se a aplicação se destina a proteger mais de um computador (o número máximo de computadores é definido pelos termos do Contrato de Licença do Utilizador Final), é necessário que a aplicação seja instalada de modo idêntico em todos os computadores.

- *Para instalar o Kaspersky Internet Security no seu computador,*

  execute o ficheiro de instalação (o ficheiro com a extensão EXE) a partir do CD com o produto.

Para instalar o Kaspersky Internet Security, também pode utilizar um pacote de distribuição transferido a partir da Internet. O Assistente de Instalação apresenta alguns passos de instalação adicionais em alguns dos idiomas de localização.

NESTA SECÇÃO

PASSO 1. PROCURAR UMA VERSÃO MAIS RECENTE DA APLICAÇÃO

Antes da instalação, o Assistente de Instalação procura uma versão mais recente do Kaspersky Internet Security nos servidores de actualização da Kaspersky Lab.

Se o Assistente de Instalação não detectar qualquer versão mais recente da aplicação nos servidores de actualização, é iniciada a instalação da versão actual.

Se o Assistente detectar uma versão mais recente do Kaspersky Internet Security nos servidores de actualização, este pode transferir e instalar a mesma no computador. Recomenda-se que instale a nova versão da aplicação, uma vez que as versões mais recentes incluem mais melhorias que lhe permitem garantir uma protecção mais fiável do seu computador. Se recusar a instalação da versão nova, o Assistente inicia a instalação da versão actual da aplicação. Se aceitar instalar a versão nova da aplicação, o Assistente de Instalação copia os ficheiros de instalação do pacote de distribuição para o computador e inicia a instalação da nova versão. Para obter mais detalhes sobre como instalar a nova versão da aplicação consulte a documentação relevante.

PASSO 2. INICIAR A INSTALAÇÃO DA APLICAÇÃO

Neste passo, o Assistente de Instalação solicita a instalação da aplicação.

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

Conforme o tipo de instalação e o idioma de localização, neste passo o Assistente apresenta o Acordo de Licença entre o utilizador e a Kaspersky Lab, permitindo também participar na Kaspersky Security Network.

PASSO 3. REVER O CONTRATO DE LICENÇA

Este passo do Assistente de Instalação é apresentado em alguns idiomas de localização ao instalar o Kaspersky Internet Security a partir de um pacote de distribuição transferido a partir da Internet.

Neste passo, o Assistente de Instalação permite rever o Acordo de Licença entre o utilizador e a Kaspersky Lab.

Leia cuidadosamente o Contrato de Licença e, se aceitar todos os termos, clique no botão **Aceitar**. A instalação irá continuar.

Se não aceitar o Acordo de Licença, a aplicação não será instalada.

PASSO 4. DECLARAÇÃO DA KASPERSKY SECURITY NETWORK

Neste passo, o Assistente de Configuração permite participar na Kaspersky Security Network. A Participação no programa envolve o envio de informação à Kaspersky Lab sobre novas ameaças detectadas no seu computador, aplicações em execução e aplicações assinadas transferidas assim como informação sobre o seu sistema. Não são recolhidos, processados ou armazenados dados pessoais recebidos do utilizador.

Reveja a Declaração da Kaspersky Security Network. Se aceitar todos os termos, clique no botão **Aceitar** na janela do Assistente.

Se não pretender participar na Kaspersky Security Network, clique no botão **Não aceito**.

Após aceitar ou não participar na Kaspersky Security Network, a instalação da aplicação continua.

PASSO 5. INSTALAÇÃO

Algumas versões do Kaspersky Internet Security são distribuídas com subscrição e o fornecedor de serviços fornece uma password que tem de ser introduzida antes da instalação.

Após introduzir a password, a instalação da aplicação é iniciada.

A instalação da aplicação pode demorar algum tempo. Aguarde até que a mesma esteja concluída.

Depois de a instalação estar concluída, o Assistente irá, automaticamente, continuar para o passo seguinte.

O Kaspersky Internet Security realiza várias verificações durante a instalação. Essas verificações podem permitir detectar os problemas seguintes:

- **Não conformidade do sistema operativo com os requisitos do software**. Durante a instalação, o Assistente verifica as condições seguintes:

  - Se o sistema operativo e o Service Pack cumprem os requisitos de software
  - Se todas as aplicações necessárias estão disponíveis
  - Se o espaço livre em disco é suficiente para a instalação

  Se algum dos requisitos acima listados não for satisfeito, será apresentada no ecrã a respectiva notificação.

- **Presença de aplicações incompatíveis no computador**. Se forem detectadas aplicações incompatíveis, estas são apresentadas numa lista no ecrã e ser-lhe-á dada a opção de as remover. As aplicações que o Kaspersky Internet Security não conseguir remover automaticamente deverão ser manualmente removidas. Ao remover aplicações incompatíveis, terá de reiniciar o seu sistema operativo, após o qual a instalação do Kaspersky Internet Security continuará automaticamente.

- **Presença de software malicioso no computador**. Se forem detectadas no computador aplicações maliciosas que interferem com a instalação do software antivírus, o Assistente de Instalação solicita que transfira uma ferramenta dedicada concebida para neutralizar a infecção, denominada *Kaspersky Virus Removal Tool*.

  Se aceitar instalar o utilitário, o Assistente de Instalação transfere-o a partir dos servidores da Kaspersky Lab e depois a instalação do utilitário começará automaticamente. Se o Assistente não conseguir transferir o utilitário, ser-lhe-á pedido para transferi-lo por si próprio, clicando na ligação fornecida.

PASSO 6. CONCLUIR A INSTALAÇÃO

Neste passo, o Assistente informa o utilizador de que a instalação da aplicação foi concluída com êxito. Para começar a utilizar o Kaspersky Internet Security imediatamente, certifique-se de que a caixa de selecção **Iniciar o Kaspersky Internet Security** está seleccionada e clique no botão **Concluir**.

Se tiver desmarcado a caixa de selecção **Iniciar o Kaspersky Internet Security** antes de fechar o Assistente, deverá executar a aplicação manualmente.

Em alguns casos, pode ser necessário reiniciar o seu sistema operativo para concluir a instalação.

PASSO 7. ACTIVAR A APLICAÇÃO

Neste passo, o Assistente de Instalação solicita a activação da aplicação.

A *Activação* é o processo de colocação em funcionamento de uma versão da aplicação com todas as funcionalidades, por um determinado período de tempo.

Se adquiriu uma licença do Kaspersky Internet Security e transferiu a aplicação a partir de uma loja online, a activação da aplicação pode ser efectuada automaticamente durante a instalação.

Ser-lhe-ão disponibilizadas as seguintes opções para activar o Kaspersky Internet Security:

- **Activar a aplicação**. Seleccione esta opção e insira um código de activação se tiver adquirido uma licença para a aplicação.

  Se especificar o código de activação para o Kaspersky Anti-Virus no campo de registo, o procedimento de mudança para o Kaspersky Anti-Virus terá início quando concluir a activação.

- **Activar a versão de avaliação da aplicação**. Seleccione esta opção de activação se pretender instalar a versão de avaliação da aplicação, antes de tomar a decisão de comprar uma licença. Poderá utilizar a versão com todas as funcionalidades da aplicação durante o período limitado pelas condições de utilização da versão de avaliação. Quando a licença expirar, a versão de avaliação não pode ser activada pela segunda vez.

Vai precisar de uma ligação à Internet para activar a aplicação.

PASSO 8. REGISTAR UM UTILIZADOR

Este passo não está disponível em todas as versões do Kaspersky Internet Security.

Os utilizadores registados podem enviar pedidos ao Serviço de Suporte Técnico e ao Laboratório de Vírus através da Conta Kaspersky no site da Kaspersky Lab, gerir códigos de activação de forma conveniente e receber as informações mais recentes sobre novos produtos e ofertas especiais.

Se aceitar registar-se, especifique os seus dados de registo nos respectivos campos e clique no botão **Seguinte** para enviar os dados para a Kaspersky Lab.

Em alguns casos, é necessário o registo do utilizador para começar a utilizar a aplicação.

PASSO 9. CONCLUIR A ACTIVAÇÃO

O Assistente informa-o de que o Kaspersky Internet Security foi activado com sucesso. Adicionalmente, é fornecida informação sobre a licença em vigor: data de expiração da licença e o número de anfitriões abrangidos pela licença.

Se tiver solicitado uma subscrição, é apresentada a informação sobre o estado da subscrição, em vez da data de expiração da licença.

Clique no botão **Concluir** para fechar o Assistente.

ACTUALIZAR UMA VERSÃO ANTERIOR DA APLICAÇÃO

Instalar uma versão nova do Kaspersky Internet Security sobre uma versão anterior do Kaspersky Internet Security

Se uma versão anterior do Kaspersky Internet Security já estiver instalada no computador, poderá efectuar a actualização para a versão mais recente do Kaspersky Internet Security. Se tiver uma licença em vigor para uma versão anterior do Kaspersky Internet Security, não será necessário activar a aplicação: o Assistente de Instalação irá obter automaticamente a informação sobre a licença para a versão actual do Kaspersky Internet Security e aplicá-la durante a instalação da versão mais recente do Kaspersky Internet Security.

Instalar uma versão nova do Kaspersky Internet Security sobre uma versão anterior do Kaspersky Anti-Virus

Se instalar uma versão nova do Kaspersky Internet Security num computador com uma versão anterior do Kaspersky Anti-Virus instalada com uma licença activa, o Assistente de Activação solicita ao utilizador que seleccione uma das opções seguintes:

- Continuar a utilizar o Kaspersky Anti-Virus com a licença actual. Neste caso, o Assistente de Migração será iniciado. Quando o Assistente de Migração terminar, a nova versão do Kaspersky Anti-Virus será instalada no seu computador. Pode utilizar o Kaspersky Anti-Virus antes de a licença para a versão anterior do Kaspersky Anti-Virus expirar.

- Continuar a instalação da nova versão do Kaspersky Internet Security. Neste caso, a aplicação será instalada e activada de acordo com o cenário padrão.

O Kaspersky Internet Security será instalado no seu computador, de forma interactiva, utilizando o Assistente de Instalação.

O Assistente consiste numa série de janelas (passos), entre as quais pode navegar utilizando os botões **Anterior** e **Seguinte**. Para fechar o Assistente depois de este concluir a sua tarefa, clique no botão **Concluir**. Para parar a actividade do assistente em qualquer passo da instalação, feche a janela do assistente.

Se a aplicação se destina a proteger mais de um computador (o número máximo de computadores é definido pelos termos do Contrato de Licença do Utilizador Final), é necessário que a aplicação seja instalada de modo idêntico em todos os computadores.

➧ *Para instalar o Kaspersky Internet Security no seu computador,*

execute o ficheiro de instalação (o ficheiro com a extensão EXE) a partir do CD com o produto.

Para instalar o Kaspersky Internet Security, também pode utilizar um pacote de distribuição transferido a partir da Internet. O Assistente de Instalação apresenta alguns passos de instalação adicionais em alguns dos idiomas de localização.

NESTA SECÇÃO

PASSO 1. PROCURAR UMA VERSÃO MAIS RECENTE DA APLICAÇÃO

Antes da instalação, o Assistente de Instalação procura uma versão mais recente do Kaspersky Internet Security nos servidores de actualização da Kaspersky Lab.

Se o Assistente de Instalação não detectar qualquer versão mais recente da aplicação nos servidores de actualização, é iniciada a instalação da versão actual.

Se o Assistente detectar uma versão mais recente do Kaspersky Internet Security nos servidores de actualização, este pode transferir e instalar a mesma no computador. Recomenda-se que instale a nova versão da aplicação, uma vez que as versões mais recentes incluem mais melhorias que lhe permitem garantir uma protecção mais fiável do seu computador. Se recusar a instalação da versão nova, o Assistente inicia a instalação da versão actual da aplicação. Se aceitar instalar a versão nova da aplicação, o Assistente de Instalação copia os ficheiros de instalação do pacote de distribuição para o computador e inicia a instalação da nova versão. Para obter mais detalhes sobre como instalar a nova versão da aplicação consulte a documentação relevante.

PASSO 2. INICIAR A INSTALAÇÃO DA APLICAÇÃO

Neste passo, o Assistente de Instalação solicita a instalação da aplicação.

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

Conforme o tipo de instalação e o idioma de localização, neste passo o Assistente apresenta o Acordo de Licença entre o utilizador e a Kaspersky Lab, permitindo também participar na Kaspersky Security Network.

PASSO 3. REVER O CONTRATO DE LICENÇA

Este passo do Assistente de Instalação é apresentado em alguns idiomas de localização ao instalar o Kaspersky Internet Security a partir de um pacote de distribuição transferido a partir da Internet.

Neste passo, o Assistente de Instalação permite rever o Acordo de Licença entre o utilizador e a Kaspersky Lab.

Leia cuidadosamente o Contrato de Licença e, se aceitar todos os termos, clique no botão **Aceitar**. A instalação irá continuar.

Se não aceitar o Acordo de Licença, a aplicação não será instalada.

PASSO 4. DECLARAÇÃO DA KASPERSKY SECURITY NETWORK

Neste passo, o Assistente de Configuração permite participar na Kaspersky Security Network. A Participação no programa envolve o envio de informação à Kaspersky Lab sobre novas ameaças detectadas no seu computador, aplicações em execução e aplicações assinadas transferidas assim como informação sobre o seu sistema. Não são recolhidos, processados ou armazenados dados pessoais recebidos do utilizador.

Reveja a Declaração da Kaspersky Security Network. Se aceitar todos os termos, clique no botão **Aceitar** na janela do Assistente.

Se não pretender participar na Kaspersky Security Network, clique no botão **Não aceito**.

Após aceitar ou não participar na Kaspersky Security Network, a instalação da aplicação continua.

PASSO 5. INSTALAÇÃO

Algumas versões do Kaspersky Internet Security são distribuídas com subscrição e o fornecedor de serviços fornece uma password que tem de ser introduzida antes da instalação.

Após introduzir a password, a instalação da aplicação é iniciada.

A instalação da aplicação pode demorar algum tempo. Aguarde até que a mesma esteja concluída.

Depois de a instalação estar concluída, o Assistente irá, automaticamente, continuar para o passo seguinte.

O Kaspersky Internet Security realiza várias verificações durante a instalação. Essas verificações podem permitir detectar os problemas seguintes:

- **Não conformidade do sistema operativo com os requisitos do software**. Durante a instalação, o Assistente verifica as condições seguintes:
  - Se o sistema operativo e o Service Pack cumprem os requisitos de software
  - Se todas as aplicações necessárias estão disponíveis
  - Se o espaço livre em disco é suficiente para a instalação

  Se algum dos requisitos acima listados não for satisfeito, será apresentada no ecrã a respectiva notificação.
- **Presença de aplicações incompatíveis no computador**. Se forem detectadas aplicações incompatíveis, estas são apresentadas numa lista no ecrã e ser-lhe-á dada a opção de as remover. As aplicações que o Kaspersky Internet Security não conseguir remover automaticamente deverão ser manualmente removidas. Ao remover aplicações incompatíveis, terá de reiniciar o seu sistema operativo, após o qual a instalação do Kaspersky Internet Security continuará automaticamente.
- **Presença de software malicioso no computador**. Se forem detectadas no computador aplicações maliciosas que interferem com a instalação do software antivírus, o Assistente de Instalação solicita que transfira uma ferramenta dedicada concebida para neutralizar a infecção, denominada *Kaspersky Virus Removal Tool*.

  Se aceitar instalar o utilitário, o Assistente de Instalação transfere-o a partir dos servidores da Kaspersky Lab e depois a instalação do utilitário começará automaticamente. Se o Assistente não conseguir transferir o utilitário, ser-lhe-á pedido para transferi-lo por si próprio, clicando na ligação fornecida.

PASSO 6. CONCLUIR A INSTALAÇÃO

Esta janela do Assistente informa-o de que a instalação da aplicação foi concluída com sucesso.

Reinicie o sistema operativo após a aplicação ter sido instalada.

Se a caixa **Iniciar o Kaspersky Internet Security** estiver assinalada, a aplicação será, automaticamente, executada depois de reiniciar o seu sistema operativo.

Se tiver desmarcado a caixa de selecção **Iniciar o Kaspersky Internet Security** antes de fechar o Assistente, terá de executar a aplicação manualmente.

REMOVER A APLICAÇÃO

Depois de remover o Kaspersky Internet Security, o seu computador e dados privados ficarão desprotegidos!

O Kaspersky Internet Security é desinstalado com a ajuda do Assistente de Instalação.

Para iniciar o Assistente,

No menu **Iniciar** seleccione **Programas→ Kaspersky Internet Security→ Remover o Kaspersky Internet Security**.

NESTA SECÇÃO

PASSO 1. INTRODUZIR A PASSWORD PARA REMOVER A APLICAÇÃO

Para remover o Kaspersky Internet Security, deverá introduzir a password para aceder às definições da aplicação. Se, por algum motivo, não for possível especificar a password, a remoção da aplicação não será permitida.

Este passo é apresentado apenas se tiver sido definida uma password para remover a aplicação.

PASSO 2. GUARDAR DADOS PARA UTILIZAÇÃO POSTERIOR

Nesta fase, pode especificar quais os dados utilizados pela aplicação que deseja reter para reutilizar durante a próxima instalação da aplicação (por exemplo, uma versão mais recente da aplicação).

Por predefinição, a aplicação solicita que guarde as informações sobre a licença.

➧ *Para guardar dados para utilização posterior, seleccione as caixas de selecção junto aos itens de dados que pretende guardar:*

- **Informações sobre a licença** – um conjunto de dados que exclui a necessidade de activar a nova aplicação, permitindo utilizá-la com a licença actual, excepto se a licença expirar antes de iniciar a instalação.
- Os **Ficheiros da Quarentena** são ficheiros verificados pela aplicação e movidos para a quarentena.

  Depois de o Kaspersky Internet Security ser removido do computador, os ficheiros colocados na quarentena ficam indisponíveis. Deve instalar o Kaspersky Internet Security para lidar com estes ficheiros.
- As **Configurações operacionais da aplicação** são valores das definições da aplicação seleccionadas durante a configuração.

  A Kaspersky Lab não garante o suporte das definições das versões anteriores da aplicação. Após a instalação da nova versão, é recomendado verificar se as suas definições estão correctas.

  Também pode exportar as definições de protecção na linha de comandos, utilizando o comando seguinte:

  avp.com EXPORT <file_name>
- Os **Dados do iChecker** são ficheiros que contêm informações sobre objectos que já foram verificados com a tecnologia iChecker.
- As **Bases de dados de Anti-Spam** são bases de dados que contêm amostras de mensagens de spam transferidas e guardadas pela aplicação.

PASSO 3. CONFIRMAR A REMOÇÃO DA APLICAÇÃO

Uma vez que a remoção da aplicação ameaça a segurança do computador e dos seus dados privados, ser-lhe-á solicitado que confirme a sua intenção de remover a aplicação. Para o fazer, clique no botão **Remover**.

PASSO 4. REMOVER A APLICAÇÃO. CONCLUIR A REMOÇÃO

Neste passo, o Assistente remove a aplicação do seu computador. Aguarde até a remoção estar concluída.

Após terminar a remoção do Kaspersky Internet Security, poderá especificar os motivos da remoção da aplicação no site da Kaspersky Lab. Para tal, deve aceder ao site da Kaspersky Lab clicando no botão **Preencher formulário**.

Ao remover a aplicação, é necessário reiniciar o sistema operativo. Se cancelar a reinicialização imediata, a conclusão do procedimento de remoção será adiada até que o sistema operativo seja reiniciado ou o computador seja desligado e depois reiniciado.

LICENCIAMENTO DA APLICAÇÃO

Esta secção fornece informação acerca dos termos gerais relacionados com a activação da aplicação. Leia esta secção para saber mais sobre o objectivo do Contrato de Licença do Utilizador Final, as formas de activação da aplicação e a renovação da licença.

NESTA SECÇÃO

ACERCA DO CONTRATO DE LICENÇA DO UTILIZADOR FINAL

O Contrato de Licença do Utilizador Final é um acordo vinculativo entre o utilizador e a Kaspersky Lab ZAO, que define os termos de utilização da aplicação.

Leia atentamente os termos do Contrato de Licença antes de começar a utilizar a aplicação.

É necessário aceitar os termos do Contrato de Licença do Utilizador Final, confirmando a sua aceitação ao instalar a aplicação. Se não aceitar os termos do Contrato de Licença, terá de interromper a instalação da aplicação ou renunciar à utilização da aplicação.

SOBRE A LICENÇA

Uma *licença* constitui uma autorização de utilização da aplicação durante um período limitado, que é concedida ao abrigo do Contrato de Licença do Utilizador Final. A licença estabelece um código único para a activação da sua cópia do Kaspersky Internet Security.

Uma licença actualizada permite aceder aos seguintes tipos de serviços:

- O direito de utilizar a aplicação em um ou vários dispositivos.

  O número de dispositivos nos quais pode utilizar a aplicação está especificado no Contrato de Licença do Utilizador Final.

- Assistência do Suporte técnico da Kaspersky Lab.

- Outros serviços disponibilizados pela Kaspersky Lab ou pelos seus parceiros durante o período da licença (consulte a secção "Serviço para utilizadores" na página 14).

Para gerir a aplicação, deve adquirir uma licença para utilizar a aplicação.

A licença tem uma validade limitada. Quando a licença expira, a aplicação continua em execução, embora com funcionalidades limitadas (por exemplo, não é possível actualizar a aplicação ou utilizar a Kaspersky Security Network). Pode continuar a beneficiar de todos os componentes da aplicação e a realizar verificações quanto à presença de vírus e outro software malicioso, mas apenas utilizando as bases de dados que foram instaladas antes da expiração da licença. Para continuar a utilizar o Kaspersky Internet Security com todas as funcionalidades, terá de renovar a licença.

É recomendado renovar a licença antes do fim da data de validade para garantir a máxima protecção do computador contra todas as ameaças de segurança.

Antes de adquirir uma licença, pode utilizar a versão de avaliação do Kaspersky Internet Security para se familiarizar com a aplicação, sem quaisquer custos. A versão de avaliação do Kaspersky Internet Security permanece funcional durante um breve período de avaliação. Quando o período de avaliação termina, o Kaspersky Internet Security interrompe a execução de todas as suas funcionalidades. Para continuar a utilizar a aplicação, deverá adquirir uma licença.

SOBRE O CÓDIGO DE ACTIVAÇÃO

O *código de activação* é um código recebido ao adquirir a licença para o Kaspersky Internet Security. Este código é necessário para a activação da aplicação.

O código de activação é uma sequência exclusiva de vinte dígitos e letras no formato xxxxx-xxxxx-xxxxx-xxxxx.

Conforme a forma de aquisição da aplicação, pode obter o código de activação das seguintes formas:

- Se adquiriu a versão embalada do Kaspersky Internet Security, o código de activação é especificado na documentação incluída na caixa que contém o CD de instalação.
- Se adquiriu o Kaspersky Internet Security numa loja online, o código de activação é enviado para o endereço de e-mail que especificou ao encomendar o produto.
- Se participar no programa Protect a Friend (consulte a secção "Participação no programa Protect a Friend" na página 71), pode receber um código de activação de bónus em troca de pontos de bónus.

O período da licença tem início na data de activação da aplicação. Se adquiriu uma licença destinada à utilização do Kaspersky Internet Security em vários dispositivos, o período da licença tem início no momento em que aplica pela primeira vez o código de activação.

Se perdeu ou eliminou acidentalmente o código de activação após a activação da aplicação, contacte o Suporte Técnico da Kaspersky Lab para recuperar o código de activação (http://support.kaspersky.com).

SOBRE A SUBSCRIÇÃO

A *Subscrição do Kaspersky Internet Security* é uma encomenda da aplicação com as definições seleccionadas (data de expiração e número de dispositivos protegidos). Pode encomendar uma subscrição do Kaspersky Internet Security a um fornecedor de serviços (por exemplo, o seu fornecedor de Internet). Pode colocar em pausa ou retomar a sua subscrição, renovar em modo automático ou cancelar a mesma. Pode gerir a sua subscrição através da sua área pessoal ou no site do fornecedor de serviços.

Os fornecedores de serviços podem fornecer dois tipos de subscrição para o Kaspersky Internet Security: subscrição de actualização e subscrição de actualização e protecção.

A subscrição pode ser limitada (por exemplo, um ano) ou ilimitada (sem data de fim). Para continuar a utilizar o Kaspersky Internet Security depois de a subscrição limitada expirar, deverá renovar a mesma. A subscrição ilimitada é renovada automaticamente desde que o pré-pagamento ao fornecedor de serviços tenha sido efectuado atempadamente.

Se o termo da subscrição for limitado, ao cessar a sua validade será concedido ao utilizador um período para o prolongamento da subscrição durante o qual as funcionalidades da aplicação permanecem inalteradas.

Se a subscrição não for renovada quando esse período terminar, o Kaspersky Internet Security deixa de actualizar as bases de dados da aplicação (para subscrição de actualizações), e de fornecer protecção ao computador e de executar tarefas de verificação (para subscrição de actualização e protecção).

Para utilizar o Kaspersky Internet Security com subscrição, deve utilizar o código de activação recebido do fornecedor de serviços. Em alguns casos, um código de activação pode ser transferido e aplicado automaticamente. Quando utilizar a aplicação com subscrição, não é possível aplicar outro código de activação para renovar a licença. Tal é possível apenas quando o termo da subscrição expirar.

Se o Kaspersky Internet Security já estiver a ser utilizado com a licença actual quando efectuar o registo da subscrição, o Kaspersky Internet Security será utilizado com a subscrição após o registo. O código de activação utilizado para activar a aplicação pode ser aplicado noutro computador.

Para recusar a subscrição, é necessário contactar o fornecedor de serviços a que o Kaspersky Internet Security foi adquirido.

Conforme o fornecedor da subscrição, o conjunto de opções de gestão da subscrição pode variar. Adicionalmente, poderá não ter acesso ao período de tolerância durante o qual pode renovar a subscrição.

ACERCA DA PROVISÃO DE DADOS

De modo a aumentar o nível de protecção, ao aceitar a provisão de dados do Contrato de Licença, está a aceitar fornecer as seguintes informações à Kaspersky Lab de forma automática:

- informações sobre as somas de verificação dos ficheiros processados (MD5);
- informações necessárias para avaliar a reputação de URLs;
- estatísticas sobre a utilização das notificações de produtos;
- dados estatísticos para protecção contra spam;
- dados sobre a activação do Kaspersky Internet Security e a versão actualmente utilizada;
- informações sobre os tipos de ameaças detectadas;
- informações sobre os certificados digitais actualmente em utilização e as informações necessárias para verificá-los;
- detalhes de funcionamento da aplicação e detalhes da licença necessários para configurar a apresentação do conteúdo dos sites confiáveis.

Se o computador estiver equipado com TPM (Trusted Platform Module), poderá também aceitar fornecer à Kaspersky Lab o relatório de TPM sobre o início do sistema operativo bem como as informações necessárias para o verificar. Caso ocorra um erro ao instalar o Kaspersky Internet Security, aceita fornecer de forma automática à Kaspersky Lab informações sobre o código do erro, o pacote de distribuição actualmente em utilização e sobre o seu computador.

Se participar na Kaspersky Security Network (consulte a secção "Participar na Kaspersky Security Network (KSN)" na página 69), as informações seguintes são enviadas automaticamente do computador para a Kaspersky Lab:

- informações sobre o hardware e software instalados no computador;
- Informações sobre o estado da protecção antivírus do computador, bem como sobre todos os objectos potencialmente infectados e as decisões tomadas relativamente a esses objectos;
- informações sobre aplicações transferidas e executadas;
- Informações sobre o licenciamento da versão instalada do Kaspersky Internet Security;
- informações sobre erros da interface e a utilização da interface do Kaspersky Internet Security;

- detalhes da aplicação, incluído a versão da aplicação, informações sobre ficheiros dos módulos transferidos e versões das bases de dados actuais da aplicação;
- estatísticas sobre as actualizações e ligações aos servidores da Kaspersky Lab;
- informações sobre a ligação sem fios utilizada actualmente;
- estatísticas do tempo real gasto pelos componentes da aplicação na verificação de objectos;
- estatísticas dos atrasos ocorridos ao iniciar as aplicações relacionadas com o funcionamento do Kaspersky Internet Security;
- ficheiros que podem ser utilizados por criminosos para danificar o seu computador, ou fragmentos desses ficheiros, incluindo ficheiros detectados por ligações maliciosas.

As informações para envio à Kaspersky Lab podem ser armazenadas no seu computador durante o prazo máximo de 30 dias, a contar da data de criação. Os itens de dados são mantidos num formato protegido interno. O volume máximo dos dados a armazenar é 30 MB.

Além disso, a verificação adicional na Kaspersky Lab poderá necessitar do envio de ficheiros (ou partes de ficheiros) que representam um risco acrescido de exploração por intrusos e que podem afectar o computador ou os dados do utilizador.

A Kaspersky Lab protege qualquer informação recebida desta forma conforme previsto pela lei. A Kaspersky Lab utiliza as informações recolhidas apenas para efeitos estatísticos gerais. Estas estatísticas gerais são criadas automaticamente utilizando as informações originais obtidas e não contêm quaisquer dados pessoais ou outras informações confidenciais. As informações originais obtidas são armazenadas num formato encriptado; estas informações são eliminadas à medida que são acumuladas (duas vezes por ano). As estatísticas gerais são armazenadas indefinidamente.

RESOLVER TAREFAS TÍPICAS

Esta secção contém instruções detalhadas para realizar tarefas de utilizador típicas fornecidas pela aplicação.

NESTA SECÇÃO

ACTIVAR A APLICAÇÃO

É necessário activar a aplicação para utilizar as suas funcionalidades e serviços associados (consulte a secção "Sobre o código de activação" na página 25).

Se não activou a aplicação durante a instalação, pode fazê-lo mais tarde. Será relembrado da necessidade de activar a aplicação, através das mensagens do Kaspersky Internet Security que aparecem na área de notificação da barra de ferramentas. O Kaspersky Internet Security pode ser activado utilizando o Assistente de Instalação.

Para executar o assistente de activação do Kaspersky Internet Security, execute uma das seguintes acções:

- Clique na ligação **Activar** na janela de aviso do Kaspersky Internet Security, que aparece na área de notificação da barra de ferramentas.
- Na parte inferior da janela principal da aplicação clique na ligação **Licenciamento**. Na janela **Licenciamento** apresentada, clique no botão **Activar a aplicação**.

Ao trabalhar com o assistente de configuração da aplicação, deve especificar valores para um conjunto de definições.

Passo 1. Introduzir código de activação

Introduza o código de activação no campo correspondente e clique no botão **Activar**.

Passo 2. Solicitar a activação

Se o pedido de activação for enviado com sucesso, o Assistente continua automaticamente, para o passo seguinte.

Passo 3. Introduzir dados de registo

Este passo não está disponível em todas as versões do Kaspersky Internet Security.

Os utilizadores registados podem utilizar as seguintes funcionalidades:

- Enviar pedidos para o Suporte Técnico e para o Laboratório de Antivírus, a partir da Conta Kaspersky, no site da Kaspersky Lab.
- Gerir códigos de activação.
- Receber informações sobre novos produtos e ofertas especiais da Kaspersky Lab.

Especifique os seus dados de registo e clique no botão **Seguinte**.

Passo 4. Activação

Se o pedido de activação da aplicação tiver sido bem sucedido, o Assistente continua automaticamente para a janela seguinte.

Passo 5. Conclusão do Assistente

Esta janela do assistente apresenta informações sobre os resultados da activação.

Clique no botão **Concluir** para fechar o Assistente.

COMPRAR E RENOVAR UMA LICENÇA

Se tiver instalado o Kaspersky Internet Security sem adquirir uma licença, pode comprar uma após a instalação. Ao comprar uma licença, recebe um código de activação que é utilizado para activar a aplicação (consulte a secção "Activar a aplicação" na página 29).

Quando a sua licença expirar, pode renová-la. Para tal, pode adicionar um código de activação novo sem que a licença actual tenha expirado. Quando a licença actual expirar, o Kaspersky Internet Security será automaticamente activado com o novo código de activação.

Para comprar uma licença:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela principal, clique na ligação **Inserir código de activação/Licenciamento**. É apresentada a janela **Licenciamento**.
3. Na janela que se abre, clique no botão **Comprar código de activação**.

Abrir-se-á a página de Internet da eLoja, onde pode comprar uma licença.

Para adicionar um código de activação novo:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela principal, clique na ligação **Inserir código de activação/Licenciamento**. É apresentada a janela **Licenciamento**.
3. Na janela apresentada, clique no botão **Activar a aplicação**.

   O Assistente de Activação da Aplicação abre-se.
4. Introduza o código de activação nos campos correspondentes e clique no botão **Activar**.

   Em seguida, o Kaspersky Internet Security envia os dados para o servidor de activação para que sejam verificados. Se a verificação for bem sucedida, o Assistente de Activação continua automaticamente para o passo seguinte.
5. Após concluir o Assistente, clique no botão **Concluir**.

GERIR NOTIFICAÇÕES DA APLICAÇÃO

As notificações apresentadas na área de notificação da barra de ferramentas informam-no sobre eventos ocorridos no funcionamento da aplicação e que requerem a sua atenção. Dependendo do nível de criticalidade do evento, pode receber os seguintes tipos de notificação:

- *Notificações críticas* – informam-no dos eventos que têm uma importância crítica para a segurança do computador, tal como a detecção de um objecto malicioso ou uma actividade perigosa no sistema. As janelas das notificações críticas e das mensagens instantâneas são apresentadas a vermelho.
- *Notificações importantes* – informam-no de eventos que são potencialmente importantes para a segurança do computador, tal como a detecção de objectos provavelmente infectados ou de actividade suspeita no sistema. As janelas das notificações importantes e das mensagens instantâneas são apresentadas a amarelo.
- *Notificações importantes* – informam-no de eventos que não são de importância crítica para a segurança do computador. As janelas das notificações informativas e das mensagens instantâneas são apresentadas a verde.

Se este tipo de notificação for apresentado no ecrã, deve seleccionar uma das opções sugeridas na notificação. A opção óptima é a recomendada, por defeito, pelos especialistas da Kaspersky Lab. Uma notificação pode ser fechada automaticamente, reiniciando o computador, fechando o Kaspersky Internet Security ou activando o modo de espera ligado no Windows 8. Ao fechar uma notificação automaticamente, o Kaspersky Internet Security executa a acção recomendada por predefinição.

As notificações não são apresentadas durante a primeira hora de funcionamento da aplicação se adquiriu um computador com o Kaspersky Internet Security pré-instalado (distribuição OEM). Os processos da aplicação detectaram objectos conforme as acções recomendadas. Os resultados de processamento são guardados num relatório.

AVALIAR O ESTADO DE PROTECÇÃO DO COMPUTADOR E SOLUCIONAR PROBLEMAS DE SEGURANÇA

Os problemas com a protecção do computador são indicados por um indicador na parte esquerda da janela principal da aplicação (consulte a figura seguinte). O indicador está representado como um ícone de monitor que muda de cor conforme o estado de protecção do computador: a cor verde significa que o computador está protegido, a cor amarela indica problemas relacionados com a protecção, a cor vermelha alerta para graves ameaças à segurança do computador. Recomenda-se que corrija imediatamente os problemas e ameaças de segurança.

Figura 1. Indicador do estado da protecção

Se clicar no indicador na janela principal da aplicação, abre-se a janela **Problemas de Segurança** (ver figura abaixo) que contém informações detalhadas sobre o estado de protecção do computador e sugestões de resolução de problemas para os problemas e ameaças detectados.

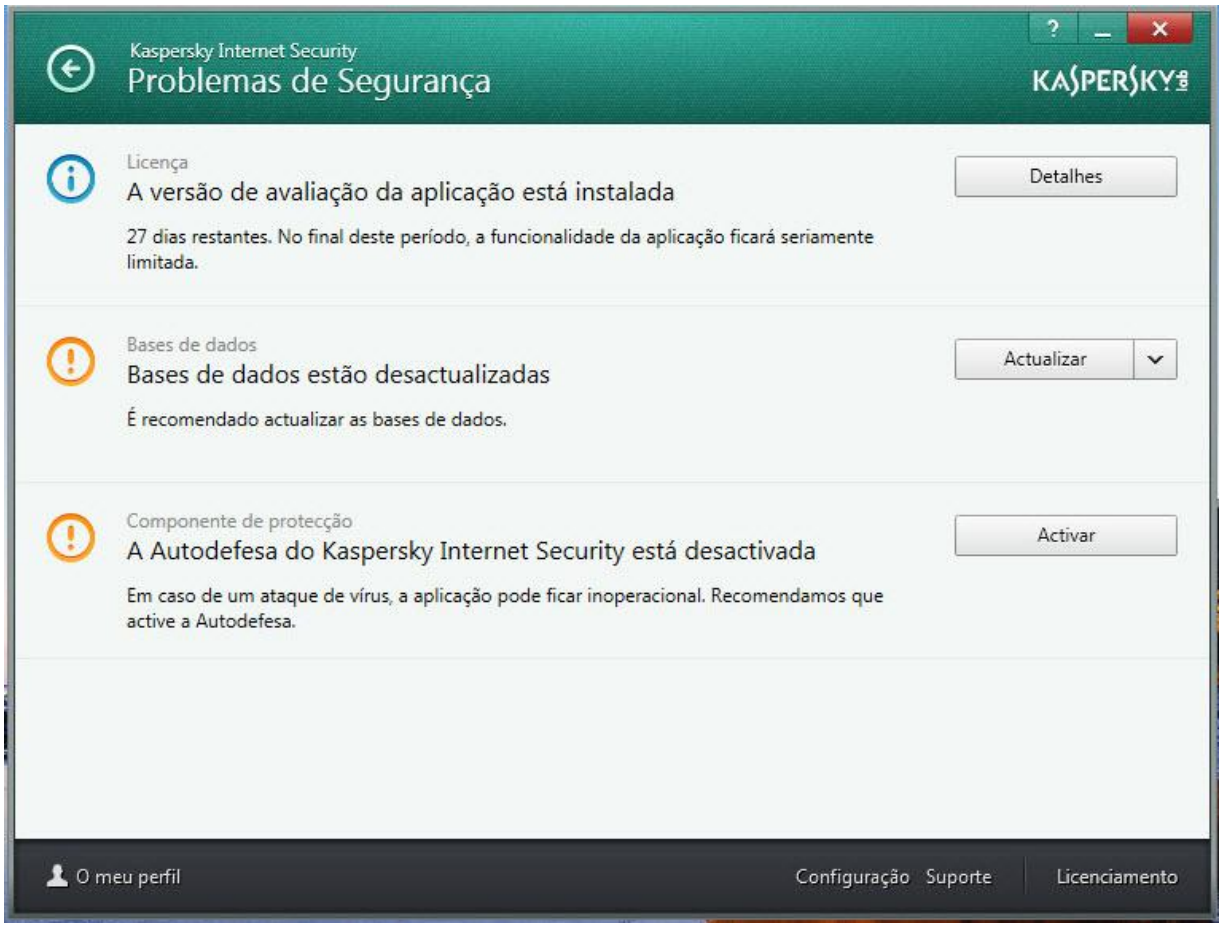

Figura 2. Janela Problemas de Segurança

Os problemas com a protecção estão agrupados por categorias. Para cada problema, estão listadas as acções que pode utilizar para resolver o problema.

ACTUALIZAR AS BASES DE DADOS E OS MÓDULOS DA APLICAÇÃO

Por defeito, o Kaspersky Internet Security verifica, automaticamente, a existência de actualizações nos servidores de actualização da Kaspersky Lab. Se o servidor guardar um conjunto de actualizações recentes, o Kaspersky Internet Security transfere e instala as mesmas em modo de segundo plano. Pode executar uma actualização do Kaspersky Internet Security manualmente, em qualquer altura, a partir da janela principal da aplicação ou do menu de contexto do ícone da aplicação na área de notificação da barra de tarefas.

Para transferir as actualizações a partir dos servidores da Kaspersky Lab, deve estar ligado à Internet.

No Microsoft Windows 8, as actualizações não são transferidas se for estabelecida uma ligação de Internet de banda larga e existir um limite de tráfego para este tipo de ligação. Para transferir actualizações, deve remover manualmente as limitações na subsecção **Rede** da janela de definições da aplicação.

- *Para executar uma actualização a partir do menu de contexto do ícone da aplicação na área de notificação da barra de ferramentas,*

  no menu de contexto do ícone da aplicação, seleccione o item **Actualização**.

- *Para executar uma actualização a partir da janela principal da aplicação:*

  1. Abra a janela principal da aplicação e seleccione a secção **Actualização** na parte inferior da janela.

     A janela apresenta a secção **Actualizar**.

  2. Na secção **Actualizar** clique no botão **Executar actualização**.

VERIFICAÇÃO COMPLETA DO COMPUTADOR QUANTO À PRESENÇA DE VÍRUS

Durante uma verificação completa, o Kaspersky Internet Security verifica os objectos seguintes, por predefinição:

- memória do sistema;
- objectos carregados aquando da inicialização do sistema operativo;
- cópia de segurança do sistema;
- discos rígidos e unidades removíveis.

É recomendado executar uma verificação completa imediatamente após instalar o Kaspersky Internet Security no computador.

- *Para iniciar uma verificação completa a partir da janela principal da aplicação:*

  1. Abra a janela principal da aplicação e seleccione a secção **Verificação** na parte inferior da janela.

     A janela apresenta a secção **Verificar**.

  2. Seleccione a secção **Verificação completa** na parte direita da janela.

     A janela apresenta a secção **Verificação completa**.

  3. Clique no botão **Iniciar verificação**.

  O Kaspersky Internet Security inicia a verificação completa do seu computador.

VERIFICAR A EXISTÊNCIA DE VÍRUS NUM FICHEIRO, PASTA, DISCO OU OUTRO OBJECTO

Pode utilizar os seguintes métodos para verificar a existência de vírus num objecto:

- a partir do menu de contexto do objecto
- Na janela principal da aplicação
- Através da Ferramenta Kaspersky Internet Security (apenas em Microsoft Windows Vista e Microsoft Windows 7)

Para iniciar uma verificação de vírus a partir do menu de contexto do objecto:

1. Abra o Explorador do Microsoft Windows e aceda à pasta que contém o objecto a verificar.
2. Clique com o botão direito do rato no menu de contexto do objecto (consulte a figura seguinte) e seleccione **Verificar Vírus**.

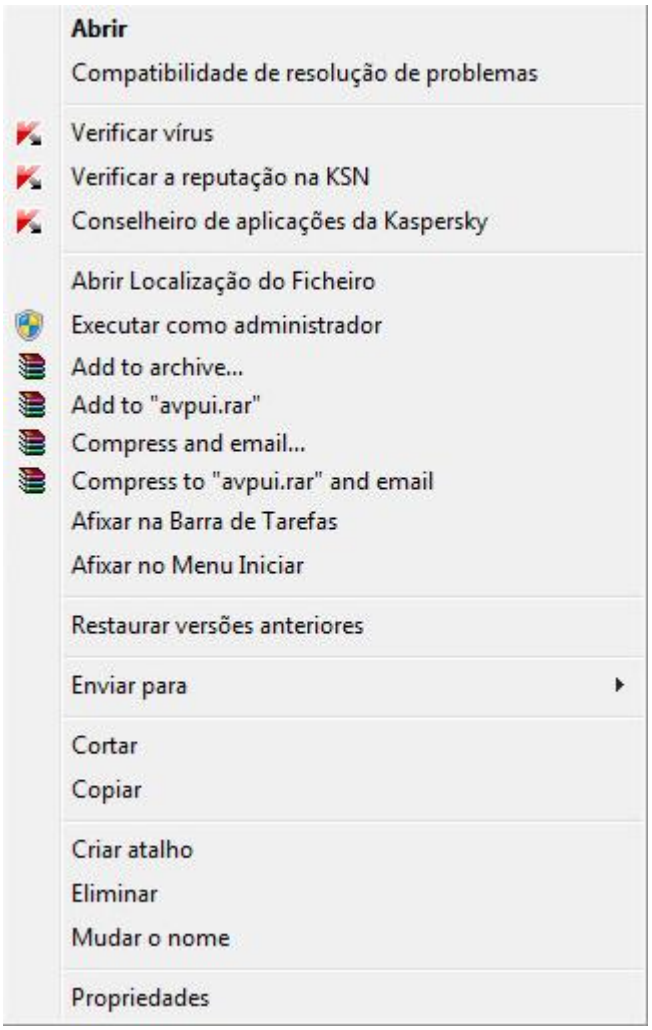

Figura 3. Menu de contexto de um ficheiro executável no Microsoft Windows

Para iniciar a verificação de um objecto a partir da janela principal da aplicação:

1. Abra a janela principal da aplicação e seleccione a secção **Verificação** na parte inferior da janela.
2. Avance para a secção **Verificação personalizada** na parte direita da janela.
3. Especifique os objectos a verificar, de uma das formas seguintes:
   - Arraste os objectos para a janela **Verificação personalizada**.
   - Clique no botão **Adicionar** e especifique um objecto na selecção de ficheiros ou pastas apresentada.
4. Clique no botão **Iniciar verificação**.

A janela **Gestor de Tarefas** é apresentada com os detalhes do progresso da verificação.

- *Para verificar um objecto, quanto à presença de vírus, através da ferramenta,*

  arraste o objecto para a ferramenta.

VERIFICAR O COMPUTADOR QUANTO A VULNERABILIDADES

Vulnerabilidades são partes de código de software desprotegidas que os intrusos poderão usar propositadamente para os seus fins, por exemplo, para copiar dados utilizados em aplicações desprotegidas. A verificação de vulnerabilidades no seu computador ajuda-o a identificar qualquer desses pontos fracos no seu computador. Recomenda-se que remova as vulnerabilidades detectadas.

- *Para iniciar uma verificação de vulnerabilidade:*

  1. Abra a janela principal da aplicação.
  2. Na parte inferior da janela, clique no botão  e seleccione a secção **Ferramentas**.

     A janela apresenta a secção **Ferramentas**.
  3. Na secção **Verificação de vulnerabilidade** clique no botão **Iniciar**.

  O Kaspersky Internet Security inicia a verificação do computador quanto a vulnerabilidades.

VERIFICAÇÃO DAS ÁREAS CRÍTICAS DO SEU COMPUTADOR QUANTO À PRESENÇA DE VÍRUS

A verificação de áreas críticas significa verificar os seguintes objectos:

- objectos carregados na inicialização do sistema operativo;
- memória do sistema;
- sectores de inicialização do disco.

- *Para iniciar uma Verificação de Áreas Críticas na janela principal da aplicação:*

  1. Abra a janela principal da aplicação e seleccione a secção **Verificação** na parte inferior da janela.

     A janela apresenta a secção **Verificar**.
  2. Abra a secção **Verificação Rápida** na parte direita da janela.

     A janela apresenta a secção **Verificação Rápida**.
  3. Clique no botão **Iniciar verificação**.

  O Kaspersky Internet Security inicia o processo de verificação.

VERIFICAR OBJECTOS PROVAVELMENTE INFECTADOS

Se suspeitar que um objecto está infectado, verifique-o utilizando o Kaspersky Internet Security.

Se a aplicação concluir a verificação e reportar que um objecto é seguro, embora o utilizador suspeite do contrário, pode enviar este objecto para o *Laboratório de vírus*: os especialistas do Laboratório de vírus verificarão o objecto. Caso se conclua que o objecto está infectado com um vírus, estes irão adicionar a descrição do novo vírus às bases de dados que serão transferidas pela aplicação através de uma actualização.

Para enviar um ficheiro para o Laboratório de Vírus:

1. Aceda à página de pedido do Laboratório de Vírus (http://support.kaspersky.com/virlab/helpdesk.html?LANG=pt).

2. Siga as instruções nesta página para enviar o seu pedido.

RESTAURAR UM OBJECTO QUE FOI APAGADO OU DESINFECTADO PELA APLICAÇÃO

A Kaspersky Lab recomenda que evite restaurar ficheiros apagados ou desinfectados, uma vez que estes poderão representar uma ameaça para o seu computador.

Para repor um objecto apagado ou desinfectado, pode utilizar a cópia de segurança criada pela aplicação durante a verificação do objecto.

O Kaspersky Internet Security não desinfecta aplicações na Loja Windows. Se após a verificação a aplicação for identificada como perigosa, será eliminada do computador.

Quando elimina uma aplicação da Loja Windows, o Kaspersky Internet Security não cria uma cópia de segurança. Para restaurar tais objectos, é necessário utilizar as ferramentas de recuperação do sistema operativo (para obter informações detalhadas, consulte a documentação do sistema operativo instalado no seu computador) ou actualize as aplicações através da Loja Windows.

Para restaurar um ficheiro que foi apagado ou desinfectado pela aplicação:

1. Abra a janela principal da aplicação.

2. Na parte inferior da janela seleccione a secção **Quarentena**.

3. Na janela **Quarentena** apresentada, seleccione o ficheiro necessário na lista e clique no botão **Restaurar** (consulte a figura seguinte).

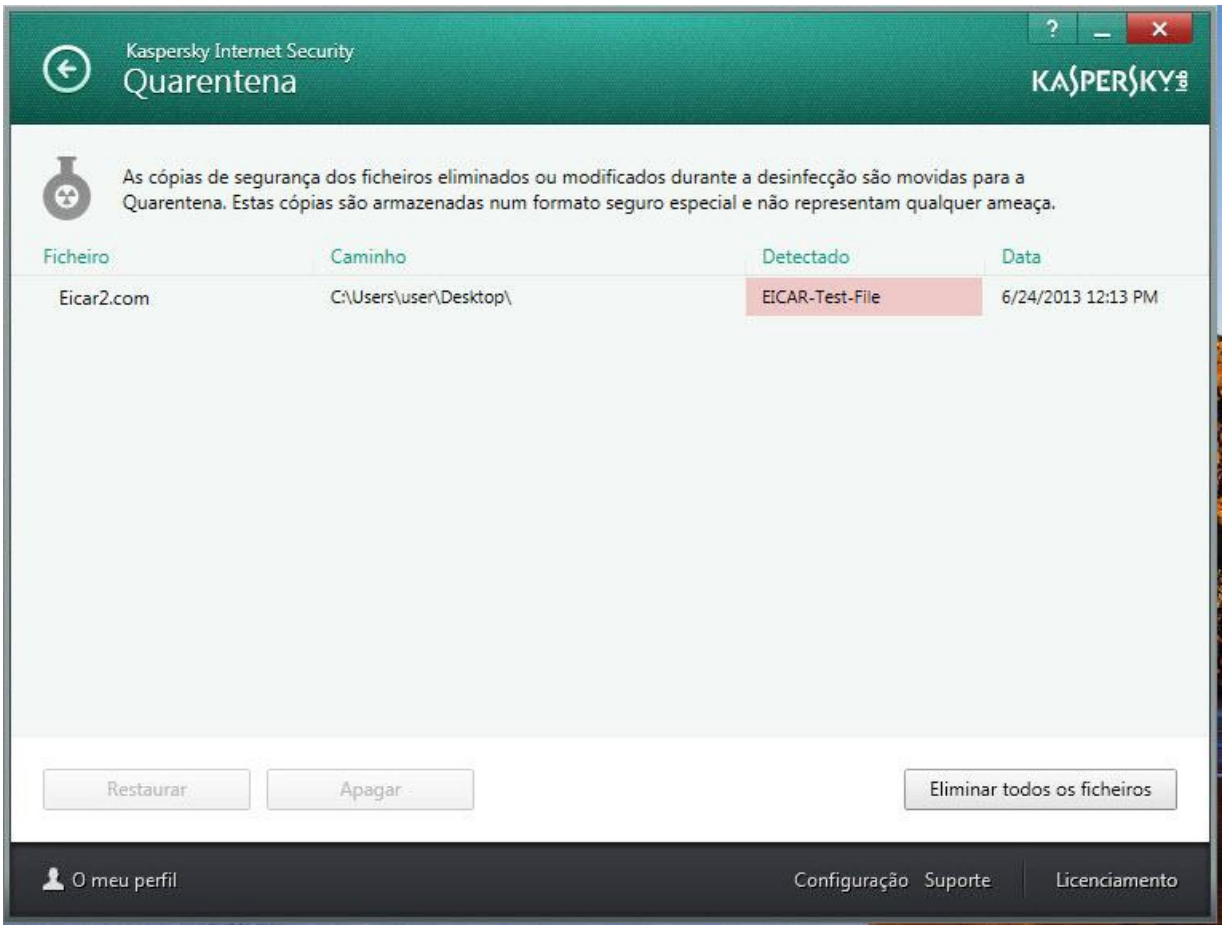

Figura 4. Janela Quarentena

RECUPERAR O SISTEMA OPERATIVO APÓS INFECÇÃO

Se suspeitar que o sistema operativo do seu computador está corrompido ou foi modificado devido a actividade de software malicioso ou a uma falha do sistema, utilize o *Assistente de Resolução de Problemas do Microsoft pós-infecção* que limpa o sistema de quaisquer vestígios de objectos maliciosos. A Kaspersky Lab recomenda que execute o Assistente depois de o computador ter sido desinfectado, para se certificar que todas as ameaças e danos causados pela infecção foram corrigidos.

O assistente verifica se existem alterações no sistema, como, por exemplo, as seguintes: acesso à rede bloqueado, extensões de formatos de ficheiro conhecidas que foram alteradas, o Painel de Controlo está bloqueado, entre outras. Existem diferentes motivos para estes tipos diferentes de alterações. Esses motivos podem incluir a actividade de programas maliciosos, configuração do sistema incorrecta, falhas do sistema ou mesmo o funcionamento incorrecto de aplicações de optimização do sistema.

Depois de a verificação estar concluída, o Assistente analisa a informação para avaliar se existem danos no sistema que requeiram atenção imediata. Com base na análise, é gerada a lista de acções necessárias para eliminar os problemas. O Assistente agrupa estas acções por categoria, com base na gravidade dos problemas detectados.

➧ *Para executar o Assistente de Resolução de Problemas do Microsoft Windows pós-infecção:*

1. Abra a janela principal da aplicação.

2. Na parte inferior da janela, seleccione a secção **Ferramentas**.

3. Na janela que se abre, na secção **Resolução de Problemas do Microsoft Windows**, clique no botão **Iniciar**.

É apresentada a janela do Assistente de Resolução de Problemas do Microsoft Windows pós-infecção.

O Assistente consiste numa série de janelas (passos), entre as quais pode navegar utilizando os botões **Anterior** e **Seguinte**. Para fechar o Assistente depois de este concluir a sua tarefa, clique no botão **Concluir**. Para parar o Assistente em qualquer altura, clique no botão **Cancelar**.

Vamos analisar em maior detalhe os passos do Assistente.

Passo 1. Iniciar o restauro do sistema

Certifique-se de que a opção do Assistente para **Procurar problemas causados por actividades de software malicioso** está seleccionada e clique no botão **Seguinte**.

Passo 2. Pesquisa de problemas

O Assistente irá procurar os problemas e danos que devem ser corrigidos. Quando a procura concluir, o Assistente avança, automaticamente, para o passo seguinte.

Passo 3. Seleccionar acções de resolução de problemas

Todos os danos detectados no passo anterior são agrupados com base no tipo de perigo que representam. Para cada grupo de danos, a Kaspersky Lab recomenda uma sequência de acções para reparar os danos. Existem três grupos de acções:

- *Acções vivamente recomendadas* eliminam problemas que constituem uma séria ameaça à segurança. Recomenda-se que execute todas as acções deste grupo.
- As *Acções recomendadas* destinam-se a reparar os danos que constituem uma ameaça. Recomenda-se que também execute todas as acções deste grupo.
- *Acções adicionais* reparam danos no sistema que não representam uma ameaça actualmente, mas que podem representar um perigo para a segurança do computador no futuro.

Para ver as acções dentro de um grupo, clique no ícone **+** à esquerda do nome do grupo.

Para que o Assistente execute uma determinada acção, seleccione a caixa de selecção à esquerda da acção correspondente. Por defeito, o Assistente executa todas as acções recomendadas e vivamente recomendadas. Se não pretender executar uma determinada acção, desmarque a caixa junto à mesma.

Recomenda-se vivamente que não desmarque as caixas seleccionadas por defeito, uma vez que ao fazê-lo deixará o seu computador vulnerável a ameaças.

Depois de definir o conjunto de acções que o Assistente irá executar, clique no botão **Seguinte**.

Passo 4. Eliminar problemas

O Assistente irá executar as acções seleccionadas no passo anterior. A correcção de problemas poderá demorar algum tempo. Depois de a resolução de problemas estar concluída, o Assistente irá, automaticamente, continuar para o passo seguinte.

Passo 5. Conclusão do Assistente

Clique no botão **Concluir** para fechar o Assistente.

CONFIGURAÇÃO DO ANTIVÍRUS DE E-MAIL

O Kaspersky Internet Security permite verificar mensagens de e-mail quanto a objectos perigosos utilizando o Antivírus de E-mail. O Antivírus de E-mail é iniciado quando o sistema operativo é iniciado e permanece em execução na RAM permanentemente, verificando todas as mensagens de e-mail que são enviadas ou recebidas através de POP3, SMTP, IMAP, MAPI e NNTP, bem como através de ligações encriptadas (SSL) em POP3, SMTP e IMAP.

Por defeito, o Antivírus de E-mail verifica quer as mensagens de entrada quer as mensagens de saída. Se necessário, pode activar a verificação apenas das mensagens recebidas.

Para configurar o Antivírus de E-mail:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, clique na ligação **Configuração**.
3. Na parte esquerda da janela, na secção **Centro de Protecção**, seleccione a componente **Antivírus de E-mail**.

   As definições de Antivírus de E-mail são apresentadas na janela.
4. Certifique-se de que o botão na parte superior da janela que activa/desactiva o Antivírus de E-mail está activado.
5. Seleccione um nível de segurança:
   - **Recomendado**. Se seleccionar este nível de segurança, o Antivírus de E-mail verifica as mensagens recebidas e enviadas e verifica os arquivos anexos.
   - **Baixo**. Se seleccionar este nível de segurança, o Antivírus de E-mail verifica apenas as mensagens recebidas sem verificar os arquivos anexos.
   - **Elevado**. Se seleccionar este nível de segurança, o Antivírus de E-mail verifica as mensagens recebidas e enviadas e verifica os arquivos anexos. Seleccionar o nível de segurança elevado significa aplicar análise heurística profunda.
6. Na lista pendente **Acção após detecção de ameaças** seleccione uma acção que o Antivírus de E-mail deve executar quando um objecto infectado é detectado (por exemplo, desinfectar).

Caso não tenham sido detectadas quaisquer ameaças numa mensagem de e-mail, ou caso todos os objectos infectados tenham sido desinfectados com êxito, a mensagem fica disponível para operações adicionais. Se o componente falhar a desinfecção de um objecto infectado, o Antivírus de E-mail renomeia ou elimina o objecto da mensagem e expande o assunto da mensagem, com uma notificação que indica que a mensagem foi processada pelo Kaspersky Internet Security. Antes de eliminar um objecto, o Kaspersky Internet Security cria um cópia de segurança do mesmo e coloca esta cópia na Quarentena (consulte a secção "Restaurar um objecto eliminado ou desinfectado pela aplicação" na página 36).

BLOQUEAR E-MAIL INDESEJADO (SPAM)

Se receber grandes quantidades de mensagens indesejadas (spam), active a componente Anti-Spam e defina o nível de segurança recomendado para o mesmo.

Para activar o Anti-Spam e definir o nível de segurança recomendado:

1. Abra a janela principal da aplicação.
2. Clique na ligação **Configuração** na parte inferior da janela para aceder à secção **Configuração**.
3. Na parte esquerda da janela, seleccione a secção **Protecção**.

4. Na parte direita da secção **Centro de protecção**, seleccione o componente **Anti-Spam**.

   A janela apresenta das definições de Anti-Spam.

5. Na parte direita da janela, active o Anti-Spam com o botão adequado.

6. Certifique-se de que o nível de segurança **Recomendado** está definido na secção **Nível de segurança**.

PROCESSAR APLICAÇÕES DESCONHECIDAS

O Kaspersky Internet Security ajuda a minimizar o risco da utilização de aplicações desconhecidas (bem como o risco de infecção de vírus e alterações não pretendidas nas definições do sistema operativo).

O Kaspersky Internet Security inclui componentes e ferramentas que permitem a verificação da reputação de uma aplicação e o controlo das respectivas actividades no computador.

NESTA SECÇÃO

VERIFICAR A REPUTAÇÃO DA APLICAÇÃO

O Kaspersky Internet Security permite-lhe saber a reputação das aplicações de utilizadores de todo o mundo. A reputação de uma aplicação inclui os seguintes critérios:

- nome do fornecedor;
- informações sobre a assinatura digital (disponíveis se existir uma assinatura digital);
- informações sobre o grupo, em que a aplicação foi incluída pelo Controlo das Aplicações ou uma maioria de utilizadores do Kaspersky Security Network;
- número de utilizadores do Kaspersky Security Network que utilizam a aplicação (disponível se a aplicação tiver sido incluída no grupo Confiável na base de dados do Kaspersky Security Network);
- hora, em que a aplicação se tornou conhecida no Kaspersky Security Network;
- países, em que a aplicação é mais comum.

A verificação da reputação da aplicação está disponível se tiver aceite participar na Kaspersky Security Network.

- *Para saber a reputação de uma aplicação,*

  abra o menu de contexto do ficheiro executável da aplicação e seleccione **Verificar a reputação na KSN** (consulte a figura seguinte).

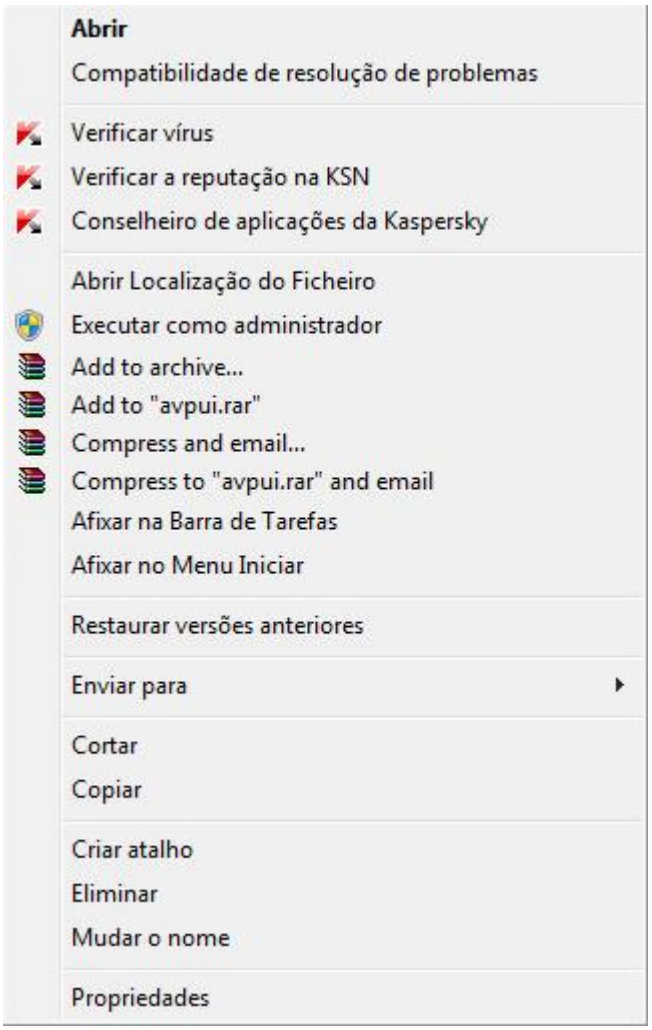

Figura 5. Menu de contexto de um ficheiro executável no Microsoft Windows

É apresentada uma janela com informação sobre a reputação da aplicação na KSN.

VEJA TAMBÉM:

Participar na Kaspersky Security Network (KSN) 69

CONTROLAR AS ACTIVIDADES DAS APLICAÇÕES NO COMPUTADOR E NA REDE

O Controlo das Aplicações impede as aplicações de executarem acções que possam ser perigosas para o sistema e garante o controlo do acesso aos recursos do sistema operativo e aos seus dados pessoais.

O Controlo das Aplicações acompanha as acções desempenhadas no sistema pelas aplicações instaladas no computador e regula-as com base em regras. Estas regras regulam actividades potencialmente perigosas das aplicações, incluindo o acesso das aplicações a recursos protegidos, tais como ficheiros e pastas, chaves de registo e endereços de rede.

Em sistemas operativos de 64-bits, os direitos das aplicações para configurar as acções seguintes não estão disponíveis:

- Acesso directo à memória física
- Gestão de controladores de impressão
- Criação de serviços
- Leitura de serviços
- Edição de serviços
- Reconfiguração de serviços
- Gestão de serviços
- Início de serviços
- Remoção de serviços
- Acesso aos dados internos do navegador
- Acesso ao objectos críticos do sistema
- Acesso ao armazenamento de passwords
- Configuração dos direitos de depuração
- Utilização das interfaces do sistema
- Utilização das interfaces do sistema (DNS).

No Microsoft Windows 8 de 64-bits, os direitos das aplicações para configurar as acções seguintes também não estão disponíveis:

- Envio de mensagem por janela a outros processos
- Operações suspeitas
- Instalação de interceptores
- Intercepção de eventos de fluxo de entrada
- Criação de capturas de ecrã.

A actividade de rede das aplicações é controlada pela componente Firewall.

Quando uma aplicação é executada pela primeira vez no computador, o Controlo das Aplicações verifica a respectiva segurança e move a aplicação para um dos grupos (Confiável, Não confiável, Restrições altas, ou Restrições baixas). O grupo define as regras que o Kaspersky Internet Security deve aplicar para controlar a actividade desta aplicação.

Pode editar as regras de controlo das aplicações manualmente.

Para editar regras de aplicações manualmente:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, clique no botão  e seleccione a secção **Controlo das Aplicações**.

   A janela apresenta a secção **Controlo de Aplicações**.

3. Na secção **Aplicações**, clique na ligação **Gerir aplicações**.

   A janela apresenta a secção **Gestão de aplicações**.

4. Clique na aplicação requerida na lista.

   É apresentada a janela de **Regras da aplicação**.

5. Especifique as regras de controlo das aplicações:

   - Para configurar regras de acesso a recursos do sistema operativo a partir de uma aplicação:

     a. No separador **Ficheiros e registo do sistema**, seleccione a categoria de recurso necessária.

     b. Clique com o botão direito na coluna com uma acção disponível no recurso (**Ler**, **Escrever**, **Apagar** ou **Criar**) para abrir o menu de contexto e seleccionar o valor necessário (**Permitir**, **Bloquear** ou **Perguntar o que fazer**).

   - Para configurar os direitos de uma aplicação para realizar várias acções no sistema operativo:

     a. No separador **Direitos**, seleccione a categoria de direitos pretendida.

     b. Clique com o botão direito do rato na coluna **Permissão** para abrir o menu de contexto e seleccione o valor pretendido (**Permitir**, **Bloquear** ou **Perguntar o que fazer**).

   - Para configurar os direitos de uma aplicação para realizar várias acções na rede:

     a. No separador **Regras de rede**, clique no botão **Adicionar**.

        É apresentada a janela **Regra de rede**.

     b. Na janela apresentada, especifique as definições de regra necessárias e clique no botão **OK**.

     c. Atribua uma prioridade à nova regra, utilizando os botões **Mover cima** e **Mover baixo** para movê-la acima ou abaixo na lista.

   - Para excluir algumas acções do âmbito do Controlo das Aplicações, no separador **Exclusões**, seleccione as caixas de verificação das acções que não devem ser controladas.

     Todas as exclusões criadas nas regras para aplicações de utilizador estão acessíveis na janela de configurações da aplicação, na secção **Ameaças e Exclusões**.

     O Controlo das Aplicações irá monitorizar e restringir as acções da aplicação de acordo com as definições especificadas.

UTILIZAR O MODO APLICAÇÕES CONFIÁVEIS

No Kaspersky Internet Security, pode criar um ambiente seguro no seu computador, o modo Aplicações Confiáveis, em que apenas as aplicações com o estado confiável podem ser executadas. O modo Aplicações Confiáveis poderá ser-lhe útil se utilizar um conjunto estável de aplicações conhecidas e não necessitar de transferir e executar frequentemente ficheiros novos e desconhecidos da Internet. Quando o modo Aplicações Confiáveis está activado, o Kaspersky Internet Security bloqueia todas as aplicações que não foram classificadas como confiáveis, segundo qualquer critério (por exemplo, informações da KSN sobre a aplicação, confiança no programa de instalação e origem da aplicação).

O modo Aplicações Confiáveis pode não existir ou não estar disponível na versão actual do Kaspersky Internet Security. A disponibilidade do modo Aplicações Confiáveis no Kaspersky Internet Security também depende da sua região e fornecedor. Indique se necessitar do modo Aplicações Confiáveis quando comprar a aplicação.

Se o modo Aplicações Confiáveis for fornecido para a sua versão do Kaspersky Internet Security mas não estiver disponível actualmente, poderá utilizar o mesmo após actualizar (consulte a secção "Actualizar bases de dados e módulos da aplicação" na página 32) da aplicação.

O modo Aplicações Confiáveis pode estar indisponível se os ficheiros de sistema se encontrarem em partições de uma unidade de disco rígido com um sistema de ficheiros não NTFS.

Antes de activar o modo Aplicações confiáveis, o Kaspersky Internet Security analisa o seu sistema operativo e as aplicações instaladas no computador. Se a análise detectar software que não pode ser classificado como confiável, não é recomendado activar o modo Aplicações Confiáveis. Bloquear aplicações não confiáveis pode afectar a utilização do computador. Pode permitir manualmente a execução das aplicações que considerar confiáveis e activar o modo Aplicações Confiáveis.

A análise do sistema operativo e das aplicações instaladas é executada quando o modo Aplicações Confiáveis é activado pela primeira vez. A análise pode demorar bastante tempo (cerca de algumas horas). A análise pode ser executada em segundo plano.

Para utilizar o modo Aplicações Confiáveis, certifique-se de que os componentes de protecção seguintes estão activados: Controlo de Aplicações, Antivírus de Ficheiros e Monitorização do Sistema. Se algum destes componentes deixar de ser executado, o modo Aplicações Confiáveis é desactivado.

Pode desactivar o modo Aplicações Confiáveis em qualquer altura, se necessário.

Para activar o modo Aplicações Confiáveis:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, clique no botão  e seleccione a secção **Controlo das Aplicações**.

   A janela apresenta a secção **Controlo de Aplicações**.
3. Na parte inferior da janela, na secção **O modo de aplicações confiáveis está desactivado**, clique na ligação **Activar**.

   Se todos os componentes de protecção requeridos estiverem activados, a janela **Activar o modo Aplicações confiáveis** é apresentada com informações sobre os componentes de protecção que têm de estar activados para que seja possível activar o modo Aplicações Confiáveis.
4. Clique no botão **Continuar**.

   A análise dos ficheiros de sistema e das aplicações instaladas é iniciada. O progresso da análise é apresentado na janela **Analisar as aplicações instaladas** apresentada.

   Aguarde até que a análise das aplicações instaladas termine. Pode minimizar a janela **Análise das aplicações instaladas**. A análise será efectuada em segundo plano. Pode ver o progresso da análise das aplicações instaladas, clicando na ligação **Progresso da análise das aplicações instaladas (<N> %)** na janela **Controlo das Aplicações**.
5. Pode ver informações sobre os resultados da análise na janela **A análise das aplicações instaladas está concluída**.

   Se forem detectados ficheiros de sistema com propriedades não reconhecidas durante a análise, é recomendado evitar activar o modo Aplicações Confiáveis. É também recomendado evitar activar o modo Aplicações Confiáveis se forem detectadas várias aplicações para as quais o Kaspersky Internet Security não tem informações suficientes para as classificar como completamente seguras. Decida se deve usar o modo Aplicações Confiáveis.
6. Clique na ligação **Permitir a execução de ficheiros de sistema desconhecidos e continuar**.

   Pode ver informações sobre os ficheiros de sistema não confiáveis clicando na ligação **Aceder à lista de ficheiros de sistema desconhecidos**. A lista de ficheiros de sistema não confiáveis é apresentada na janela **Ficheiros de sistema desconhecidos**. Também pode cancelar a utilização do modo Aplicações Confiáveis clicando no botão **Não activar o modo de aplicações confiáveis**.
7. Clique no botão **Activar o modo de aplicações confiáveis**.

O modo Aplicações Confiáveis está agora activado. O Kaspersky Internet Security irá bloquear todas as aplicações que não forem classificadas como confiáveis. Após este passo, a aplicação continua para a janela Controlo da Aplicações.

Para desactivar o modo Aplicações Confiáveis:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, clique no botão  e seleccione a secção **Controlo das Aplicações**.

   A janela apresenta a secção **Controlo de Aplicações**.
3. Na parte inferior da janela, na secção **O modo de aplicações confiáveis está activado**, clique na ligação **Desactivar**.

O modo Aplicações Confiáveis está agora desactivado.

PROTEGER DADOS PRIVADOS CONTRA ROUBO

O Kaspersky Internet Security ajuda-o a proteger os dados privados contra roubo:

- Passwords, nomes de utilizador e outros dados de registo
- Números de contas e números de cartões bancários

O Kaspersky Internet Security inclui componentes e ferramentas que permitem proteger os seus dados privados contra roubo por criminosos, através de phishing e intercepção dos dados introduzidos no teclado.

A protecção contra phishing é garantida pelo Anti-Phishing, implementado nas componentes Antivírus de Internet, Anti-Spam e Antivírus de MI. Active estes componentes para garantir uma protecção abrangente contra phishing.

A protecção contra a intercepção de dados introduzidos no teclado é assegurada pelo Teclado Virtual, bem como a introdução de dados segura com o teclado do computador.

O Assistente de Limpeza de vestígio de actividade limpa o computador de todas as informações sobre as actividades do utilizador.

O Pagamento Seguro protege os dados quando utiliza serviços bancários na Internet e faz compras em lojas online.

A protecção contra a transferência de dados privados é fornecida por uma das ferramentas do Controlo Parental (consulte a secção "Utilizar o Controlo Parental" na página 54).

NESTA SECÇÃO

TECLADO VIRTUAL

Ao utilizar Internet, necessita frequentemente de introduzir os seus dados pessoais ou o seu nome de utilizador e password. Isto acontece, por exemplo, quando regista contas em sites, quando faz compras online ou quando utiliza serviços bancários na Internet.

Existe o risco de estas informações pessoais serem interceptadas através de interceptores de teclado ou registadores de teclas digitadas (keyloggers), os quais são programas que registam as sequências de teclas.

A ferramenta do Teclado virtual impede a intercepção dos dados inseridos através do teclado.

O Teclado virtual impede a intercepção de dados pessoais apenas quando utilizado com os navegadores Microsoft Internet Explorer, Mozilla Firefox ou Google Chrome. Quando é utilizado com outros navegadores, o Teclado virtual não protege os dados pessoais introduzidos contra intercepção.

O Teclado virtual não está disponível no Microsoft Internet Explorer 10 a partir da Loja Windows, bem como no Microsoft Internet Explorer 10 se a caixa de selecção **Modo de protecção avançada** estiver seleccionada nas definições do navegador. Neste caso, é recomendado abrir o Teclado virtual na interface do Kaspersky Internet Security.

O Teclado virtual não consegue proteger os seus dados pessoais se o site, que requer a inserção desses dados, tiver sido pirateado, uma vez que neste caso a informação será directamente obtida pelos intrusos.

Muitos programas classificados como spyware podem fazer capturas de ecrã, que, em seguida, são transmitidas automaticamente a um intruso para análise subsequente e para furtar os dados pessoais do utilizador. O Teclado virtual protege os dados pessoais introduzidos de tentativas de interceptar os mesmos, utilizando capturas de ecrã.

O Teclado virtual não impede as capturas de ecrã com a tecla **Print Screen** e com outros combinações de teclas permitidas definidas pelo sistema operativo, ou utilizando DirectX®.

O Teclado virtual tem as funcionalidades seguintes:

- Pode clicar nos botões do Teclado virtual com o rato.
- Ao contrário dos teclados de hardware, no Teclado virtual não é possível premir várias teclas em simultâneo. É por este motivo que para utilizar combinações de teclas (como **ALT**+**F4**) é necessário premir a primeira tecla (por exemplo, **ALT**), em seguida, a segunda tecla (por exemplo, **F4**) e, em seguida, a primeira tecla novamente. O segundo clique na tecla funciona da mesma forma que o libertar de uma tecla num teclado de hardware.
- O idioma do Teclado virtual pode ser alterado utilizando o mesmo atalho do sistema operativo para o teclado de hardware. Para tal, pode clicar com o botão direito do rato noutra tecla (por exemplo, se o atalho **LEFT ALT**+**SHIFT** estiver configurado nas definições do sistema operativo para mudar o idioma do teclado, clique com o botão esquerdo na tecla **LEFT ALT** e, em seguida, em clique com o botão direito na tecla **SHIFT**).

Para garantir a protecção dos dados introduzidos com o Teclado virtual, reinicie o seu computador depois de instalar o Kaspersky Internet Security.

Pode abrir o Teclado virtual de uma das seguintes formas:

- No menu de contexto do ícone da aplicação na área de notificação da barra de ferramentas
- Na janela principal da aplicação
- Nas janelas dos navegadores Microsoft Internet Explorer, Mozilla Firefox ou Google Chrome
- Utilizando o ícone de início rápido do Teclado virtual nos campos de introdução de dados em sites

  Pode configurar a apresentação do ícone de início rápido nos campos de introdução de dados em sites.

  Quando o Teclado virtual é utilizado, o Kaspersky Internet Security desactiva a opção de preenchimento automático para os campos de introdução nos sites.

- Premindo uma combinação de teclas do teclado
- Através da Ferramenta Kaspersky Internet Security (apenas em Microsoft Windows Vista e Microsoft Windows 7)

- *Para abrir o Teclado virtual a partir do menu de contexto do ícone da aplicação na área de notificação da barra de ferramentas,*

  no menu de contexto do ícone da aplicação (consulte a imagem seguinte), seleccione **Ferramentas → Virtual Teclado virtual** (consulte a imagem seguinte)

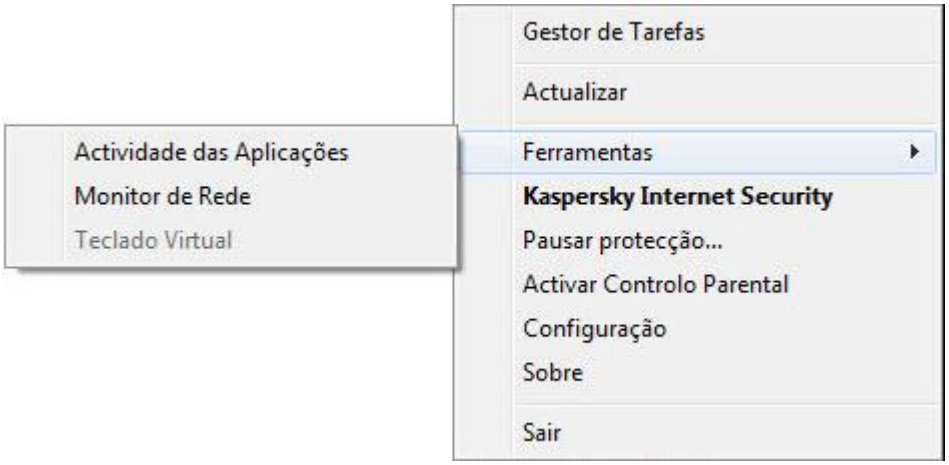

Figura 6. Menu de contexto do Kaspersky Internet Security

- *Para abrir o Teclado virtual a partir da janela principal da aplicação,*

  seleccione a secção **Teclado virtual** na parte inferior da janela principal da aplicação.

- *Para abrir o Teclado Virtual a partir de uma janela do navegador,*

  na barra de ferramentas do Microsoft Internet Explorer, Mozilla Firefox ou Google Chrome, clique o botão 

Teclado virtual.

- *Para abrir o Teclado virtual utilizando o teclado de hardware,*

  prima o atalho **CTRL+ALT+SHIFT+P**.

- *Para abrir o Teclado virtual com a ferramenta,*

  clique o botão ferramenta ao qual esta acção foi atribuída.

- *Para configurar a apresentação do ícone de início rápido do Teclado virtual nos campos de introdução de dados em sites:*

  1. Abra a janela principal da aplicação.
  2. Na parte inferior da janela, clique na ligação **Configuração**.
  3. Na janela **Configuração** apresentada, na secção **Adicional**, seleccione a sub-secção **Introdução de dados segura**.

     A janela apresenta as definições da introdução de dados segura.
  4. Se necessário, na secção do **Teclado Virtual**, seleccione a caixa de selecção **Abrir o Teclado Virtual premindo as teclas CTRL+ALT+SHIFT+P**.
  5. Se pretender que o ícone de início rápido do Teclado Virtual seja apresentado nos campos de introdução de dados, seleccione a caixa de verificação **Mostrar ícone de início rápido nos campos de introdução de dados**.
  6. Se pretender que o ícone de início rápido do Teclado Virtual seja apresentado apenas quando são acedidos sites especificados:

a. Na secção **Teclado Virtual**, clique na ligação **Editar categorias**.

   A janela **Categorias do Teclado virtual** é aberta.

b. Seleccione as caixas de verificação para categorias de sites, nos quais o ícone de início rápido deverá ser apresentado nos campos de introdução de dados.

   O ícone de início rápido do Teclado Virtual será apresentado quando aceder a um site pertencente a qualquer uma das categorias seleccionadas.

c. Se pretender activar ou desactivar a apresentação do ícone de início rápido do Teclado Virtual num site específico:

   a. Clique na ligação **Configurar exclusões**.

      A janela **Exclusões para o Teclado virtual** é aberta.

   b. Na parte inferior da janela, clique no botão **Adicionar**.

      É apresentada uma janela para adicionar uma exclusão para o Teclado virtual.

   c. No campo **URL**, introduza o URL de um site.

   d. Se pretender que o ícone de início rápido do Teclado Virtual seja apresentado (ou não apresentado) apenas numa página da Web especificada, na secção **Âmbito**, seleccione **Aplicar à página especificada**.

   e. Na secção **Ícone do Teclado Virtual**, especifique se o ícone de início rápido do Teclado Virtual deve ser apresentado na página da Internet especificada.

   f. Clique no botão **Adicionar**.

      O site especificado é apresentado na lista na janela **Exclusões para o Teclado Virtual**. Ao aceder ao site especificado, o ícone de início rápido do Teclado Virtual será apresentado de acordo com as definições especificadas.

PROTECÇÃO DA INTRODUÇÃO DE DADOS COM O TECLADO DO COMPUTADOR

A protecção da introdução de dados com o teclado do computador permite evitar a intercepção dos dados introduzidos com o teclado.

A protecção de introdução de dados a partir do teclado do computador está disponível apenas para os navegadores Microsoft Internet Explorer, Mozilla Firefox e Google Chrome. Quando utilizar outros navegadores, os dados introduzidos com o teclado do computador não estão protegidos contra intercepção.

A protecção de introdução de dados não está disponível no Microsoft Internet Explorer a partir da Loja Windows, bem como no Microsoft Internet Explorer 10 se a caixa de selecção **Modo de protecção avançada** estiver seleccionada nas definições do navegador.

A protecção da introdução de dados com o teclado do computador não protege os seus dados pessoais caso um site que requeira a introdução desses dados tiver sido alvo de ataque, já que neste caso as informações são obtidas pelos intrusos directamente a partir do site.

Pode configurar a protecção da introdução de dados com o teclado do computador em vários sites. Após configurar a protecção de introdução de dados a partir do teclado do computador, não é necessário efectuar acções adicionais ao introduzir dados.

Para proteger os dados introduzidos com o teclado do computador, reinicie o seu computador após instalar o Kaspersky Internet Security.

Para configurar a protecção da introdução de dados com o teclado do computador:

1. Abra a janela principal da aplicação.
2. Clique na ligação **Configuração** na parte inferior da janela para aceder à secção **Configuração**.
3. Na secção **Adicional** seleccione a sub-secção **Introdução de dados segura**.

   A janela apresenta as definições da introdução de dados segura.
4. Seleccione a caixa de selecção **Activar a introdução de dados segura** na secção **Teclado de hardware** na secção inferior da janela.
5. Especifique o âmbito de protecção para a introdução de dados no teclado de hardware:
   a. Abra a janela **Categorias de teclado de hardware** clicando na ligação **Editar categorias** na parte inferior da secção **Teclado de hardware**.
   b. Seleccione as caixas de selecção das categorias de sites para as quais pretende proteger os dados introduzidos com o teclado.
   c. Se pretender activar a protecção da introdução de dados com o teclado num site específico:
      a. Abra a janela **Exclusões de teclado de hardware** clicando na ligação **Configurar exclusões**.
      b. Na janela apresentada, clique no botão **Adicionar**.

         É apresentada uma janela para adicionar uma exclusão para o teclado de hardware.
      c. Na janela apresentada, no campo **URL**, introduza um URL de um site.
      d. Seleccione uma das opções de Introdução de dados segura neste site (**Aplicar a uma página especificada** ou **Aplicar a todo o site**).
      e. Seleccione uma acção a realizar pela Introdução de dados segura neste site (**Proteger** ou **Não proteger**).
      f. Clique no botão **Adicionar**.

O site especificado é apresentado na lista na janela **Exclusões de teclado de hardware**. Ao aceder a este site, a Introdução de dados segura estará activa e a funcionar de acordo com as definições especificadas.

CONFIGURAÇÃO DO PAGAMENTO SEGURO

Para facultar protecção para os dados confidenciais introduzidos em sites bancários e sistemas de pagamento (tais como, números de cartões bancários, palavras-passe para acesso a serviços bancários online), bem como para impedir o furto de activos ao efectuar pagamentos online, o Kaspersky Internet Security permite abrir esses websites no modo Execução Segura para Sites.

A Execução Segura para Sites não pode ser executada se a caixa de selecção **Activar Autodefesa** estiver desmarcada na secção **Configurações avançadas**, na subsecção **Autodefesa** da janela de configuração da aplicação.

Pode configurar o Pagamento Seguro de modo a que seja executado automaticamente em sites de bancos e sistemas de pagamento.

Esta função não está disponível no Microsoft Internet Explorer 10, se a caixa de selecção **Modo de protecção**

avançada estiver assinalada nas definições do navegador. Pode activar o modo Execução Segura para Sites a partir da interface do Kaspersky Internet Security.

Ao ser executado em Microsoft Windows 8 x64, o Kaspersky Internet Security não protege as janelas da Execução Segura para Sites de capturas de ecrã não autorizadas.

Para configurar o Pagamento Seguro:

1. Abra a janela principal da aplicação.
2. Clique na ligação **Configuração** na parte inferior da janela principal aceda à secção **Configuração**.
3. Na parte esquerda da janela, seleccione a secção **Protecção**.
4. Na parte direita da secção **Centro de protecção**, seleccione a sub-secção **Pagamento Seguro**.

   A janela apresenta as definições do componente Pagamento Seguro.
5. Pode activar o componente Pagamento Seguro utilizando o botão na parte superior da janela.
6. Para activar a notificação de vulnerabilidades detectadas no sistema operativo antes de executar a Execução Segura para Sites, seleccione a caixa de selecção **Notificar sobre vulnerabilidades do sistema operativo**.

Para configurar o Pagamento Seguro para um site específico:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela principal, seleccione a secção **Pagamento Seguro**.

   A janela apresenta a secção **Pagamento Seguro**.
3. Clique no botão **Adicionar site de banco ou sistema de pagamento**.

   A parte direita da janela apresenta campos para adicionar os detalhes do site.
4. No campo **Site de banco ou sistema de pagamento**, introduza o URL de um site que pretende abrir na Execução Segura para Sites.

   O URL de um site tem de ser antecedido pelo prefixo do protocolo https://, inserido por predefinição pela Execução Segura para Sites.
5. Se necessário, no campo **Descrição**, introduza o nome ou a descrição do site.
6. Seleccione a acção que a Execução Segura para Sites realiza quando abre o site:
   - Se pretender que o Kaspersky Internet Security solicite a execução da Execução Segura para Sites sempre que abrir o site, seleccione **Perguntar o que fazer**.
   - Se pretender que o Kaspersky Internet Security abra o site na Execução Segura para Sites automaticamente, seleccione **Executar o navegador protegido**.
   - Se pretender desactivar o Pagamento Seguro para o site, seleccione **Não executar o navegador protegido**.
7. Na parte direita da janela, clique no botão **Adicionar**.

O site de um banco ou sistema de pagamento é apresentado numa lista na parte esquerda da janela.

ELIMINAÇÃO DE VESTÍGIOS DE ACTIVIDADE

As acções do utilizador no computador são gravadas no sistema operativo. São guardadas as seguintes informações:

- Detalhes das consultas de procuras introduzidas pelos utilizadores e os sites da Internet visitados
- Informações sobre aplicações iniciadas e ficheiros abertos e guardados
- entradas do registo de eventos do Microsoft Windows
- Outras informações sobre a actividade do utilizador

A informação sobre as acções do utilizador que incluem informações confidenciais podem ficar disponíveis a intrusos e a utilizadores não autorizados.

O Kaspersky Internet Security inclui o Assistente de Eliminação de vestígios de actividade que limpa vestígios da actividade do utilizador no sistema.

Para executar o Assistente de Eliminação de vestígios de actividade:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, seleccione a secção **Ferramentas**.
3. Na janela que se abre, na secção **Eliminar vestígio de actividade**, clique no botão **Iniciar**.

O Assistente consiste numa série de janelas (passos), entre as quais pode navegar utilizando os botões **Anterior** e **Seguinte**. Para fechar o Assistente depois de este concluir a sua tarefa, clique no botão **Concluir**. Para parar o Assistente em qualquer altura, clique no botão **Cancelar**.

Vamos analisar em maior detalhe os passos do Assistente.

Passo 1. Iniciar o Assistente

Certifique-se de que a caixa de selecção **Procurar vestígios de actividades de utilizador** estiver seleccionada. Clique no botão **Seguinte** para iniciar o Assistente.

Passo 2. Pesquisa de sinais de actividades

Este assistente procura vestígios de actividades de software malicioso no seu computador. A pesquisa poderá demorar algum tempo. Quando a procura concluir, o Assistente avança, automaticamente, para o passo seguinte.

Passo 3. Seleccionar acções para Eliminação de vestígios de actividade

Quando procura está concluída, o Assistente informa o utilizador dos vestígios de actividade detectados e indica as acções que podem ser executadas para eliminar os vestígios de actividade detectados (consulte a figura seguinte).

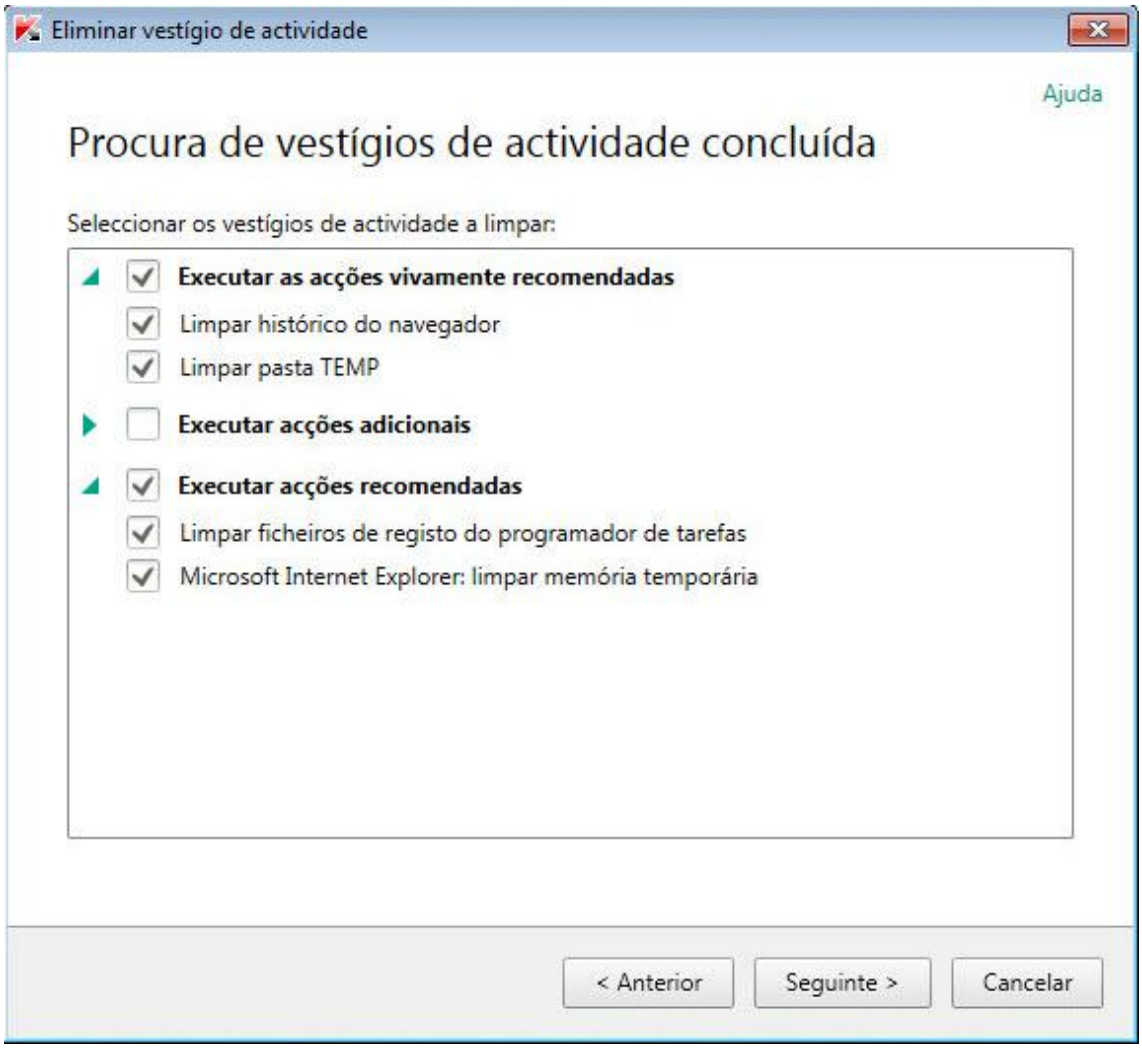

Figura 7. Vestígios de actividade detectados e recomendações para os eliminar

Para ver as acções dentro de um grupo, clique no ícone ▸ à esquerda do nome do grupo.

Para que o Assistente execute uma determinada acção, seleccione a caixa de selecção à esquerda da acção correspondente. Por defeito, o Assistente executa todas as acções recomendadas e vivamente recomendadas. Se não pretender executar uma determinada acção, desmarque a caixa junto à mesma.

Não é recomendado desmarcar as caixas de selecção seleccionadas por defeito. Tal pode colocar em perigo a segurança do seu computador.

Depois de definir o conjunto de acções que o Assistente irá executar, clique no botão **Seguinte**.

Passo 4. Eliminação de vestígios de actividade

O Assistente irá executar as acções seleccionadas no passo anterior. A eliminação de vestígios de actividades pode demorar algum tempo. Para limpar determinados vestígios de actividade, poderá ser necessário reiniciar o computador. Nesse caso, será notificado pelo Assistente.

Quando a limpeza concluir, o Assistente avança automaticamente para o passo seguinte.

Passo 5. Conclusão do Assistente

Clique no botão **Concluir** para fechar o Assistente.

VERIFICAR A SEGURANÇA DOS SITES

O Kaspersky Internet Security permite verificar um site quanto à segurança antes de aceder a esse site através de uma ligação. Os sites são verificados utilizando o *Conselheiro de URLs da Kaspersky* e o *Filtro da Internet* integrados no componente Antivírus de Internet.

O Conselheiro de URLs da Kaspersky não está disponível no navegador Microsoft Internet Explorer 10 a partir da Loja Windows, bem como no Microsoft Internet Explorer 10 se a caixa de selecção **Modo de protecção avançada** estiver seleccionada nas definições do navegador.

O Conselheiro de URLs da Kaspersky está integrado nos navegadores Microsoft Internet Explorer, Google Chrome e Mozilla Firefox, verificando ligações de páginas da Web abertas no navegador. O Kaspersky Internet Security apresenta um dos seguintes ícones junto a cada ligação:

- – se a página da Web aberta ao clicar na ligação for segura, de acordo com a Kaspersky Lab.
- – se não existirem informações sobre o estado de segurança da página da Web aberta ao clicar na ligação.
- – se a página da Web aberta ao clicar na ligação for perigosa, de acordo com a Kaspersky Lab.

Para ver uma janela instantânea com mais detalhes sobre a ligação, aponte para o ícone correspondente.

Por predefinição, o Kaspersky Internet Security verifica ligações apenas nos resultados da pesquisa. Pode activar a verificação de ligações em cada site.

Para activar a verificação de ligações em sites:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela principal, clique na ligação **Configuração**. É apresentada a janela **Configuração**.
3. Na secção **Centro de protecção** seleccione a sub-secção **Antivírus de Internet**.

   A janela apresenta das definições do Antivírus de Internet.
4. Na parte inferior da janela, clique na ligação **Configurações avançadas**. É apresentada a janela de configurações avançadas do Antivírus de Internet.
5. Na secção **Conselheiro de URLs da Kaspersky** seleccione a caixa de selecção **Verificar URLs**.
6. Se pretende que o Antivírus de Internet verifique os conteúdos de todos os sites, seleccione **Em todos os sites excepto nos especificados**.

   Se necessário, especifique as páginas confiáveis, clicando no botão **Configurar exclusões**. O Antivírus de Internet não verifica o conteúdo das páginas de Internet especificadas e das ligações encriptadas com os sites especificados.
7. Se pretender que o Antivírus de Internet verifique apenas os conteúdos das páginas especificadas:

   a. Seleccione **Apenas nos sites especificados**.

   b. Clique na ligação **Configurar sites verificados**.

   c. Na janela **Configurar sites verificados** apresentada, clique no botão **Adicionar**.

d. Na janela **Adicionar URL** apresentada, introduza o URL de uma página da Internet cujo conteúdo pretende verificar.

e. Seleccione um estado para a verificação da página da Internet (se o estado for *Activo*, o Antivírus de Internet verifica os conteúdos da página da Internet).

f. Clique no botão **Adicionar**.

A página especificada é apresentada na lista na janela **URLs verificados**. O Antivírus de Internet verifica os URLs nesta página da Internet.

8. Se pretender editar as definições avançadas da verificação de URLs, na janela **Definições avançadas de Antivírus de Internet**, na secção **Conselheiro de URLs da Kaspersky** clique na ligação **Configurar o Conselheiro de URLs da Kaspersky**.

A janela **Configurar o Conselheiro de URLs da Kaspersky** é apresentada.

9. Se pretender que o Antivírus de Internet o notifique quanto à segurança das ligações em todas as páginas da Internet, na secção **URLs verificados** seleccione **Todos os URLs**.

10. Se pretender que o Antivírus de Internet apresenta informações sobre se uma ligação pertence a uma categoria específica de conteúdo de sites (por exemplo, *Linguagem explícita*):

a. Seleccione a caixa de selecção **Mostrar informações sobre as categorias de conteúdo de objectos da Internet**.

b. Seleccione as caixas de selecção junto às categorias de conteúdos de sites relativamente às quais as informações serão apresentadas em comentários.

O Antivírus de Internet verifica as ligações em páginas da Internet especificadas e apresenta informações sobre as categorias das ligações de acordo com as definições actuais.

UTILIZAR O CONTROLO PARENTAL

O *Controlo Parental* permite monitorizar as acções realizadas pelos utilizadores no computador local e online. Pode utilizar o Controlo Parental para restringir o acesso aos recursos e aplicações da Internet, bem como visualizar os relatórios das actividades dos utilizadores.

Actualmente, cada vez mais crianças e adolescentes têm acesso a computadores e à Internet. A utilização de computadores e da Internet representa vários desafios para as crianças:

- Perda de tempo e/ou dinheiro em visitas a salas de chat, recursos de jogos, lojas online e leilões
- Acesso a sites destinados a adultos, como por exemplo os que apresentam pornografia, conteúdos extremistas, armas de fogo, abuso de drogas e violência explícita
- Transferência de ficheiros infectados com software malicioso
- Riscos para a saúde pela utilização excessiva do computador
- Contacto com pessoas desconhecidas, que podem fazer-se passar por colegas para obterem informações pessoais de utilizadores menores de idade, tais como o nome real, morada física, horas do dia em que ninguém está em casa.

O Controlo Parental permite reduzir os riscos inerentes à utilização do computador e da Internet. Para tal, estão disponíveis as seguintes funções do módulo:

- Limitação do tempo de utilização do computador e da Internet
- Criação de listas de aplicações e jogos permitidos e bloqueados, bem como restringir temporariamente a utilização das aplicações permitidas

- Criação de listas de sites permitidos e bloqueados e bloqueio selectivo de categorias de sites com conteúdos inapropriados
- Activação de um modo de pesquisa segura através de motores de pesquisa (as ligações a sites com conteúdos duvidosos não são apresentadas nos resultados de pesquisa)
- Restrição da transferência de ficheiros a partir da Internet
- Criação de listas de contactos permitidos ou bloqueados para clientes de mensagens instantâneas (MI) e redes sociais
- Visualização de registos de mensagens de clientes de MI e redes sociais
- Bloqueio do envio de determinados dados pessoais
- Procura de determinadas palavras-chave em registos de mensagens

Pode configurar as funções do Controlo Parental para cada conta de utilizador num computador individualmente. Também pode ver os relatórios do Controlo Parental sobre as actividades dos utilizadores monitorizados.

NESTA SECÇÃO

CONTROLAR A UTILIZAÇÃO DO COMPUTADOR

O Controlo Parental permite limitar o tempo despendido pelo utilizado no computador. Pode especificar um intervalo de tempo durante o qual o Controlo Parental deve bloquear o acesso ao computador (à noite), bem como o limite de tempo total de utilização diária do computador. Pode especificar limites diferentes para dias da semana e para fins-de-semana.

Para configurar as restrições impostas ao tempo de utilização do computador:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, clique no botão  e seleccione a secção **Controlo Parental**.

   A janela apresenta a secção **Controlo Parental**.
3. Clique na ligação com o nome de uma conta de utilizador para aceder a uma janela que fornece estatísticas das actividades do utilizador.
4. Clique na ligação **Configuração** na secção **Computador** para aceder à janela de definições do Controlo de utilização do computador.
5. Para especificar um intervalo durante o qual o Controlo Parental irá bloquear o acesso ao computador, seleccione a caixa de selecção **Bloquear o acesso ao fim do dia** nas secções **Dias da semana** e **Fins-de-semana** e seleccione as horas do intervalo nas listas pendentes junto às caixas de selecção.

Pode configurar uma agenda de utilização do computador utilizando uma tabela. Para ver a tabela, clique no botão  .

O Controlo Parental irá bloquear o acesso do utilizador ao computador durante o intervalo de tempo especificado.

6. Para limitar o tempo total de utilização do computador, seleccione as caixas de selecção **Restringir o acesso diário até** nas secções **Dias da semana** e **Fins-de-semana** e seleccione as horas do intervalo nas listas pendentes junto às caixas de selecção.

   O Controlo Parental irá bloquear o acesso do utilizador ao computador quando o tempo total de utilização do computador ao longo do dia exceder o intervalo especificado.

7. Para definir intervalos nas sessões de utilização do computador, na secção **Falha** seleccione a caixa de selecção **Bloquear o acesso a cada** e, em seguida, seleccione os valores para a frequência (por exemplo, de hora em hora) e a duração (por exemplo, 10 minutos) de intervalos nas listas pendentes junto à caixa de selecção.

O Controlo Parental irá bloquear o acesso do utilizador ao computador de acordo com as definições actuais.

CONTROLAR A UTILIZAÇÃO DA INTERNET

Ao utilizar o Controlo Parental, pode limitar o tempo de utilização da Internet e proibir os utilizadores de aceder a determinadas categorias de site ou sites especificados. Adicionalmente, pode proibir o utilizador de transferir ficheiros de determinados tipos (tais como arquivos ou vídeos) da Internet.

- *Para definir uma limitação ao tempo de utilização da Internet:*

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, clique no botão  e seleccione a secção **Controlo Parental**.

   A janela apresenta a secção **Controlo Parental**.
3. Clique na ligação com o nome de uma conta de utilizador para aceder a uma janela que fornece estatísticas das actividades do utilizador.
4. Clique na ligação **Configuração** na secção **Internet** para abrir a janela de definições do controlo de utilização da Internet.
5. Se pretender limitar o tempo total de utilização da Internet durante os dias da semana, na secção **Restrição de acesso à Internet** seleccione a caixa de selecção **Acesso restrito durante dias da semana** e, em seguida, seleccione um valor para o tempo limite na lista pendente junto à caixa de selecção.
6. Se pretender limitar o tempo total de utilização da Internet durante os fins-de-semana, seleccione **Acesso restrito durante fins de semana** e, em seguida, seleccione um valor para o tempo limite na lista pendente junto à caixa de selecção.

O Controlo Parental irá limitar o tempo total gasto na Internet pelo utilizar, conforme os valores especificados.

- *Para restringir a visita de sites específicos:*

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, clique no botão  e seleccione a secção **Controlo Parental**.

   A janela apresenta a secção **Controlo Parental**.
3. Clique na ligação com o nome de uma conta de utilizador para aceder a uma janela que fornece estatísticas das actividades do utilizador.
4. Clique na ligação **Configuração** na secção **Internet** para abrir a janela de definições do controlo de utilização da Internet.

5. Para evitar conteúdo sexual nos resultados da procura, na secção **Controlo da Navegação na Internet** seleccione a caixa de selecção **Activar Pesquisa Segura**.

   Não será apresentado qualquer conteúdo sexual nos resultados de pesquisa ao procurar informações com motores de busca (tais como Google, Bing®, Yahoo!™).

6. Para bloquear o acesso aos sites de determinadas categorias:

   a. Na secção **Controlo da Navegação na Internet** seleccione a caixa de selecção **Bloquear acesso aos sites seguintes**.

   b. Seleccione **Sites para adultos** e clique na ligação **Seleccionar categorias de sites** para abrir a janela **Bloquear o acesso às categorias de sites seguintes**.

   c. Seleccione as caixas de selecção junto às categorias de sites que devem ser bloqueadas.

      O Controlo Parental irá bloquear todas as tentativas do utilizador de abrir um site se os seus conteúdos estiverem classificados entre uma das categorias bloqueadas.

7. Para bloquear o acesso a sites específicos:

   a. Na secção **Controlo da Navegação na Internet** seleccione a caixa de selecção **Bloquear acesso aos sites seguintes**.

   b. Seleccione **Todos os sites excepto as exclusões permitidas na lista** e clique na ligação **Adicionar exclusões** para abrir a janela **Excluir sites**.

   c. Na parte inferior da janela, clique no botão **Adicionar**.

      É apresentada a janela **Adicionar novo site**.

   d. Introduza o endereço do site a que pretende proibir o acesso, preenchendo o campo **URL**.

   e. Defina um âmbito de bloqueio na secção **Âmbito**: todo o site ou apenas a página especificada.

   f. Se pretender bloquear o site especificado, na secção **Acção**, seleccione **Bloquear**.

   g. Clique no botão **Adicionar**.

O site especificado é apresentado na lista na janela **Excluir sites**. O Controlo Parental irá bloquear todas as tentativas do utilizador de abrir qualquer site incluído na lista, de acordo com as definições actuais.

Para proibir a transferência de ficheiros de determinados tipos da Internet:

1. Abra a janela principal da aplicação.

2. Na parte inferior da janela, clique no botão  e seleccione a secção **Controlo Parental**.

   A janela apresenta a secção **Controlo Parental**.

3. Clique na ligação com o nome de uma conta de utilizador para aceder a uma janela que fornece estatísticas das actividades do utilizador.

4. Clique na ligação **Configuração** na secção **Internet** para abrir a janela de definições do controlo de utilização da Internet.

5. Na secção **Limitar a transferência de ficheiros** seleccione as caixas de selecção junto aos tipos de ficheiro que devem ser bloqueados quando for efectuada uma tentativa de transferência.

O Controlo Parental irá bloquear a transferência de ficheiros dos tipos especificados da Internet.

CONTROLAR A EXECUÇÃO DE JOGOS E APLICAÇÕES

Ao utilizar o Controlo Parental pode permitir ou interditar que o utilizador inicie jogos, conforme a respectiva classificação etária. Pode também proibir o utilizador de iniciar aplicações especificadas (tais como jogos ou clientes de MI) ou limitar o tempo de utilização dessas aplicações.

Para bloquear jogos com conteúdo inapropriado à idade do utilizador:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, clique no botão  e seleccione a secção **Controlo Parental**.

   A janela apresenta a secção **Controlo Parental**.
3. Clique na ligação com o nome de uma conta de utilizador para aceder a uma janela que fornece estatísticas das actividades do utilizador.
4. Clique na ligação **Configuração** na secção **Aplicações** para aceder à janela de definições do Controlo de Arranque das Aplicações.
5. Na secção **Bloquear jogos por conteúdo** pode bloquear o início dos jogos que não são apropriados para o utilizador seleccionado, devido à idade do utilizador e/ou devido ao conteúdo do jogo:
   a. Se pretender bloquear todos os jogos com conteúdo inapropriado para a idade do utilizador, seleccione a caixa de selecção **Bloquear jogos por classificação etária** e seleccione uma opção de restrição de idade na lista pendente, junto à caixa de selecção.
   b. Se pretender bloquear jogos com conteúdo de uma determinada categoria:
      a. Seleccione a caixa de selecção **Bloquear jogos de categorias de adultos**.
      b. Clique na ligação **Seleccionar categorias de jogos** para abrir a janela **Restringir o início de jogos por conteúdo**.
      c. Seleccione as caixas de selecção junto às categorias de conteúdo correspondentes aos jogos que pretende bloquear.

Para restringir o início de uma aplicação específica:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, clique no botão  e seleccione a secção **Controlo Parental**.

   A janela apresenta a secção **Controlo Parental**.
3. Clique na ligação com o nome de uma conta de utilizador para aceder a uma janela que fornece estatísticas das actividades do utilizador.
4. Clique na ligação **Configuração** na secção **Aplicações** para aceder à janela de definições do Controlo de Arranque das Aplicações.
5. Na parte inferior da janela, clique no botão **Adicionar aplicação** e seleccione o ficheiro executável de uma aplicação na janela apresentada.

   A aplicação seleccionada é apresentada na lista na secção **Bloquear as aplicações especificadas**. O Kaspersky Internet Security adiciona a aplicação automaticamente a uma categoria especificada, por exemplo, *Jogos*.
6. Se pretender bloquear uma aplicação, seleccione a caixa de selecção junto ao nome respectivo na lista. Também pode bloquear todas as aplicações que pertencem a uma categoria especificada, seleccionando a caixa de selecção junto ao nome de uma categoria na lista (por exemplo, pode bloquear a categoria *Jogos*).

7. Se pretender definir um limite ao tempo de utilização de uma aplicação, seleccione uma aplicação ou uma categoria de aplicação da lista e clique no botão **Configurar regras**.

   É apresentada a janela **Restringir aplicações**.

8. Se pretender limitar o tempo de utilização da aplicação durante dias da semana e fins-de-semana, seleccione as caixas de selecção correspondentes nas secções **Dias da semana** e **Fins-de-semana** e seleccione os valores do limite nas listas pendentes. Também pode especificar um período em que o utilizador está autorizado ou proibido de utilizar a aplicação, utilizando uma tabela. Para ver a tabela, clique no botão  .

9. Se pretender definir intervalos na utilização de uma aplicação, na secção **Falha** seleccione a caixa de selecção **Bloquear o acesso a cada** e seleccione um valor para a duração do intervalo na lista pendente.

10. Clique no botão **Guardar**.

O Controlo Parental irá aplicar as restrições especificadas quando o utilizador utilizar a aplicação.

CONTROLAR MENSAGENS EM REDES SOCIAIS

Ao utilizar o Controlo Parental pode ver as mensagens do utilizador nas redes sociais e nos clientes de MI, bem como bloquear a troca de mensagens com contactos especificados.

Para configurar a monitorização das mensagens do utilizador:

1. Abra a janela principal da aplicação.

2. Na parte inferior da janela, clique no botão  e seleccione a secção **Controlo Parental**.

   A janela apresenta a secção **Controlo Parental**.

3. Clique na ligação com o nome de uma conta de utilizador para aceder a uma janela que fornece estatísticas das actividades do utilizador.

4. Clique na ligação **Configuração** na secção **Mensagens** para aceder à janela de definições do controlo de mensagens do utilizador.

5. Para ver os registos de mensagens e bloquear contactos especificados, se necessário:

   a. Na secção **Comunicação em programas de mensagens instantâneas e redes sociais**, seleccione **Bloquear comunicação com os contactos especificados**.

   b. Clique na ligação **Contactos** para abrir a janela **Contactos**.

   c. Ver os contactos com quem o utilizador tem trocado mensagens. Pode tornar os contactos especificados visíveis na janela utilizando um dos métodos seguintes:

      - Para ver os registos das mensagens do utilizar numa rede social ou cliente de IM específico, seleccione o item requerido na lista pendente na parte superior da janela.

      - Para ver os contactos com quem o utilizador têm trocado mais mensagens, na lista pendente **Ordenação** seleccione **Por número de mensagens**.

      - Para ver os contactos com quem o utilizador tem trocado mensagens recentemente, na lista pendente **Ordenação** seleccione **Mensagens recentes primeiro**.

   d. Para ver a troca de mensagens do utilizador com um contacto especificado, clique no contacto na lista.

      É apresentada a janela **Registo de mensagens**.

   e. Se pretender bloquear a troca de mensagens entre o utilizador e o contacto seleccionado, clique no botão **Bloquear**.

O Controlo Parental irá bloquear a troca de mensagens entre o utilizador e o contacto seleccionado.

CONTROLAR CONTEÚDO DE MENSAGENS

Ao utilizar o Controlo Parental, pode monitorizar e proibir as tentativas do utilizar de inserir dados privados especificados (tais como nomes, número de telefone, números de cartões bancários) e palavras-chave (tais como palavras obscena) em mensagens.

- *Para configurar o controlo da transferência de dados privados:*

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, clique no botão  e seleccione a secção **Controlo Parental**.

   A janela apresenta a secção **Controlo Parental**.
3. Clique na ligação com o nome de uma conta de utilizador para aceder a uma janela que fornece estatísticas das actividades do utilizador.
4. Clique na ligação **Configuração** na secção **Controlo de conteúdo** para aceder à janela de definições do Controlo de partilha de dados.
5. Na secção **Controlo de transferência de dados privados** seleccione a caixa de selecção **Bloquear a transferência de dados privados a terceiros**.
6. Clique na ligação **Editar a lista de dados privados** para abrir a janela **Lista de dados privados**.
7. Na parte inferior da janela, clique no botão **Adicionar**.

   É apresentada uma janela para adicionar os dados privados.
8. Introduza os seus dados privados (tais como o seu apelido ou número de telefone) no campo **Valor**.
9. Para adicionar uma descrição para um item de dados privados (por exemplo, "número de telefone"), clique na ligação correspondente na secção **Tipos de dados privados** ou introduza uma descrição no campo **Nome do campo**.
10. Clique no botão **Adicionar**.

Os dados pessoais serão apresentados na janela **Lista de dados privados**. O Controlo Parental irá monitorizar e bloquear as tentativas do utilizador de utilizar os dados privados especificados em mensagens em clientes de MI e em sites.

- *Para configurar o Controlo da Utilização de Palavras nas mensagens:*

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, clique no botão  e seleccione a secção **Controlo Parental**.

   A janela apresenta a secção **Controlo Parental**.
3. Clique na ligação com o nome de uma conta de utilizador para aceder a uma janela que fornece estatísticas das actividades do utilizador.
4. Clique na ligação **Configuração** na secção **Controlo de conteúdo** para aceder à janela de definições do Controlo de partilha de dados.
5. Na secção **Controlo de palavras-chave**, seleccione a caixa de selecção **Activar o Controlo de palavras-chave**.
6. Clique na ligação **Editar a lista de palavras-chave** para abrir a janela **Controlo de palavras-passe**.
7. Na parte inferior da janela, clique no botão **Adicionar**.

   É apresentada uma janela para adicionar uma palavra-chave.
8. Introduza uma expressão chave no campo **Valor** e clique no botão **Adicionar**.

A expressão chave especificada é apresentada na lista de palavras-chave na janela **Controlo de palavras-passe**. O Controlo Parental irá bloquear a transmissão de mensagens com a expressão chave especificada, quer as mensagens sejam enviadas pela Internet ou em clientes de MI.

VISUALIZAR O RELATÓRIO DAS ACTIVIDADES DE UM UTILIZADOR

No Controlo Parental, pode aceder aos relatórios sobre as actividades de cada conta de utilizador, revendo individualmente cada categoria de eventos controlados.

Para ver um relatório sobre as actividades de uma conta de utilizador controlada:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, clique no botão  e seleccione a secção **Controlo Parental**.

   A janela apresenta a secção **Controlo Parental**.
3. Clique na ligação com o nome de uma conta de utilizador para aceder a uma janela que fornece estatísticas das actividades do utilizador.
4. Na secção com o tipo de restrição pretendida (por exemplo, **Internet** ou **Mensagens**) abra o relatório das acções monitorizadas clicando na ligação **Detalhes**.

A janela apresenta um relatório com as acções monitorizadas.

UTILIZAR O PERFIL JOGOS PARA O MODO DE ECRÃ COMPLETO

Quando o Kaspersky Internet Security é executado em simultâneo com algumas aplicações (em especial jogos de vídeo), podem ocorrer as seguintes situações em modo de ecrã completo:

- O desempenho da aplicação ou jogo é reduzido, devido à falta de recursos do sistema
- As janelas de notificação do Kaspersky Internet Security distraem o utilizador do jogo.

Para evitar ter de alterar as definições do Kaspersky Internet Security manualmente, sempre que mudar para o modo de ecrã completo, pode usar o Perfil Jogos. Quando o Perfil Jogos está activo, ao mudar para o modo de ecrã inteiro alteram-se, automaticamente, as definições de todos os componentes do Kaspersky Internet Security, para assegurar o funcionamento ideal do sistema naquele modo. Ao sair do modo de ecrã inteiro, as definições do produto regressam aos valores iniciais utilizados antes de entrar no modo de ecrã inteiro.

Para activar o Perfil Jogos:

1. Abra a janela principal da aplicação.
2. Clique na ligação **Configuração** na parte inferior da janela principal aceda à secção **Configuração**.
3. Na parte esquerda da janela, seleccione a secção **Desempenho**.

   A janela apresenta as definições de desempenho do Kaspersky Internet Security.
4. Na secção **Perfil Jogos** seleccione a caixa de selecção **Usar Perfil Jogos**.

CRIAR E UTILIZAR O DISCO DE RECUPERAÇÃO

O Disco de Recuperação é uma aplicação designada Kaspersky Rescue Disk e registada num meio removível (CD ou unidade flash USB).

Pode utilizar o Kaspersky Rescue Disk para verificar e desinfectar computadores infectados que não possam ser desinfectados através de outros métodos (por exemplo, com aplicações antivírus).

NESTA SECÇÃO

CRIAR UM DISCO DE RECUPERAÇÃO

Criar um Disco de Recuperação consiste na criação de uma imagem do disco (ficheiro ISO) com a versão actualizada do Kaspersky Rescue Disk e na gravação da mesma num meio removível.

Pode transferir a imagem do disco original a partir do servidor da Kaspersky Lab ou copiá-la a partir de uma origem local.

- O Disco de Recuperação é criado através do *Assistente de Criação do Kaspersky Rescue Disk*. O ficheiro rescued.iso criado pelo Assistente é guardado no disco rígido do seu computador.

Para iniciar o Assistente de Criação do Kaspersky Rescue Disk:

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela principal, clique no botão  e seleccione a secção **Ferramentas**.
3. Na janela que se abre, na secção **Kaspersky Rescue Disk**, clique no botão **Criar**.

O Assistente consiste numa série de janelas (passos), entre as quais pode navegar utilizando os botões **Anterior** e **Seguinte**. Para fechar o Assistente depois de este concluir a sua tarefa, clique no botão **Concluir**. Para parar o Assistente em qualquer altura, clique no botão **Cancelar**.

Vamos analisar em maior detalhe os passos do Assistente.

Passo 1. Iniciar o Assistente. Procurar uma imagem do disco existente

A primeira janela do Assistente contém informação sobre o Kaspersky Rescue Disk. Para continuar com o Assistente, clique no botão **Seguinte**. O Assistente irá deslocar-se até à janela **Seleccionar uma fonte da imagem do disco**.

Passo 2. Seleccionar uma fonte da imagem do disco

Neste passo, deve seleccionar uma origem de imagem do disco a partir da lista de opções:

- Se não possuir um ficheiro de imagem ISO criado para o Disco de Recuperação e pretende transferir um a partir do servidor da Kaspersky Lab (o tamanho do ficheiro é de cerca de 175 MB), seleccione **Transferir imagem ISO a partir do servidor da Kaspersky Lab**.
- Se já tiver uma imagem do Kaspersky Rescue Disk, seleccione **Utilizar imagem existente do Kaspersky Rescue Disk**.
- Se já possuir uma cópia gravada do Disco de Recuperação ou uma imagem ISO e guardada no seu computador ou num recurso de rede local, seleccione **Copiar imagem ISO a partir da unidade local ou de rede**.

  Clique no botão **Procurar**. Depois de especificar o caminho para o ficheiro, clique no botão **Seguinte**.

Passo 3. Copiar (transferir) a imagem do disco

Se seleccionou **Utilizar imagem existente do Kaspersky Rescue Disk** na janela anterior do Assistente, este passo será ignorado.

Quando a cópia ou transferência da imagem ISO estiver concluída, o Assistente prossegue automaticamente para o passo seguinte.

Passo 4. Actualizar o ficheiro de imagem ISO

O procedimento de actualização para o ficheiro de imagem ISO é constituído pelas seguintes operações:

- actualização das bases de dados da aplicação
- actualização dos ficheiros de configuração.

Os ficheiros de configuração determinam se o computador pode ser iniciado a partir de um suporte removível (tal como um CD / DVD ou uma unidade flash USB com o Kaspersky Rescue Disk) criado pelo Assistente.

Ao actualizar as bases de dados da aplicação, são utilizadas as bases distribuídas com a última actualização do Kaspersky Internet Security. Se as bases de dados estiverem desactualizadas, é aconselhável que execute a tarefa de actualização e inicie o Assistente de Criação do Kaspersky Rescue Disk novamente.

Para começar a actualizar o ficheiro ISO, clique no botão **Seguinte**. A evolução da actualização será apresentada na janela do Assistente.

Passo 5. Gravar a imagem do disco num suporte de dados

Neste passo, o Assistente informa-o da criação bem sucedida de uma imagem do disco e dá-lhe a opção de gravá-lo num suporte de dados.

Especifique um suporte de dados para gravar o Kaspersky Rescue Disk:

- Para gravar a imagem de disco em CD/DVD, seleccione **Gravar em CD/DVD**.
- Para gravar a imagem de disco numa unidade USB, seleccione **Gravar em unidade flash USB**.

Os especialistas da Kaspersky Lab não recomendam guardar a imagem de disco em dispositivos que não se destinam exclusivamente a armazenamento de dados, como, por exemplo, smartphones, telemóveis, computadores de bolso ou leitores de MP3. Após serem utilizados para armazenar a imagem de disco, tais dispositivos podem não funcionar correctamente.

- Para gravar a imagem de disco na unidade de disco rígido do seu computador ou de outro computador a que tem acesso através da rede, seleccione **Guardar imagem do disco em ficheiro na unidade local ou de rede**.

Passo 6. Seleccione um dispositivo/ficheiro para gravar a imagem de disco

Neste passo, o Assistente solicita que especifique o caminho para um dispositivo/ficheiro onde a imagem de disco será guardada.

- Se seleccionou a opção **Gravar em CD/DVD** no passo anterior do Assistente, seleccione na lista pendente o disco onde pretende gravar a imagem de disco.
- Se seleccionou a opção **Gravar em unidade flash USB** no passo anterior do Assistente, seleccione na lista pendente o dispositivo onde pretende gravar a imagem de disco.
- Se seleccionou a opção **Guardar imagem do disco em ficheiro na unidade local ou de rede** no passo anterior do Assistente, especifique uma pasta onde pretende gravar a imagem de disco, e o nome do ficheiro ISO.

Passo 7. Gravar a imagem de disco num dispositivo/ficheiro

Neste passo do Assistente pode monitorizar o progresso da gravação da imagem de disco em CD/DVD ou numa unidade USB, ou a gravação em ficheiro.

Passo 8. Conclusão do Assistente

Para fechar o Assistente depois de este concluir a sua tarefa, clique no botão **Concluir**. Pode utilizar o Disco de Recuperação recentemente criado para iniciar o computador se não conseguir iniciá-lo e executar o Kaspersky Internet Security em modo padrão devido ao impacto causado por vírus ou software malicioso.

INICIAR O COMPUTADOR A PARTIR DO DISCO DE RECUPERAÇÃO

Se o sistema operativo não puder ser iniciado como resultado de um ataque de vírus, utilize o Disco de Recuperação.

Para reinicializar o sistema operativo, deve utilizar um CD / DVD, ou uma unidade Flash USB, com uma cópia do Disco de Recuperação do Kaspersky (consulte a secção "Criar um Disco de Recuperação" na página 62).

Iniciar um computador a partir de um meio removível nem sempre é possível. Em particular, este modo não é suportado por alguns modelos de computador obsoletos. Antes de encerrar o seu computador para posteriormente iniciá-lo a partir de um meio removível, certifique-se de que esta operação pode ser executada.

Para iniciar o seu computador com o Disco de Recuperação:

1. Nas configurações do BIOS, active a inicialização a partir de um CD/DVD ou dispositivo USB (para obter informação detalhada, consulte a documentação da motherboard do seu computador).
2. Insira o CD/DVD na unidade de CD/DVD de um computador infectado ou ligue um dispositivo flash USB com uma cópia do Kaspersky Rescue Disk.
3. Reinicie o seu computador.

Para obter informação detalhada sobre a utilização do Disco de Recuperação, por favor consulte o Manual de Utilizador do Kaspersky Rescue Disk.

PROTEGER POR PASSWORD O ACESSO AO KASPERSKY INTERNET SECURITY

Um computador pode ser partilhado por vários utilizadores com diversos níveis de experiência e conhecimentos informáticos. O acesso sem restrições de diferentes utilizadores ao Kaspersky Internet Security e às suas definições pode comprometer o nível de segurança do computador.

Para restringir o acesso à aplicação, pode definir uma password de administrador e especificar as acções que devem requerer a introdução da password:

- configurar as definições da aplicação;
- encerramento da aplicação;
- remoção da aplicação.

Para proteger por password o acesso ao Kaspersky Internet Security:

1. Abra a janela principal da aplicação.
2. Clique na ligação **Configuração** na parte inferior da janela principal aceda à secção **Configuração**.

3. Na parte à esquerda da janela, seleccione a secção **Geral** e clique na ligação **Configurar protecção por password** para abrir a janela **Protecção por Password**.

4. Na janela apresentada, preencha os campos **Nova password** e **Confirmar password**.

5. Para alterar uma password criada previamente, introduza a mesma no campo **Password antiga**.

6. No grupo de definições **Âmbito da Password**, especifique as operações das aplicações em que o acesso tem de ser protegido por password.

Uma password esquecida não pode ser recuperada. Caso se tenha esquecido da sua password, terá de contactar o Suporte Técnico para recuperar o acesso às definições do Kaspersky Internet Security.

PAUSAR E RETOMAR A PROTECÇÃO DO COMPUTADOR

Colocar a protecção em pausa significa desactivar temporariamente todos os componentes de protecção durante algum tempo.

Para pausar a protecção do seu computador:

1. No menu de contexto do ícone da aplicação na área de notificações da barra de tarefa, seleccione o item **Pausar protecção**.

   A janela **Pausar protecção** é apresentada (consulte a figura seguinte).

Figura 8. Janela Pausar protecção

2. Na janela **Pausar protecção**, seleccione o intervalo de tempo após o qual a protecção deve ser retomada:

   - **Pausar durante o tempo especificado** – a protecção é activada após expirar o intervalo de tempo seleccionado na lista pendente abaixo.
   - **Colocar em pausa até reiniciar** – a protecção é activada após a reinicialização da aplicação ou do sistema operativo (desde que a inicialização automática da aplicação esteja activada).
   - **Pausar** – a protecção será retomada pretender.

Para retomar a protecção do computador,

seleccione o item **Retomar protecção** no menu de contexto do ícone da aplicação na área de notificações da barra de ferramentas.

RESTAURAR AS PREDEFINIÇÕES DA APLICAÇÃO

Pode restaurar as definições recomendadas pela Kaspersky Lab para o Kaspersky Internet Security em qualquer momento. As definições podem ser restauradas através do *Assistente de Configuração da Aplicação*.

Quando o Assistente concluir as suas operações, o nível de segurança *Recomendado* é definido para todas as componentes de protecção. Ao restaurar o nível de segurança recomendado, pode guardar os valores das definições previamente especificadas para os componentes da aplicação.

➧ *Para executar o Assistente de Resolução de Problemas do Microsoft Windows pós-infecção:*

1. Abra a janela principal da aplicação.
2. Na parte inferior da janela, clique na ligação **Configuração**.

   A janela apresenta a secção **Configuração**.
3. Seleccione a secção **Geral**.

   A janela apresenta as definições do Kaspersky Internet Security.
4. Na secção inferior da janela, clique na ligação **Restaurar configurações** (consulte a imagem seguinte).

*Figura 9. janela **Configuração**, subsecção **Geral***

Vamos analisar em maior detalhe os passos do Assistente.

Passo 1. Iniciar o Assistente

Clique no botão **Seguinte** para continuar com o Assistente.

Passo 2. Restaurar configurações

Esta janela do Assistente apresenta quais as componentes de protecção do Kaspersky Internet Security que têm definições diferentes do valor predefinido, por terem sido alteradas pelo utilizador ou acumuladas pelo Kaspersky Internet Security através do treino (Firewall ou Anti-Spam). Se tiverem sido criadas definições especiais para algum dos componentes, essas definições serão também apresentadas na janela (consulte a figura seguinte).

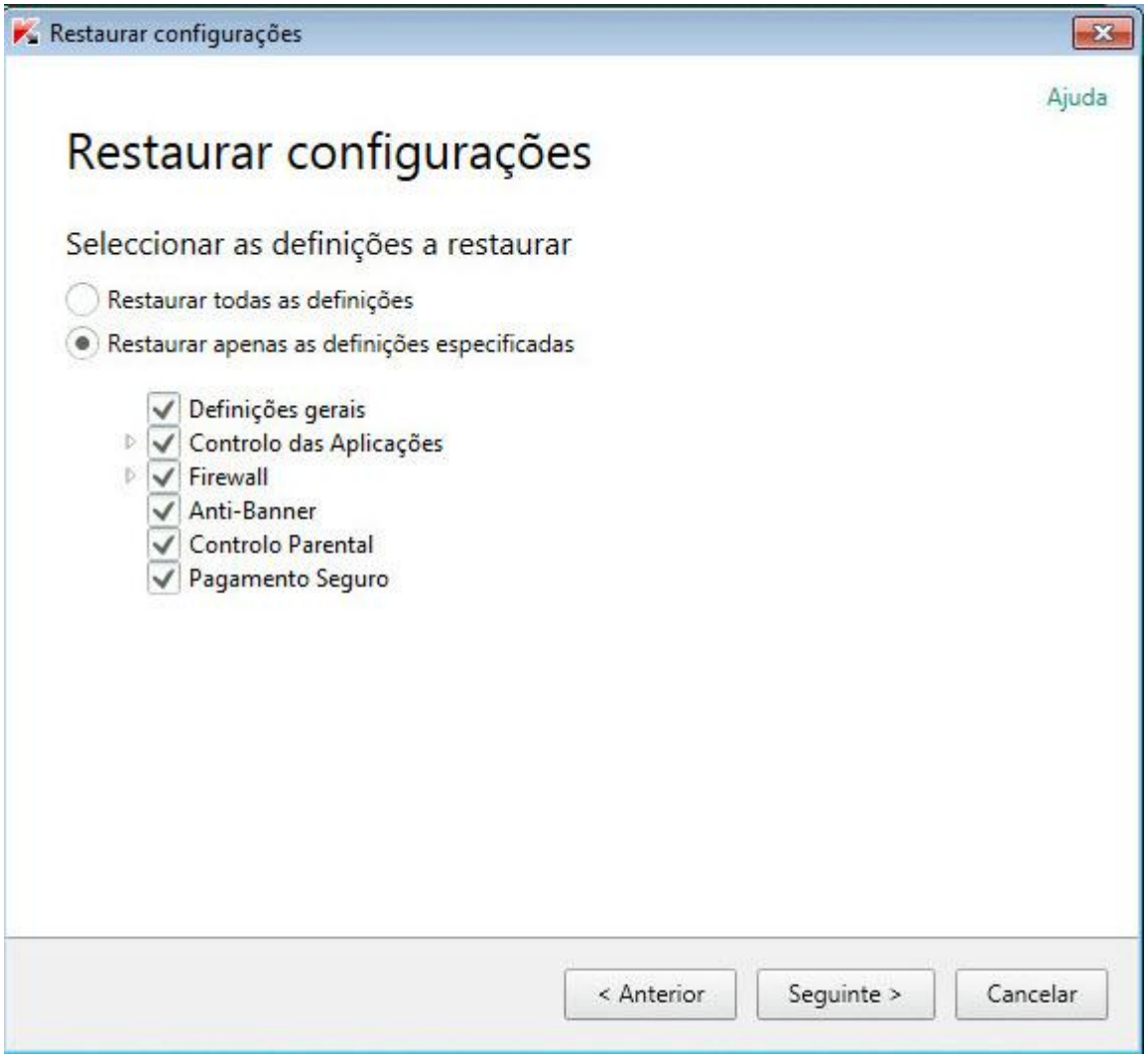

*Figura 10. Janela **Restaurar configurações***

As definições especiais incluem listas de expressões e endereços permitidos e bloqueados que são utilizados pelo Anti-Spam, listas de endereços de Internet e números de telefone ISP confiáveis, regras de exclusão criadas para as componentes da aplicação e as regras de filtragem de pacotes e aplicações da Firewall.

As definições especiais são criadas ao trabalhar com o Kaspersky Internet Security no que respeita a tarefas e requisitos de segurança individuais. A Kaspersky Lab recomenda que guarde as suas definições especiais ao restaurar as predefinições da aplicação.

Assinale as caixas para as definições que deseja guardar e clique no botão **Seguinte**.

Passo 3. Análise do sistema

Durante esta etapa, é recolhida informação sobre as aplicações do Microsoft Windows. Estas aplicações são adicionadas à lista de aplicações confiáveis, que não têm restrições impostas às acções que executam no sistema.

Depois de a análise estar concluída, o Assistente irá, automaticamente, continuar para o passo seguinte.

Passo 4. Concluir o restauro

Para fechar o Assistente depois de este concluir a sua tarefa, clique no botão **Concluir**.

VISUALIZAR O RELATÓRIO DA APLICAÇÃO

O Kaspersky Internet Security mantém os relatórios de funcionamento para cada um dos componentes de protecção. Através de um relatório, pode obter informações estatísticas acerca do funcionamento da aplicação (por exemplo, saber quantos objectos maliciosos foram detectados e neutralizados durante um período de tempo especificado, quantas vezes a aplicação foi actualizada durante o mesmo período, quantas mensagens de spam foram detectadas e muito mais).

Quando trabalha num computador com o Microsoft Windows Vista ou o Microsoft Windows 7, pode ver relatórios utilizando a Ferramenta Kaspersky. Para tal, a opção de abrir relatórios deve estar atribuída a um dos botões da Ferramenta Kaspersky.

Para ver o relatório de funcionamento da aplicação:

1. Abra a janela **Relatórios** utilizando um dos seguintes métodos:

   - Na parte inferior da janela principal da aplicação seleccione a secção **Relatórios**.
   - Na interface da Ferramenta Kaspersky (apenas para Microsoft Windows Vista e Microsoft Windows 7), clique no botão com o ícone **Relatórios**.

   A janela **Relatórios** apresenta os relatórios do funcionamento da aplicação ao longo do dia actual (na secção à esquerda da janela) e durante um período (na secção à direita da janela).

2. Se pretender ver um relatório detalhado sobre o funcionamento da aplicação, abra a janela **Relatório detalhado** clicando na ligação **Todos os eventos** situada na secção superior da janela **Relatórios**.

A janela **Relatório detalhado** apresenta os dados em forma de tabela. Para uma visualização conveniente dos relatórios, pode seleccionar várias opções de ordenação.

UTILIZAR A FERRAMENTA KASPERSKY

Ao utilizar o Kaspersky Internet Security num computador com o Microsoft Windows Vista ou Microsoft Windows 7, também pode utilizar a Ferramenta Kaspersky (daqui em diante designada por *ferramenta*). Depois de instalar o Kaspersky Internet Security num computador com o Microsoft Windows 7, a ferramenta é apresentada automaticamente no seu ambiente de trabalho. Depois de instalar a aplicação num computador com o Microsoft Windows Vista, deverá adicionar a ferramenta à barra lateral do Microsoft Windows manualmente (ver a documentação do sistema operativo).

O indicador cromático da Ferramenta mostra o estado de protecção do computador da mesma forma que o indicador na janela principal da aplicação (consulte a secção "Avaliar o estado de protecção do computador e solucionar problemas de segurança" na página 31). A cor verde indica que o seu computador está devidamente protegido, enquanto a cor amarela indica que existem problemas de protecção e a cor vermelha indica que a segurança do seu computador está em grande risco. A cor cinzenta indica que a aplicação está parada.

Pode utilizar a ferramenta para executar as seguintes acções:

- retomar a aplicação se tiver sido pausada anteriormente;
- abrir a janela principal da aplicação;

- verificar a existência de vírus em determinados objectos;
- abrir a janela de notícias.

Adicionalmente pode configurar os botões da ferramenta de modo a que ela possa iniciar acções adicionais:

- executar uma actualização;
- editar as definições da aplicação;
- visualizar relatórios da aplicação;
- visualizar relatórios do Controlo Parental;
- visualizar informação sobre a actividade de rede (Monitor de Rede) e actividade das aplicações;
- pausar a protecção;
- abrir o Teclado virtual;
- abrir a janela do Gestor de Tarefas.

Para iniciar a aplicação através da ferramenta,

clique no ícone **Activar** situado no centro da ferramenta.

Para abrir a janela principal da aplicação através da ferramenta,

clique no ícone do monitor na área central da ferramenta.

Para verificar um objecto, quanto à presença de vírus, através da ferramenta,

arraste o objecto a verificar para cima da ferramenta.

O progresso da tarefa será apresentado na janela do **Gestor de Tarefas**.

Para abrir a janela de notícias através da ferramenta,

clique no ícone que é apresentado no centro da ferramenta quando é publicada uma notícia.

Para configurar a ferramenta:

1. Abra a janela de definições da ferramenta clicando no ícone apresentado no canto superior direito da secção da ferramenta quando passa com o cursor do rato por cima do mesmo.
2. Nas listas pendentes correspondentes aos botões da ferramenta, seleccione as acções que devem ser desempenhadas quando clicar nesses botões.
3. Clique em **OK**.

PARTICIPAR NA KASPERSKY SECURITY NETWORK (KSN)

Para aumentar a eficiência da protecção do seu computador, o Kaspersky Internet Security usa dados recebidos de utilizadores a nível mundial. O Kaspersky Security Network foi concebido para recolher esses dados.

O Kaspersky Security Network (KSN) é uma infra-estrutura de serviços online que permite o acesso à Base de Conhecimento online da Kaspersky Lab, a qual contém informação sobre a reputação de ficheiros, recursos da Internet e software. A utilização de dados da Kaspersky Security Network garante uma resposta mais rápida do Kaspersky Internet Security face a novas ameaças, melhora o desempenho de alguns componentes de protecção e reduz o risco de falsos diagnósticos positivos.

A participação dos utilizadores na Kaspersky Security Network permite à Kaspersky Lab recolher rapidamente informações sobre tipos e fontes de novas ameaças, desenvolver soluções para neutralizá-las e minimizar o número de falsos positivos. A participação no Kaspersky Security Network permite-lhe aceder a estatísticas de reputação para aplicações e sites.

Ao iniciar o Kaspersky Internet Security, após o arranque do sistema operativo, a aplicação envia para a Kaspersky Security Network os detalhes da configuração do seu sistema, bem como informações sobre a hora de início e de conclusão dos processos do Kaspersky Internet Security.

NESTA SECÇÃO

ACTIVAR E DESACTIVAR A PARTICIPAÇÃO NO KASPERSKY SECURITY NETWORK

A participação no Kaspersky Security Network é voluntária. Pode activar ou desactivar a utilização do Kaspersky Security Network ao instalar o Kaspersky Internet Security e/ou em qualquer momento após a instalação da aplicação.

Para activar e desactivar a participação no Kaspersky Security Network:

1. Abra a janela principal da aplicação.
2. Clique na ligação **Configuração** na parte inferior da janela principal para abrir a janela **Configuração**.
3. Na secção **Adicional** seleccione a sub-secção **Enviar comentários**.

   A janela apresenta os detalhes da Kaspersky Security Network (KSN) e as definições de participação na KSN.
4. Pode activar ou desactivar a participação na Kaspersky Security Network utilizando os botões **Activar**/**Desactivar**:
   - Se pretender participar na KSN, clique no botão **Activar**.
   - Se não pretender participar na KSN, clique no botão **Desactivar**.

VERIFICAR A LIGAÇÃO AO KASPERSKY SECURITY NETWORK

A ligação ao Kaspersky Security Network pode perder-se pelas razões seguintes:

- Não participa no Kaspersky Security Network.
- O seu computador não está ligado à Internet.
- O estado da chave actual não permite ligar à Kaspersky Security Network.

O estado actual da chave é apresentado na janela **Licenciamento**.

Para testar a ligação ao Kaspersky Security Network:

1. Abra a janela principal da aplicação.
2. Clique na ligação **Configuração** na parte inferior da janela principal para abrir a janela **Configuração**.
3. Na secção **Adicional** seleccione a sub-secção **Enviar comentários**.

A janela apresenta o estado da ligação à Kaspersky Security Network.

PARTICIPAR NO PROGRAMA PROTECT A FRIEND

O programa Protect a Friend permite publicar no Twitter e na sua página no Facebook ou vk.com uma ligação para transferir o pacote de distribuição do Kaspersky Internet Security com um período de avaliação prolongado. Se um dos seus amigos no Twitter, Facebook, ou vk.com transferir o pacote do Kaspersky Internet Security clicando na ligação publicada e, em seguida, activar a aplicação, irá receber pontos de bónus. Pode trocar os pontos de bónus recebidos por um código de activação de bónus para o Kaspersky Internet Security.

Tenha em atenção que a opção de participar no programa Protect a Friend não está disponível para cada um dos utilizadores.

Se participar no programa Protect a Friend, é-lhe atribuída uma classificação de utilizador. A classificação do utilizador depende da versão da aplicação e das funções e componentes de aplicação mais utilizados (por exemplo, verificação, Controlo Parental, Pagamento Seguro).

Para participar no programa Protect a Friend, abra a página da Internet com o seu perfil no programa Protect a Friend. Pode ver a página da Internet com o seu perfil clicando na ligação **perfil** na secção inferior da janela principal do Kaspersky Internet Security. O seu perfil é criado automaticamente quando inicia sessão pela primeira vez.

Para iniciar sessão no seu perfil no programa Protect a Friend, deverá efectuar a autenticação com uma conta Kaspersky. Se ainda não tem uma conta Kaspersky, pode criar uma quando abrir o seu perfil pela primeira vez no programa Protect a Friend.

Na página da Internet com o seu perfil no programa Protect a Friend, poderá executar as acções seguintes:

- Consultar a sua classificação no programa Protect a Friend bem com o número de pontos acumulados
- Publicar ligações para transferir o pacote de instalação do Kaspersky Internet Security
- Editar as propriedades do seu perfil (a imagem de utilizador e o nome apresentado no Twitter, em redes sociais, e no seu blogue, juntamente com uma ligação para transferir o pacote de instalação do Kaspersky Internet Security).

NESTA SECÇÃO

INICIAR SESSÃO NO SEU PERFIL NO PROGRAMA PROTECT A FRIEND

Para iniciar sessão no seu perfil no programa Protect a Friend, deverá efectuar a autenticação com uma conta Kaspersky. Se ainda não tiver uma conta Kaspersky, deverá criar uma quando iniciar sessão pela primeira vez na página da Internet do programa Protect a Friend.

A Conta Kaspersky é o endereço do seu e-mail e a password (pelo menos oito caracteres) especificada durante o registo.

Depois de criar uma conta, é enviada uma mensagem para o seu endereço de e-mail, com uma ligação para activar a sua Conta Kaspersky.

Após a activação, pode utilizar a sua Conta Kaspersky para iniciar sessão na página de Internet com o seu perfil no programa Protect a Friend.

Para criar a sua Conta Kaspersky:

1. Abra a janela principal da aplicação e clique na ligação **O meu perfil** na parte inferior da janela.

   É apresentada uma página da Internet do programa Protect a Friend, com os campos para registo ou autenticação com a Conta Kaspersky.

2. Criar e activar a sua Conta Kaspersky:

   a. Na secção à esquerda da página da Internet, introduza um endereço de e-mail no campo **E-mail**.

   b. Introduza uma password e, em seguida, introduza-a novamente para confirmar nos campos **Password** e **Confirmar password**. A password deve incluir pelo menos oito caracteres.

   c. Clique no botão **Registo**.

      A página da Internet apresenta uma mensagem a informar o utilizador do registo bem sucedido da Conta Kaspersky. Será enviada uma mensagem para o seu endereço de e-mail, com uma ligação que deverá utilizar para activar a sua Conta Kaspersky.

   d. Clique na ligação para activar a sua Conta Kaspersky.

      A página da Internet apresenta uma mensagem a informar o utilizador da activação bem sucedida da Conta Kaspersky. Pode utilizar a sua nova Conta Kaspersky para iniciar sessão no seu perfil no programa Protect a Friend.

Se já tem a sua conta Kaspersky, pode utilizá-la para iniciar sessão na página da Internet com o seu perfil.

Para iniciar sessão na página da Internet com o seu perfil no programa Protect a Friend:

1. Abra a janela principal da aplicação e clique na ligação **O meu perfil** na parte inferior da janela.

   É apresentada uma página da Internet do programa Protect a Friend, com os campos para registo ou autenticação com a Conta Kaspersky.

2. Na secção à direita da página da Internet, preencha os campos introduzindo o endereço de e-mail e a password especificada durante o registo da Conta Kaspersky.

3. Clique no botão **Iniciar sessão**.

A página da Internet apresenta o seu perfil no programa Protect a Friend.

COMO PARTILHAR UMA LIGAÇÃO PARA O KASPERSKY INTERNET SECURITY COM AMIGOS

Tendo sessão iniciada na página da Internet com o seu perfil no programa Protect a Friend, pode publicar uma ligação para transferir o pacote de distribuição do Kaspersky Internet Security no Twitter e nas redes sociais tais como o Facebook e vk.com. Adicionalmente, pode partilhar detalhes no seu perfil no programa Protect a Friend com uma ligação para o pacote de distribuição, colando a informação no seu site ou blogue. Pode também enviar uma ligação para o pacote de distribuição do Kaspersky Internet Security por e-mail ou usando clientes de mensagens instantâneas (tais como o ICQ).

- *Para publicar uma ligação para transferir o pacote de distribuição do Kaspersky Internet Security no Twitter ou em redes sociais:*

  1. Abra a janela principal do Kaspersky Internet Security e clique na ligação **O meu perfil** na parte inferior da janela.

     A página de autenticação no programa Protect a Friend é apresentada.

  2. Efectue a autenticação na página da Internet com a sua Conta Kaspersky.

     A página da Internet apresenta os detalhes do seu perfil no programa Protect a Friend.

  3. Na secção à esquerda da página da Internet, clique no botão com o logótipo da rede social pretendida (Facebook ou vk.com) ou com o logótipo do Twitter.

  O site da rede social seleccionada ou do Twitter é apresentado. É apresentada uma ligação para transferir o pacote de distribuição do Kaspersky Internet Security com um período de avaliação alargado, nos feeds de notícias dos seus amigos. Pode introduzir texto adicional no formulário da publicação, se necessário.

  Se ainda não iniciou sessão na sua página numa rede social ou no Twitter, a página de autorização é apresentada.

- *Para publicar um widget da Internet com uma ligação para transferir o pacote de distribuição do Kaspersky Internet Security:*

  1. Abra a janela principal do Kaspersky Internet Security e clique na ligação **O meu perfil** na parte inferior da janela.

     A página de autenticação no programa Protect a Friend é apresentada.

  2. Efectue a autenticação na página da Internet com a sua Conta Kaspersky.

     A página da Internet apresenta os detalhes do seu perfil no programa Protect a Friend.

  3. Na secção superior da página da Internet, na lista pendente **Partilhar**, seleccione **Obter o código do widget da Internet**.

     É apresentada a janela **Web widget code** com um código do widget da Internet para colar no seu site.

Pode copiar o código do widget da Internet para a área de transferência e, em seguida, colar na página de código HTML do seu site ou blogue.

- *Para obter uma ligação para transferir o pacote de distribuição do Kaspersky Internet Security para enviar por email ou utilizando um cliente de mensagens instantâneas:*

  1. Abra a janela principal do Kaspersky Internet Security e clique na ligação **O meu perfil** na parte inferior da janela.

     A página de autenticação no programa Protect a Friend é apresentada.

  2. Efectue a autenticação na página da Internet com a sua Conta Kaspersky.

     A página da Internet apresenta os detalhes do seu perfil no programa Protect a Friend.

  3. Na secção à esquerda da página da Internet, clique na ligação **Obter uma ligação**.

     A janela **Ligação para transferir o programa de instalação** é apresentada incluindo uma ligação para transferir o pacote de distribuição do Kaspersky Internet Security.

Pode copiar a ligação para a área de transferência e, em seguida, enviar a mesma por e-mail ou utilizando um cliente de mensagens instantâneas.

TROCAR PONTOS POR UM CÓDIGO DE ACTIVAÇÃO DE BÓNUS

Quando participa no programa Protect a Friend, pode receber um código de activação de bónus para o Kaspersky Internet Security em troca de um número especificado de pontos de bónus. Os pontos de bónus são atribuídos quando os utilizadores activam o Kaspersky Internet Security transferido a partir da ligação partilhada no seu perfil.

Os códigos de activação de bónus são atribuídos nos casos seguintes:

- Quando um utilizador com quem partilhou a ligação efectua a activação da versão de avaliação do Kaspersky Internet Security
- Quando um utilizador com quem partilhou a ligação efectua a activação de uma licença do Kaspersky Internet Security versão 2013 ou posterior.

Na página da Internet com o seu perfil, pode ver o histórico dos pontos de bónus recebidos, bem como informações sobre os códigos de activação de bónus que lhe foram atribuídos. Cada código de activação de bónus fornecido será também enviado para o seu e-mail.

Um código de activação de bónus também pode ser indicado na aplicação como código de activação novo.

Um código de activação de bónus pode ser utilizado para activar a aplicação noutro computador (por exemplo, pode atribuir um código a outro utilizador).

Um código de activação de bónus não pode ser utilizado nos casos seguintes:

- A aplicação está a ser utilizada com uma subscrição. Neste caso, pode utilizar o código de activação de bónus quando a subscrição expirar. Também pode aplicar o seu código de activação de bónus noutro computador.
- Já está definido na aplicação um código de activação como o código novo. Neste caso, pode utilizar o código de activação de bónus quando a licença expirar.

Para receber um código de activação de bónus e activar a aplicação com esse código:

1. Abra a janela principal do Kaspersky Internet Security e clique na ligação **O meu perfil** na parte inferior da janela.

   É apresentada a página da Internet com o seu perfil no programa Protect a Friend.

2. Efectue a autenticação na página da Internet com a sua Conta Kaspersky.

   A página da Internet apresenta os detalhes do seu perfil no programa Protect a Friend.

   Pode consultar as informações sobre os pontos de bónus que lhe foram atribuídos na secção **Os meus pontos de bónus**. Se tiver acumulado pontos de bónus suficientes para obter um código de activação de bónus, é apresentada uma notificação 1. junto ao botão **Receber um código de activação de bónus** na secção à direita da página da Internet.

3. Para receber um código de activação de bónus e activar a aplicação com esse código:

   a. Clique no botão **Receber um código de activação de bónus**.

      Aguarde até que lhe seja enviado um código de activação de bónus. O código de activação de bónus recebido é indicado na janela apresentada.

   b. Clique no botão **Activar**.

A janela **Activação** é apresentada com uma mensagem de verificação do código de activação. Após verificar o código de activação, é apresentada uma janela com uma mensagem a confirmar a activação bem sucedida do Kaspersky Internet Security.

Para consultar o histórico de códigos de activação de bónus recebidos e activar a aplicação com um código anterior:

1. Abra a janela principal do Kaspersky Internet Security e clique na ligação **O meu perfil** na parte inferior da janela.

   É apresentada a página da Internet com o seu perfil no programa Protect a Friend.

2. Efectue a autenticação na página da Internet com a sua Conta Kaspersky.

   A página da Internet apresenta os detalhes do seu perfil no programa Protect a Friend.

3. Na secção inferior da página da Internet, clique na ligação **Códigos de activação de bónus**.

   É apresentada a janela **Pontos de bónus** com o separador **Códigos de activação de bónus**.

4. Na lista de códigos de activação de bónus recebidos, clique no código que pretende utilizar para activar a aplicação.

   É apresentada uma janela com um código de activação de bónus.

5. Clique no botão **Activar**.

A janela **Activação** é apresentada com uma mensagem de verificação do código de activação. Após verificar o código de activação, é apresentada uma janela com uma mensagem a confirmar a activação bem sucedida do Kaspersky Internet Security.

CONTACTAR O SUPORTE TÉCNICO

Esta secção fornece informações sobre como obter suporte técnico e sobre os requisitos para receber ajuda do Suporte Técnico.

NESTA SECÇÃO

COMO OBTER SUPORTE TÉCNICO

Se não encontrar uma solução para o problema na documentação da aplicação ou numa das fontes de informação acerca da aplicação (consulte a secção "Fontes de informação sobre a aplicação" na página 9), recomendamos que contacte o Suporte Técnico da Kaspersky Lab. Os especialistas do Suporte Técnico irão responder a todas as suas questões sobre a instalação e utilização da aplicação.

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

Pode contactar o Suporte Técnico através de uma das seguintes formas:

- Por telefone: (351) 22 510 6476 ou (351) 21 381 09 22. Este método permite-lhe contactar os nossos especialistas.
- Enviando uma questão a partir da sua Conta Kaspersky no site de Suporte Técnico. Este método permite-lhe contactar os nossos especialistas através do formulário de consulta.

O suporte técnico está disponível apenas para os utilizadores que adquiriram uma licença para utilizar a aplicação. Não é fornecido suporte técnico aos utilizadores das versões de avaliação.

SUPORTE TÉCNICO POR TELEFONE

Se surgir uma questão urgente, pode contactar os especialistas de Suporte Técnico por telefone: (351) 707 500 322. (http://www.kaspersky.com/pt/support/tech_support/).

Antes de contactar o Suporte Técnico, leia as regras relativas ao suporte (http://support.kaspersky.com/support/rules). Isto permitirá aos nossos especialistas ajudá-lo mais rapidamente.

OBTER SUPORTE TÉCNICO ATRAVÉS DA CONTA KASPERSKY

A *Conta Kaspersky* é a sua área pessoal (https://my.kaspersky.pt) no site do Suporte Técnico.

Para obter acesso à Conta Kaspersky, deve passar pelo procedimento de registo na página de registo (https://my.kaspersky.com/pt/registration). Insira o seu endereço de e-mail e uma password para iniciar sessão em A Minha Conta Kaspersky.

Em Conta Kaspersky, pode executar as seguintes acções:

- Contactar o Suporte Técnico e o Laboratório de Vírus.
- Contactar o Suporte Técnico sem utilizar o e-mail.
- Acompanhar o estado dos seus pedidos em tempo real.
- Visualizar um histórico detalhado dos pedidos ao Suporte Técnico.
- Receber uma cópia do ficheiro da chave, caso este tenha sido perdido ou removido.

Suporte Técnico por e-mail

Pode enviar um pedido online para o Suporte Técnico em russo, inglês, alemão, francês ou espanhol.

Nos campos do formulário de pedido online, especifique os seguintes dados:

- Tipo de pedido
- Nome e número da versão da aplicação
- Descrição do pedido
- ID e password do cliente
- Endereço de e-mail

O especialista do Suporte Técnico envia a resposta à sua questão para a sua Conta Kaspersky e para o endereço de e-mail que especificou no seu pedido online.

Pedido online para o Laboratório de Vírus

Alguns pedidos têm de ser enviados para o Laboratório de Vírus e não para o Suporte Técnico.

Pode enviar pedidos de pesquisa de ficheiros e recursos da Internet suspeitos para o Laboratório de Vírus. Também pode contactar o Laboratório de Vírus em caso de falsos positivos do Kaspersky Internet Security em ficheiros e recursos da Internet que não considera perigosos.

Pode também enviar pedidos para o Laboratório de Vírus a partir da página com o formulário de pedido (http://support.kaspersky.com/virlab/helpdesk.html?LANG=pt) sem estar registado na Conta Kaspersky. Nesta página, não tem de especificar o código de activação da aplicação.

UTILIZAR FICHEIROS DE RASTREIO E SCRIPTS AVZ

Após notificar os especialistas do Suporte Técnico relativamente a um problema, estes poderão pedir-lhe para criar um relatório com informação do seu sistema operativo e enviá-lo para o Suporte Técnico. Além disso, os especialistas do Serviço de Suporte Técnico poderão também solicitar que crie um *ficheiro de rastreio*. O ficheiro de rastreio permite rastrear o processo de realizar comandos de aplicações passo a passo e determinar a etapa do funcionamento de uma aplicação na qual ocorre um erro.

Depois de os especialistas do Suporte Técnico analisarem os dados que enviou, estes podem criar um script AVZ e enviá-lo para si. A execução de scripts AVZ permite-lhe analisar os processos activos e verificar o sistema quanto a código malicioso, desinfectar/apagar ficheiros infectados e criar relatórios relativos aos resultados de verificações do sistema.

NESTA SECÇÃO

CRIAR UM RELATÓRIO SOBRE O ESTADO DO SISTEMA

Para criar um relatório sobre o estado do sistema:

1. Abra a janela principal da aplicação.
2. Clique na ligação **Suporte** na parte inferior da janela para abrir a janela **Suporte**.
3. Na janela apresentada, clique na ligação **Ferramentas de Suporte**.

   É apresentada a janela **Ferramentas de Suporte**.
4. Na janela apresentada, clique na ligação **Criar relatório sobre estado do sistema**.

O relatório sobre o estado do sistema é criado nos formatos HTML e XML e é guardado no arquivo sysinfo.zip. Quando a informação sobre o sistema for recolhida, pode ver o relatório.

Para ver o relatório:

1. Abra a janela principal da aplicação.
2. Clique na ligação **Suporte** na parte inferior da janela para abrir a janela **Suporte**.
3. Na janela apresentada, clique na ligação **Ferramentas de Suporte**.

   É apresentada a janela **Ferramentas de Suporte**.
4. Na janela que se abre, clique na ligação **Ver relatório**.

   É apresentada a janela do Microsoft Windows Explorer.
5. Na janela apresentada, abra o arquivo denominado sysinfo.zip que contém ficheiros de relatório.

ENVIAR FICHEIROS DE DADOS

Depois de criar os ficheiros de rastreio e o relatório de estado do sistema, precisa de enviá-los aos especialistas do Suporte Técnico da Kaspersky Lab.

Irá precisar de um número de pedido para carregar ficheiros no servidor do Suporte Técnico. Este número fica disponível na sua Conta Kaspersky no site do Suporte Técnico se o seu pedido estiver activo.

Para carregar os ficheiros de dados para o servidor de Suporte Técnico:

1. Abra a janela principal da aplicação.
2. Clique na ligação **Suporte** na parte inferior da janela para abrir a janela **Suporte**.
3. Na janela apresentada, clique na ligação **Ferramentas de Suporte**.

   É apresentada a janela **Ferramentas de Suporte**.
4. Na janela apresentada, clique na ligação **Enviar informações do serviço para o Suporte Técnico**.

   A janela **Enviar relatório** abre.

5. Seleccione as caixas de selecção junto aos dados que pretende enviar para o Suporte Técnico.

6. Clique no botão **Enviar relatório**.

Os ficheiros de dados seleccionados são comprimidos e enviados para o servidor do Suporte Técnico.

Se, por algum motivo, não for possível contactar o Suporte Técnico, os ficheiros de dados podem ser guardados no seu computador e enviados mais tarde a partir da Conta Kaspersky.

Para guardar os ficheiros de dados num disco:

1. Abra a janela principal da aplicação.

2. Clique na ligação **Suporte** na parte inferior da janela para abrir a janela **Suporte**.

3. Na janela apresentada, clique na ligação **Ferramentas de Suporte**.

4. É apresentada a janela **Ferramentas de Suporte**.

5. Na janela apresentada, clique na ligação **Enviar informações do serviço para o Suporte Técnico**.

   A janela **Enviar relatório** abre.

6. Seleccione as caixas de selecção junto aos dados que pretende enviar para o Suporte Técnico.

7. Clique na ligação **Guardar relatório**.

   É apresentada uma janela para guardar o arquivo.

8. Especifique o nome do arquivo e confirme a operação de guardar.

O arquivo criado pode ser enviado para o Suporte Técnico a partir da Conta Kaspersky.

EXECUÇÃO DE SCRIPT AVZ

Recomenda-se que não altere o texto de um script AVZ recebido dos especialistas da Kaspersky Lab. Se ocorrerem problemas durante a execução de um script, contacte o Suporte Técnico(ver secção "Como obter suporte técnico" na página 76).

Para executar um script AVZ:

1. Abra a janela principal da aplicação.

2. Clique na ligação **Suporte** na parte inferior da janela para abrir a janela **Suporte**.

3. Na janela apresentada, clique na ligação **Ferramentas de Suporte**.

   É apresentada a janela **Ferramentas de Suporte**.

4. Na janela apresentada, clique na ligação **Executar script**.

   É apresentada a janela **Execução de script**.

5. Copie o texto do script enviado pelos especialistas do Suporte Técnico, cole-o no campo de introdução de dados na janela apresentada e clique no botão **Seguinte**.

O script é executado.

Se o script for executado com êxito, o Assistente fecha-se automaticamente. Se ocorrer um erro durante a execução de um script, o Assistente apresenta uma mensagem para o efeito.

GLOSSÁRIO

A

ACTIVAR A APLICAÇÃO

Mudar a aplicação para o modo de funcionalidade completa. A activação da aplicação é efectuada pelo utilizador durante ou após a instalação da aplicação. O utilizador necessita de um código de activação para activar a aplicação.

ACTUALIZAÇÃO

O procedimento de substituição/adição de novos ficheiros (bases de dados ou módulos da aplicação) recolhidos a partir dos servidores de actualização da Kaspersky Lab.

ANALISADOR HEURÍSTICO

Uma tecnologia para detectar informações de ameaças que ainda não foram adicionadas às bases de dados da Kaspersky Lab. O analisador heurístico detecta objectos cujas actividades no sistema podem constituir uma ameaça de segurança. Os objectos detectados pelo analisador heurístico são considerados como provavelmente infectados. Por exemplo, um objecto pode ser considerado como provavelmente infectado se incluir sequências de comandos típicos de objectos maliciosos (abrir ficheiros, escrever em ficheiros).

APLICAÇÃO INCOMPATÍVEL

Uma aplicação antivírus de um fabricante terceiro ou uma aplicação da Kaspersky Lab que não suporta a gestão através do Kaspersky Internet Security.

ASSINATURA DIGITAL

Um bloco de dados encriptado incorporado num documento ou aplicação. É utilizada uma assinatura digital para identificar o autor do documento ou da aplicação. Para criar uma assinatura digital, é necessário que o autor do documento ou da aplicação tenha um certificado digital com a identidade do autor.

Uma assinatura digital permite verificar a origem dos dados e a integridade dos dados e fornecer protecção contra falsificações.

B

BASE DE DADOS DE ENDEREÇOS DE PHISHING

Lista de endereços web que são definidos como phishing pelos especialistas da Kaspersky Lab. A base de dados é regularmente actualizada e faz parte da aplicação da Kaspersky Lab.

BASE DE DADOS DE ENDEREÇOS WEB MALICIOSOS

A lista de endereços web cujo conteúdo pode ser considerado perigoso. A lista foi criada por especialistas da Kaspersky Lab. É regularmente actualizada e está incluída no pacote da aplicação da Kaspersky Lab.

BASES DE DADOS

Estas bases de dados incluem informações sobre as ameaças informáticas conhecidas da Kaspersky Lab na data de disponibilização da base de dados. Os registos incluídos nas bases de dados permitem detectar código malicioso nos objectos verificados. As bases de dados são criadas pelos especialistas da Kaspersky Lab e são actualizadas de hora em hora.

BLOQUEAR UM OBJECTO

Recusar o acesso a um objecto por parte de aplicações externas. Um objecto bloqueado não pode ser lido, executado, alterado ou apagado.

C

CLASSIFICAÇÃO DO UTILIZADOR

O índice de actividade do utilizador quando utiliza o Kaspersky Internet Security. A classificação do utilizador é apresentada no perfil de utilizador e depende das definições e da versão da aplicação.

COMPONENTES DE PROTECÇÃO

Partes integrais do Kaspersky Internet Security destinadas à protecção contra tipos de ameaças específicos (por exemplo, Anti-Spam, Anti-Phishing). Cada componente é relativamente independente dos restantes, pelo que pode ser desactivado ou configurado individualmente.

CONFIGURAÇÕES DE TAREFAS

Configurações da aplicação que são específicas para cada tipo de tarefa.

CÓDIGO DE ACTIVAÇÃO

Um código recebido ao adquirir uma licença do Kaspersky Internet Security. Este código é necessário para a activação da aplicação.

O código de activação é uma sequência exclusiva de vinte caracteres alfanuméricos no formato xxxxx-xxxxx-xxxxx-xxxxx.

CÓDIGO DE ACTIVAÇÃO DE BÓNUS

Um código de activação para o Kaspersky Internet Security fornecido ao utilizador em troca de pontos de bónus.

F

FALSO ALARME

Uma situação em que uma aplicação da Kaspersky Lab considere um objecto não infectado como estando infectado porque o seu código é semelhante ao de um vírus.

FICHEIRO COMPRIMIDO

Um ficheiro de arquivo que contém um programa de descompressão e instruções para a execução no sistema operativo.

G

GRUPO CONFIÁVEL

Um grupo em que o Kaspersky Internet Security coloca uma aplicação ou processo, conforme os critérios seguintes: presença de uma assinatura digital, reputação na KSN, nível de confiança da origem da aplicação e potencial perigo das acções realizadas pela aplicação ou processo. Com base no grupo confiável a que uma aplicação pertence, o Kaspersky Internet Security pode restringir as acções realizadas pela aplicação.

No Kaspersky Internet Security, as aplicações que pertence a um dos grupos de confiança seguintes: Confiáveis, Restrições baixas, Restrições altas, ou Não confiável.

K

KASPERSKY SECURITY NETWORK (KSN)

Uma infra-estrutura de serviços online que permite o acesso à Base de Conhecimento online da Kaspersky Lab, que contém informação sobre a reputação de ficheiros, recursos de Internet e software. A utilização de dados da Kaspersky Security Network garante uma resposta mais rápida das aplicações da Kaspersky Lab face a ameaças desconhecidas, melhora a eficácia de alguns componentes de protecção e reduz o risco de falsos diagnósticos positivos.

M

MÁSCARA DE FICHEIRO

Representação de um nome de ficheiro utilizando meta caracteres. Os meta caracteres padrão utilizados em máscaras de ficheiros são * e ?, em que * representa qualquer número de quaisquer caracteres e ? representa qualquer carácter único.

MÓDULOS DA APLICAÇÃO

Ficheiro incluídos no pacote de instalação da Kaspersky Lab que são responsáveis por realizar as suas principais tarefas. Um módulo executável particular corresponde a cada tipo de tarefa realizada pela aplicação (protecção em tempo real, verificação sob pedido, actualizações). Ao executar uma verificação completa do seu computador a partir da janela principal, você inicia a execução do módulo desta tarefa.

N

NÍVEL DE AMEAÇA

Consiste num índice que indica a probabilidade de uma aplicação constituir uma ameaça para o sistema operativo. O nível de ameaça é calculado utilizando a análise heurística, com base em dois tipos de critérios:

- estáticos (tais como, informação sobre o ficheiro executável de uma aplicação: tamanho, data de criação, etc.);
- dinâmicos, os quais são usados ao simular o funcionamento da aplicação num ambiente virtual (análise dos pedidos de funções do sistema por parte da aplicação).

O nível de ameaça permite detectar comportamentos típicos de software malicioso. Quanto menor for o nível de ameaça, maior é o número de acções que a aplicação tem permissão para executar no sistema.

NÍVEL DE SEGURANÇA

O nível de segurança é definido como um conjunto predefinido de definições para um componente da aplicação.

O

OBJECTO INFECTADO

É o objecto que contém uma parte de código que corresponde na íntegra a uma parte de código de uma aplicação perigosa conhecida. A Kaspersky Lab não recomenda a utilização de tais objectos.

OBJECTO PROVAVELMENTE INFECTADO

Um objecto cujo código contém código modificado de uma ameaça conhecida ou código semelhante ao de uma ameaça, tendo em consideração o seu comportamento.

OBJECTOS DE INICIALIZAÇÃO

O conjunto de programas necessários para iniciar e utilizar correctamente o sistema operativo e o software instalado no seu computador. Estes objectos são executados sempre que o sistema operativo é iniciado. Existem vírus capazes de infectar especificamente objectos execução automática, podendo levar, por exemplo, ao bloqueio do arranque do sistema operativo.

P

PACOTE DE ACTUALIZAÇÃO

Um pacote de ficheiros para actualizar módulos da aplicação. A aplicação da Kaspersky Lab copia os pacotes de actualização dos servidores de actualização da Kaspersky Lab e instala e aplica os mesmos automaticamente.

PERFIL DE UTILIZADOR

O resumo da participação do utilizador no programa Protect a Friend. O perfil de utilizador contém a classificação do utilizador, o número de pontos de bónus reunidos, uma ligação para a página para transferir o Kaspersky Internet Security, e os códigos de activação de bónus atribuídos ao utilizador.

PERÍODO DA LICENÇA

Um período durante o qual o utilizador tem acesso às funcionalidades da aplicação e direitos de utilização dos serviços adicionais.

PONTOS DE BÓNUS

Os pontos de bónus são pontos atribuídos pela Kaspersky Lab aos utilizadores que participam no programa Protect a Friend. Os pontos de bónus são fornecidos ao utilizador se o utilizador publicar uma ligação para uma aplicação da Kaspersky Lab em redes sociais ou colar a ligação numa mensagem de e-mail e o amigo do utilizar transferir o pacote de instalação com esta ligação.

PROCESSO CONFIÁVEL

Um processo de programa cujas operações de ficheiros não são monitorizadas pela aplicação da Kaspersky Lab no modo de protecção em tempo real. Ao eliminar uma actividade suspeita de um processo confiável, o Kaspersky Internet Security exclui o processo da lista de processos confiáveis e bloqueia todas as actividades do mesmo.

PROCESSOS OCULTOS

Um programa ou um conjunto de programas desenvolvido para ocultar vestígios de um intruso ou software malicioso no sistema operativo.

Em sistemas operativos baseados em Windows, os processos ocultos significam geralmente um programa que penetra no sistema operativo e intercepta as funções do sistema (Windows APIs). Principalmente, a intercepção e modificação de funções API de baixo nível permitem que esse programa dissimule a sua presença no sistema operativo. Normalmente, um processo oculto também pode dissimular a presença de quaisquer processos, pastas e ficheiros armazenados numa unidade de disco, além de chaves de registos, se estes estiverem descritos na configuração do processo oculto. Muitos processos ocultos instalam os seus próprios controladores e serviços no sistema operativo (são também "invisíveis").

PROTOCOLO

Um conjunto de regras claramente definido e padronizado que rege a interacção entre um cliente e um servidor. Os protocolos mais conhecidos e os serviços a eles associados incluem: HTTP, FTP e NNTP.

PROVÁVEL SPAM

Uma mensagem que não pode ser considerada inequivocamente como spam, mas que apresenta vários atributos de spam (por exemplo, certos tipos de e-mails e mensagens de publicidade).

Q

QUARENTENA

Um armazenamento dedicado no qual a aplicação coloca cópias de segurança de ficheiros que foram modificados ou eliminados durante a desinfecção. As cópias dos ficheiros são armazenadas num formato especial, não constituindo qualquer ameaça para o computador.

R

RASTREIOS

Executar a aplicação no modo de depuração, após cada comando ser executado, a aplicação é interrompida e o resultado deste passo é apresentado.

REGISTADOR DE TECLAS DIGITADAS

Um programa concebido para o registo oculto de informações sobre teclas premidas pelo utilizador. Os programas registadores de teclas digitadas também são denominados interceptadores ou espiões de teclas.

S

SCRIPT

Um pequeno programa de computador ou uma parte independente de um programa (função) que, por norma, é desenvolvida para executar uma tarefa específica. Na maioria dos casos, é utilizado com programas incorporados em hipertexto. Os scripts são executados, por exemplo, quando abre determinados sites.

Se a protecção em tempo real estiver activada, a aplicação vigia a inicialização dos scripts, intercepta-os e verifica-os quanto à presença de vírus. Dependendo do resultado da verificação, você pode bloquear ou permitir a execução de um script.

SECTOR DE INICIALIZAÇÃO DO DISCO

Um sector de inicialização é uma área especial no disco rígido de um computador, numa disquete ou num outro dispositivo de armazenamento de dados. Contém informações acerca do sistema de ficheiros do disco e um programa de carregamento de inicialização que é responsável por iniciar o sistema operativo.

Existem vários vírus que infectam os sectores de inicialização do disco, por isso são denominados de vírus de inicialização. A aplicação do Kaspersky Lab permite a verificação de vírus nos sectores de inicialização e desinfectá-los se for encontrada uma infecção.

SERVIDORES DE ACTUALIZAÇÃO DA KASPERSKY LAB

Os servidores HTTP da Kaspersky Lab para os quais as bases de dados de antivírus actualizadas e os módulos da aplicação são transferidos.

SITES DE PHISHING

Um tipo de fraude na Internet, quando são enviadas mensagens de e-mail com a intenção de roubar informações confidenciais. Por norma, estas informações dizem respeito a dados financeiros.

SPAM

O envio em massa de e-mails não solicitados contém, frequentemente, mensagens publicitárias.

T

TAREFA

As funções realizadas pela aplicação da Kaspersky Lab são implementadas como tarefas, como: Protecção de ficheiros em tempo real, Verificação completa do computador, Actualização da base de dados.

TECNOLOGIA ICHECKER

Uma tecnologia iChecker que permite aumentar a velocidade das verificações de antivírus, excluindo os objectos que não foram modificados desde a última verificação, desde que os parâmetros de verificação (a base de dados antivírus e as definições) não tenham sido alterados. A informação para cada ficheiro é armazenada numa base de dados especial. Esta tecnologia é utilizada na protecção em tempo real e nos modos de verificação a pedido.

Por exemplo, possui um ficheiro de arquivo que foi verificado pela aplicação da Kaspersky Lab e foi-lhe atribuído o estado de não infectado. Da próxima vez, a aplicação irá ignorar este arquivo, a não ser que tenha sido alterado ou as definições de verificação tenham sido modificadas. Se alterou o conteúdo do arquivo adicionando um novo objecto, se modificou as definições de verificação ou actualizou a base de dados de antivírus, o arquivo volta a ser verificado.

Limitações da tecnologia iChecker:

- esta tecnologia não funciona com ficheiros grandes, uma vez que é mais rápido verificar um ficheiro do que ver se foi modificado desde a última verificação;
- a tecnologia é compatível com um número limitado de formatos.

V

VERIFICAÇÃO DO TRÁFEGO

Uma verificação em tempo real que utiliza a informação da versão actual (a mais recente) das bases de dados, para os objectos transferidos através de todos os protocolos (por exemplo, HTTP, FTP, etc.).

VULNERABILIDADE

Uma falha num sistema operativo ou numa aplicação que pode ser explorada por criados de software malicioso para penetrar no sistema ou na aplicação e corromper a sua integridade. Um grande número de vulnerabilidades num sistema torna o mesmo pouco fiável, uma vez que os vírus que penetraram no sistema podem causar falhas de funcionamento no próprio sistema e nas aplicações instaladas.

VÍRUS

Um programa que infecta outros programas adicionando código aos mesmos, de forma a obter o controlo quando os ficheiros infectados são executados. Esta definição simples permitir expor a principal acção realizada por qualquer infecção de vírus.

VÍRUS DESCONHECIDO

Um novo vírus acerca do qual não existem informações nas bases de dados. Geralmente, os vírus desconhecidos são detectados pela aplicação em objectos, utilizando o analisador heurístico. Esses objectos são classificados como provavelmente infectados.

KASPERSKY LAB ZAO

O software da Kaspersky Lab é internacionalmente reconhecido pela sua protecção contra vírus, software malicioso, spam, ataques de rede e de hackers e outras ameaças.

Em 2008, a Kaspersky Lab foi classificada como um dos quatro principais fornecedores mundiais de soluções de software de segurança de informação para utilizadores finais (IDC Worldwide Endpoint Security Revenue by Vendor). A Kaspersky Lab é a programadora favorita dos utilizadores domésticos na Rússia em termos de sistemas de protecção de computadores, de acordo com o inquérito "TGI-Rússia 2009" da COMCON.

A Kaspersky Lab foi fundada na Rússia em 1997. Actualmente, é um grupo internacional de empresas sediado em Moscovo com cinco divisões regionais que gerem a actividade da empresa na Rússia, Europa Ocidental e de Leste, Médio Oriente, África, América do Norte e do Sul, Japão, China e outros países na região Ásia-Pacífico. A empresa emprega mais de 2000 especialistas qualificados.

Produtos. Os produtos da Kaspersky Lab proporcionam protecção para todos os sistemas—desde computadores domésticos até grandes redes empresariais.

A gama de produtos pessoais inclui aplicações antivírus para computadores de secretária e de bolso, portáteis e para smartphones e outros dispositivos móveis.

A Kaspersky Lab oferece aplicações e serviços para protecção de estações de trabalho, servidores de ficheiros e Internet, gateways de e-mail e firewalls. Quando utilizadas juntamente com o sistema de gestão centralizada da Kaspersky Lab, estas soluções asseguram uma protecção automática eficaz contra ameaças informáticas para empresas e organizações. Os produtos da Kaspersky Lab são certificados pelos maiores laboratórios de teste, são compatíveis com o software de muitos fornecedores de aplicações informáticas e são optimizados para funcionar em muitas plataformas de hardware.

Os analistas de vírus da Kaspersky Lab trabalham 24 horas por dia. Todos os dias descobrem centenas de novas ameaças informáticas e criam ferramentas para detectar e desinfectar as mesmas, sendo incluídas nas bases de dados utilizadas pelas aplicações da Kaspersky Lab. *A base de dados do Antivírus da Kaspersky Lab é actualizada de hora em hora*; e a *base de dados do Anti-Spam de cinco em cinco minutos*.

Tecnologias. Muitas das tecnologias que são agora parte integrante das ferramentas modernas de antivírus foram inicialmente desenvolvidas pela Kaspersky Lab. É portanto lógico que muitas empresas programadoras de software utilizem o kernel do Kaspersky Anti-Virus nas suas próprias aplicações. Essas empresas incluem: SafeNet (EUA), Alt-N Technologies (EUA), Blue Coat Systems (EUA), Check Point Software Technologies (Israel), Clearswift (Reino Unido), CommuniGate Systems (EUA), Critical Path (Irlanda), D-Link (Taiwan), M86 Security (EUA), GFI (Malta), IBM (EUA), Juniper Networks (EUA), LANDesk (EUA), Microsoft (EUA), NETASQ (França), NETGEAR (EUA), Parallels (Rússia), SonicWALL (EUA), WatchGuard Technologies (EUA) e ZyXEL Communications (Taiwan). Muitas das tecnologias inovadoras da empresa estão patenteadas.

Êxitos. Ao longo dos anos, a Kaspersky Lab ganhou centenas de prémios pelos seus serviços no combate às ameaças informáticas. Por exemplo, em 2010, o Kaspersky Anti-Virus recebeu vários dos principais prémios Advanced+ após vários testes realizados pelo AV-Comparatives, um reconhecido laboratório de antivírus austríaco. Contudo, o grande feito da Kaspersky Lab é a lealdade dos seus utilizadores em todo o mundo. Os produtos e tecnologias da empresa protegem mais de 300 milhões de utilizadores e o seu número de clientes empresariais é superior a 200 000.

Site da Web da Kaspersky Lab:	http://www.kaspersky.pt
Enciclopédia de Vírus:	http://www.securelist.com
Laboratório de vírus:	newvirus@kaspersky.com (apenas para o envio de ficheiros provavelmente infectados em formato de arquivo)
	http://support.kaspersky.com/virlab/helpdesk.html?LANG=pt
	(para colocar questões aos analistas de vírus)
Fórum na Internet da Kaspersky Lab:	http://forum.kaspersky.com

INFORMAÇÃO ACERCA DE CÓDIGO DE TERCEIROS

A informação acerca de código de terceiros está incluída no ficheiro legal_notices.txt, na pasta de instalação da aplicação.

AVISOS DE MARCAS COMERCIAIS

As marcas comerciais registadas e marcas de serviços são propriedade dos respectivos detentores.

Google Chrome é uma marca comercial propriedade da Google, Inc.

ICQ é uma marca comercial e/ou uma marca de serviço da ICQ LLC.

Intel e Pentium são marcas comerciais da Intel Corporation registadas nos Estados Unidos da América e noutros países.

Bing, DirectX, Internet Explorer, Microsoft, Windows e Windows Vista são marcas comerciais da Microsoft Corporation registadas nos Estados Unidos da América e noutros países.

Mozilla e Firefox são marcas comerciais da Mozilla Foundation.

ÍNDICE

A

B

C

D

E

F

I

K

L

M

N

O

P

Q

R

S

T

V