Kaspersky Anti-Virus 2012

Manual do Usuário

VERSÃO DO APLICATIVO: 12.0

Prezado usuário,

Obrigado por escolher nosso produto. Esperamos que este documento seja útil para você e responda à maioria das dúvidas que possam aparecer.

Data de revisão do documento: 19/4/2011

http://brazil.kaspersky.com
http://suporte.kasperskyamericas.com/usuarios-domesticos/env%C3%ADe-um-caso-de-suporte

CONTEÚDO

SOBRE ESTE MANUAL

Saudações dos especialistas da Kaspersky Lab!

Este manual contém informações sobre como instalar, configurar e usar o Kaspersky Anti-Virus. Esperamos que as informações fornecidas neste manual o ajudem a trabalhar com o aplicativo da forma mais fácil.

Este manual tem a finalidade de:

- ajudá-lo a instalar, ativar e usar o Kaspersky Anti-Virus;
- assegurar a pesquisa rápida de informações sobre problemas relacionados ao aplicativo;
- indicar outras fontes de informações sobre o aplicativo e formas de colaboração com o Serviço de Suporte Técnico.

Para o uso apropriado do aplicativo, é necessário ter habilidades básicas de computação: estar familiarizado com a interface do sistema operacional que você usa, lidar com as principais técnicas específicas desse sistema, saber como trabalhar com email e com a Internet.

NESTA SEÇÃO:

NESTE MANUAL

Este manual contém as seguintes seções:

Fontes de informações sobre o aplicativo

Esta seção descreve as fontes de informações sobre o aplicativo e lista os sites que podem ser usados para discutir a operação do aplicativo.

Kaspersky Anti-Virus

Esta seção descreve os recursos do aplicativo e fornece informações resumidas sobre as funções e os componentes do aplicativo. Você saberá os itens que estão incluídos no kit de distribuição e os serviços que estão disponíveis para usuários registrados do aplicativo. Esta seção fornece informações sobre os requisitos de software e hardware que um computador deve atender para permitir a instalação do aplicativo pelo usuário.

Instalando e removendo o aplicativo

Esta seção fornece informações sobre como instalar e desinstalar o aplicativo em um computador.

Licenciando o aplicativo

Esta seção fornece informações sobre os termos gerais relacionados à ativação do aplicativo. Leia esta seção para saber mais sobre a finalidade do contrato de licença, os tipos de licença, as formas de ativação do aplicativo e a renovação da licença.

Interface do aplicativo

Esta seção fornece informações sobre os elementos básicos da interface gráfica do aplicativo: o ícone do aplicativo e o menu de contexto do ícone do aplicativo, a janela principal, a janela de configurações e as janelas de notificações.

Iniciando e interrompendo o aplicativo

Esta seção contém informações sobre como iniciar e encerrar o aplicativo.

Gerenciando a proteção do computador

Esta seção fornece informações sobre como detectar ameaças à segurança do computador e como configurar o nível de segurança. Leia esta seção para saber mais sobre como ativar, desativar e pausar a proteção ao usar o aplicativo.

Solucionando tarefas típicas

Esta seção fornece informações sobre como resolver os problemas mais comuns relacionados à proteção do computador usando o aplicativo.

Configurações avançadas do aplicativo

Esta seção fornece informações detalhadas sobre como configurar cada componente do aplicativo.

Testando a operação do aplicativo

Esta seção fornece informações sobre como garantir que o aplicativo detecte vírus e suas modificações, e execute as ações corretas com eles.

Entrando em contato com o Serviço de Suporte Técnico

Esta seção fornece informações sobre como entrar em contato com o Serviço de Suporte Técnico da Kaspersky Lab.

Apêndice

Esta seção fornece informações que complementam o texto da documentação.

Glossário

Esta seção contém uma lista de termos mencionados na documentação e suas respectivas definições.

Kaspersky Lab ZAO

Esta seção fornece informações sobre a Kaspersky Lab.

Informações sobre código de terceiros

Esta seção fornece informações sobre os códigos de terceiros usados no aplicativo.

Índice

Nesta seção, é possível localizar rapidamente as informações desejadas no documento.

CONVENÇÕES DA DOCUMENTAÇÃO

O texto contido nesta documentação vem acompanhado de elementos semânticos que devem receber atenção: avisos, dicas, exemplos.

São usadas convenções no documento para realçar os elementos semânticos. As convenções do documento e exemplos de sua utilização são mostrados na tabela a seguir.

Tabela 1. Convenções da documentação

TEXTO DE EXEMPLO	DESCRIÇÃO DAS CONVENÇÕES DA DOCUMENTAÇÃO
Observe que...	Os avisos são realçados com a cor vermelha e mostrados em caixas. Os avisos fornecem informações sobre ações provavelmente indesejadas que podem levar à perda de dados ou falhas na operação do computador.
É recomendável usar...	As observações são mostradas em caixas. As observações podem conter dicas úteis, recomendações, valores específicos ou situações específicas importantes de operação do aplicativo.
Exemplo: ...	Os exemplos são exibidos sobre fundo amarelo sob o título "Exemplo".

TEXTO DE EXEMPLO	DESCRIÇÃO DAS CONVENÇÕES DA DOCUMENTAÇÃO
Atualização significa... Ocorreu o evento *Bancos de dados desatualizados*.	Os seguintes elementos semânticos são exibidos no texto em itálico: • termos novos; • nomes de status e eventos do aplicativo.
Pressione **ENTER**. Pressione **ALT**+**F4**.	Os nomes de teclas do teclado são exibidos em uma fonte em negrito e em letras maiúsculas. Os nomes das teclas seguidos de um sinal de + (adição) indicam o uso de uma combinação de teclas. Essas teclas devem ser pressionadas simultaneamente.
Clique no botão **Ativar**.	Os nomes de elementos da interface do aplicativo, como campos de entrada, itens de menu e botões são exibidos em negrito.
➡ *Para configurar a programação da tarefa:*	As frases introdutórias de instruções são exibidas em itálico e acompanhadas de um sinal de seta.
Insira help na linha de comando. Em seguida, a seguinte mensagem será exibida: Especifique a data no formato dd:mm:aa.	Os seguintes tipos de conteúdo de texto são exibidos com uma fonte especial: • texto da linha de comando; • texto de mensagens exibidas pelo aplicativo na tela; • dados que o usuário deve inserir.
<Endereço IP do computador>	As variáveis são colocadas entre colchetes angulares. Em vez de uma variável, deve ser inserido o valor correspondente omitindo os colchetes angulares.

FONTES DE INFORMAÇÕES SOBRE O APLICATIVO

Esta seção descreve as fontes de informações sobre o aplicativo e lista os sites que podem ser usados para discutir a operação do aplicativo.

Você pode selecionar a fonte de informações mais adequada de acordo com o nível de importância e a urgência de sua pergunta.

NESTA SEÇÃO:

FONTES DE INFORMAÇÕES PARA PESQUISAS INDEPENDENTES

Você pode usar as seguintes fontes para encontrar informações sobre o aplicativo:

- a página do aplicativo no site da Kaspersky Lab;
- a página do aplicativo no site do Serviço de Suporte Técnico (Base de Dados de Conhecimento);
- ajuda online;
- documentação.

Se você não conseguir resolver um problema sozinho, é recomendável entrar em contato com o Serviço de Suporte Técnico da Kaspersky Lab (consulte a seção "Suporte técnico por telefone" na página 116).

Para usar as fontes de informações no site da Kaspersky Lab, é necessário estabelecer uma conexão com a Internet.

A página do aplicativo no site da Kaspersky Lab

O site da Kaspersky Lab apresenta uma página individual para cada aplicativo.

Nessa página (http://brazil.kaspersky.com/produtos/produtos-para-usuarios-domesticos/anti-virus), é possível exibir informações gerais sobre os aplicativos, suas funções e recursos.

A página http://brazil.kaspersky.com apresenta um URL para a Loja Virtual. Nela, você pode comprar ou renovar o aplicativo.

A página do aplicativo no site do Serviço de Suporte Técnico (Base de Dados de Conhecimento)

A Base de Dados de Conhecimento é uma seção do site do Serviço de Suporte Técnico que fornece recomendações de como trabalhar com os aplicativos da Kaspersky Lab. A Base de Dados de Conhecimento compreende artigos de referência agrupados por tópicos.

Na página do aplicativo na Base de Dados de Conhecimento (http://support.kaspersky.com/kav2012), é possível ler artigos que fornecem informações úteis, recomendações e respostas às perguntas frequentes sobre como comprar, instalar e usar o aplicativo.

Os artigos podem responder perguntas que estão fora do escopo do Kaspersky Anti-Virus, relacionadas a outros aplicativos da Kaspersky Lab. Eles também podem conter notícias do Serviço de Suporte Técnico.

Ajuda online

A ajuda online do aplicativo compreende os arquivos de ajuda.

A ajuda contextual fornece informações sobre cada janela do aplicativo, listando e descrevendo as configurações correspondentes e uma lista de tarefas.

A ajuda completa fornece informações detalhadas sobre como gerenciar a proteção do computador usando o aplicativo.

Documentação

O Manual do Usuário do aplicativo fornece informações sobre como instalar, ativar e configurar o aplicativo, além de dados de operação do aplicativo. O documento também descreve a interface do aplicativo e fornece maneiras de resolver as tarefas normais do usuário ao trabalhar com o aplicativo.

DISCUTINDO OS APLICATIVOS DA KASPERSKY LAB NO FÓRUM

Se a sua pergunta não precisar de uma resposta urgente, você poderá discuti-la com os especialistas da Kaspersky Lab e com outros usuários no nosso Fórum (http://forum.kaspersky.com/index.php?showforum=87).

Neste fórum, é possível exibir os tópicos existentes, deixar seus comentários e criar novos tópicos.

ENTRANDO EM CONTATO COM O DEPARTAMENTO DE VENDAS

Se você tiver dúvidas sobre como selecionar, comprar ou renovar o aplicativo, poderá entrar em contato com os especialistas do nosso Departamento de Vendas de uma das seguintes maneiras:

- Ligando para o nosso escritório central em Moscou por telefone (http://www.kaspersky.com/contacts).
- Enviando uma mensagem com sua pergunta para sales@kaspersky.com.

O serviço é fornecido em russo e em inglês.

ENTRANDO EM CONTATO COM A EQUIPE DE DESENVOLVIMENTO DA DOCUMENTAÇÃO POR EMAIL

Para entrar em contato com a Equipe de Desenvolvimento da Documentação, envie um email para docfeedback@kaspersky.com. Use "Kaspersky Help Feedback: Kaspersky Anti-Virus" como assunto da mensagem.

KASPERSKY ANTI-VIRUS

Esta seção descreve os recursos do aplicativo e fornece informações resumidas sobre as funções e os componentes do aplicativo. Você saberá os itens que estão incluídos no kit de distribuição e os serviços que estão disponíveis para usuários registrados do aplicativo. Esta seção fornece informações sobre os requisitos de software e hardware que um computador deve atender para permitir a instalação do aplicativo pelo usuário.

NESTA SEÇÃO:

NOVIDADES

O Kaspersky Anti-Virus oferece os novos recursos a seguir:

- A interface aprimorada da janela principal do Kaspersky Anti-Virus garante o acesso rápido às funções do aplicativo.
- A lógica das operações com a Quarentena e o Backup (veja a página 96) foi aperfeiçoada: agora, eles são representados em duas guias separadas, cada uma com seu respectivo escopo exclusivo.
- Foi adicionado um Gerenciador de Tarefas para facilitar o gerenciamento de tarefas no Kaspersky Anti-Virus (consulte a seção "Gerenciando tarefas de verificação. Gerenciador de Tarefas" na página 63).
- A participação no Kaspersky Security Network (veja a página 109) permite identificar a reputação de aplicativos e sites de acordo com os dados recebidos de usuários de todo o mundo.
- Quando o Antivírus da Web está ativado, é possível ativar separadamente a análise heurística para verificar páginas da Web quanto à presença de phishing (consulte a seção "Usando a análise heurística ao trabalhar com o Antivírus da Web" na página 81). Ao verificar as páginas da Web quanto à presença de phishing, a análise heurística será aplicada independentemente de ter sido ativada para o Antivírus da Web.
- A aparência do Kaspersky Gadget foi redesenhada (veja a página 32).

KIT DE DISTRIBUIÇÃO

Você pode comprar o aplicativo das seguintes maneiras:

- **Na caixa**. Distribuído nas lojas de nossos parceiros.
- **Na Loja Virtual**. Distribuído em lojas virtuais da Kaspersky Lab (por exemplo, http://brazil.kaspersky.com, seção **Loja Virtual**) ou de empresas parceiras.

Se você comprou a versão do aplicativo na caixa, o kit de distribuição conterá os seguintes itens:

- envelope lacrado com o CD de instalação, que contém os arquivos do aplicativo e da documentação;
- Manual do Usuário resumido com um código de ativação;
- contrato de licença que estipula os termos sob os quais você pode usar o aplicativo.

O conteúdo do kit de distribuição pode ser diferente de acordo com a região na qual o aplicativo é distribuído.

Se você comprar o Kaspersky Anti-Virus em uma loja virtual, deverá copiar o aplicativo do site da loja. As informações necessárias para a ativação do aplicativo serão enviadas por email após o pagamento.

Para obter mais detalhes sobre as formas de compra e o kit de distribuição, entre em contato com o Departamento de Vendas.

SERVIÇOS PARA USUÁRIOS REGISTRADOS

Ao comprar uma licença de usuário do aplicativo, você se torna usuário registrado dos aplicativos da Kaspersky Lab e pode tirar proveito dos seguintes serviços durante todo o período de validade da licença:

- atualização dos bancos de dados e novas versões do aplicativo;
- consultoria por telefone e por email sobre problemas relacionados à instalação, configuração e uso do aplicativo;
- notificações sobre o lançamento de novos aplicativos da Kaspersky Lab e novos vírus. Para usar este serviço, você deve assinar a entrega de notícias da Kaspersky Lab no site do Serviço de Suporte Técnico.

Não são fornecidos serviços de consultoria sobre problemas relacionados ao funcionamento de sistemas operacionais, software e tecnologias de terceiros.

REQUISITOS DE HARDWARE E SOFTWARE

Para assegurar o funcionamento correto do Kaspersky Anti-Virus, o computador deve atender aos seguintes requisitos:

Requisitos gerais:

- 480 MB de espaço disponível no disco rígido (incluindo 380 MB na unidade do sistema).
- Unidade de CD/DVD (para instalar o Kaspersky Anti-Virus do CD de distribuição).
- Acesso à Internet (para a ativação do aplicativo e a atualização dos bancos de dados e módulos do software).
- Microsoft Internet Explorer 6.0 ou superior.
- Microsoft Windows Installer 2.0.

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

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

Requisitos para Microsoft Windows Vista Home Basic, Microsoft Windows Vista Home Premium, Microsoft Windows Vista Business, Microsoft Windows Vista Enterprise, Microsoft Windows Vista Ultimate, Microsoft Windows 7 Starter, Microsoft Windows 7 Home Basic, Microsoft Windows 7 Home Premium, Microsoft Windows 7 Professional e Microsoft Windows 7 Ultimate:

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

Requisitos para netbooks:

- Processador Intel Atom 1,6 GHz ou um equivalente compatível.
- Placa de vídeo Intel GMA950 com pelo menos 64 MB de RAM de vídeo (ou um equivalente compatível).
- Tamanho de tela não inferior a 10,1".

INSTALANDO E REMOVENDO O APLICATIVO

Esta seção fornece informações sobre como instalar e desinstalar o aplicativo em um computador.

NESTA SEÇÃO:

PROCEDIMENTO DE INSTALAÇÃO PADRÃO

O Kaspersky Anti-Virus será instalado no computador no modo interativo, usando o Assistente de Instalação.

O Assistente consiste em uma série de telas (etapas) nas quais você pode navegar usando os botões **Voltar** e **Avançar**. Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**. Para interromper o Assistente em qualquer estágio, clique no botão **Cancelar**.

Se o aplicativo proteger mais de um computador (o número máximo de computadores depende da licença), ele será instalado da mesma maneira em todos os computadores. Nesse caso, de acordo com o contrato de licença, o período da licença começa na data da primeira ativação. Quando você ativa o aplicativo no segundo computador e nos seguintes, o período de validade da licença é reduzido pelo tempo decorrido desde a primeira ativação. Portanto, o período de validade da licença vai expirar simultaneamente para todas as cópias instaladas do aplicativo.

- *Para instalar o Kaspersky Anti-Virus no computador,*

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

A instalação do Kaspersky Anti-Virus a partir de um arquivo de instalação baixado online é idêntica à instalação a partir do CD.

NESTA SEÇÃO:

ETAPA 1. PESQUISANDO A VERSÃO MAIS RECENTE DO APLICATIVO

Antes da instalação, o Assistente de Instalação verifica nos servidores de atualização da Kaspersky Lab uma versão mais nova do Kaspersky Anti-Virus.

Se não for encontrada nenhuma versão mais recente do produto nos servidores de atualização da Kaspersky Lab, o Assistente de Instalação da versão atual será executado.

Se os servidores de atualização tiverem uma versão mais recente do Kaspersky Anti-Virus, você verá uma solicitação para baixar e instalar essa versão no computador. É recomendável instalar a nova versão do aplicativo, pois as versões mais recentes incluem aprimoramentos que garantem uma proteção mais confiável do computador. Se você cancelar o download da nova verão, o Assistente de Instalação da versão atual será executado. Se você decidir instalar a versão mais recente, os arquivos de distribuição do produto serão baixados no computador e o Assistente de Instalação da nova versão será executado automaticamente. Para obter uma descrição mais detalhada do procedimento de instalação da versão mais recente, consulte a documentação correspondente.

ETAPA 2. VERIFICANDO SE O SISTEMA ATENDE AOS REQUISITOS DE INSTALAÇÃO

Antes da instalação do Kaspersky Anti-Virus no computador, o instalador verifica o sistema operacional e os service packs para confirmar se eles atendem aos requisitos de software para a instalação do produto (consulte a seção "Requisitos de hardware e software" na página 14). Além disso, o instalador verifica a presença dos softwares e das credenciais necessários para instalar aplicativos. Se algum dos requisitos acima não for atendido, será exibida uma notificação correspondente na tela.

Se o computador atender a todos os requisitos, o Assistente procurará aplicativos da Kaspersky Lab que, quando executados simultaneamente com o Kaspersky Anti-Virus, podem gerar conflitos. Se esses aplicativos forem encontrados, será solicitado que você os remova manualmente.

Se for encontrada uma versão anterior do Kaspersky Anti-Virus ou do Kaspersky Internet Security, todos os dados que podem ser usados pelo Kaspersky Anti-Virus 2012 (por exemplo, informações de ativação ou configurações do aplicativo) serão salvos e usados ao instalar o novo aplicativo, enquanto o anterior será removido automaticamente.

ETAPA 3. SELECIONANDO O TIPO DE INSTALAÇÃO

Neste estágio, você pode escolher o tipo de instalação do Kaspersky Anti-Virus mais adequado:

- *Instalação padrão*. Se você escolher esta opção (a caixa **Alterar configurações de instalação** estará desmarcada), o aplicativo será totalmente instalado no computador com as configurações de proteção recomendadas pela Kaspersky Lab.
- *Instalação personalizada*. Nesse caso (a caixa **Alterar configurações de instalação** está marcada), será solicitado que você especifique a pasta de destino na qual o aplicativo deve ser instalado (consulte a seção "Etapa 7. Selecionando a pasta de destino" na página 17) e desative a proteção do processo de instalação, se necessário (consulte a seção "Etapa 8. Preparando a instalação" na página 17).

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

ETAPA 4. EXAMINANDO O CONTRATO DE LICENÇA

Nesta etapa, você deve examinar o contrato de licença firmado entre você e a Kaspersky Lab.

Leia o contrato atentamente e, se aceitar todos os termos, clique no botão **Eu concordo**. A instalação continuará.

Se não desejar aceitar o contrato de licença, cancele a instalação do aplicativo clicando no botão **Cancelar**.

ETAPA 5. DECLARAÇÃO SOBRE COLETA DE DADOS DO KASPERSKY SECURITY NETWORK

Nesta etapa, você será convidado a participar do Kaspersky Security Network. A participação no programa envolve o envio de informações à Kaspersky Lab sobre as novas ameaças detectadas, os aplicativos em execução e os

aplicativos assinados baixados no seu computador, além das informações do seu sistema. Nós asseguramos que nenhum dos seus dados pessoais serão divulgados.

Analise a Declaração Sobre Coleta de Dados do Kaspersky Security Network. Para ler a versão completa da Declaração, clique no botão **Contrato completo do KSN**. Se você concordar todos os termos da Declaração, marque a caixa **Eu aceito os termos de participação no Kaspersky Security Network** na janela do Assistente.

Se tiver selecionado a instalação personalizada, clique no botão **Avançar** (consulte a seção "Etapa 3. Selecionando o tipo de instalação" na página 16). Se estiver executando a instalação padrão, clique no botão **Instalar**. A instalação continuará.

ETAPA 6. PROCURANDO APLICATIVOS INCOMPATÍVEIS

Nesta etapa, o programa verifica se há aplicativos incompatíveis com o Kaspersky Anti-Virus instalados no computador.

Se não for encontrado nenhum aplicativo incompatível, o Assistente continuará automaticamente na etapa seguinte.

Se forem detectados aplicativos incompatíveis, eles serão exibidos em uma lista na tela e será solicitado que você os remova. Os aplicativos que não puderem ser removidos automaticamente pelo Kaspersky Anti-Virus deverão ser removidos manualmente. Ao remover os aplicativos incompatíveis, você precisará reiniciar o sistema operacional; em seguida, a instalação do Kaspersky Anti-Virus continuará automaticamente.

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

ETAPA 7. SELECIONANDO A PASTA DE DESTINO

Esta etapa do Assistente de Instalação estará disponível somente se a instalação personalizada estiver selecionada (consulte a seção "Etapa 3. Selecionando o tipo de instalação" na página 16). Ao executar a instalação padrão, essa etapa é ignorada e o aplicativo é instalado na pasta padrão.

Neste estágio, você pode escolher a pasta na qual Kaspersky Anti-Virus será instalado. O caminho a seguir é definido por padrão:

- **<disco>\Arquivos de Programas\Kaspersky Lab\Kaspersky Anti-Virus 2012** – para sistemas de 32 bits;
- **<disco>\Arquivos de Programas (x86)\Kaspersky Lab\Kaspersky Anti-Virus 2012** – para sistemas de 64 bits.

Para instalar o Kaspersky Anti-Virus em outra pasta, especifique o caminho da pasta desejada no campo de entrada ou clique no botão **Procurar** e escolha uma pasta na janela que é aberta.

Lembre-se das seguintes restrições:

- O aplicativo não pode ser instalado em unidades de rede ou removíveis, nem em unidades virtuais (criadas usando o comando SUBST).
- É recomendável evitar instalar o aplicativo em uma pasta que já contenha arquivos ou outras pastas, pois essa pasta ficará indisponível para edição.
- O caminho da pasta de instalação não pode ter mais de 160 caracteres, nem conter os caracteres especiais **/**, **?**, **:**, *****, **"**, **>**, **<** ou **|**.

Para saber se há espaço em disco suficiente no computador para instalar o aplicativo, clique no botão **Uso do Disco**. Na janela que é aberta, você pode ver as informações de espaço em disco. Para fechar a janela, clique em **OK**.

Para continuar a instalação, clique no botão **Avançar** na janela do Assistente.

ETAPA 8. PREPARANDO PARA INSTALAR

Esta etapa do Assistente de Instalação estará disponível somente se a instalação personalizada estiver selecionada (consulte a seção "Etapa 3. Selecionando o tipo de instalação" na página 16). Na instalação padrão, essa etapa é ignorada.

Como o computador pode estar infectado com programas maliciosos que podem afetar a instalação do Kaspersky Anti-Virus, o processo de instalação deve ser protegido.

Por padrão, a proteção do processo de instalação está ativada; a caixa **Proteger o processo de instalação** está marcada na janela do Assistente.

Quando não for possível instalar o aplicativo, é recomendável desmarcar essa caixa (por exemplo, ao executar a instalação remota usando a Área de Trabalho Remota do Windows). Talvez o motivo seja essa proteção.

Nesse caso, interrompa a instalação, reinicie-a, marque a caixa **Alterar configurações de instalação** na etapa Selecionar o tipo de instalação (consulte a seção "Etapa 3. Selecionando o tipo de instalação" na página 16) e, na etapa Preparando a instalação, desmarque a caixa **Proteger o processo de instalação**.

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

Ao instalar o aplicativo em um computador com o Microsoft Windows XP, as conexões de rede ativas são interrompidas. A maioria das conexões interrompidas será restaurada após uma pausa.

ETAPA 9. INSTALANDO

A instalação do aplicativo pode levar algum tempo. Aguarde sua conclusão.

Quando a instalação for concluída, o Assistente continuará automaticamente na próxima etapa.

Se ocorrer um erro de instalação que pode ser devido a programas maliciosos que impedem a instalação de aplicativos antivírus no computador, o Assistente de Instalação solicitará que você baixe a *Ferramenta de Remoção de Vírus Kaspersky*, um utilitário especial para neutralizar infecções.

Se concordar em instalar o utilitário, o Assistente de Instalação o baixará dos servidores da Kaspersky Lab e, em seguida, a instalação do utilitário será iniciada automaticamente. Se o Assistente não puder baixar o utilitário, será solicitado que você o faça clicando no link fornecido.

Depois de concluir o trabalho com o utilitário, exclua-o e reinicie a instalação do Kaspersky Anti-Virus.

ETAPA 10. CONCLUINDO A INSTALAÇÃO

Esta janela do Assistente informa sobre a conclusão bem-sucedida da instalação do aplicativo. Para executar o Kaspersky Anti-Virus, confirme se a caixa **Executar o Kaspersky Anti-Virus** está marcada e clique no botão **Concluir**.

Em alguns casos, pode ser necessário reiniciar o sistema operacional. Se a caixa **Executar o Kaspersky Anti-Virus 2012** estiver marcada, o aplicativo será executado automaticamente após a reinicialização do sistema operacional.

Se você tiver desmarcado a caixa antes de fechar o Assistente, execute o aplicativo manualmente (consulte a seção "Executando e fechando o aplicativo manualmente" na página 34).

ETAPA 11. ATIVANDO O APLICATIVO

A *ativação* é o procedimento para ativar a licença que permite usar uma versão totalmente funcional do aplicativo até a expiração da licença.

Você precisará de uma conexão com a Internet para ativar o aplicativo.

As seguintes opções de ativação do Kaspersky Anti-Virus estarão disponíveis:

- **Ativar a versão comercial**. Se tiver comprado uma versão comercial do aplicativo, selecione esta opção e insira o código de ativação.

  Se você especificar um código de ativação do Kaspersky Anti-Virus no campo de entrada, o procedimento para migrar para o Kaspersky Anti-Virus será iniciado após a conclusão da ativação.

- **Ativar versão de avaliação**. Use esta opção de ativação se desejar instalar a versão de avaliação do aplicativo antes de decidir comprar a versão comercial. Você poderá usar a versão totalmente funcional do aplicativo durante o período limitado pela licença da versão de avaliação do aplicativo. Quando a licença expirar, ela não poderá ser ativada pela segunda vez.

ETAPA 12. REGISTRANDO UM USUÁRIO

Esta etapa está disponível somente ao ativar a versão comercial do aplicativo. Na ativação da versão de avaliação, essa etapa é ignorada.

É necessário se registrar para poder entrar em contato com o Serviço de Suporte Técnico da Kaspersky Lab no futuro.

Se você concordar em se registrar, especifique a data do registro nos campos correspondentes e clique no botão **Avançar**.

ETAPA 13. CONCLUINDO A ATIVAÇÃO

O Assistente informará que o Kaspersky Anti-Virus foi ativado com êxito. Além disso, são fornecidas informações sobre a licença: o tipo de licença (comercial ou de avaliação), a data de expiração e o número de hosts com a licença.

Se você tiver ativado uma assinatura, serão exibidas informações sobre o status da assinatura em vez da data de expiração da licença.

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

ATUALIZANDO A VERSÃO ANTERIOR DO KASPERSKY ANTI-VIRUS

Se o Kaspersky Anti-Virus 2010 ou 2011 já estiver instalado no computador, atualize o aplicativo para o Kaspersky Anti-Virus 2012. Se você tiver uma licença ativa do Kaspersky Anti-Virus 2010 ou 2011, não será necessário ativar o aplicativo: o Assistente de Instalação recuperará as informações da licença do Kaspersky Anti-Virus 2010 ou 2011 automaticamente e as usará durante o processo de instalação.

O Kaspersky Anti-Virus será instalado no computador no modo interativo, usando o Assistente de Instalação.

O Assistente consiste em uma série de telas (etapas) nas quais você pode navegar usando os botões **Voltar** e **Avançar**. Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**. Para interromper o Assistente em qualquer estágio, clique no botão **Cancelar**.

Se o aplicativo proteger mais de um computador (o número máximo de computadores depende da licença), ele será instalado da mesma maneira em todos os computadores. Nesse caso, de acordo com o contrato de licença, o período da licença começa na data da primeira ativação. Quando você ativa o aplicativo no segundo computador e nos seguintes, o período de validade da licença é reduzido pelo tempo decorrido desde a primeira ativação. Portanto, o período de validade da licença vai expirar simultaneamente para todas as cópias instaladas do aplicativo.

- *Para instalar o Kaspersky Anti-Virus no computador,*

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

  A instalação do Kaspersky Anti-Virus a partir de um arquivo de instalação baixado online é idêntica à instalação a partir do CD.

NESTA SEÇÃO:

ETAPA 1. PESQUISANDO A VERSÃO MAIS RECENTE DO APLICATIVO

Antes da instalação, o Assistente de Instalação verifica nos servidores de atualização da Kaspersky Lab uma versão mais nova do Kaspersky Anti-Virus.

Se não for encontrada nenhuma versão mais recente do produto nos servidores de atualização da Kaspersky Lab, o Assistente de Instalação da versão atual será executado.

Se os servidores de atualização tiverem uma versão mais recente do Kaspersky Anti-Virus, você verá uma solicitação para baixar e instalar essa versão no computador. É recomendável instalar a nova versão do aplicativo, pois as versões mais recentes incluem aprimoramentos que garantem uma proteção mais confiável do computador. Se você cancelar o download da nova verão, o Assistente de Instalação da versão atual será executado. Se você decidir instalar a versão mais recente, os arquivos de distribuição do produto serão baixados no computador e o Assistente de Instalação da nova versão será executado automaticamente. Para obter uma descrição mais detalhada do procedimento de instalação da versão mais recente, consulte a documentação correspondente.

ETAPA 2. VERIFICANDO SE O SISTEMA ATENDE AOS REQUISITOS DE INSTALAÇÃO

Antes de instalar o Kaspersky Internet Security no computador, o instalador verifica o sistema operacional e os service packs para confirmar se eles atendem aos requisitos de software para a instalação do produto (consulte a seção "Requisitos de hardware e software" na página 14). Além disso, o instalador verifica a presença dos softwares e das credenciais necessários para instalar aplicativos. Se algum dos requisitos acima não for atendido, será exibida uma notificação correspondente na tela.

Se o computador atender a todos os requisitos, o Assistente procurará aplicativos da Kaspersky Lab que, quando executados simultaneamente com o Kaspersky Anti-Virus, podem gerar conflitos. Se esses aplicativos forem encontrados, será solicitado que você os remova manualmente.

Se for encontrada uma versão anterior do Kaspersky Anti-Virus ou do Kaspersky Internet Security, todos os dados que podem ser usados pelo Kaspersky Anti-Virus 2012 (por exemplo, informações de ativação ou configurações do aplicativo) serão salvos e usados ao instalar o novo aplicativo, enquanto o anterior será removido automaticamente.

ETAPA 3. SELECIONANDO O TIPO DE INSTALAÇÃO

Neste estágio, você pode escolher o tipo de instalação do Kaspersky Anti-Virus mais adequado:

- *Instalação padrão*. Se você escolher esta opção (a caixa **Alterar configurações de instalação** estará desmarcada), o aplicativo será totalmente instalado no computador com as configurações de proteção recomendadas pela Kaspersky Lab.
- *Instalação personalizada*. Nesse caso (a caixa **Alterar configurações de instalação** está marcada), você poderá especificar a pasta de destino na qual o aplicativo será instalado (consulte a seção "Etapa 7.

Selecionando a pasta de destino" na página 17) e desativar a proteção do processo de instalação, se necessário (consulte a seção "Etapa 8. Preparando a instalação" na página 17).

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

ETAPA 4. EXAMINANDO O CONTRATO DE LICENÇA

Nesta etapa, você deve examinar o contrato de licença firmado entre você e a Kaspersky Lab.

Leia o contrato atentamente e, se aceitar todos os termos, clique no botão **Eu concordo**. A instalação continuará.

Se não desejar aceitar o contrato de licença, cancele a instalação do aplicativo clicando no botão **Cancelar**.

ETAPA 5. DECLARAÇÃO SOBRE COLETA DE DADOS DO KASPERSKY SECURITY NETWORK

Nesta etapa, você será convidado a participar do Kaspersky Security Network. A participação no programa envolve o envio de informações à Kaspersky Lab sobre as novas ameaças detectadas, os aplicativos em execução e os aplicativos assinados baixados no seu computador, além das informações do seu sistema. Nós asseguramos que nenhum dos seus dados pessoais serão divulgados.

Analise a Declaração Sobre Coleta de Dados do Kaspersky Security Network. Para ler a versão completa da Declaração, clique no botão **Contrato completo do KSN**. Se você concordar todos os termos da Declaração, marque a caixa **Eu aceito os termos de participação no Kaspersky Security Network** na janela do Assistente.

Se tiver selecionado a instalação personalizada, clique no botão **Avançar** (consulte a seção "Etapa 3. Selecionando o tipo de instalação" na página 16). Se estiver executando a instalação padrão, clique no botão **Instalar**. A instalação continuará.

ETAPA 6. PROCURANDO APLICATIVOS INCOMPATÍVEIS

Nesta etapa, o programa verifica se há aplicativos incompatíveis com o Kaspersky Anti-Virus instalados no computador.

Se não for encontrado nenhum aplicativo incompatível, o Assistente continuará automaticamente na etapa seguinte.

Se forem detectados aplicativos incompatíveis, eles serão exibidos em uma lista na tela e será solicitado que você os remova. Os aplicativos que não puderem ser removidos automaticamente pelo Kaspersky Anti-Virus deverão ser removidos manualmente. Ao remover os aplicativos incompatíveis, você precisará reiniciar o sistema operacional; em seguida, a instalação do Kaspersky Anti-Virus continuará automaticamente.

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

ETAPA 7. SELECIONANDO A PASTA DE DESTINO

Esta etapa do Assistente de Instalação estará disponível somente se a instalação personalizada estiver selecionada (consulte a seção "Etapa 3. Selecionando o tipo de instalação" na página 16). Ao executar a instalação padrão, essa etapa é ignorada e o aplicativo é instalado na pasta padrão.

Neste estágio, você pode escolher a pasta na qual Kaspersky Anti-Virus será instalado. O caminho a seguir é definido por padrão:

- **<disco>\Arquivos de Programas\Kaspersky Lab\Kaspersky Anti-Virus 2012** – para sistemas de 32 bits;
- **<disco>\Arquivos de Programas (x86)\Kaspersky Lab\Kaspersky Anti-Virus 2012** – para sistemas de 64 bits.

Para instalar o Kaspersky Anti-Virus em outra pasta, especifique o caminho da pasta desejada no campo de entrada ou clique no botão **Procurar** e escolha uma pasta na janela que é aberta.

Lembre-se das seguintes restrições:

- O aplicativo não pode ser instalado em unidades de rede ou removíveis, nem em unidades virtuais (criadas usando o comando SUBST).

- É recomendável evitar instalar o aplicativo em uma pasta que já contenha arquivos ou outras pastas, pois essa pasta ficará indisponível para edição.
- O caminho da pasta de instalação não pode ter mais de 160 caracteres, nem conter os caracteres especiais **/**, **?**, **:**, *****, **"**, **>**, **<** ou **|**.

Para saber se há espaço em disco suficiente no computador para instalar o aplicativo, clique no botão **Uso do Disco**. Na janela que é aberta, você pode ver as informações de espaço em disco. Para fechar a janela, clique em **OK**.

Para continuar a instalação, clique no botão **Avançar** na janela do Assistente.

ETAPA 8. PREPARANDO PARA INSTALAR

Esta etapa do Assistente de Instalação estará disponível somente se a instalação personalizada estiver selecionada (consulte a seção "Etapa 3. Selecionando o tipo de instalação" na página 16). Na instalação padrão, essa etapa é ignorada.

Como o computador pode estar infectado com programas maliciosos que podem afetar a instalação do Kaspersky Anti-Virus, o processo de instalação deve ser protegido.

Por padrão, a proteção do processo de instalação está ativada; a caixa **Proteger o processo de instalação** está marcada na janela do Assistente.

Quando não for possível instalar o aplicativo, é recomendável desmarcar essa caixa (por exemplo, ao executar a instalação remota usando a Área de Trabalho Remota do Windows). Talvez o motivo seja essa proteção.

Nesse caso, interrompa a instalação, reinicie-a, marque a caixa **Alterar configurações de instalação** na etapa Selecionar o tipo de instalação (consulte a seção "Etapa 3. Selecionando o tipo de instalação" na página 16) e, na etapa Preparando a instalação, desmarque a caixa **Proteger o processo de instalação**.

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

Ao instalar o aplicativo em um computador com o Microsoft Windows XP, as conexões de rede ativas são interrompidas. A maioria das conexões interrompidas será restaurada após uma pausa.

ETAPA 9. INSTALANDO

A instalação do aplicativo pode levar algum tempo. Aguarde sua conclusão.

Quando a instalação for concluída, o Assistente continuará automaticamente na próxima etapa.

Se ocorrer um erro de instalação que pode ser devido a programas maliciosos que impedem a instalação de aplicativos antivírus no computador, o Assistente de Instalação solicitará que você baixe a *Ferramenta de Remoção de Vírus Kaspersky*, um utilitário especial para neutralizar infecções.

Se concordar em instalar o utilitário, o Assistente de Instalação o baixará dos servidores da Kaspersky Lab e, em seguida, a instalação do utilitário será iniciada automaticamente. Se o Assistente não puder baixar o utilitário, será solicitado que você o faça clicando no link fornecido.

Depois de concluir o trabalho com o utilitário, exclua-o e reinicie a instalação do Kaspersky Anti-Virus.

ETAPA 10. CONCLUSÃO DO ASSISTENTE

Esta janela do Assistente informa sobre a conclusão bem-sucedida da instalação do aplicativo. Para executar o Kaspersky Anti-Virus, confirme se a caixa **Executar o Kaspersky Anti-Virus** está marcada e clique no botão **Concluir**.

Em alguns casos, pode ser necessário reiniciar o sistema operacional. Se a caixa **Executar o Kaspersky Anti-Virus 2012** estiver marcada, o aplicativo será executado automaticamente após a reinicialização do sistema operacional.

Se você tiver desmarcado a caixa antes de fechar o Assistente, execute o aplicativo manualmente (consulte a seção "Executando e fechando o aplicativo manualmente" na página 34).

CENÁRIOS DE INSTALAÇÃO DIFERENTES DO PADRÃO

Esta seção descreve cenários de instalação do aplicativo diferentes da instalação padrão ou da atualização da versão anterior.

Instalando o Kaspersky Anti-Virus e ativando mais tarde usando um código de ativação do Kaspersky Internet Security

Se, ao instalar o Kaspersky Anti-Virus, na etapa Ativando o aplicativo, você inserir um código de ativação do Kaspersky Internet Security, o processo de upgrade será executado, migrando do Kaspersky Anti-Virus para o Kaspersky Internet Security.

Se, ao instalar o Kaspersky Anti-Virus, na etapa Ativando o aplicativo, você selecionar **Ativar mais tarde** e ativar o aplicativo instalado com o código de ativação do Kaspersky Internet Security, o processo de upgrade também será executado, migrando do Kaspersky Anti-Virus para o Kaspersky Internet Security.

Instalando o Kaspersky Anti-Virus 2012 sobre o Kaspersky Internet Security 2010 ou 2011

Se você executar a instalação do Kaspersky Anti-Virus 2012 em um computador em que o Kaspersky Internet Security 2010 ou 2011 com uma licença ativa já estiver instalado, o Assistente de Instalação detectará as informações da licença e solicitará que você selecione uma das seguintes ações:

- Usar a licença atual do Kaspersky Internet Security 2010 ou 2011. Nesse caso, o procedimento de upgrade será iniciado, resultando na instalação do Kaspersky Internet Security 2012 no computador. Você poderá usar o Kaspersky Internet Security 2012 enquanto a licença do Kaspersky Internet Security 2010 ou 2011 for válida.
- Continuar a instalação do Kaspersky Anti-Virus 2012. Nesse caso, o procedimento de instalação continuará de acordo com o cenário padrão a partir da etapa Ativando o aplicativo.

INICIANDO

Após a instalação, o aplicativo está pronto para ser usado. Para garantir a proteção adequada do computador, é recomendável executar o seguinte imediatamente após a instalação e configuração:

- Atualizar os bancos de dados do aplicativo (consulte a seção "Como atualizar os bancos de dados e módulos do aplicativo" na página 40).
- Verificar o computador quanto à presença de vírus (consulte a seção "Como executar a verificação completa do computador quanto à presença de vírus" na página 42) e vulnerabilidades (consulte a seção "Como verificar o computador quanto à presença de vulnerabilidades" na página 42).
- Verifique o status de proteção do computador e elimine problemas na proteção, se necessário.

REMOVENDO O APLICATIVO

Depois que o Kaspersky Anti-Virus for desinstalado, o computador e seus dados pessoais estarão desprotegidos.

O Kaspersky Anti-Virus será desinstalado com a ajuda do Assistente de Instalação.

Para iniciar o Assistente,

no menu **Iniciar**, selecione **Programas → Kaspersky Anti-Virus 2012 → Remover o Kaspersky Anti-Virus 2012**.

NESTA SEÇÃO:

ETAPA 1. SALVANDO DADOS PARA REUTILIZAÇÃO

Neste momento, é possível especificar os dados usados pelo aplicativo que você deseja manter para reutilizar na próxima instalação do aplicativo (por exemplo, uma versão mais nova do aplicativo).

Por padrão, o aplicativo é removido completamente do computador.

Para salvar dados para reutilização:

1. Escolha a opção **Salvar objetos do aplicativo**.
2. Marque as caixas correspondentes aos tipos de dados que deseja salvar:
   - **Dados de ativação** – dados que eliminam a necessidade de ativar o aplicativo futuramente através do uso automático da licença atual, desde que ela não tenha expirado até o momento da próxima instalação.
   - **Arquivos do Backup e da Quarentena** – arquivos verificados pelo aplicativo e colocados no armazenamento de Backup ou na Quarentena.
   - **Configurações de operação do aplicativo** – valores das configurações do aplicativo selecionadas durante sua configuração.
   - **Dados do iChecker** – arquivos que contêm informações sobre os objetos que já foram verificados quanto à presença de vírus.

ETAPA 2. CONFIRMAÇÃO DA REMOÇÃO DO APLICATIVO

Como a remoção do aplicativo ameaça a segurança do computador e de seus dados pessoais, será solicitado que você confirme sua intenção de remover o aplicativo. Para fazer isso, clique no botão **Remover**.

Para interromper a remoção do aplicativo a qualquer momento, a operação pode ser cancelada clicando no botão **Cancelar**.

ETAPA 3. REMOVENDO O APLICATIVO. CONCLUINDO A REMOÇÃO

Nesta etapa, o Assistente remove o aplicativo do computador. Aguarde a conclusão da remoção.

Ao remover o aplicativo, talvez seja necessário reiniciar o sistema operacional. Se você cancelar a reinicialização imediata, a conclusão do procedimento de remoção será adiada até que o sistema operacional seja reiniciado ou o computador seja desligado e reiniciado.

LICENCIANDO O APLICATIVO

Esta seção fornece informações sobre os termos gerais relacionados à ativação do aplicativo. Leia esta seção para saber mais sobre a finalidade do contrato de licença, os tipos de licença, as formas de ativação do aplicativo e a renovação da licença.

NESTA SEÇÃO:

SOBRE O CONTRATO DE LICENÇA DO USUÁRIO FINAL

O Contrato de Licença é um contrato legal firmado entre você e a Kaspersky Lab ZAO que estipula os termos de uso do aplicativo.

Leia atentamente todos os termos do Contrato de Licença antes de começar a usar o aplicativo.

Você pode ler os termos do Contrato de Licença ao instalar o aplicativo da Kaspersky Lab.

É considerado que você aceitou os termos do Contrato de Licença nas seguintes situações:

- Ao romper o lacre da caixa com o CD de instalação (somente se você tiver comprado o aplicativo na versão em caixa ou em uma loja de qualquer de nossos parceiros).
- Ao confirmar sua aceitação do texto do Contrato de Licença ao instalar o aplicativo.

Se você não aceitar os termos do Contrato de Licença, deverá interromper a instalação do aplicativo.

SOBRE O FORNECIMENTO DE DADOS

Para aumentar o nível da proteção em tempo real, o aceite dos termos do Contrato de Licença indica que você concorda em enviar automaticamente informações sobre somas de verificação de objetos processados (MD5), informações necessárias para determinar a reputação de URLs e dados estatísticos da proteção antispam. As informações recuperadas não contêm dados particulares e outros tipos de informações confidenciais. As informações recuperadas são protegidas pela Kaspersky Lab de acordo com os requisitos estipulados pela legislação existente. Você pode obter mais detalhes no site: http://suporte.kasperskyamericas.com/usuarios-domesticos/env%C3%ADe-um-caso-de-suporte.

SOBRE A LICENÇA

A *licença* é o direito com tempo limitado de uso do aplicativo fornecido a você de acordo com o Contrato de Licença. A licença contém um código exclusivo para a ativação da sua cópia do Kaspersky Anti-Virus.

A licença concede a você o direito de tirar proveito dos seguintes serviços:

- Usar o aplicativo em um ou em vários dispositivos.

  O número de dispositivos nos quais você pode usar o aplicativo está especificado no Contrato de Licença.

- Entrar em contato com o Serviço de Suporte Técnico da Kaspersky Lab.
- Aproveitar o conjunto completo de serviços fornecidos pela Kaspersky Lab ou por seus parceiros durante o período de validade da licença (consulte a seção "Serviços para usuários registrados" na página 14).

O escopo dos serviços fornecidos e o período de validade do aplicativo dependem do tipo de licença usada para ativar o aplicativo.

São oferecidos os seguintes tipos de licença:

- *Avaliação* – uma licença gratuita com período de validade limitado, oferecida para você se familiarizar com o aplicativo.

  Se você copiar o aplicativo do site http://brazil.kaspersky.com, se tornará proprietário da licença de avaliação automaticamente. Assim que a licença expirar, todos os recursos do Kaspersky Anti-Virus serão desativados. Para continuar usando o aplicativo, você deverá comprar a licença comercial.

- *Comercial* – uma licença paga com um período de validade limitado, oferecida mediante a compra do aplicativo.

  Após a expiração da licença comercial, o aplicativo continuará sendo executado no modo de funcionalidade limitada. Você ainda poderá verificar o computador quanto à presença de vírus e usar outros componentes do aplicativo, mas somente com os bancos de dados instalados antes da expiração da licença. Para continuar usando o Kaspersky Anti-Virus, você deverá renovar a licença comercial.

  É recomendável renovar a licença no máximo no dia em que a licença atual expirar para garantir a proteção antivírus mais abrangente do computador.

SOBRE O CÓDIGO DE ATIVAÇÃO

O *código de ativação* é um código que você recebe ao comprar a licença comercial do Kaspersky Anti-Virus. Esse código é necessário para a ativação do aplicativo.

O código de ativação é uma cadeia de caracteres latinos alfanumérica no formato xxxxx-xxxxx-xxxxx-xxxxx.

O código de ativação é fornecido de uma das seguintes maneiras, dependendo de como você comprou o aplicativo:

- Se você comprou a versão na caixa do Kaspersky Anti-Virus, o código de ativação será especificado na documentação ou na caixa que contém o CD de instalação.
- Se você comprou o Kaspersky Anti-Virus em uma loja virtual, o código de ativação será enviado para o email especificado ao solicitar o produto.

O período de validade da licença começa no momento em que você ativa o aplicativo. Se você tiver comprado uma licença destinada ao uso do Kaspersky Anti-Virus em vários dispositivos, o período de validade da licença começará no momento em que você inserir o código no primeiro desses dispositivos.

Se você perder ou excluir acidentalmente seu código após a ativação, deverá enviar uma solicitação ao Serviço de Suporte Técnico da Kaspersky Lab através da Minha conta Kaspersky (consulte a seção "Obtendo suporte técnico através da Minha conta Kaspersky" na página 116).

Ao concluir a ativação do aplicativo com um código, você receberá um *ID do cliente*. ID do cliente é a identificação pessoal do usuário, necessária para obter suporte técnico por telefone ou através da Minha conta Kaspersky (consulte a seção "Obtendo suporte técnico através da Minha conta Kaspersky" na página 116).

INTERFACE DO APLICATIVO

Esta seção fornece informações sobre os elementos básicos da interface gráfica do aplicativo: o ícone do aplicativo e o menu de contexto do ícone do aplicativo, a janela principal, a janela de configurações e as janelas de notificações.

NESTA SEÇÃO:

O ÍCONE NA ÁREA DE NOTIFICAÇÃO

Imediatamente após a instalação do aplicativo, seu ícone será exibido na área de notificação da barra de tarefas do Microsoft Windows.

Por padrão, no sistema operacional Microsoft Windows 7, o ícone do aplicativo fica oculto, mas você pode exibi-lo para acessar o aplicativo mais facilmente (consulte a documentação do sistema operacional).

O ícone tem as seguintes finalidades:

- É um indicador da operação do aplicativo.
- Dá acesso ao menu de contexto, à janela principal do aplicativo e a janela de notícias.

Indicação de operação do aplicativo

Esse ícone é um indicador da operação do aplicativo. Ele também indica o status da proteção e exibe as funções básicas em execução pelo aplicativo no momento:

 – verificação de uma mensagem de email;

 – verificação do tráfego da Web;

 – atualização os bancos de dados e módulos do aplicativo;

 – o computador deve ser reiniciado para aplicar as atualizações;

 – ocorreu uma falha na operação de algum componente do aplicativo.

Por padrão, o ícone é animado: por exemplo, durante a verificação de emails, um pequeno símbolo de carta pisca na frente do ícone do aplicativo; quando a atualização está em andamento, você vê um globo girando. A animação pode ser desativada (consulte a seção "Translucidez das janelas de notificações" na página 107).

Quando a animação é desativada, o ícone pode ter as seguintes formas:

 (símbolo colorido) – todos ou alguns componentes de proteção são ativados;

 (símbolo preto e branco) – todos os componentes de proteção são desativados.

Acesso ao menu de contexto e às janelas do aplicativo

Usando o ícone, é possível abrir o menu de contexto (na página 28) (clicando com o botão direito do mouse) e a janela principal do aplicativo (consulte a seção "A janela principal do Kaspersky Anti-Virus" na página 29) (clicando com o botão esquerdo do mouse).

Se houver notícias da Kaspersky Lab disponíveis, o ícone será exibido na área de notificação da barra de tarefas do Microsoft Windows. Clique duas vezes nesse ícone para abrir o Agente de Notícias (consulte a seção "Agente de Notícias" na página 33).

O MENU DE CONTEXTO

Usando o menu de contexto, é possível executar várias ações com o aplicativo rapidamente.

O menu do Kaspersky Anti-Virus contém os seguintes itens:

- **Gerenciador de Tarefas** – abre a janela do **Gerenciador de Tarefas**.
- **Atualização** – executa a atualização dos bancos de dados e módulos do aplicativo.
- **Teclado Virtual** – exibe o Teclado Virtual.
- **Kaspersky Anti-Virus** – abre a janela principal do aplicativo.
- **Pausar a proteção / Reiniciar proteção** – desativa/ativa temporariamente os componentes de proteção em tempo real. Esse item do menu não afeta as atualizações do aplicativo, nem a execução das verificações de vírus.
- **Configurações** – abre a janela de configurações do aplicativo.
- **Sobre** – abre uma janela com informações sobre o aplicativo.
- **Notícias** – abre a janela Agente de Notícias (consulte a seção "Agente de Notícias" na página 33). Este item de menu será exibido se houver notícias não lidas.
- **Sair** – fecha o Kaspersky Anti-Virus (quando este item for selecionado, o aplicativo será descarregado da RAM do computador).

Figura 1. O menu de contexto

Se uma tarefa de verificação de vírus ou de atualização estiver em execução quando você abrir o menu de contexto, seu nome e o status de andamento (porcentagem concluída) serão exibidos no menu de contexto. Se você selecionar um item de menu com o nome de uma tarefa, poderá alternar para a janela principal com um relatório dos resultados da execução da tarefa atual.

Para abrir o menu de contexto,

posicione o cursor sobre o ícone do aplicativo na área de notificação da barra de tarefas e clique nele com o botão direito do mouse.

Por padrão, no sistema operacional Microsoft Windows 7, o ícone do aplicativo fica oculto, mas você pode exibi-lo para acessar o aplicativo mais facilmente (consulte a documentação do sistema operacional).

A JANELA PRINCIPAL DO KASPERSKY ANTI-VIRUS

A janela principal do aplicativo contém os elementos de interface que dão acesso a todos os principais recursos do aplicativo.

A janela principal pode ser dividida em duas partes:

- A parte superior da janela fornece informações sobre o status de proteção do computador.

Figura 2. Parte superior da janela principal

- Na parte inferior da janela, é possível alternar rapidamente para o uso dos principais recursos do aplicativo (por exemplo, executar tarefas de verificação de vírus, atualizar os bancos de dados e módulos do software).

Figura 3. Parte inferior da janela principal

Se você selecionar alguma das seções na parte inferior da janela, a janela da função correspondente será aberta. Você pode retornar à seleção de funções clicando no botão **Voltar** no canto superior esquerdo da janela.

Você também pode usar os seguintes botões e links:

- **Proteção em nuvem** – para alternar para as informações sobre o Kaspersky Security Network (na página 109).
- **Configurações** – para abrir a janela de configurações do aplicativo (consulte a seção "A janela de configurações do aplicativo" na página 31).
- **Relatórios** – para alternar para os relatórios de operação do aplicativo.
- **Notícias** – para alternar para a exibição de notícias na janela Agente de Notícias (consulte a seção "Agente de Notícias" na página 33). Esse link será exibido depois que o aplicativo receber uma notícia.
- **Ajuda** – para exibir o sistema de Ajuda do Kaspersky Anti-Virus.
- **Minha Conta Kaspersky** – para entrar na conta pessoal do usuário no site do Serviço de Suporte Técnico.
- **Suporte** – para abrir a janela com informações do sistema e links para os recursos de informações da Kaspersky Lab (site do Serviço de Suporte Técnico, fórum).
- **Gerenciar Licença** – para ir para a ativação e renovação da licença do Kaspersky Anti-Virus.

Você pode abrir a janela principal do aplicativo usando um dos seguintes métodos:

- Clicando no ícone do aplicativo na área de notificação da barra de tarefas.

  Por padrão, no sistema operacional Microsoft Windows 7, o ícone do aplicativo fica oculto, mas você pode exibi-lo para acessar o aplicativo mais facilmente (consulte a documentação do sistema operacional).

- Selecionando **Kaspersky Anti-Virus** no menu de contexto (consulte a seção "Menu de contexto" na página 28).
- Clicando no ícone do Kaspersky Anti-Virus localizado no centro do Kaspersky Gadget (apenas no Microsoft Windows Vista e no Microsoft Windows 7).

JANELAS DE NOTIFICAÇÃO E MENSAGENS POP-UP

O Kaspersky Anti-Virus notifica sobre eventos importantes que ocorrem durante sua operação, usando *janelas de notificação* e *mensagens pop-up* que são exibidas sobre o ícone do aplicativo na área de notificação da barra de tarefas.

As *janelas de notificação* são exibidas pelo Kaspersky Anti-Virus quando é possível executar diversas ações em relação a um evento: por exemplo, se um objeto malicioso for detectado, você poderá bloquear o acesso a ele, excluí-lo ou tentar desinfetá-lo. O aplicativo solicita que você selecione uma das ações disponíveis. A janela de notificações desaparecerá da tela somente se você selecionar uma das ações.

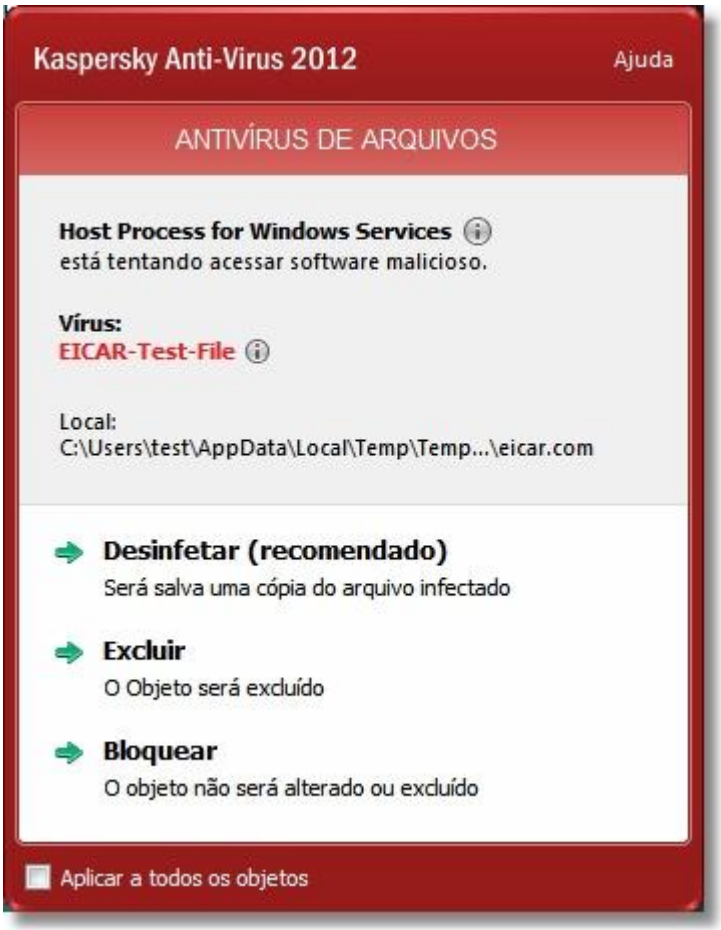

Figura 4. Janela de notificações

As *mensagens pop-up* são exibidas pelo Kaspersky Anti-Virus para informar sobre eventos que não exigem que você selecione uma ação. Algumas mensagens pop-up contêm links que podem ser usados para executar uma ação disponibilizada pelo aplicativo: por exemplo, executar a atualização dos bancos de dados ou iniciar a ativação do aplicativo). As mensagens pop-up desaparecem da tela automaticamente logo após sua exibição.

Figura 5. Mensagem pop-up

De acordo com a importância de um evento em relação à segurança do computador, as notificações e mensagens pop-up são divididas em três tipos:

- Notificações críticas – informam sobre os eventos de importância crítica para a segurança do computador, como a detecção de um objeto malicioso ou uma atividade perigosa no sistema. As janelas das notificações e mensagens pop-up críticas são vermelhas.
- Notificações importantes – informam sobre os eventos que possivelmente são importantes para a segurança do computador, como a detecção de um objeto possivelmente infectado ou uma atividade suspeita no sistema. As janelas das notificações e mensagens pop-up importantes são amarelas.
- Notificações informativas – informam sobre os eventos que não têm importância crítica para a segurança do computador. As janelas das notificações e mensagens pop-up informativas são verdes.

A JANELA DE CONFIGURAÇÕES DO APLICATIVO

A janela de configurações do Kaspersky Anti-Virus (também chamada de "janela de configurações") foi criada para configurar todo o aplicativo e componentes de proteção individuais, tarefas de verificação e atualização e para executar outras tarefas de configuração avançada (consulte a seção "Configurações avançadas do aplicativo" na página 55).

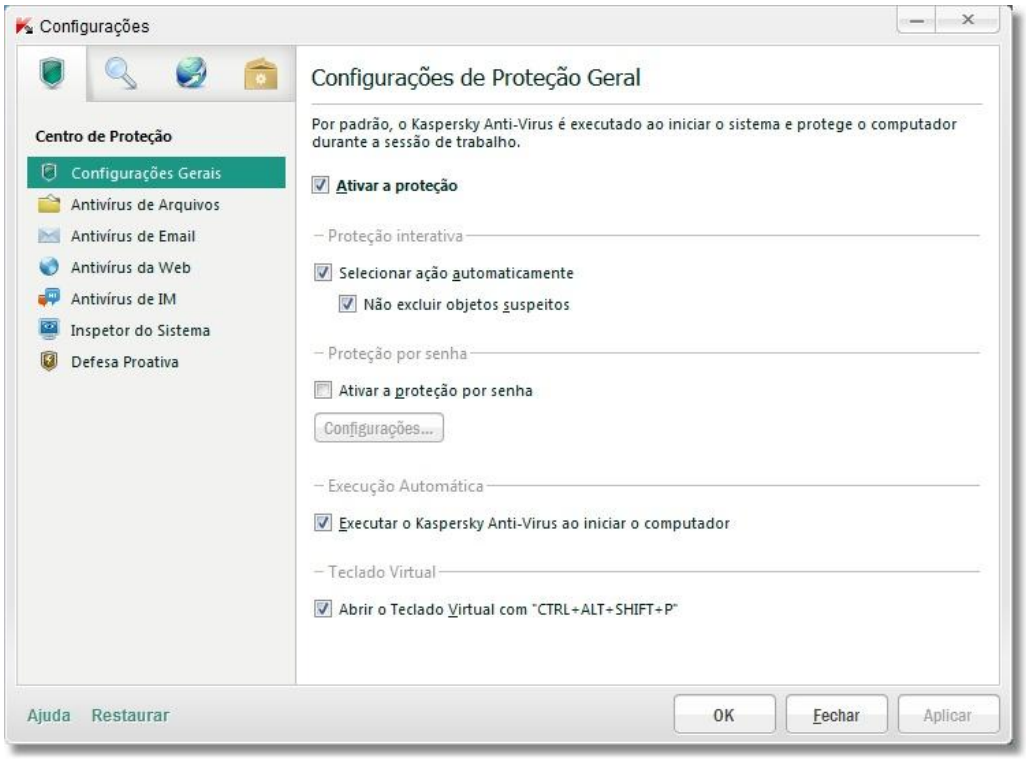

Figura 6. A janela de configurações do aplicativo

A janela de configurações do aplicativo consiste em duas partes:

- à esquerda da janela, você pode escolher o componente, a tarefa ou outro item do aplicativo para ser configurado;
- à direita da janela estão os controles que podem ser usados para configurar o item selecionado à esquerda.

Os componentes, as tarefas e outros itens à esquerda da janela estão agrupados nas seguintes seções:

– **Centro de Proteção**;

– **Verificação**;

– **Atualização**;

– **Configurações Avançadas**.

Você pode abrir a janela de configurações do aplicativo usando um dos seguintes métodos:

- clicando no link **Configurações** na parte superior da janela principal do aplicativo (consulte a seção "A janela principal do Kaspersky Anti-Virus" na página 29);
- selecionando **Configurações** no menu de contexto (consulte a seção "Menu de contexto" na página 28);
- clicando no botão com o ícone **Configurações** na interface do Kaspersky Gadget (apenas nos sistemas operacionais Microsoft Windows Vista e Microsoft Windows 7). É necessário atribuir a função de abrir a janela de configurações ao botão (consulte a seção "Como usar o Kaspersky Gadget" na página 53).

O KASPERSKY GADGET

Ao usar o Kaspersky Anti-Virus em um computador com o Microsoft Windows Vista ou o Microsoft Windows 7, você também pode usar o Kaspersky Gadget (aqui chamado de *gadget*). O Kaspersky Gadget foi criado para acessar rapidamente os principais recursos do aplicativo (por exemplo, a indicação do status de proteção, a verificação de objetos quanto à presença de vírus, os relatórios de operação do aplicativo).

Depois de instalar o Kaspersky Anti-Virus em um computador com o Microsoft Windows 7, o gadget é exibido automaticamente na área de trabalho. Depois de instalar o aplicativo em um computador com o Microsoft Windows Vista, você deverá adicionar o gadget manualmente à Barra Lateral do Microsoft Windows (consulte a documentação do sistema operacional).

Figura 7. O Kaspersky Gadget

AGENTE DE NOTÍCIAS

Através do *Agente de Notícias*, a Kaspersky Lab fornece informações sobre todos os eventos importantes relacionados ao Kaspersky Anti-Virus e à proteção contra ameaças de computador.

O aplicativo o notificará sobre as notícias exibindo um ícone especial na área de notificação da barra de tarefas (veja a seguir) e uma mensagem pop-up. Também são exibidas informações sobre o número de itens de notícias não lidos na janela principal do aplicativo. Um ícone de jornal é exibido na interface do gadget do Kaspersky Anti-Virus.

Você pode ler as notícias das seguintes maneiras:

- clicando no ícone  na área de notificação da barra de tarefas;
- clicando no link **Ler as notícias** na mensagem pop-up de notícias;
- clicando no link **Notícias** na janela principal do aplicativo;
- clicando no ícone exibido no centro do Gadget quando for exibida uma notícia (somente no Microsoft Windows Vista e no Microsoft Windows 7).

Os métodos listados acima para abrir a janela do Agente de Notícias funcionarão somente se houver notícias não lidas disponíveis.

Se você não desejar receber notícias, poderá desativar sua entrega.

INICIANDO E INTERROMPENDO O APLICATIVO

Esta seção contém informações sobre como iniciar e encerrar o aplicativo.

NESTA SEÇÃO:

ATIVANDO E DESATIVANDO A EXECUÇÃO AUTOMÁTICA

A execução automática do aplicativo indica que o Kaspersky Anti-Virus é iniciado após a inicialização do sistema operacional. Este é o modo de inicialização padrão.

- *Para ativar ou desativar a execução automática do aplicativo:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione a subseção **Configurações Gerais**.
  3. Para desativar a execução automática do aplicativo, desmarque a caixa **Executar o Kaspersky Anti-Virus ao iniciar o computador** na seção **Execução automática** à direita da janela. Marque esta caixa para ativar a execução automática do aplicativo.

INICIANDO E FECHANDO O APLICATIVO MANUALMENTE

Os especialistas da Kaspersky Lab não recomendam interromper o Kaspersky Anti-Virus, pois a proteção do computador e de seus dados pessoais estará em risco. É recomendável pausar temporariamente a proteção do computador sem fechar o aplicativo.

O Kaspersky Anti-Virus deverá ser iniciado manualmente se você tiver desativado a execução automática do aplicativo (consulte a seção "Ativando e desativando a execução automática" na página 34).

- *Para executar o aplicativo manualmente,*

  no menu **Iniciar**, selecione **Programas → Kaspersky Anti-Virus 2012 → Kaspersky Anti-Virus 2012**.

- *Para sair do aplicativo,*

  clique com o botão direito do mouse para abrir o menu de contexto do ícone do aplicativo na área de notificações da barra de tarefas e selecione **Sair**.

Por padrão, no sistema operacional Microsoft Windows 7, o ícone do aplicativo fica oculto, mas você pode exibi-lo para acessar o aplicativo mais facilmente (consulte a documentação do sistema operacional).

GERENCIANDO A PROTEÇÃO DO COMPUTADOR

Esta seção fornece informações sobre como detectar ameaças à segurança do computador e como configurar o nível de segurança. Leia esta seção para saber mais sobre como ativar, desativar e pausar a proteção ao usar o aplicativo.

NESTA SEÇÃO:

DIAGNÓSTICO E ELIMINAÇÃO DE PROBLEMAS NA PROTEÇÃO DO COMPUTADOR

Os problemas com a proteção do computador são indicados por seu indicador localizado à esquerda da janela principal do aplicativo (consulte a seção "A janela principal do Kaspersky Anti-Virus" na página 29). O indicador tem a forma de um ícone de monitor que muda de cor de acordo com o status de proteção do computador: o verde significa que o computador está protegido, o amarelo indica problemas relacionados à proteção, o vermelho alerta sobre ameaças graves à segurança do computador.

Figura 8. Indicador do status de proteção

É recomendável corrigir os problemas e as ameaças de segurança imediatamente.

Ao clicar no indicador na janela principal do aplicativo, é aberta a janela **Problemas de Segurança** (veja a figura a seguir), que contém informações detalhadas sobre o status de proteção do computador e sugestões para a solução dos problemas e ameaças detectados.

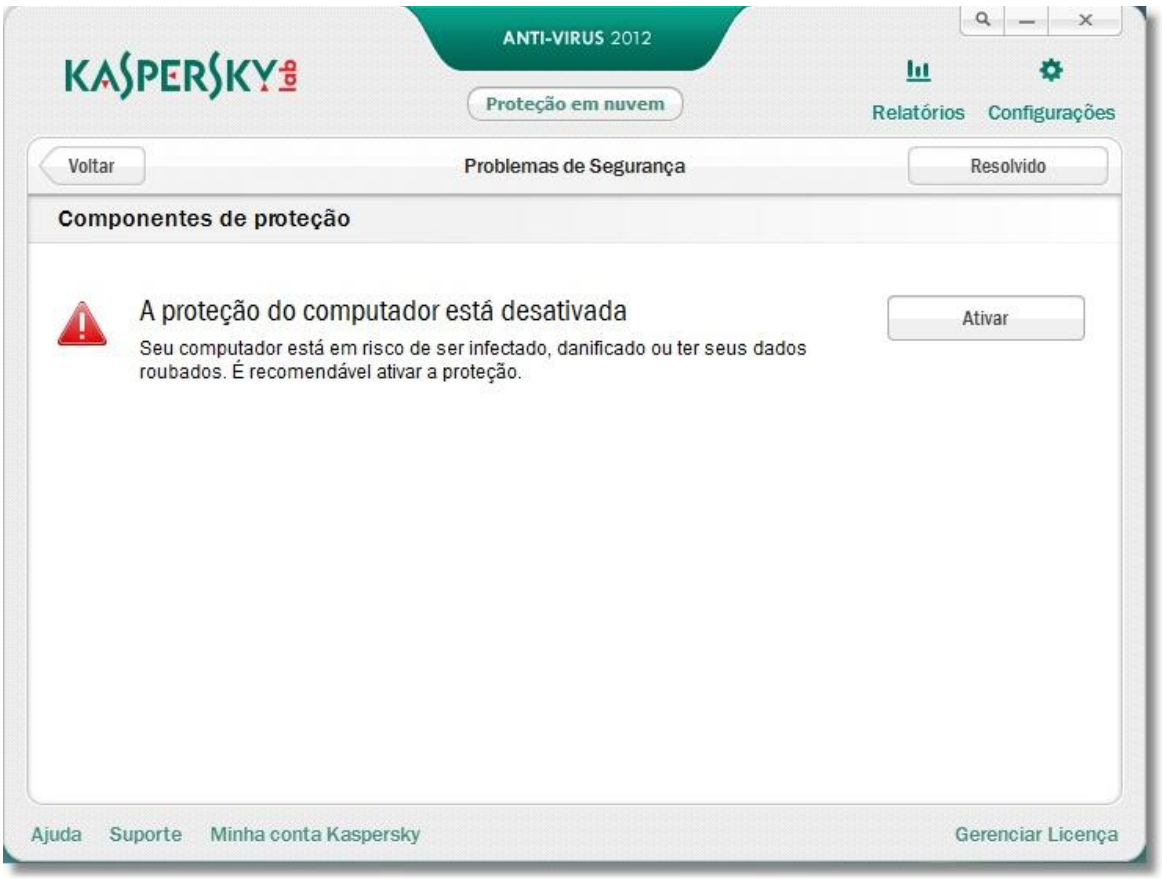

Figura 9. A janela Problemas de Segurança

Os problemas com a proteção são agrupados em categorias. Para cada problema, são listadas ações que podem ser usadas para solucionar o problema.

ATIVANDO E DESATIVANDO A PROTEÇÃO

Por padrão, o Kaspersky Anti-Virus é executado ao carregar o sistema operacional e protege o computador até que ele seja desligado. Todos os componentes de proteção são executados.

Você pode desativar a proteção fornecida pelo Kaspersky Anti-Virus total ou parcialmente.

Os especialistas da Kaspersky Lab recomendam enfaticamente que você não desative a proteção, pois isso pode levar à infecção do computador e à perda de dados. É recomendável pausar a proteção pelo intervalo de tempo necessário (consulte a seção "Pausando e reiniciando a proteção" na página 37).

Os seguintes sinais indicam que a proteção está pausada ou desativada:

- ícone do aplicativo inativo (cinza) na área de notificação da barra de tarefas (consulte a seção "O ícone da área de notificação" na ´página 27);
- um indicador de segurança vermelho na parte superior da janela principal do aplicativo.

Nesse caso, a proteção é considerada como o conjunto de componentes de proteção. Desativar ou pausar os componentes de proteção não afeta o desempenho das tarefas de verificação de vírus e das atualizações do Kaspersky Anti-Virus.

Você pode ativar ou desativar a proteção ou componentes individuais do aplicativo na janela de configurações do aplicativo (consulte a seção "A janela de configurações do aplicativo" na página 31).

Para ativar ou desativar a proteção completamente:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione a subseção **Configurações Gerais**.
3. Desmarque a caixa **Ativar proteção** para desativar a proteção. Se desejar ativar a proteção, marque a caixa.

Para ativar ou desativar um componente de proteção:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente que deve ser ativado ou desativado.
3. À direita da janela, desmarque a caixa **Ativar <nome do componente>** para desativar esse componente. Se desejar ativar o componente, marque a caixa.

PAUSANDO E REINICIANDO A PROTEÇÃO

Pausar a proteção significa desativar todos os componentes de proteção por um determinado período.

Os seguintes sinais indicam que a proteção está pausada ou desativada:

- ícone do aplicativo inativo (cinza) na área de notificações da barra de tarefas (consulte a seção "Ícone da área de notificação" na ´página 27);
- um indicador de segurança vermelho na parte superior da janela principal do aplicativo.

Nesse caso, a proteção é considerada como o conjunto de componentes de proteção. Desativar ou pausar os componentes de proteção não afeta o desempenho das tarefas de verificação de vírus e das atualizações do Kaspersky Anti-Virus.

Se forem estabelecidas conexões de rede enquanto em que a proteção estava pausada, será exibida uma notificação sobre o encerramento dessas conexões.

Ao trabalhar em um computador com o Microsoft Windows Vista ou o Microsoft Windows 7, você pode pausar a proteção usando o Kaspersky Gadget. Para fazer isso, atribua a função de pausar a proteção a um botão do gadget (consulte a seção "Como usar o Kaspersky Gadget" na página 53).

Para pausar a proteção do computador:

1. Abra a janela **Pausar a proteção** usando um dos seguintes métodos:
   - selecione **Pausar a proteção** no menu de contexto do ícone do aplicativo (consulte a seção "O menu de contexto" na página 28);
   - clique no botão com o ícone **Pausar a proteção** na interface do Kaspersky Gadget (apenas nos sistemas operacionais Microsoft Windows Vista e Microsoft Windows 7).
2. Na janela **Pausar a proteção**, selecione o intervalo de tempo depois do qual a proteção deve ser reiniciada:
   - **Pausar pelo tempo especificado** – a proteção será ativada quando o intervalo de tempo selecionado na lista suspensa abaixo expirar.
   - **Pausar até reiniciar** – a proteção será ativada depois que o aplicativo ou o sistema operacional forem reiniciados (desde que a execução automática do aplicativo esteja ativada (consulte a seção "Ativando e desativando a execução automática" na página 34)).
   - **Pausar** – a proteção será ativada quando você decidir reiniciá-la (veja a seguir).

Para reiniciar a proteção do computador,

selecione **Reiniciar a proteção** no menu de contexto do ícone do aplicativo (consulte a seção "O menu de contexto" na página 28).

Você pode usar este método para reiniciar a proteção do computador quando a opção **Pausar** tiver sido selecionada ou quanto você tiver selecionado **Pausar pelo tempo especificado** ou **Pausar até reiniciar**.

SOLUCIONANDO TAREFAS TÍPICAS

Esta seção fornece informações sobre como resolver os problemas mais comuns relacionados à proteção do computador usando o aplicativo.

NESTA SEÇÃO:

COMO ATIVAR O APLICATIVO

A *ativação* é o procedimento para ativar a licença que permite usar uma versão totalmente funcional do aplicativo até a expiração da licença.

Se você não ativou o aplicativo durante a instalação, pode fazer isso posteriormente. Você será lembrado da necessidade de ativar o aplicativo por mensagens do Kaspersky Anti-Virus que serão exibidas na área de notificação da barra de tarefas.

Para executar o Assistente de Ativação do Kaspersky Anti-Virus:

- Clique no link **Ativar** na janela de notificação do Kaspersky Anti-Virus exibida na área de notificação da barra de tarefas.
- Clique no link **Insira seu código de ativação aqui** na parte inferior da janela principal do aplicativo. Na janela **Gerenciar Licença** que é aberta, clique no botão **Ativar o aplicativo** .

Ao trabalhar com o Assistente de Ativação do aplicativo, você deve especificar valores para diversas configurações.

Etapa 1. Inserir o código de ativação

Insira o código de ativação no campo correspondente e clique no botão **Avançar**.

Etapa 2. Solicitando a ativação

Se a solicitação de ativação for enviada com êxito, o Assistente continuará automaticamente na etapa seguinte.

Etapa 3. Inserção de dados de registro

O registro do usuário é necessário para que ele possa entrar em contato com o Serviço de Suporte Técnico. Os usuários não registrados recebem apenas um suporte mínimo.

Especifique seus dados de registro e clique no botão **Avançar**.

Etapa 4. Ativação

Se a ativação do aplicativo tiver êxito, o Assistente continuará automaticamente na etapa seguinte.

Etapa 5. Conclusão do Assistente

Esta janela exibe informações sobre os resultados da ativação: o tipo de licença usado e a data de expiração da licença.

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

COMO COMPRAR OU RENOVAR A LICENÇA

Se você tiver instalado o Kaspersky Anti-Virus sem uma licença, poderá comprar uma após a instalação. Ao comprar uma licença, você recebe um código de ativação que deve ser usado para ativar o aplicativo (consulte a seção "Como ativar o aplicativo" na página 38).

Quando sua licença expirar, você poderá renová-la. Você pode comprar uma nova licença antes da expiração do período de validade do seu código de ativação atual. Para fazer isso, você deve adicionar o novo código como um código de ativação de reserva. Quando o período de validade da licença atual expirar, o Kaspersky Anti-Virus será ativado automaticamente usando o código de ativação de reserva.

- *Para comprar uma licença:*

  1. Abra a janela principal do aplicativo.
  2. Clique no link **Gerenciar Licença** na parte inferior da janela principal para abrir a janela **Gerenciar Licença**.
  3. Na janela que é aberta, clique no botão **Comprar código de ativação**.

     A página da loja virtual na Web na qual você pode comprar uma licença é aberta.

- *Para adicionar um código de ativação de reserva:*

  1. Abra a janela principal do aplicativo.
  2. Clique no link **Gerenciar Licença** na parte inferior da janela principal para abrir a janela **Gerenciar Licença**.

     A janela **Gerenciar Licença** é aberta.
  3. Na janela que é aberta, na seção **Novo código de ativação**, clique no botão **Inserir o código de ativação**.

     O Assistente de Ativação do aplicativo é aberto.
  4. Insira o código de ativação nos campos correspondentes e clique no botão **Avançar**.

     Em seguida, o Kaspersky Anti-Virus envia os dados para serem verificados pelo servidor de ativação. Se a verificação tiver êxito, o Assistente continuará automaticamente na etapa seguinte.
  5. Selecione **Novo código** e clique no botão **Avançar**.
  6. Ao concluir com o Assistente, clique no botão **Concluir**.

O QUE FAZER QUANDO FOREM EXIBIDAS NOTIFICAÇÕES DO APLICATIVO

As notificações que são exibidas na área de notificação da barra de tarefas informam sobre eventos ocorridos durante a operação do aplicativo e que exigem sua atenção. Dependendo do grau de importância do evento, você poderá receber os seguintes tipos de notificações:

- Notificações críticas – informam sobre os eventos de importância crítica para a segurança do computador, como a detecção de um objeto malicioso ou uma atividade perigosa no sistema. As janelas das notificações e mensagens pop-up críticas são vermelhas.
- Notificações importantes – informam sobre os eventos que possivelmente são importantes para a segurança do computador, como a detecção de um objeto possivelmente infectado ou uma atividade suspeita no sistema. As janelas das notificações e mensagens pop-up importantes são amarelas.
- Notificações informativas – informam sobre os eventos que não têm importância crítica para a segurança do computador. As janelas das notificações e mensagens pop-up informativas são verdes.

Se for exibida alguma dessas notificações na tela, selecione uma das opções sugeridas. A opção ideal é aquela recomendada como padrão pelos especialistas da Kaspersky Lab.

COMO ATUALIZAR OS BANCOS DE DADOS E MÓDULOS DO APLICATIVO

Por padrão, o Kaspersky Anti-Virus verifica automaticamente as atualizações nos servidores de atualização da Kaspersky Lab. Se o servidor armazenar um conjunto de atualizações recentes, o Kaspersky Anti-Virus as baixará e instalará em segundo plano. Você pode iniciar a atualização do Kaspersky Anti-Virus manualmente a qualquer momento.

Para baixar atualizações dos servidores da Kaspersky Lab, é necessário estar conectado à Internet.

Para iniciar uma atualização do menu de contexto,

selecione **Atualização** no menu de contexto do ícone do aplicativo.

Para iniciar uma atualização da janela principal do aplicativo:

1. Abra a janela principal do aplicativo e selecione a seção **Atualização** na parte inferior da janela.
2. Na janela **Atualização** que é aberta, clique no botão **Executar atualização**.

COMO VERIFICAR AS ÁREAS CRÍTICAS DO COMPUTADOR QUANTO À PRESENÇA DE VÍRUS

A verificação de áreas críticas compreende a verificação dos seguintes objetos:

- objetos carregados ao iniciar o sistema operacional;
- memória do sistema;
- setores de inicialização do disco;
- objetos adicionados pelo usuário (consulte a seção "Criando uma lista de objetos a serem verificados" na página 59).

Você pode executar a verificação de áreas críticas usando um dos métodos a seguir:

- usando um atalho criado anteriormente (veja a página 63).
- na janela principal do aplicativo (consulte a seção "A janela principal do Kaspersky Anti-Virus" na página 29).

Para iniciar a verificação usando um atalho:

1. Abra a janela do Microsoft Windows Explorer e vá para a pasta na qual você criou o atalho.
2. Clique duas vezes no atalho para iniciar a verificação.

Para iniciar a verificação na janela principal do aplicativo:

1. Abra a janela principal do aplicativo e selecione a seção **Verificação** na parte inferior da janela.
2. Na janela **Verificação** que é aberta, na seção **Verificação de Áreas Críticas**, clique no botão  .

COMO VERIFICAR UM ARQUIVO, PASTA, DISCO OU OUTRO OBJETO QUANTO À PRESENÇA DE VÍRUS

Você pode usar os seguintes métodos para verificar um objeto quanto à presença de vírus:

- usando o menu de contexto do objeto;
- na janela principal do aplicativo (consulte a seção "A janela principal do Kaspersky Anti-Virus" na página 29);
- usando o Gadget do Kaspersky Anti-Virus (apenas nos sistemas operacionais Microsoft Windows Vista e Microsoft Windows 7).

Para iniciar a tarefa de verificação de vírus no menu de contexto do objeto:

1. Abra o Microsoft Windows Explorer e vá para a pasta que contém o objeto que deve ser verificado.
2. Clique com o botão direito do mouse no menu de contexto do objeto (veja a figura a seguir) e selecione **Verificar Vírus**.

   O processo e o resultado da tarefa serão exibidos na janela do **Gerenciador de Tarefas**.

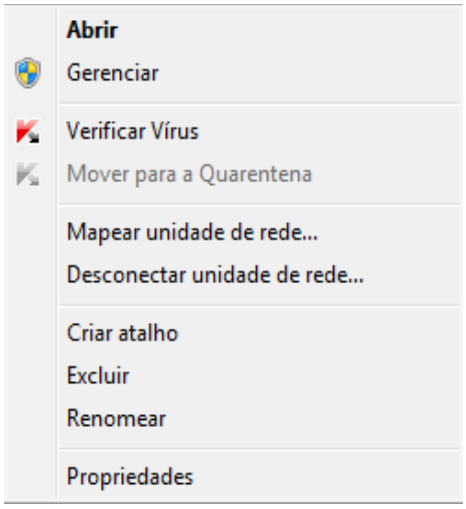

Figura 10. O menu de contexto de um objeto no Microsoft Windows

Para iniciar a verificação de um objeto na janela principal do aplicativo:

1. Abra a janela principal do aplicativo e selecione a seção **Verificação** na parte inferior da janela.
2. Especifique o objeto que deve ser verificado usando um dos seguintes métodos:
   - Clique no link **procure-o** à direita da janela para abrir a janela **Verificação Personalizada** e marque as caixas ao lado das pastas e unidades que você deseja verificar.

     Se a janela não exibir nenhum objeto a ser verificado:

     a. Clique no botão **Adicionar**.

     b. Na janela **Selecionar objeto a ser verificado** que é aberta, selecione um objeto.
   - Arraste um objeto a ser verificado para a área exclusiva da janela principal (veja a figura a seguir).

O andamento da tarefa será exibido na janela do **Gerenciador de Tarefas**.

Figura 11. Uma área da janela Verificação para a qual você deve arrastar o objeto a ser verificado

- *Para verificar um objeto quanto à presença de vírus usando o gadget,*

  arraste o objeto a ser verificado para o gadget.

  O andamento da tarefa será exibido na janela do **Gerenciador de Tarefas**.

COMO EXECUTAR UMA VERIFICAÇÃO COMPLETA DO COMPUTADOR QUANTO À PRESENÇA DE VÍRUS

Você pode executar a verificação completa de vírus usando um dos seguintes métodos:

- usando um atalho criado anteriormente (veja a página 63);
- na janela principal do aplicativo (consulte a seção "A janela principal do Kaspersky Anti-Virus" na página 29).

- *Para iniciar uma verificação completa usando um atalho:*

  1. Abra a janela do Microsoft Windows Explorer e vá para a pasta na qual você criou o atalho.
  2. Clique duas vezes no atalho para iniciar a verificação.

- *Para iniciar a verificação completa na janela principal do aplicativo:*

  1. Abra a janela principal do aplicativo e selecione a seção **Verificação** na parte inferior da janela.
  2. Na janela **Verificação** que é aberta, na seção **Verificação Completa**, clique no botão .

COMO VERIFICAR O COMPUTADOR QUANTO À PRESENÇA DE VULNERABILIDADES

Vulnerabilidades são partes não protegidas do código do software que os invasores podem usar deliberadamente para atingir seus objetivos, como copiar os dados usados em aplicativos não protegidos. A verificação de vulnerabilidades no computador ajuda a descobrir esses pontos fracos. É recomendável remover as vulnerabilidades detectadas.

Você pode usar os seguintes métodos para verificar vulnerabilidades no sistema:

- na janela principal do aplicativo (consulte a seção "A janela principal do Kaspersky Anti-Virus" na página 29);
- usando um atalho criado anteriormente (veja a página 63).

- *Para iniciar a tarefa usando um atalho:*

  1. Abra a janela do Microsoft Windows Explorer e vá para a pasta na qual você criou o atalho.
  2. Clique duas vezes no atalho para executar a verificação de vulnerabilidades no sistema.

Para iniciar a tarefa na janela principal do aplicativo:

1. Abra a janela principal do aplicativo e selecione a seção **Verificação** na parte inferior da janela.
2. Na janela **Verificação** que é aberta, na seção **Verificação de Vulnerabilidades**, clique no botão  .

COMO PROTEGER SEUS DADOS PESSOAIS CONTRA ROUBO

Com o Kaspersky Anti-Virus, você pode proteger seus dados pessoais contra roubo; incluindo dados como:

- senhas, nomes de usuário e outros dados de registro;
- números de contas e cartões bancários.

O Kaspersky Anti-Virus compreende os seguintes componentes e ferramentas para ajudar a proteger seus dados particulares:

- Antiphishing. Protege contra roubo de dados envolvendo phishing.
- Teclado Virtual. Evita a interceptação de dados inseridos no teclado.

NESTA SEÇÃO:

PROTEÇÃO CONTRA PHISHING

A proteção contra phishing é garantida pelo Antiphishing implementado nos componentes Antivírus da Web e Antivírus de IM. A Kaspersky Lab recomenda ativar a verificação de phishing em todos os componentes de proteção.

Para ativar a proteção contra phishing quando o Antivírus da Web está em execução:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
3. Clique no botão **Configurações** à direita da janela.
4. A janela **Antivírus da Web** é aberta.
5. Na janela que é aberta, na guia **Geral**, na seção **Consultor de URLs Kaspersky**, marque a caixa **Verificar páginas da Web quanto à presença de phishing**.

Para ativar a proteção contra phishing quando o Antivírus de IM está em execução:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de IM**.
3. À direita da janela, na seção **Métodos de verificação**, marque a caixa **Verificar se os URLs estão listados no banco de dados de URLs de phishing**.

PROTEÇÃO CONTRA INTERCEPTAÇÃO DE DADOS PELO TECLADO

Ao trabalhar na Internet, frequentemente você precisa inserir seus dados pessoais ou seu nome de usuário e sua senha. Isso acontece, por exemplo, ao registrar uma conta em sites, fazer compras online ou usar um banco virtual.

Existe um risco de que essas informações pessoais sejam interceptadas usando interceptadores de teclado ou keyloggers, que são programas que registram o pressionamento de teclas.

A ferramenta Teclado Virtual evita a interceptação dos dados inseridos usando o teclado.

O Teclado Virtual não poderá proteger seus dados pessoais se o site que exibe a inserção desses dados tiver sido invadido; nesse caso, as informações são obtidas diretamente pelos invasores.

Vários aplicativos classificados como spyware têm a função de fazer capturas de tela que são então transmitidas para o invasor para análise e extração dos dados pessoais do usuário. O Teclado Virtual evita que os dados pessoais inseridos sejam interceptados por meio de capturas de tela.

O Teclado Virtual evita apenas a interceptação de dados pessoais ao trabalhar com os navegadores Microsoft Internet Explorer, Mozilla Firefox e Google Chrome.

O Teclado Virtual possui os seguintes recursos:

- Você pode clicar nos botões do Teclado Virtual usando o mouse.
- Diferentemente dos teclados reais, no Teclado Virtual não é possível clicar em várias teclas simultaneamente. Portanto, para usar combinações de teclas (por exemplo, **ALT+F4**), clique na primeira tecla (por exemplo, **ALT**) e depois na próxima tecla (por exemplo **F4**); em seguida, clique na primeira tecla novamente. O segundo clique na tecla funciona da mesma forma que a liberação da mesma em um teclado real.
- O idioma de entrada do Teclado Virtual é alternado usando as combinações de teclas **CTRL+SHIFT** (a tecla **SHIFT** deve ser clicada usando o botão direito do mouse) ou **CTRL+LEFT ALT** (a tecla **LEFT ALT** deve ser clicada usando o botão direito do mouse) de acordo com as configurações especificadas.

Você pode abrir o Teclado Virtual das seguintes formas:

- no menu de contexto do ícone do aplicativo;
- na janela principal do aplicativo;
- nas janelas dos navegadores Microsoft Internet Explorer, Mozilla Firefox ou Google Chrome;
- usando atalhos do teclado.

Para abrir o Teclado Virtual no menu de contexto do ícone do aplicativo,

selecione **Teclado Virtual** no menu de contexto do ícone do aplicativo.

Para abrir o Teclado Virtual na janela principal do aplicativo,

na parte inferior da janela principal do aplicativo, selecione **Teclado Virtual**.

Para abrir o Teclado Virtual na janela do navegador,

clique no botão  **Teclado Virtual** na barra de ferramentas do Microsoft Internet Explorer, Mozilla Firefox ou Google Chrome.

Para abrir o Teclado Virtual usando o teclado do computador,

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

O QUE FAZER SE VOCÊ SUSPEITAR QUE UM OBJETO ESTÁ INFECTADO COM UM VÍRUS

Se você suspeitar que um objeto está infectado, primeiro verifique-o usando o Kaspersky Anti-Virus (consulte a seção "Como verificar um arquivo, pasta, disco ou outro objeto quanto à presença de vírus" na página 41).

Se o aplicativo verificar um objeto e considerar que ele não está infectado, mas você suspeitar do contrário, será possível executar as seguintes ações:

- Mover o objeto para a *Quarentena.* Os objetos movidos para a Quarentena não representam uma ameaça ao computador. Depois que os bancos de dados forem atualizados, o Kaspersky Anti-Virus poderá identificar claramente e remover a ameaça.
- Enviar o objeto para o *Laboratório de Vírus*. Os especialistas do Laboratório de Vírus verificam o objeto. Se ele estiver infectado com um vírus, será adicionado à descrição dos novos vírus nos bancos de dados que serão baixados pelo aplicativo com uma atualização (consulte a seção "Como atualizar os bancos de dados e módulos do aplicativo" na página 40).

Você pode mover um arquivo para a Quarentena usando um dos dois métodos:

- clicando no botão **Mover para a Quarentena** na janela **Quarentena**;
- usando o menu de contexto do arquivo.

- *Para mover um arquivo para a Quarentena na janela Quarentena:*

  1. Abra a janela principal do aplicativo.
  2. Na parte inferior da janela, selecione a seção **Quarentena**.
  3. Na guia **Quarentena**, clique no botão **Mover para a Quarentena**.
  4. Na janela que é aberta, selecione o arquivo que você deseja mover para a Quarentena.

- *Para mover um arquivo para a Quarentena usando o menu de contexto:*

  1. Abra o Microsoft Windows Explorer e vá para a pasta que contém o arquivo que você deseja mover para a Quarentena.
  2. Clique com o botão direito do mouse para abrir o menu de contexto do arquivo e selecione **Mover para a Quarentena**.

- *Para enviar um arquivo para o Laboratório de Vírus:*

  1. Vá para a página de solicitação do Laboratório de Vírus (http://support.kaspersky.com/virlab/helpdesk.html?LANG=pt).
  2. Siga as instruções na página para enviar sua solicitação.

O QUE FAZER SE VOCÊ SUSPEITAR QUE O COMPUTADOR ESTÁ INFECTADO

Se você suspeitar que o sistema operacional está corrompido devido à atividade de malware ou a falhas do sistema, use a *Solução de Problemas do Microsoft Windows*, que remove todos os rastros de objetos maliciosos do sistema. A Kaspersky Lab recomenda executar o Assistente depois de desinfetar o computador para assegurar que todas as ameaças e os danos causados pelas infecções tenham sido corrigidos.

A Solução de Problemas do Microsoft Windows verifica no sistema modificações e falhas (como modificações de extensões de arquivos, bloqueio do ambiente de rede e do painel de controle). As modificações e falhas podem ser causadas pela atividade de malware, a configuração incorreta do sistema, falhas do sistema ou a operação incorreta dos aplicativos de otimização do sistema.

Depois de concluir a análise, o Assistente examina as informações a fim de avaliar se houve danos no sistema que exigem atenção imediata. Dependendo da análise, será gerada uma lista de ações necessárias para eliminar os problemas. O Assistente agrupa essas ações em categorias de acordo com a gravidade dos problemas detectados.

- *Para iniciar o Assistente de Restauração do Sistema:*

  1. Abra a janela principal do aplicativo (veja a página 29).
  2. Na parte inferior da janela, selecione a seção **Ferramentas**.
  3. Na janela que é aberta, na seção **Solução de Problemas do Microsoft Windows**, clique no botão **Iniciar**.

     A janela da Solução de Problemas do Microsoft Windows é aberta.

O Assistente consiste em uma série de telas (etapas) nas quais você pode navegar usando os botões **Voltar** e **Avançar**. Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**. Para interromper o Assistente em qualquer estágio, clique no botão **Cancelar**.

Etapa 1. Iniciando a restauração do sistema

Confirme se a opção do Assistente para **Pesquisar problemas causados por atividade de malware** está selecionada e clique no botão **Avançar**.

Etapa 2. Pesquisa de problemas

O Assistente procurará problemas e danos que devem ser corrigidos. Quando a pesquisa for concluída, o Assistente continuará automaticamente na próxima etapa.

Etapa 3. Selecionando as ações de solução de problemas

Todos os problemas encontrados na etapa anterior são agrupados de acordo com o tipo de perigo que representam. Para cada grupo de problemas, a Kaspersky Lab recomenda uma sequência de ações para reparar os danos. Há três grupos de ações:

- *Ações altamente recomendadas* eliminam os problemas que representam uma ameaça de segurança grave. É recomendável executar todas as ações desse grupo.
- *Ações recomendadas* eliminam os problemas que representam uma possível ameaça. Também é recomendável executar todas as ações desse grupo.
- *Ações adicionais* reparam danos ao sistema que não representam uma ameaça atual, mas que podem colocar a segurança do computador em perigo no futuro.

Para exibir as ações em um grupo, clique no ícone **+** à esquerda do nome do grupo.

Para fazer o Assistente executar uma determinada ação, marque a caixa à esquerda da descrição da ação correspondente. Por padrão, o Assistente executa todas as ações recomendadas e altamente recomendadas. Se não desejar executar uma determinada ação, desmarque a caixa ao lado dela.

É altamente recomendável não desmarcar as caixas selecionadas por padrão, pois isso pode deixar o computador vulnerável a ameaças.

Depois de definir o conjunto de ações que serão executadas pelo Assistente, clique no botão **Avançar**.

Etapa 4. Eliminando problemas

O Assistente executará as ações selecionadas na etapa anterior. A eliminação de problemas pode levar algum tempo. Quando a solução de problemas for concluída, o Assistente continuará automaticamente na próxima etapa.

Etapa 5. Conclusão do Assistente

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

COMO RESTAURAR UM ARQUIVO EXCLUÍDO OU DESINFETADO PELO APLICATIVO

A Kaspersky Lab recomenda que você evite restaurar arquivos excluídos e desinfetados, pois eles podem representar uma ameaça ao computador.

Se desejar restaurar um arquivo excluído ou desinfetado, você poderá usar uma cópia de backup criada pelo aplicativo durante a verificação.

Para restaurar um arquivo excluído ou desinfetado pelo aplicativo:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, selecione a seção **Quarentena**.
3. Na guia **Armazenamento**, selecione o arquivo desejado na lista e clique no botão **Restaurar**.

COMO CRIAR E USAR UM DISCO DE RECUPERAÇÃO

Depois de instalar o Kaspersky Anti-Virus e executar a primeira verificação do computador, é recomendável criar o Disco de Recuperação.

O Disco de Recuperação consiste em um aplicativo denominado Kaspersky Rescue Disk e gravado em uma mídia removível (CD ou unidade flash USB).

Você poderá então usar o Kaspersky Rescue Disk para verificar e desinfetar computadores infectados que não podem ser desinfetados usando outros métodos (por exemplo, com aplicativos antivírus).

NESTA SEÇÃO:

CRIANDO UM DISCO DE RECUPERAÇÃO

A criação de um Disco de Recuperação consiste em criar uma imagem do disco (arquivo ISO) com a versão atualizada do Kaspersky Rescue Disk e gravá-la em uma mídia removível.

Você pode baixar a imagem original do disco do servidor da Kaspersky Lab ou copiá-la de uma fonte local.

O Disco de Recuperação é criado usando o *Assistente para Criação do Kaspersky Rescue Disk*. O arquivo rescuecd.iso criado pelo Assistente é salvo no disco rígido do computador:

- no Microsoft Windows XP – na seguinte pasta: Documents and Settings\All Users\Dados de Aplicativos\Kaspersky Lab\AVP12\Data\Rdisk\;
- nos sistemas operacionais Microsoft Windows Vista e Microsoft Windows 7 – na seguinte pasta: ProgramData\Kaspersky Lab\AVP12\Data\Rdisk\.

Para criar um Disco de Recuperação:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, selecione a seção **Ferramentas**.
3. Na janela que é aberta, na seção **Kaspersky Rescue Disk**, clique no botão **Criar**.

   A janela do **Assistente para Criação do Kaspersky Rescue Disk** é aberta.

O Assistente consiste em uma série de telas (etapas) nas quais você pode navegar usando os botões **Voltar** e **Avançar**. Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**. Para interromper o Assistente em qualquer estágio, clique no botão **Cancelar**.

Vamos revisar as etapas do Assistente mais detalhadamente.

Etapa 1. Iniciando o Assistente. Pesquisando uma imagem de disco existente

A primeira janela do Assistente contém informações sobre o Kaspersky Rescue Disk.

Se o Assistente detectar um arquivo ISO do Disco de Recuperação existente na pasta exclusiva (veja acima), a caixa **Usar imagem ISO existente** será exibida na primeira janela do Assistente. Marque a caixa para usar o arquivo detectado como a imagem ISO original e vá diretamente para a etapa **Atualizando imagem do disco** (veja a seguir). Desmarque esta caixa se não desejar usar a imagem do disco que foi detectada. O Assistente continuará na janela **Selecionar fonte da imagem do disco**.

Etapa 2. Selecionando a origem da imagem do disco

Se você marcou a caixa **Usar imagem ISO existente** na primeira janela do Assistente, esta etapa será ignorada.

Nesta etapa, você deve selecionar a fonte da imagem do disco dentre as opções sugeridas:

- Se você já tiver uma cópia gravada do Disco de Recuperação ou uma imagem ISO salva no computador ou em um recurso de rede local, selecione **Copiar a imagem ISO da unidade local ou de rede**.
- Se você não tiver um arquivo de imagem ISO criado para o Disco de Recuperação e desejar baixá-lo do servidor da Kaspersky Lab (o tamanho do arquivo é aproximadamente 175 MB), selecione **Baixar a imagem ISO do servidor da Kaspersky Lab**.

Etapa 3. Copiando (baixando) a imagem do disco

Se você marcou a caixa **Usar imagem ISO existente** na primeira janela do Assistente, esta etapa será ignorada.

Se você tiver selecionado **Copiar a imagem ISO da unidade local ou de rede** na etapa anterior, clique no botão **Procurar**. Depois de especificar o caminho do arquivo, clique no botão **Avançar**. O andamento da cópia da imagem do disco será exibido na janela do Assistente.

Se você selecionou **Baixar a imagem ISO do servidor da Kaspersky Lab**, o andamento do download da imagem do disco será exibido imediatamente.

Quando a cópia ou o download da imagem ISO for concluído, o Assistente continuará automaticamente na etapa seguinte.

Etapa 4. Atualizando o arquivo da imagem ISO

O procedimento de atualização do arquivo da imagem ISO compreende as seguintes operações:

- atualização dos bancos de dados de antivírus;
- atualização dos arquivos de configuração.

Os arquivos de configuração determinam se o computador pode ser inicializado a partir de uma mídia removível (como um CD/DVD ou uma unidade flash USB com o Kaspersky Rescue Disk) criada pelo Assistente.

Ao atualizar os bancos de dados de antivírus, são usados aqueles distribuídos na última atualização do Kaspersky Anti-Virus. Se os bancos de dados estiverem desatualizados, é recomendável executar a tarefa de atualização e executar o Assistente para Criação do Kaspersky Rescue Disk novamente.

Para iniciar a atualização do arquivo ISO, clique no botão **Avançar**. O andamento da atualização será exibido na janela do Assistente.

Etapa 5. Gravando a imagem do disco em uma mídia

Nesta etapa, o Assistente informa sobre a criação bem-sucedida de uma imagem do disco e permite sua gravação em uma mídia.

Especifique uma mídia de dados para gravar o Kaspersky Rescue Disk:

- Para gravar a imagem do disco em um CD/DVD, selecione **Gravar em CD/DVD** e especifique a mídia na qual você deseja gravar a imagem do disco.
- Para gravar a imagem do disco em uma unidade flash USB, selecione **Gravar na unidade flash USB** e especifique o dispositivo no qual você deseja gravar a imagem do disco.

  A Kaspersky Lab recomenda não gravar a imagem ISO em dispositivos que não foram criados especificamente para armazenamento de dados, como smartphones, celulares, PDAs e MP3 players. A gravação de imagens ISO nesses dispositivos pode causar seu funcionamento incorreto no futuro.

- Para gravar a imagem do disco no disco rígido do computador ou de outro computador que você possa acessar através de uma rede, selecione **Salvar a imagem do disco em arquivo na unidade local ou de rede** e especifique a pasta na qual você deseja gravar a imagem do disco e o nome do arquivo ISO.

Etapa 6. Conclusão do Assistente

Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**. Você poderá usar o Disco de Recuperação recém criado para iniciar o computador (veja a página 48) caso não seja possível inicializá-lo e executar o Kaspersky Anti-Virus no modo normal devido ao impacto causado por vírus ou malware.

INICIALIZANDO O COMPUTADOR COM O DISCO DE RECUPERAÇÃO

Se não for possível iniciar o sistema operacional devido a um ataque de vírus, use o Disco de Recuperação.

Para iniciar o sistema operacional, você deve usar um CD/DVD ou uma unidade flash USB com o Kaspersky Rescue Disk gravado (consulte a seção "Criando um Disco de Recuperação" na página 47).

Nem sempre é possível iniciar o computador a partir de uma mídia removível. Especificamente, não há suporte para esse modo em alguns modelos de computador obsoletos. Antes de desligar o computador para a inicialização posterior a partir de uma mídia removível, verifique se essa operação pode ser executada.

Para inicializar o computador com o Disco de Recuperação:

1. Nas configurações do BIOS, ative a inicialização a partir do CD/DVD ou do dispositivo USB (para obter informações detalhadas, consulte a documentação da placa mãe do computador).
2. Insira um CD/DVD na unidade correspondente do computador infectado ou conecte um dispositivo flash USB com o Kaspersky Rescue Disk copiado.
3. Reinicie o computador.

Para obter informações detalhadas sobre o uso do Disco de Recuperação, consulte o Manual do Usuário do Kaspersky Rescue Disk.

COMO EXIBIR O RELATÓRIO DE OPERAÇÃO DO APLICATIVO

O Kaspersky Anti-Virus cria relatórios de operação para cada componente. Nos relatórios, você pode obter informações estatísticas de operação do aplicativo (por exemplo, saber quantos objetos maliciosos foram detectados e neutralizados em um período especificado, quantas vezes o aplicativo foi atualizado no mesmo período, quantos spams foram detectados e muito mais).

Ao trabalhar em um computador com o Microsoft Windows Vista ou o Microsoft Windows 7, você pode abrir relatórios usando o Kaspersky Gadget. Para fazer isso, o Kaspersky Gadget deve estar configurado de forma que a opção de abrir a janela de relatórios seja atribuída a um de seus botões (consulte a seção "Como usar o Kaspersky Gadget" na página 53).

Para exibir o relatório de operação do aplicativo:

1. Abra a janela **Relatórios** usando um dos seguintes métodos:
   - clique no botão **Relatórios** na parte superior da janela principal do aplicativo;
   - clique no botão com o ícone **Configurações** na interface do Kaspersky Gadget (apenas nos sistemas operacionais Microsoft Windows Vista e Microsoft Windows 7).

   A janela **Relatórios** exibe relatórios de operação do aplicativo representados como diagramas.
2. Se desejar exibir um relatório detalhado de operação do aplicativo (por exemplo, um relatório de operação de cada componente), clique no botão **Relatório detalhado** na parte inferior da janela **Relatório**.

   A janela **Relatório detalhado** será aberta com os dados representados em uma tabela. Para obter uma exibição conveniente dos relatórios, é possível selecionar várias opções de classificação das entradas.

COMO RESTAURAR AS CONFIGURAÇÕES PADRÃO DO APLICATIVO

Você pode restaurar as configurações padrão do Kaspersky Anti-Virus recomendadas pela Kaspersky Lab a qualquer momento. As configurações podem ser restauradas usando o *Assistente de Configuração do Aplicativo*.

Quando o Assistente concluir sua operação, o nível de segurança **Recomendado** estará definido para todos os componentes de proteção. Ao restaurar o nível de segurança recomendado, você pode salvar os valores especificados anteriormente para algumas das configurações dos componentes do aplicativo.

Para restaurar as configurações padrão do aplicativo:

1. Abra a janela de configurações do aplicativo.
2. Execute o Assistente de Configuração do Aplicativo usando um dos métodos a seguir:
   - clique no link **Restaurar** na parte inferior da janela;
   - à esquerda da janela, selecione a subseção **Gerenciar Configurações** na seção **Configurações Avançadas** e clique no botão **Restaurar** na seção **Restaurar configurações padrão**.

Vamos revisar as etapas do Assistente mais detalhadamente.

Etapa 1. Iniciando o Assistente

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

Etapa 2. Restaurar configurações

Esta janela do Assistente mostra os componentes do Kaspersky Anti-Virus cujas configurações são diferentes do valor padrão, por terem sido alteradas pelo usuário. Se tiverem sido criadas configurações especiais para algum componente, elas também serão mostradas nessa janela.

Marque as caixas correspondentes às configurações que você deseja salvar e clique no botão **Avançar**.

Etapa 3. Concluindo a restauração

Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**.

COMO TRANSFERIR AS CONFIGURAÇÕES PARA O KASPERSKY ANTI-VIRUS INSTALADO EM OUTRO COMPUTADOR

Depois de configurar o produto, você poderá aplicar suas configurações ao Kaspersky Anti-Virus instalado em outro computador. Assim, o aplicativo será configurado da mesma maneira nos dois computadores. Esse recurso é útil quando, por exemplo, o Kaspersky Anti-Virus é instalado no seu computador doméstico e no seu escritório.

As configurações do aplicativo são armazenadas em um arquivo de configuração especial que pode ser transferido para outro computador.

As configurações do Kaspersky Anti-Virus podem ser transferidas para outro computador em três etapas:

1. Salvando as configurações do aplicativo em um arquivo de configuração.
2. Transferindo um arquivo de configuração para outro computador (por exemplo, por email ou em uma mídia removível).
3. Aplicando as configurações de um arquivo de configuração ao aplicativo instalado em outro computador.

- *Para exportar as configurações atuais do Kaspersky Anti-Virus:*

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Gerenciar Configurações**.
3. Clique no botão **Salvar** à direita da janela.
4. Na janela que é aberta, insira o nome do arquivo de configuração e o caminho no qual ele deve ser salvo.
5. Clique no botão **OK**.

- *Para importar as configurações do aplicativo de um arquivo de configuração salvo:*

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Gerenciar Configurações**.
3. Clique no botão **Carregar** à direita da janela.
4. Na janela que é aberta, selecione o arquivo do qual você deseja importar as configurações do Kaspersky Anti-Virus.
5. Clique no botão **OK**.

COMO MIGRAR DO KASPERSKY ANTI-VIRUS PARA O KASPERSKY INTERNET SECURITY

O Kaspersky Anti-Virus permite migrar para o Kaspersky Internet Security sem nenhum download ou instalação de software adicional.

O *Kaspersky Internet Security* é um aplicativo criado para assegurar a proteção abrangente do computador. Ele fornece um conjunto completo de recursos avançados implementados com os seguintes módulos e funções:

- Controle de Aplicativos;
- Controle para Pais;
- Firewall;
- Bloqueador de Ataques de Rede;
- Filtro Geográfico;
- Bloqueio do acesso a sites inseguros;
- Monitor de Rede;
- Antispam;
- Antibanner;
- Limpeza de Dados Particulares;
- Execução Segura.

É possível migrar temporariamente para a versão de avaliação do Kaspersky Internet Security para analisar seus recursos ou começar a usar a versão comercial do aplicativo imediatamente.

Se você usar a licença com uma assinatura ou usar o aplicativo em determinadas regiões, sua cópia do Kaspersky Internet Security não permitirá migrar temporariamente para a versão de avaliação.

NESTA SEÇÃO:

ALTERNANDO PARA A VERSÃO COMERCIAL

Se desejar migrar para a versão comercial do Kaspersky Internet Security, você precisará de um código de ativação da versão comercial do aplicativo que possa ser usado para ativá-lo (consulte a seção "Como ativar o aplicativo" na página 38).

Para comprar um código de ativação do Kaspersky Internet Security:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, selecione a seção **Upgrade**.
3. Na janela que é aberta, clique no botão **Comprar código de ativação**.

   Você será redirecionado ao site da Loja Virtual, no qual é possível comprar um código de ativação do Kaspersky Internet Security.

   Se você comprar o aplicativo em determinadas regiões ou usar a licença com uma assinatura, a seção **Upgrade** não será exibida na janela principal do aplicativo.

MIGRANDO TEMPORARIAMENTE PARA A VERSÃO COMERCIAL

Você pode migrar temporariamente para a versão de avaliação do Kaspersky Internet Security a fim de avaliar sua funcionalidade. Depois disso, também é possível comprar uma licença para continuar usando o aplicativo.

Para alternar temporariamente para o Kaspersky Internet Security:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, selecione a seção **Upgrade**.
3. Na janela que é aberta, clique no botão **Versão de avaliação**.

   O Assistente de Configuração do aplicativo é aberto.

> Se você comprar o aplicativo em determinadas regiões ou usar a licença com uma assinatura, a seção **Upgrade** não será exibida na janela principal do aplicativo.

Ao trabalhar com o Assistente de Ativação do aplicativo, você deve especificar valores para diversas configurações.

Etapa 1. Solicitando a ativação da versão de avaliação do Kaspersky Internet Security

Se a solicitação de ativação do Kaspersky Internet Security for enviada com êxito, o Assistente continuará automaticamente na etapa seguinte.

Etapa 2. Iniciando o upgrade

Nesta etapa, o Assistente exibe uma mensagem na tela informando que todos os pré-requisitos do upgrade foram atendidos. Para continuar com o Assistente, clique no botão **Avançar**.

Etapa 3. Removendo aplicativos incompatíveis

Nesta etapa, o Assistente verifica se há aplicativos incompatíveis com o Kaspersky Internet Security instalados no computador. Se não for encontrado nenhum aplicativo incompatível, o Assistente continuará automaticamente na etapa seguinte. Se forem encontrados aplicativos incompatíveis, o Assistente os listará na janela e permitirá desinstalá-los.

Depois que os aplicativos incompatíveis forem desinstalado, talvez seja necessário reiniciar o sistema operacional. Depois que o sistema operacional for reiniciado, o Assistente será aberto automaticamente para reiniciar o processo de upgrade.

Etapa 4. Fazendo upgrade

Nesta etapa, o Assistente conecta os módulos de upgrade, o que pode levar algum tempo. Ao concluir o processo, o Assistente continuará automaticamente na etapa seguinte.

Etapa 5. Reiniciando o aplicativo

Na etapa final do upgrade, o aplicativo deverá ser reiniciado. Para fazer isso, clique no botão **Concluir** na janela do Assistente.

Etapa 6. Concluindo a ativação

Depois de reiniciar o aplicativo, o Assistente será aberto automaticamente. Depois de ativar a versão de avaliação do Kaspersky Internet Security com êxito, a janela do Assistente exibirá informações sobre o período durante o qual você pode usar a versão de avaliação.

Etapa 7. Análise do sistema

Nesta etapa, são coletadas informações sobre os aplicativos do Microsoft Windows. Esses aplicativos são adicionados à lista de aplicativos confiáveis que não têm restrições sobre as ações que executam no sistema.

Quando a análise for concluída, o Assistente continuará automaticamente na próxima etapa.

Etapa 8. Concluindo o upgrade

Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**.

Não é possível migrar o aplicativo para a versão de avaliação do Kaspersky Internet Security uma segunda vez.

COMO USAR O KASPERSKY GADGET

Ao usar o Kaspersky Anti-Virus em um computador com o Microsoft Windows Vista ou o Microsoft Windows 7, você também pode usar o Kaspersky Gadget (aqui chamado de *gadget*). Depois de instalar o Kaspersky Anti-Virus em um computador com o Microsoft Windows 7, o gadget é exibido automaticamente na área de trabalho. Depois de instalar o aplicativo em um computador com o Microsoft Windows Vista, você deverá adicionar o gadget manualmente à Barra Lateral do Microsoft Windows (consulte a documentação do sistema operacional).

O indicador colorido do gadget exibe o status de proteção do computador da mesma forma que o indicador de status na janela principal do aplicativo (consulte a seção "Diagnóstico e eliminação de problemas na proteção do computador" na página 35). O verde indica que o computador está totalmente protegido, o amarelo indica que há problemas com a proteção e o vermelho indica que a segurança do computador está em risco. A cor cinza indica que o aplicativo foi interrompido.

Ao atualizar os bancos de dados e módulos de software do aplicativo, um ícone em formato de globo girando é exibido na parte central do gadget.

Você pode usar o gadget para executar as seguintes ações:

- reiniciar o aplicativo, caso ele tenha sido pausado anteriormente;
- abrir a janela principal do aplicativo;
- verificar objetos especificados quanto à presença de vírus;
- abrir a janela de notícias.

Além disso, você pode configurar os botões do gadget de forma que eles possam executar ações adicionais:

- executar uma atualização;
- editar as configurações do aplicativo;
- exibir os relatórios do aplicativo;
- pausar a proteção;
- abrir o Teclado Virtual;
- abrir a janela do Gerenciador de Tarefas.

Para executar o aplicativo usando o gadget,

clique no ícone **Ativar** localizado no centro do gadget.

Para abrir a janela principal do aplicativo usando o gadget,

clique no ícone do monitor na área central do gadget.

Para verificar um objeto quanto à presença de vírus usando o gadget,

arraste o objeto a ser verificado para o gadget.

O andamento da tarefa será exibido na janela do **Gerenciador de Tarefas**.

Para abrir a janela de notícias usando o gadget,

clique no ícone exibido no centro do gadget quando forem lançadas notícias.

Para configurar o gadget:

1. Abra a janela de configurações do gadget clicando no ícone exibido no canto superior direito do bloco do gadget se você passar o cursor sobre ele.
2. Nas listas suspensas correspondentes aos botões do gadget, selecione as ações que devem ser executadas quando você clicar nesses botões.
3. Clique no botão **OK**.

COMO SABER A REPUTAÇÃO DE UM APLICATIVO

O Kaspersky Anti-Virus permite que você conheça a reputação de aplicativos dentre os usuários de todo o mundo. A reputação de um aplicativo compreende os seguintes critérios:

- nome do fornecedor;
- informações sobre a assinatura digital (disponíveis se houver uma assinatura digital);
- informações sobre o grupo no qual o aplicativo foi incluído pela maioria dos usuários do Kaspersky Security Network;
- número de usuários do Kaspersky Security Network que usam o aplicativo (disponível se o aplicativo tiver sido incluído no grupo Confiável do banco de dados do Kaspersky Security Network);
- hora em que o aplicativo ficou conhecido no Kaspersky Security Network;
- países nos quais o aplicativo é mais disseminado.

Para verificar a reputação de um aplicativo, você deve concordar em participar do Kaspersky Security Network (veja a página 109) ao instalar o Kaspersky Anti-Virus.

Para saber a reputação de um aplicativo,

abra o menu de contexto do arquivo executável do aplicativo e selecione **Verificar reputação no KSN**.

CONSULTE TAMBÉM:

CONFIGURAÇÕES AVANÇADAS DO APLICATIVO

Esta seção fornece informações detalhadas sobre como configurar cada componente do aplicativo.

NESTA SEÇÃO:

CONFIGURAÇÕES DE PROTEÇÃO GERAL

Na janela de configurações do aplicativo, na subseção **Configurações Gerais** da seção **Centro de Proteção**, é possível:

- desativar todos os componentes de proteção (consulte a seção "Ativando e desativando a proteção" na página 36);
- selecionar o modo de proteção interativa ou automática (consulte a seção "Selecionando um modo de proteção" na página 56);
- restringir o acesso dos usuários ao aplicativo definindo uma senha (consulte a seção "Restringindo o acesso ao Kaspersky Anti-Virus" na página 56);
- ativar ou desativar a execução automática do aplicativo ao iniciar o sistema operacional (consulte a seção "Ativando e desativando a execução automática" na página 34);
- ativar uma combinação de teclas personalizada para exibir o teclado virtual na tela (consulte a seção "Proteção contra interceptação de dados pelo teclado" na página 43).

NESTA SEÇÃO:

RESTRINGINDO O ACESSO AO KASPERSKY ANTI-VIRUS

O computador pode ser usado por diversos usuários com níveis de experiência em computação diferentes. O acesso irrestrito dos usuários ao Kaspersky Anti-Virus e a suas configurações pode resultar em um nível reduzido de proteção do computador.

Para restringir o acesso ao aplicativo, é possível definir uma senha e especificar as ações que exigem a inserção da senha:

- alteração das configurações do aplicativo;
- encerramento do aplicativo;
- remoção do aplicativo.

Cuidado ao usar uma senha para restringir o acesso à remoção do aplicativo. Se você esquecer a senha, será difícil remover o aplicativo do computador.

Para restringir o acesso ao Kaspersky Anti-Virus usando uma senha:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione a subseção **Configurações Gerais**.
3. À direita da janela, na seção **Proteção por senha**, marque a caixa **Ativar proteção por senha** e clique no botão **Configurações**.
4. Na janela **Proteção por senha** que é aberta, insira a senha e especifique a área que deve ser coberta pela restrição de acesso.

SELECIONANDO UM MODO DE PROTEÇÃO

Por padrão, o Kaspersky Anti-Virus é executado no *modo de proteção automática*. Nesse modo, o aplicativo aplica automaticamente as ações recomendadas pela Kaspersky Lab em resposta a eventos perigosos. Se desejar ser notificado pelo Kaspersky Anti-Virus sobre todos os eventos perigosos e suspeitos no sistema e poder decidir quais das ações oferecidas pelo aplicativo devem ser aplicadas, você pode ativar o *modo de proteção interativa*.

Para selecionar um modo de proteção:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione a subseção **Configurações Gerais**.
3. Na seção **Proteção interativa**, marque ou desmarque as caixas de acordo com sua opção de modo de proteção:
   - para ativar o modo de proteção interativa, desmarque a caixa **Selecionar ação automaticamente**;
   - para ativar o modo de proteção automática, marque a caixa **Selecionar ação automaticamente**.

     Se não desejar que o Kaspersky Anti-Virus exclua os objetos suspeitos ao ser executado no modo automático, marque a caixa **Não excluir objetos suspeitos**.

VERIFICAÇÃO

A verificação do computador quanto à presença de vulnerabilidades, vírus e outros riskwares é uma das tarefas mais importantes para garantir a segurança do computador.

É necessário verificar o computador periodicamente quanto à presença de vírus e outros riskwares para descartar a possibilidade de disseminação de programas maliciosos que não foram detectados pelos componentes de proteção, por exemplo, devido à definição de um baixo nível de segurança ou por outros motivos.

A verificação de vulnerabilidades executa o diagnóstico de segurança do sistema operacional e detecta recursos de software que poderiam ser usados por invasores para disseminar objetos maliciosos e obter acesso a informações pessoais.

Esta seção contém informações sobre os recursos e a configuração da tarefa de verificação, níveis de segurança, métodos e tecnologias de verificação.

NESTA SEÇÃO:

VERIFICAÇÃO DE VÍRUS

Para detectar vírus e outros riskwares, o Kaspersky Anti-Virus oferece as seguintes tarefas:

- **Verificação completa**. Verificação de todo o sistema. Por padrão, o Kaspersky Anti-Virus verifica os seguintes objetos:
  - memória do sistema;
  - objetos carregados ao iniciar o sistema operacional;
  - backup do sistema;
  - bancos de dados de email;
  - mídia de armazenamento removível, discos rígidos e unidades de rede.
- **Verificação de Áreas Críticas**. Por padrão, o Kaspersky Anti-Virus verifica os objetos carregados ao iniciar o sistema operacional.
- **Verificação Personalizada**. O Kaspersky Anti-Virus verifica os objetos selecionados pelo usuário. Você pode verificar qualquer objeto da lista a seguir:
  - memória do sistema;
  - objetos carregados ao iniciar o sistema operacional;
  - backup do sistema;
  - bancos de dados de email;
  - mídia de armazenamento removível, discos rígidos e unidades de rede;
  - qualquer arquivo ou pasta selecionados.

As tarefas Verificação Completa e Verificação de Áreas Críticas têm características específicas. Para essas tarefas, não é recomendável editar as listas de objetos que devem ser verificados.

Cada tarefa de verificação é executada na área especificada e pode ser iniciada de acordo com uma programação criada anteriormente. Cada tarefa de verificação também se caracteriza por um nível de segurança (combinação de configurações que afetam a profundidade da verificação). Por padrão, o *modo de assinatura* (de uso de registros dos bancos de dados do aplicativo para procurar ameaças) está sempre ativado. Você também pode aplicar diversos métodos e tecnologias de verificação.

Após o início da tarefa de verificação completa ou de verificação das áreas críticas, o andamento de execução da verificação é exibido na janela **Verificação**, na seção com o nome da tarefa em execução, e no Gerenciador de Tarefas (consulte a seção "Gerenciando tarefas de verificação. Gerenciador de Tarefas" na página 63).

Se for detectada uma ameaça, o Kaspersky Anti-Virus atribuirá um dos seguintes status ao objeto encontrado:

- Programa malicioso (como um *vírus* ou um *cavalo de Troia*).
- *Possivelmente infectado* (suspeito), quando a verificação não pode determinar se o objeto está infectado ou não. O arquivo pode conter uma sequência de código característica de vírus ou o código modificado de um vírus conhecido.

O aplicativo exibe uma notificação (veja a página 107) sobre a ameaça detectada e executa a ação definida. Você pode alterar as ações que devem ser executadas ao detectar uma ameaça.

Se você estiver trabalhando no modo automático (consulte a seção "Selecionando um modo de proteção" na página 56) quando forem detectados objetos perigosos, o Kaspersky Anti-Virus aplicará as ações recomendadas pelos especialistas da Kaspersky Lab automaticamente. Para objetos maliciosos, a ação é **Desinfetar. Excluir se a desinfecção falhar** e, para objetos suspeitos, é **Mover para a Quarentena**. Se forem detectados objetos perigosos ao trabalhar no modo interativo (consulte a seção "Selecionando um modo de proteção" na página 56), o aplicativo exibirá uma notificação na tela que poderá ser usada para selecionar a ação desejada na lista de ações disponíveis.

Antes de tentar desinfetar ou excluir um objeto infectado, o Kaspersky Anti-Virus cria uma cópia de backup para posterior restauração ou desinfecção. Os objetos suspeitos (possivelmente infectados) são colocados em quarentena. Você pode ativar a verificação automática de objetos em quarentena após cada atualização.

As informações sobre os resultados e eventos da verificação ocorridos durante a execução da tarefa são registrados em um relatório do Kaspersky Anti-Virus (veja a página 103).

NESTA SEÇÃO:

ALTERANDO E RESTAURANDO O NÍVEL DE SEGURANÇA

Dependendo de suas necessidades atuais, é possível selecionar um dos níveis de segurança predefinidos ou modificar manualmente as configurações da verificação.

Ao configurar a tarefa de verificação, você pode reverter para a configuração recomendada a qualquer momento. Essas configurações são consideradas ideais, são recomendadas pela Kaspersky Lab e estão agrupadas no nível de segurança **Recomendado**.

➧ *Para alterar o nível de segurança estabelecido:*

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).
3. Na seção **Nível de segurança**, defina o nível de segurança necessário para a tarefa selecionada ou clique no botão **Configurações** para modificar as configurações manualmente.

Se você modificar as configurações manualmente, o nome do nível de segurança será alterado para **Personalizado**.

Para restaurar as configurações de verificação padrão:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).
3. Na seção **Nível de segurança**, clique no botão **Nível padrão** da tarefa selecionada.

CRIANDO A PROGRAMAÇÃO DE INICIALIZAÇÃO DA VERIFICAÇÃO

Você pode criar uma programação para iniciar automaticamente as tarefas de verificação de vírus: especificar a frequência de execução da tarefa, a hora de início (se necessário) e configurações avançadas.

Se por algum motivo não for possível executar a tarefa (por exemplo, se o computador não estiver ligado naquela hora), você poderá configurar a tarefa ignorada para ser iniciada automaticamente assim que possível. Você pode pausar a verificação automaticamente quando a proteção de tela está inativa ou o computador está desbloqueado. Essa funcionalidade adia a execução da tarefa até que o usuário tenha concluído o trabalho no computador. Então, a verificação não utilizará recursos do sistema durante o trabalho.

O modo de Verificação Ociosa especial (consulte a seção "Executando tarefas em segundo plano" na página 94) permite iniciar as atualizações automáticas quando o computador está ocioso.

Para modificar a programação das tarefas de verificação:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação de Vulnerabilidades**).
3. Clique no botão **Modo de execução** à direita da janela.
4. Na janela que é aberta, na guia **Modo de execução**, na seção **Programar**, selecione **Por programação** e configure o modo de execução da verificação especificando os valores desejados para a configuração **Frequência**.

Para ativar a execução automática de uma tarefa ignorada:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação de Vulnerabilidades**).
3. Clique no botão **Modo de execução** à direita da janela.
4. Na janela que é aberta, na guia **Modo de execução**, na seção **Programar**, selecione **Por programação** e marque a caixa **Executar tarefas ignoradas**.

Para executar as tarefas somente quando o computador não estiver em uso:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação de Vulnerabilidades**).
3. Clique no botão **Modo de execução** à direita da janela.
4. Na janela que é aberta, na guia **Modo de execução**, na seção **Programar**, selecione **Por programação** e marque a caixa **Executar a verificação programada quando a proteção de tela estiver ativa ou o computador estiver bloqueado**.

CRIANDO UMA LISTA DE OBJETOS A SEREM VERIFICADOS

Cada tarefa de verificação de vírus possui sua própria lista de objetos padrão. Esses objetos podem incluir itens do sistema de arquivos do computador, como unidades lógicas e bancos de dados de email, ou outros tipos de objetos, como unidades de rede. É possível editar essa lista.

Se o escopo da verificação estiver vazio ou não contiver nenhum objeto selecionado, a tarefa de verificação não poderá ser iniciada.

Para criar uma lista de objetos para uma tarefa de verificação personalizada:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, selecione a seção **Verificação**.
3. Na parte inferior da janela que é aberta, clique no link **selecionar** para abrir a lista de objetos a serem verificados.
4. Na janela **Verificação Personalizada** que é aberta, clique no botão **Adicionar**.
5. Na janela **Selecionar objeto a ser verificado** que é aberta, selecione o objeto desejado e clique no botão **Adicionar**. Clique no botão **OK** depois de adicionar todos os objetos desejados. Para excluir objetos da lista de objetos a serem verificados, desmarque as caixas ao lado deles.

   Você também pode arrastar os arquivos que devem ser verificados diretamente na área marcada localizada na seção **Verificação**.

Para criar uma lista de objetos para as tarefas Verificação Completa, Verificação de Áreas Críticas ou Verificação de Vulnerabilidades:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa de verificação desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação de Vulnerabilidades**).
3. À direita da janela, clique no botão **Escopo da verificação**.
4. Na janela **Escopo da verificação** que é aberta, use os botões **Adicionar**, **Editar** e **Excluir** para criar uma lista. Para excluir objetos da lista de objetos a serem verificados, desmarque as caixas ao lado deles.

   Por padrão, não é possível editar ou excluir os objetos que aparecem na lista.

SELECIONANDO UM MÉTODO DE VERIFICAÇÃO

Durante a verificação de vírus, a *análise de assinaturas* é usada sempre: O Kaspersky Anti-Virus compara o objeto encontrado com os registros do banco de dados.

Você pode usar os métodos de verificação adicionais para aumentar a eficiência da verificação: a *análise heurística* (análise das ações executadas por um objeto no sistema) e a *verificação de rootkits* (verificação de ferramentas que podem ocultar programas maliciosos no sistema operacional).

Para selecionar o método de verificação a ser usado:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).
3. Na seção **Nível de segurança**, clique no botão **Configurações** da tarefa selecionada.
4. Na janela que é aberta, na guia **Adicional**, na seção **Métodos de verificação**, selecione os métodos de verificação desejados.

SELECIONANDO A TECNOLOGIA DE VERIFICAÇÃO

Além dos métodos de verificação, você pode usar tecnologias de verificação de objetos especiais que permitem aumentar a velocidade da verificação de vírus através da exclusão dos arquivos que não foram modificados desde sua última verificação.

Para especificar as tecnologias de verificação de objetos:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).
3. Na seção **Nível de segurança**, clique no botão **Configurações** da tarefa selecionada.
4. Na janela que é aberta, na guia **Adicional**, na seção **Tecnologias de verificação**, selecione os valores desejados.

ALTERANDO AS AÇÕES QUE DEVEM SER EXECUTADAS AO DETECTAR UMA AMEAÇA

Se forem detectados objetos infectados, o aplicativo executará a ação selecionada.

Para alterar a ação que deve ser executada ao detectar uma ameaça:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).
3. À direita da janela, na seção **Ação ao detectar ameaça**, selecione a opção desejada.

EXECUTANDO UMA VERIFICAÇÃO COM OUTRA CONTA DE USUÁRIO

Por padrão, as tarefas de verificação são executadas com sua conta do sistema. Porém, talvez seja necessário executar a tarefa com outra conta de usuário. Você pode especificar a conta que deve ser usada pelo aplicativo ao executar uma tarefa de verificação.

Para iniciar a verificação com outra conta de usuário:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação de Vulnerabilidades**).
3. Clique no botão **Modo de execução** à direita da janela.
4. Na janela que é aberta, na guia **Modo de execução**, na seção **Conta do usuário**, marque a caixa **Executar tarefa como**. Especifique o nome do usuário e a senha.

ALTERANDO O TIPO DE OBJETOS A SEREM VERIFICADOS

Ao especificar os tipos de objetos a serem verificados, você estabelece os formatos de arquivos que serão verificados quanto à presença de vírus ao executar a tarefa de verificação selecionada.

Ao selecionar os tipos de arquivos, lembre-se do seguinte:

- A probabilidade de infiltração de código malicioso em alguns formatos de arquivo (como TXT) e sua ativação posterior é bastante pequena. Entretanto, existem formatos que contêm ou que podem conter um código executável (como EXE, DLL, DOC). O risco de infiltração e ativação de código malicioso nesses arquivos é bastante grande.
- Um invasor pode enviar um vírus ao seu computador em um arquivo executável renomeado como um arquivo TXT. Se você selecionou a verificação de arquivos por extensão, esse arquivo será ignorado pela verificação. Se a verificação de arquivos por formato estiver selecionada, então, independentemente da extensão, o Antivírus de Arquivos analisará o cabeçalho do arquivo e descobrirá que trata-se de um arquivo EXE. Esse arquivo seria verificado cuidadosamente quanto à presença de vírus.

Para alterar os tipos de objetos a serem verificados:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).
3. Na seção **Nível de segurança**, clique no botão **Configurações** da tarefa selecionada.
4. Na janela que é aberta, na guia **Escopo**, na seção **Tipos de arquivos**, selecione a opção desejada.

VERIFICAÇÃO DE ARQUIVOS COMPOSTOS

Um método comum para ocultar vírus é inseri-los em arquivos compostos: arquivos comprimidos, pacotes de instalação, objetos OLE inseridos e formatos de arquivos de email. Para detectar vírus que foram ocultados dessa maneira, é necessário descompactar os arquivos compostos, o que pode reduzir significativamente a velocidade da verificação.

Para cada tipo de arquivo composto, você pode optar por verificar todos os arquivos ou apenas os arquivos novos. Para selecionar, clique no link ao lado do nome do objeto. Seu valor é mudado quando você clica nele. Se você selecionar o

modo de verificação apenas de arquivos novos e alterados (veja a página 62), os links para definir a verificação de todos ou apenas de arquivos novos não estarão disponíveis.

Você pode restringir o tamanho máximo do arquivo composto a ser verificado. Os arquivos compostos maiores que o tamanho especificado não serão verificados.

Quando arquivos grandes são extraídos de arquivos comprimidos, eles são verificados mesmo que a caixa **Não descompactar arquivos compostos grandes** esteja marcada.

- *Para modificar a lista de arquivos compostos a serem verificados:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).
  3. Na seção **Nível de segurança**, clique no botão **Configurações** da tarefa selecionada.
  4. Na janela que é aberta, na guia **Escopo**, na seção **Verificação de arquivos compostos**, selecione os tipos de arquivos compostos que devem ser verificados.

- *Para definir o tamanho máximo dos arquivos compostos a serem verificados:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).
  3. Na seção **Nível de segurança**, clique no botão **Configurações** da tarefa selecionada.
  4. Na janela que é aberta, na guia **Escopo**, na seção **Verificação de arquivos compostos**, clique no botão **Adicional**.
  5. Na janela **Arquivos compostos** que é aberta, marque a caixa **Não descompactar arquivos compostos grandes** e especifique o tamanho máximo de arquivo.

OTIMIZAÇÃO DA VERIFICAÇÃO

Você pode reduzir o tempo de verificação e aumentar a velocidade do Kaspersky Anti-Virus. Isso é possível verificando apenas os arquivos novos e aqueles que foram alterados desde a última vez que foram verificados. Esse modo se aplica a arquivos simples e compostos.

Você também pode definir uma restrição sobre a duração da verificação de um objeto. Quando o intervalo de tempo especificado acabar, o objeto será excluído da verificação atual (exceto os arquivos comprimidos e os arquivos compostos por vários objetos).

- *Para verificar somente arquivos novos e alterados:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).
  3. Na seção **Nível de segurança**, clique no botão **Configurações** da tarefa selecionada.
  4. Na janela que é aberta, na guia **Escopo**, na seção **Otimização da verificação**, marque a caixa **Verificar somente arquivos novos e alterados**.

- *Para definir uma restrição sobre a duração da verificação:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Verificação**, selecione a tarefa desejada (**Verificação Completa**, **Verificação de Áreas Críticas** ou **Verificação Personalizada**).
  3. Na seção **Nível de segurança**, clique no botão **Configurações** da tarefa selecionada.
  4. Na janela que é aberta, na guia **Escopo**, na seção **Otimização da verificação**, marque a caixa **Ignorar objetos verificados por mais de** e especifique a duração da verificação de um único arquivo.

VERIFICANDO UNIDADES REMOVÍVEIS AO CONECTAR

Atualmente, os objetos maliciosos que usam vulnerabilidades dos sistemas operacionais para se replicar através das redes e mídias removíveis estão cada vez mais difundidos. O Kaspersky Anti-Virus permite verificar as unidades removíveis ao conectá-las ao computador.

- *Para configurar a verificação de mídias removíveis ao conectar:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Verificação**, selecione **Configurações Gerais**.
  3. Na seção **Verificar unidades removíveis ao conectar**, selecione a ação e defina o tamanho máximo da unidade a ser verificada no campo abaixo, se necessário.

CRIANDO UM ATALHO DE TAREFA

O aplicativo oferece a opção de criar atalhos para as tarefas de verificação completa, rápida e de vulnerabilidades. Assim, é possível iniciar a verificação desejada sem abrir a janela principal do aplicativo ou o menu de contexto.

- *Para criar um atalho para iniciar uma verificação:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Verificação**, selecione **Configurações Gerais**.
  3. À direita da janela, na seção **Execução rápida de tarefas de verificação**, clique no botão **Criar atalho** ao lado do nome da tarefa desejada (**Verificação de Áreas Críticas**, **Verificação Completa** ou **Verificação de Vulnerabilidades**).
  4. Especifique o caminho para salvar o atalho e seu nome na janela que é aberta. Por padrão, o atalho será criado com o nome da tarefa na pasta Meu Computador do usuário do computador atual.

VERIFICAÇÃO DE VULNERABILIDADES

Podem aparecer vulnerabilidades no sistema operacional, por exemplo, devido a erros de programação, senhas inseguras ou ações de programas maliciosos. Ao executar a verificação de vulnerabilidades, o aplicativo faz referência a diversos procedimentos de segurança, por exemplo, examinando o sistema, analisando as configurações do sistema operacional e do navegador e procurando serviços vulneráveis.

O diagnóstico pode levar algum tempo. Quando concluído, os problemas detectados serão analisados considerando o perigo que representam ao sistema.

Depois que a tarefa de verificação de vulnerabilidades for iniciada (veja a página 42), o andamento de sua execução será exibido na janela **Verificação** (na seção **Verificação de Vulnerabilidades**) e no Gerenciador de Tarefas (consulte a seção "Gerenciando tarefas de verificação. Gerenciador de Tarefas" na página 63).

As informações sobre os resultados da execução da tarefa de verificação de vulnerabilidades será gravado em um relatório do Kaspersky Anti-Virus (veja a página 103).

Da mesma forma que com as tarefas de verificação de vírus, você pode definir uma programação de inicialização da tarefa de verificação de vulnerabilidades, criar uma lista de objetos a serem verificados (veja a página 59), especificar uma conta (consulte a seção "Executando a verificação com outra conta de usuário" na página 61) e criar um atalho para a execução rápida de uma tarefa. Por padrão, os aplicativos já instalados no computador são selecionados como objetos de verificação.

GERENCIANDO TAREFAS DE VERIFICAÇÃO. GERENCIADOR DE TAREFAS

O Gerenciador de Tarefas exibe informações sobre as últimas tarefas de verificação executadas ou que estão em execução (por exemplo, verificação de vírus, verificação de vulnerabilidades, verificação de rootkits ou desinfecção avançada).

Você pode usar o Gerenciador de Tarefas para exibir o andamento e o resultado da execução de uma tarefa ou para interrompê-la. Para algumas tarefas, também estão disponíveis ações adicionais (por exemplo, ao concluir a verificação de vulnerabilidades, é possível abrir a lista de vulnerabilidades detectadas e corrigi-las).

Para abrir o Gerenciador de Tarefas:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, selecione a seção **Verificação**.
3. Na janela **Verificação** que é aberta, clique no botão **Gerenciar Tarefas** no canto superior direito.

ATUALIZAÇÃO

A atualização dos bancos de dados e módulos do Kaspersky Anti-Virus garantem a proteção atualizada do computador. Diariamente aparecem novos vírus, cavalos de Troia e outros tipos de malware em todo o mundo. Informações sobre ameaças e formas de neutralizá-las são fornecidas nos bancos de dados do Kaspersky Anti-Virus. Para a detecção oportuna de novas ameaças, você deve atualizar os bancos de dados e módulos do aplicativo periodicamente.

As atualizações periódicas exigem uma licença ativa de uso do aplicativo. Se não houver uma licença instalada, você poderá executar a atualização apenas uma vez.

Ao executar uma atualização, o aplicativo baixa e instala os seguintes objetos no computador:

- Bancos de dados do Kaspersky Anti-Virus.

  A proteção das informações é garantida pelos bancos de dados, que contêm assinaturas de ameaças, descrições de ataques de rede e informações sobre como resistir a eles. Os componentes de proteção usam essas informações para procurar e desinfetar objetos perigosos do computador. Os bancos de dados são complementados a cada hora com registros de novas ameaças e formas de combatê-las. Assim, é altamente recomendável atualizá-los periodicamente.

  Além dos bancos de dados do Kaspersky Anti-Virus, os drivers de rede que ativam os componentes do aplicativo para interceptar o tráfego de rede são atualizados.

- Módulos do aplicativo.

  Além dos bancos de dados do Kaspersky Anti-Virus, você também pode atualizar os módulos do programa. As atualizações dos módulos do aplicativo corrigem as vulnerabilidades do Kaspersky Anti-Virus e acrescentam ou melhoram as funcionalidades existentes.

Durante uma atualização, os bancos de dados e módulos do aplicativo do computador são comparados com a versão atualizada na fonte de atualização. Se os bancos de dados e módulos atuais do aplicativo forem diferentes daqueles na versão atual do aplicativo, a parte ausente das atualizações será instalada no computador.

Se os bancos de dados estiverem desatualizados, o pacote de atualização pode ser grande, o que gerará um tráfego de Internet adicional (de até várias dezenas de Mb).

Antes de atualizar os bancos de dados, o Kaspersky Anti-Virus cria cópias de backup dos mesmos, caso você queira retornar à versão anterior dos bancos de dados (consulte a seção "Revertendo a última atualização" na página 67).

As informações sobre as condições atuais dos bancos de dados do Kaspersky Anti-Virus são exibidas na seção **Atualização** da janela principal do aplicativo.

As informações sobre os resultados e eventos da atualização ocorridos durante a execução da tarefa de atualização são registrados em um relatório do Kaspersky Anti-Virus (veja a página 103).

Você pode selecionar uma fonte de atualização (consulte a seção "Selecionando uma fonte de atualização" na página 65) e configure a execução automática da atualização.

NESTA SEÇÃO:

SELECIONANDO UMA FONTE DE ATUALIZAÇÃO

Uma *fonte de atualização* é um recurso que contém as atualizações dos bancos de dados e dos módulos do Kaspersky Anti-Virus.

As principais fontes de atualização são os servidores de atualização da Kaspersky Lab, nos quais são armazenadas atualizações do banco de dados e do módulo do aplicativo de todos os produtos da Kaspersky Lab.

O computador deve estar conectado com a Internet para baixar com êxito as atualizações dos nossos servidores. Por padrão, as configurações da conexão com a Internet são determinadas automaticamente. Se você usar um servidor proxy, talvez seja necessário ajustar as configurações de conexão (consulte a seção "Configurando o servidor proxy" na página 90).

Ao atualizar o Kaspersky Anti-Virus, você pode copiar as atualizações do banco de dados e dos módulos do programa recebidas dos servidores da Kaspersky Lab em uma pasta local (consulte a seção "Atualizando o aplicativo de uma pasta compartilhada" na página 66) e depois dar acesso a outros computadores da rede. Isso economiza tráfego da Internet.

Se você não tem acesso aos servidores de atualização da Kaspersky Lab (por exemplo, se o seu acesso à Internet é limitado), é possível ligar para a sede da Kaspersky Lab (http://www.kaspersky.com/contacts) para solicitar informações de contato dos parceiros da Kaspersky Lab que podem fornecer atualizações em mídia removível.

Ao solicitar atualizações em mídia removível, especifique se deseja receber também as atualizações dos módulos do aplicativo.

ADICIONANDO UMA FONTE DE ATUALIZAÇÃO

Por padrão, a lista de fontes de atualização contém apenas os servidores de atualização da Kaspersky Lab. Você pode adicionar uma pasta local ou outro servidor como fonte de atualização. Se vários recursos forem selecionados como fontes de atualização, o Kaspersky Anti-Virus tentará se conectar a cada um deles, começando pelo primeiro na lista, e recuperará as atualizações da primeira fonte disponível.

Para adicionar uma fonte de atualização:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Atualização**, selecione o componente **Configurações de Atualização**.
3. Clique no botão **Fonte de atualização** à direita da janela.
4. Na janela que é aberta, na guia **Fonte**, abra a janela de seleção clicando no botão **Adicionar**.
5. Na janela **Selecionar fonte de atualização** que é aberta, selecione uma pasta que contém as atualizações ou insira um endereço no campo **Fonte** para especificar o servidor do qual as atualizações devem ser baixadas.

SELECIONANDO A REGIÃO DO SERVIDOR DE ATUALIZAÇÃO

Se você usar os servidores da Kaspersky Lab como fonte de atualização, poderá selecionar o local do servidor ideal para o download das atualizações. Os servidores da Kaspersky Lab estão localizados em diversos países.

O uso do servidor de atualização da Kaspersky Lab mais próximo permite reduzir o tempo necessário para receber as atualizações e aumentar a velocidade de desempenho da operação. Por padrão, o aplicativo usa as informações sobre a região atual contidas no Registro do sistema operacional. Você pode selecionar a região manualmente.

Para selecionar a região do servidor:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Atualização**, selecione o componente **Configurações de Atualização**.
3. Clique no botão **Fonte de atualização** à direita da janela.
4. Na janela que é aberta, na guia **Fonte**, na seção **Configurações regionais**, selecione a opção **Selecionar na lista** e, em seguida, selecione o país mais próximo do seu local atual na lista suspensa.

ATUALIZANDO O APLICATIVO DE UMA PASTA COMPARTILHADA

Para economizar tráfego da Internet, é possível configurar as atualizações do Kaspersky Anti-Virus a partir de uma pasta compartilhada ao atualizar o aplicativo em computadores em rede. Se você fizer isso, um dos computadores em rede receberá um pacote de atualização dos servidores da Kaspersky Lab ou de outro recurso da Web que contenha o conjunto de atualizações necessário. As atualizações recebidas são copiadas em uma pasta compartilhada. Os outros computadores da rede acessam essa pasta para receber as atualizações do Kaspersky Anti-Virus.

Ao fazer login com uma conta de visitante no Microsoft Windows 7, as atualizações não são copiadas para a pasta compartilhada. É recomendável fazer login em uma outra conta para permitir a cópia das atualizações.

- *Para ativar o modo de distribuição de atualizações:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Atualização**, selecione o componente **Configurações de Atualização**.
  3. Marque a caixa **Copiar atualizações para pasta** na seção **Adicional** e, no campo abaixo, especifique o caminho da pasta pública na qual todas as atualizações baixadas serão copiadas. Você também pode selecionar uma pasta clicando no botão **Procurar**.

- *Para baixar atualizações para o seu computador de uma pasta compartilhada especificada:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Atualização**, selecione o componente **Configurações de Atualização**.
  3. Clique no botão **Fonte de atualização** à direita da janela.
  4. Na janela que é aberta, na guia **Fonte**, abra a janela de seleção clicando no botão **Adicionar**.
  5. Na janela **Selecionar fonte de atualização** que é aberta, selecione uma pasta ou insira seu caminho completo no campo **Fonte**.
  6. Na guia **Fonte**, desmarque a caixa **Servidores de atualização da Kaspersky Lab**.

CRIANDO A PROGRAMAÇÃO DE INICIALIZAÇÃO DA VERIFICAÇÃO

Você pode criar uma programação para iniciar uma tarefa de atualização automaticamente: especificar a frequência, a hora inicial (se necessário) e configurações avançadas.

Se por algum motivo não for possível executar a tarefa (por exemplo, se o computador não estiver ligado naquela hora), você poderá configurar a tarefa ignorada para ser iniciada automaticamente assim que possível.

Você também pode adiar o início automático da tarefa depois que o aplicativo é iniciado. Todas as tarefas programadas serão executadas somente depois de decorrido o intervalo de tempo especificado desde o início do Kaspersky Anti-Virus.

O modo de Verificação Ociosa especial (consulte a seção "Executando tarefas em segundo plano" na página 94) permite iniciar as atualizações automáticas quando o computador está ocioso.

- *Para configurar a programação de inicialização da tarefa de atualização:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Atualização**, selecione o componente **Configurações de Atualização**.
  3. Clique no botão **Modo de execução** à direita da janela.
  4. Na janela que é aberta, na guia **Modo de execução**, na seção **Programar**, selecione a opção **Por programação** e configure o modo de execução da atualização.

- *Para ativar a execução automática de uma tarefa ignorada:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Atualização**, selecione o componente **Configurações de Atualização**.
  3. Clique no botão **Modo de execução** à direita da janela.
  4. Na janela que é aberta, na guia **Modo de execução**, na seção **Programar**, selecione **Por programação** e marque a caixa **Executar tarefas ignoradas**.

- *Para adiar a execução de uma tarefa após o início do aplicativo:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Atualização**, selecione o componente **Configurações de Atualização**.
  3. Clique no botão **Modo de execução** à direita da janela.
  4. Na janela que é aberta, na guia **Modo de execução**, na seção **Programar**, selecione a opção **Por programação** e preencha o campo **Adiar a execução após o início do aplicativo por** para especificar por quanto tempo a execução da tarefa deve ser adiada.

REVERTENDO A ÚLTIMA ATUALIZAÇÃO

Depois da primeira atualização do Kaspersky Anti-Virus, fica disponível a opção de reverter para os bancos de dados anteriores.

O recurso de reversão da atualização é útil quando uma nova versão do banco de dados contém uma assinatura inválida que faz o Kaspersky Anti-Virus bloquear um aplicativo seguro.

Caso ocorram danos aos bancos de dados do Kaspersky Anti-Virus, é recomendável executar a tarefa de atualização para baixar o conjunto atualizado de bancos de dados.

- *Para reverter para a versão anterior do banco de dados:*

  1. Abra a janela principal do aplicativo.
  2. Selecione a seção **Atualização** na parte inferior da janela.
  3. Na janela **Atualização** que é aberta, clique no botão  e selecione **Reverter para os bancos de dados anteriores** no menu que é aberto.

EXECUTANDO ATUALIZAÇÕES COM OUTRA CONTA DE USUÁRIO

Por padrão, o procedimento de atualização é executado com sua conta do sistema. No entanto, o Kaspersky Anti-Virus pode ser atualizado a partir de uma fonte na qual você não tem direitos de acesso (por exemplo, de uma pasta de rede que contém as atualizações) ou credenciais de usuário proxy que exige autorização. Você pode executar as atualizações do Kaspersky Anti-Virus em nome de uma conta de usuário que possua esses direitos.

- *Para iniciar a atualização com uma conta de usuário diferente:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Atualização**, selecione o componente **Configurações de Atualização**.
  3. Clique no botão **Modo de execução** à direita da janela.
  4. Na janela que é aberta, na guia **Modo de execução**, na seção **Conta do usuário**, marque a caixa **Executar tarefa como**. Especifique o nome do usuário e a senha.

USANDO UM SERVIDOR PROXY

Se você usar um servidor proxy para a conexão com a Internet, reconfigure-o para permitir a atualização adequada do Kaspersky Anti-Virus.

- *Para configurar o servidor proxy:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Atualização**, selecione o componente **Configurações de Atualização**.
  3. Clique no botão **Fonte de atualização** à direita da janela.
  4. Na janela que é aberta, na guia **Fonte**, clique no botão **Servidor proxy**.
  5. Configure o servidor proxy na janela **Configurações do servidor proxy** que é aberta.

ANTIVÍRUS DE ARQUIVOS

O Antivírus de Arquivos evita a infecção do sistema de arquivos do computador. O componente é executado ao iniciar o sistema operacional, permanece na RAM do computador e verifica todos os arquivos abertos, salvos ou executados no computador e em todas as unidades conectadas quanto à presença de vírus e outros riskwares.

Você pode criar um escopo de proteção e definir um nível de segurança (uma coleção de configurações que determinam a profundidade da verificação).

Quando o usuário ou um programa tenta acessar um arquivo protegido, o Antivírus de Arquivos verifica se os bancos de dados do iChecker e do iSwift contêm informações sobre esse arquivo e decide se ele deve ser verificado.

Por padrão, a *análise de assinaturas* – um modo que usa os registros dos bancos de dados do aplicativo para procurar ameaças – está sempre ativada. Além disso, você pode ativar a análise heurística e diversas tecnologias de verificação.

Se for detectada uma ameaça em um arquivo, o Kaspersky Anti-Virus atribuirá um dos seguintes status ao arquivo:

- Status que designa o tipo do programa malicioso detectado (por exemplo, *vírus*, *cavalo de Troia*).
- *Possivelmente infectado* (suspeito), quando a verificação não puder determinar se o arquivo está infectado ou não. O arquivo pode conter uma sequência de código típica de vírus e outros malwares, ou o código modificado de um vírus conhecido.

Depois disso, o aplicativo exibe na tela uma notificação (veja a página 107) sobre a ameaça detectada e executa a ação especificada nas configurações do Antivírus de Arquivos. Você pode alterar a ação (veja a página 71) que deve ser executada pelo aplicativo caso seja detectada uma ameaça.

Se você estiver trabalhando no modo automático (consulte a seção "Selecionando um modo de proteção" na página 56) quando forem detectados objetos perigosos, o Kaspersky Anti-Virus aplicará as ações recomendadas pelos especialistas da Kaspersky Lab automaticamente. Para objetos maliciosos, a ação é **Desinfetar. Excluir se a desinfecção falhar** e, para objetos suspeitos, é **Mover para a Quarentena**. Se forem detectados objetos perigosos ao trabalhar no modo interativo (consulte a seção "Selecionando um modo de proteção" na página 56), o aplicativo exibirá uma notificação na tela que poderá ser usada para selecionar a ação desejada na lista de ações disponíveis.

Antes de tentar desinfetar ou excluir um objeto infectado, o Kaspersky Anti-Virus cria uma cópia de backup para posterior restauração ou desinfecção. Os objetos suspeitos (possivelmente infectados) são colocados em quarentena. Você pode ativar a verificação automática de objetos em quarentena após cada atualização.

NESTA SEÇÃO:

ATIVANDO E DESATIVANDO O ANTIVÍRUS DE ARQUIVOS

Por padrão, o Antivírus de Arquivos está ativado e é executado no modo recomendado pelos especialistas da Kaspersky Lab. Se necessário, você pode desativar o Antivírus de Arquivos.

Para desativar o Antivírus de Arquivos:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
3. À direita da janela, desmarque a caixa **Ativar Antivírus de Arquivos**.

PAUSANDO O ANTIVÍRUS DE ARQUIVOS AUTOMATICAMENTE

Ao executar trabalhos que utilizam muitos recursos, você pode pausar o Antivírus de Arquivos. Para reduzir a carga de trabalho e assegurar o rápido acesso aos objetos, você pode configurar a pausa automática do componente em uma hora especificada ou ao trabalhar com determinados programas.

A pausa do Antivírus de Arquivos em caso de conflito com outros aplicativos é uma medida de emergência. Se houver conflitos ao trabalhar com o componente, entre em contato com o Serviço de Suporte Técnico da Kaspersky Lab (http://suporte.kasperskyamericas.com/usuarios-domesticos/env%C3%ADe-um-caso-de-suporte). Os especialistas em suporte ajudarão a solucionar a operação simultânea do Kaspersky Anti-Virus com outros aplicativos no computador.

Para pausar o componente em uma hora especificada:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
3. Na seção **Nível de segurança** à direita da janela, clique no botão **Configurações**.
4. Na janela que é aberta, na guia **Adicional**, na seção **Pausar tarefa**, marque a caixa **Por programação** e clique no botão **Programar**.
5. Na janela **Pausar tarefa**, especifique a hora (no formato de 24 horas hh:mm) em que a proteção será pausada (campos **Pausar tarefa às** e **Reiniciar tarefa às**).

Para pausar o componente ao executar determinados aplicativos:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
3. Na seção **Nível de segurança** à direita da janela, clique no botão **Configurações**.
4. Na janela que é aberta, na guia **Adicional**, na seção **Pausar tarefa**, marque a caixa **Após iniciar o aplicativo** e clique no botão **Selecionar**.
5. Na janela **Aplicativos**, crie uma lista de aplicativos cuja execução pausará o componente.

CRIANDO O ESCOPO DE PROTEÇÃO DO ANTIVÍRUS DE ARQUIVOS

O escopo de proteção compreende o local e o tipo dos arquivos verificados. Por padrão, o Kaspersky Anti-Virus verifica apenas os arquivos possivelmente infectáveis armazenados em qualquer disco rígido, unidade de rede ou mídia removível.

Para criar o escopo de proteção:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
3. Clique no botão **Configurações** à direita da janela.
4. Na janela que é aberta, na guia **Geral**, na seção **Tipos de arquivos**, especifique o tipo de arquivos que devem ser verificados pelo Antivírus de Arquivos:
   - Se desejar verificar todos os arquivos, selecione **Todos os arquivos**.
   - Se desejar verificar os arquivos dos formatos mais vulneráveis a infecção, selecione **Arquivos verificados por formato**.
   - Se desejar verificar os arquivos com extensões mais vulneráveis a infecção, selecione **Arquivos verificados por extensão**.

   Ao selecionar os tipos de arquivos que devem ser verificados, observe que:

   - A probabilidade de infiltração de código malicioso em alguns formatos de arquivo (como TXT) e sua ativação posterior é bastante pequena. Entretanto, existem formatos que contêm ou que podem conter um código executável (como EXE, DLL, DOC). O risco de infiltração e ativação de código malicioso nesses arquivos é bastante grande.
   - Um hacker pode enviar um vírus ou outros riskwares para seu computador com um arquivo executável renomeado, como com a extensão TXT. Se você selecionou a verificação de arquivos por extensão, esse arquivo será ignorado pela verificação. Se a verificação de arquivos por formato estiver selecionada, então,

independentemente da extensão, o Antivírus de Arquivos analisará o cabeçalho do arquivo e descobrirá que trata-se de um arquivo EXE. Esse arquivo é verificado cuidadosamente quanto à presença de vírus e outros riskwares.

5. Na lista **Escopo de proteção**, execute uma das seguintes ações:

   - Se desejar adicionar um novo objeto à lista de objetos que devem ser verificados, clique no link **Adicionar**.
   - Se desejar alterar o local de um objeto, selecione-o na lista e clique no link **Editar**.

   A janela **Selecionar objeto a ser verificado** é aberta.

   - Se desejar excluir um objeto da lista de objetos a serem verificados, selecione-o na lista e clique no link **Excluir**.

     A janela de confirmação da exclusão é aberta.

6. Execute uma das seguintes ações:

   - Se desejar adicionar um novo objeto à lista de objetos a serem verificados, selecione-o na janela **Selecionar objeto a ser verificado** e clique no botão **OK**.
   - Se desejar alterar o local de um objeto, edite seu caminho para um no campo **Objeto** na janela **Selecionar objeto a ser verificado** e clique no botão **OK**.
   - Se desejar excluir um objeto da lista de objetos a serem verificados, clique no botão **Sim** na janela de confirmação da exclusão.

7. Se necessário, repita as etapas 6 – 7 para adicionar, realocar ou excluir objetos da lista de objetos a serem verificados.
8. Para excluir um objeto da lista de objetos a serem verificados, desmarque a caixa ao lado do objeto na lista **Escopo de proteção**. Contudo, o objeto permanecerá na lista de objetos a serem verificados, embora ele seja excluído da verificação pelo Antivírus de Arquivos.

ALTERANDO E RESTAURANDO O NÍVEL DE SEGURANÇA DOS ARQUIVOS

De acordo com suas necessidades atuais, você pode selecionar um dos níveis predefinidos de segurança de arquivos/da memória ou configurar você mesmo o Antivírus de Arquivos.

Ao configurar o Antivírus de Arquivos, você pode restaurar os valores recomendados a qualquer momento. Essas configurações são consideradas ideais, são recomendadas pela Kaspersky Lab e estão agrupadas no nível de segurança **Recomendado**.

Para alterar o nível de segurança de arquivos:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
3. À direita da janela, na seção **Nível de segurança**, defina o nível de segurança necessário ou clique no botão **Configurações** para modificar as configurações manualmente.

   Se você modificar as configurações manualmente, o nome do nível de segurança será alterado para **Personalizado**.

Para restaurar o nível de segurança de arquivos padrão:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
3. Clique no botão **Nível padrão** na seção **Nível de segurança** à direita da janela.

SELECIONANDO O MODO DE VERIFICAÇÃO DE ARQUIVOS

Um *modo de verificação* representa uma condição sob a qual o Antivírus de Arquivos começa a verificar os arquivos. Por padrão, o Kaspersky Anti-Virus é executado no modo inteligente. Quando executado nesse modo de verificação de arquivos, o Antivírus de Arquivos decide sobre a verificação de arquivos de acordo com a análise das ações executadas pelo usuário com os arquivos e com o tipo desses arquivos. Por exemplo, ao trabalhar com um documento do Microsoft

Office, o Kaspersky Anti-Virus verifica o arquivo quando ele é aberto pela primeira vez e fechado pela última vez. O arquivo não é verificado durante as operações intermediárias de gravação.

- *Para alterar o modo de verificação de arquivos:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
  3. Na seção **Nível de segurança** à direita da janela, clique no botão **Configurações**.
  4. Na janela que é aberta, na guia **Adicional**, na seção **Modo de verificação**, selecione o modo desejado.

  Ao selecionar o modo de verificação, você deve considerar os tipos de arquivos com os quais você precisa trabalhar na maior parte do tempo.

USANDO A ANÁLISE HEURÍSTICA AO TRABALHAR COM O ANTIVÍRUS DE ARQUIVOS

Durante a operação do Antivírus de Arquivos, a *análise de assinaturas* é usada sempre: O Kaspersky Anti-Virus compara o objeto encontrado com os registros do banco de dados.

Para melhorar a eficiência da proteção, você pode usar a *análise heurística* (ou seja, a análise da atividade que um objeto executa no sistema). Essa análise permite detectar novos objetos maliciosos que ainda não estão descritos nos bancos de dados.

- *Para ativar a análise heurística:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
  3. Na seção **Nível de segurança** à direita da janela, clique no botão **Configurações**.
  4. Na janela que é aberta, na guia **Desempenho**, na seção **Métodos de verificação**, marque a caixa **Análise heurística** e especifique o nível de detalhamento da verificação.

SELECIONANDO A TECNOLOGIA DE VERIFICAÇÃO DE ARQUIVOS

Além da análise heurística, você pode usar tecnologias específicas que permitem otimizar o desempenho da verificação de arquivos devido à exclusão de arquivos da verificação se eles não tiverem sido modificados desde a última verificação.

- *Para especificar as tecnologias de verificação de objetos:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
  3. Na seção **Nível de segurança** à direita da janela, clique no botão **Configurações**.
  4. Na janela que é aberta, na guia **Adicional**, na seção **Tecnologias de verificação**, selecione os valores desejados.

ALTERANDO A AÇÃO A SER EXECUTADA COM ARQUIVOS INFECTADOS

Se forem detectados objetos infectados, o aplicativo executará a ação selecionada.

- *Para alterar a ação que deve ser executada com objetos infectados:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
  3. À direita da janela, na seção **Ação ao detectar ameaça**, selecione a opção desejada.

VERIFICAÇÃO DE ARQUIVOS COMPOSTOS PELO ANTIVÍRUS DE ARQUIVOS

Um método comum para ocultar vírus é inseri-los em arquivos compostos: arquivos comprimidos, pacotes de instalação, objetos OLE inseridos e formatos de arquivos de email. Para detectar vírus que foram ocultados dessa maneira, é necessário descompactar os arquivos compostos, o que pode reduzir significativamente a velocidade da verificação.

Para cada tipo de arquivo composto, você pode optar por verificar todos os arquivos ou apenas os arquivos novos. Para selecionar, clique no link ao lado do nome do objeto. Seu valor é mudado quando você clica nele. Se você selecionar o modo de verificação apenas de arquivos novos e alterados, os links para definir a verificação de todos ou apenas de arquivos novos não estará disponível.

Por padrão, o Kaspersky Anti-Virus verifica apenas os objetos OLE inseridos.

Ao verificar arquivos compostos grandes, sua descompactação preliminar pode levar muito tempo. É possível reduzir esse período ativando a descompactação de arquivos compostos em segundo plano quando eles excederem o tamanho de arquivo especificado. Se for detectado um objeto malicioso enquanto você trabalha com esse arquivo, o aplicativo o notificará.

Você pode restringir o tamanho máximo do arquivo composto a ser verificado. Os arquivos compostos maiores que o tamanho especificado não serão verificados.

Quando arquivos grandes são extraídos de arquivos comprimidos, eles são verificados mesmo que a caixa **Não descompactar arquivos compostos grandes** esteja marcada.

- *Para modificar a lista de arquivos compostos a serem verificados:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
  3. Na seção **Nível de segurança** à direita da janela, clique no botão **Configurações**.
  4. Na janela que é aberta, na guia **Desempenho**, na seção **Verificação de arquivos compostos**, selecione os tipos de arquivos compostos que devem ser verificados.

- *Para definir o tamanho máximo dos arquivos compostos a serem verificados:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
  3. Na seção **Nível de segurança** à direita da janela, clique no botão **Configurações**.
  4. Na janela que é aberta, na guia **Desempenho**, na seção **Verificação de arquivos compostos**, clique no botão **Adicional**.
  5. Na janela **Arquivos compostos**, marque a caixa **Não descompactar arquivos compostos grandes** e especifique o tamanho máximo de arquivo.

- *Para descompactar arquivos compostos grandes em segundo plano:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
  3. Na seção **Nível de segurança** à direita da janela, clique no botão **Configurações**.
  4. Na janela que é aberta, na guia **Desempenho**, na seção **Verificação de arquivos compostos**, clique no botão **Adicional**.
  5. Na janela **Arquivos compostos**, marque a caixa **Extrair arquivos compostos em segundo plano** e especifique o tamanho mínimo de arquivo.

OTIMIZANDO A VERIFICAÇÃO DE ARQUIVOS

Você pode reduzir o tempo de verificação e aumentar a velocidade do Kaspersky Anti-Virus. Isso é possível verificando apenas os arquivos novos e aqueles que foram alterados desde a última vez que foram verificados. Esse modo se aplica a arquivos simples e compostos.

Para verificar somente arquivos novos e alterados:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Arquivos**.
3. Clique no botão **Configurações** à direita da janela.
4. Na janela que é aberta, na guia **Desempenho**, na seção **Otimização da verificação**, marque a caixa **Verificar somente arquivos novos e alterados**.

ANTIVÍRUS DE EMAIL

O Antivírus de Email verifica as mensagens enviadas e recebidas quanto à presença de objetos maliciosos. Ele abre ao iniciar o sistema operacional, sendo executado continuamente, verificando todos os emails enviados ou recebidos através dos protocolos POP3, SMTP, IMAP, MAPI e NNTP, além das conexões seguras (SSL) por POP3 e IMAP (consulte a seção "Verificação de conexões criptografadas" na página 88).

O indicador de operação do componente é o ícone do aplicativo na área de notificação da barra de tarefas, que tem a seguinte aparência  sempre que um email é verificado.

O Antivírus de Email intercepta e verifica cada email enviado ou recebido pelo usuário. Se não for detectada nenhuma ameaça no email, ele será disponibilizado para o usuário.

Você pode especificar os tipos de mensagens que devem ser verificados e selecionar o nível de segurança (veja a página 75) (configurações que afetam a profundidade da verificação).

Por padrão, a *análise de assinaturas* – um modo que usa os registros dos bancos de dados do aplicativo para procurar ameaças – está sempre ativada. Além disso, você pode ativar a análise heurística. E pode ativar a filtragem de anexos (veja a página 76), que permite renomear ou excluir automaticamente determinados tipos de arquivos.

Se for detectada uma ameaça em um arquivo, o Kaspersky Anti-Virus atribuirá um dos seguintes status ao arquivo:

- Status que designa o tipo do programa malicioso detectado (por exemplo, *vírus*, *cavalo de Troia*).
- *Possivelmente infectado* (suspeito), quando a verificação não puder determinar se o arquivo está infectado ou não. O arquivo pode conter uma sequência de código típica de vírus e outros malwares, ou o código modificado de um vírus conhecido.

Depois disso, o aplicativo bloqueia o email, exibe na tela uma notificação (veja a página 107) sobre a ameaça detectada e executa a ação especificada nas configurações do Antivírus de Email. Você pode alterar as ações que devem ser executadas ao detectar uma ameaça (consulte a seção "Alterando a ação a ser executada com emails infectados" na página 75).

Se você estiver trabalhando no modo automático (consulte a seção "Selecionando um modo de proteção" na página 56) quando forem detectados objetos perigosos, o Kaspersky Anti-Virus aplicará as ações recomendadas pelos especialistas da Kaspersky Lab automaticamente. Para objetos maliciosos, a ação é **Desinfetar. Excluir se a desinfecção falhar** e, para objetos suspeitos, é **Mover para a Quarentena**. Se forem detectados objetos perigosos ao trabalhar no modo interativo (consulte a seção "Selecionando um modo de proteção" na página 56), o aplicativo exibirá uma notificação na tela que poderá ser usada para selecionar a ação desejada na lista de ações disponíveis.

Antes de tentar desinfetar ou excluir um objeto infectado, o Kaspersky Anti-Virus cria uma cópia de backup para posterior restauração ou desinfecção. Os objetos suspeitos (possivelmente infectados) são colocados em quarentena. Você pode ativar a verificação automática de objetos em quarentena após cada atualização.

Se a desinfecção for bem-sucedida, o email ficará disponível. Se a desinfecção falhar, o objeto infectado será excluído do email. O Antivírus de Email expande o assunto do email, adicionando um texto que notifica o usuário de que esse email foi processado pelo Kaspersky Anti-Virus.

É fornecido um plug-in integrado para o Microsoft Office Outlook que permite ajustar precisamente o programa de email.

Se você usa o The Bat!, o Kaspersky Anti-Virus poderá ser usado em conjunto com outros aplicativos antivírus. Então, as regras de processamento do tráfego de email são configuradas diretamente no The Bat! e têm prioridade sobre as configurações da proteção de email do Kaspersky Anti-Virus.

Ao trabalhar com outros programas de email conhecidos, incluindo o Microsoft Outlook Express/Windows Mail, o Mozilla Thunderbird, o Eudora e o Incredimail, o Antivírus de Email verifica os emails nos protocolos SMTP, POP3, IMAP e NNTP.

Ao trabalhar com o programa de email Thunderbird, as mensagens transferidas por IMAP não serão verificadas quanto à presença de vírus se forem usados filtros que movem as mensagens da pasta **Caixa de entrada**.

NESTA SEÇÃO:

ATIVANDO E DESATIVANDO O ANTIVÍRUS DE EMAIL

Por padrão, o Antivírus de Email está ativado e é executado no modo recomendado pelos especialistas da Kaspersky Lab. Se necessário, você pode desativar o Antivírus de Email.

Para desativar o Antivírus de Email:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Email**.
3. À direita da janela, desmarque a caixa **Ativar Antivírus de Email**.

CRIANDO O ESCOPO DE PROTEÇÃO DO ANTIVÍRUS DE EMAIL

O escopo de proteção compreendem os tipos de emails a serem verificados, os protocolos cujo tráfego é verificado pelo Kaspersky Anti-Virus e as configurações de integração do Antivírus de Email no sistema.

Por padrão, o Kaspersky Anti-Virus é integrado ao Microsoft Office Outlook e ao The Bat!, verifica os emails enviados e recebidos e verifica o tráfego nos protocolos de email POP3, SMTP, NNTP e IMAP.

Para desativar a verificação de emails enviados:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Email**.
3. Clique no botão **Configurações** à direita da janela.
4. Use a guia **Geral** na seção **Escopo de proteção** da janela exibida para selecionar a opção **Apenas mensagens recebidas**.

Se você tiver selecionado a verificação apenas de mensagens recebidas, é recomendável verificar os emails enviados ao executar o Kaspersky Anti-Virus pela primeira vez, pois seu computador pode estar infectados com worms de email, que usam seu email para se desenvolver e disseminar. A verificação dos emails enviados evita problemas ocorridos devido ao envio descontrolado de emails do seu computador.

Para selecionar os protocolos que devem ser verificados e as configurações para integrar o Antivírus de Email ao sistema:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Email**.
3. Clique no botão **Configurações** à direita da janela.
4. Na janela que é aberta, na guia **Adicional**, na seção **Conectividade**, selecione as configurações desejadas.

ALTERANDO E RESTAURANDO O NÍVEL DE SEGURANÇA DE EMAIL

Dependendo das suas necessidades atuais, você pode selecionar um dos níveis predefinidos de segurança de email ou configurar você mesmo o Antivírus de Email.

A Kaspersky Lab recomenda não configurar o Antivírus de Email sozinho. Na maioria dos casos, basta selecionar outro nível de segurança.

Ao configurar o Antivírus de Email, você pode restaurar os valores recomendados a qualquer momento. Essas configurações são consideradas ideais, são recomendadas pela Kaspersky Lab e estão agrupadas no nível de segurança **Recomendado**.

- *Para alterar o nível de segurança de email atual:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Email**.
  3. À direita da janela, na seção **Nível de segurança**, defina o nível de segurança necessário ou clique no botão **Configurações** para modificar as configurações manualmente.

     Se você modificar as configurações manualmente, o nome do nível de segurança será alterado para **Personalizado**.

- *Para restaurar as configurações de proteção de email padrão:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Email**.
  3. Clique no botão **Nível padrão** na seção **Nível de segurança** à direita da janela.

USANDO A ANÁLISE HEURÍSTICA AO TRABALHAR COM O ANTIVÍRUS DE EMAIL

Durante o funcionamento do Antivírus de Email, a *análise de assinaturas* é usada sempre: O Kaspersky Anti-Virus compara o objeto encontrado com os registros do banco de dados.

Para melhorar a eficiência da proteção, você pode usar a *análise heurística* (ou seja, a análise da atividade que um objeto executa no sistema). Essa análise permite detectar novos objetos maliciosos que ainda não estão descritos nos bancos de dados.

- *Para ativar a análise heurística:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Email**.
  3. Na seção **Nível de segurança** à direita da janela, clique no botão **Configurações**.
  4. Na janela que é aberta, na guia **Geral**, na seção **Métodos de verificação**, marque a caixa **Análise Heurística** e especifique o nível de detalhamento da verificação.

ALTERANDO A AÇÃO A SER EXECUTADA COM EMAILS INFECTADOS

Se forem detectados objetos infectados, o aplicativo executará a ação selecionada.

- *Para alterar a ação que deve ser executada com emails infectados:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Email**.
  3. À direita da janela, na seção **Ação ao detectar ameaça**, selecione a opção desejada.

FILTRANDO ANEXOS EM EMAILS

Os programas maliciosos podem se disseminar por email, como anexos nas mensagens. Você pode configurar a filtragem por tipo de anexo nos emails, o que permite renomear ou excluir arquivos de tipos especificados automaticamente.

Para configurar a filtragem de anexos:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Email**.
3. Clique no botão **Configurações** à direita da janela.
4. Use a guia **Filtro de anexos** na janela exibida para selecionar o modo de filtragem dos anexos. Ao selecionar algum dos dois últimos modos, a lista de tipos de arquivos (extensões) será ativada; nela, você poderá selecionar os tipos desejados ou adicionar uma nova máscara de tipos.

   Para adicionar uma máscara de um novo tipo à lista, clique no link **Adicionar** para abrir a janela **Inserir máscara de nomes de arquivos** e insira as informações desejadas.

VERIFICAÇÃO DE ARQUIVOS COMPOSTOS PELO ANTIVÍRUS DE EMAIL

Um método comum para ocultar vírus é inseri-los em arquivos compostos: arquivos comprimidos, pacotes de instalação, objetos OLE inseridos e formatos de arquivos de email. Para detectar vírus que foram ocultados dessa maneira, é necessário descompactar os arquivos compostos, o que pode reduzir significativamente a velocidade da verificação.

Você pode ativar ou desativar a verificação de arquivos compostos e limitar o tamanho máximo dos arquivos compostos a serem verificados.

Se o computador não estiver protegido por nenhum software de rede local (o acesso à Internet for direto, sem um servidor proxy ou um firewall), é recomendável não desativar a verificação de arquivos compostos.

Para configurar a verificação de arquivos compostos:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de Email**.
3. Clique no botão **Configurações** à direita da janela.
4. Use a guia **Geral** na janela que é aberta para definir as configurações desejadas.

VERIFICAÇÃO DE EMAIL NO MICROSOFT OFFICE OUTLOOK

Ao instalar o Kaspersky Anti-Virus, um plug-in especial é integrado ao Microsoft Office Outlook. Ele permite alternar rapidamente à configuração do Antivírus de Email a partir do Microsoft Office Outlook e determinar quando os emails devem ser verificados quanto à presença de vírus e outros riskwares, e se isso deve ser feito ao receber, abrir ou enviar uma mensagem.

A configuração do Antivírus de Email a partir do Microsoft Office Outlook estará disponível se essa opção estiver selecionada nas configurações do escopo de proteção do Antivírus de Email.

Para alternar para as configurações de verificação de email no Microsoft Office Outlook:

1. Abra a janela principal do Microsoft Office Outlook.
2. Selecione **Ferramentas** → **Opções** no menu do aplicativo.
3. Na janela **Configurações** que é aberta, selecione a guia **Proteção de email**.

VERIFICAÇÃO DE EMAIL NO THE BAT!

As ações referentes a objetos de email infectados no The Bat! são definidas usando as ferramentas do próprio aplicativo.

As configurações do Antivírus de Email que determinam se as mensagens enviadas e recebidas devem ser verificadas, quais ações devem ser executadas com objetos perigosos em emails e quais exclusões devem ser aplicadas são ignoradas. A única opção que o The Bat! considera é a verificação de arquivos comprimidos anexos.

As configurações da proteção de email se estendem a todos os componentes antivírus instalados no computador compatíveis com o The Bat!

Os emails recebidos são verificados primeiro pelo Antivírus de Email e somente depois pelo plug-in do The Bat! Se for detectado um objeto malicioso, o Kaspersky Anti-Virus o notificará imediatamente sobre isso. Se você selecionar a ação **Desinfetar (Excluir)** na janela de notificações do Antivírus de Email, as ações para eliminar a ameaça serão executadas pelo Antivírus de Email. Se você selecionar a ação **Ignorar** na janela de notificações, o objeto será desinfetado pelo plug-in do The Bat! Ao enviar mensagens de email, a verificação é executada primeiro pelo plug-in e depois pelo Antivírus de Email.

As configurações do Antivírus de Email estarão disponíveis no The Bat! se essa opção estiver selecionada nas configurações do escopo de proteção do Antivírus de Email.

Para configurar a verificação de email no The Bat!, você deve definir os seguintes critérios:

- os fluxos de email (enviados, recebidos) que devem ser verificados;
- quando os objetos de email devem ser verificados (ao abrir um a mensagem, antes de salvá-la no disco);
- as ações que devem ser executadas pelo programa de email caso sejam detectados objetos perigosos nos emails. Por exemplo, você pode selecionar:
  - **Attempt to disinfect infected parts** – se esta opção estiver selecionada, será feita uma tentativa de desinfetar o objeto infectado e, se isso não for possível, ele permanecerá na mensagem.
  - **Delete infected parts** – se esta opção estiver selecionada, o objeto perigoso na mensagem será excluído, independentemente de ele estar infectado ou de haver uma suspeita de que esteja infectado.

Por padrão, o The Bat! coloca todos os objetos de email infectados na Quarentena sem tentar desinfetá-los.

Os emails que contêm objetos perigosos não são marcados com o complemento de assunto especial quando verificados pelo plug-in do The Bat!

Para alternar para as configurações de verificação de email no The Bat!:

1. Abra a janela principal do The Bat!
2. No menu **Propriedades**, selecione **Configurações**.
3. Selecione o objeto **Virus protection** na árvore de configurações.

ANTIVÍRUS DA WEB

Cada vez que você trabalha na Internet, coloca as informações armazenadas no computador em perigo, expondo-as a risco de serem infectadas por vírus e outros malwares. Eles podem invadir o computador quando você baixa aplicativos gratuitos ou exibe informações em sites que foram atacados por hackers antes de sua visita. Além disso, os worms de rede podem invadir seu computador antes que você abra uma página da Web ou baixe um arquivo, no momento que o computador estabelecer uma conexão com a Internet.

O Antivírus da Web protege as informações recebidas pelo computador e enviados dele através dos protocolos HTTP, HTTPS e FTP, e evita que scripts perigosos sejam executados no computador.

O Antivírus da Web monitora apenas o tráfego da Web transferido pelas portas especificadas na lista de portas monitoradas. Uma lista das portas monitoradas mais usadas para a transferência de dados é incluída no kit de distribuição do Kaspersky Anti-Virus. Se você usar portas que não estão incluídas na lista de portas monitoradas, adicione-as à lista de portas monitoradas (consulte a seção "Criando uma lista de portas monitoradas" na página 90) para garantir a proteção do tráfego da Web transferido por meio delas.

O Antivírus da Web o tráfego da Web em relação uma coleção específica de configurações denominada nível de segurança. Se o Antivírus da Web detectar uma ameaça, ele executará a ação definida. Os objetos maliciosos são detectados usando os bancos de dados e o algoritmo heurístico do Kaspersky Anti-Virus.

A Kaspersky Lab recomenda não configurar o Antivírus da Web sozinho. Na maioria dos casos, basta selecionar o nível de segurança apropriado.

Algoritmo de verificação do tráfego da Web

Cada página da Web ou arquivo que é acessado pelo usuário ou por um aplicativo através dos protocolos HTTP, HTTPS ou FTP é interceptado e verificado pelo Antivírus da Web quanto à presença de código malicioso:

- Se uma página da Web ou um arquivo acessado pelo usuário contiver código malicioso, seu acesso será bloqueado. É exibida uma notificação de que o arquivo ou a página da Web solicitada está infectada.
- Se o arquivo ou a página da Web não contiver código malicioso, o programa concederá acesso a ele imediatamente.

Algoritmo de verificação de scripts

Cada script executado é interceptado pelo Antivírus da Web e analisado quanto à presença de código malicioso:

- Se um script contiver código malicioso, o Antivírus da Web o bloqueará e exibirá uma notificação na tela.
- Se nenhum código malicioso for descoberto no script, ele será executado.

O Antivírus da Web intercepta somente os scripts baseados na funcionalidade do Microsoft Windows Script Host.

NESTA SEÇÃO:

ATIVANDO E DESATIVANDO O ANTIVÍRUS DA WEB

Por padrão, o Antivírus da Web está ativado e é executado no modo recomendado pelos especialistas da Kaspersky Lab. Se necessário, você pode desativar o Antivírus da Web.

Para desativar o Antivírus da Web:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
3. À direita da janela, desmarque a caixa **Ativar Antivírus da Web**.

ALTERANDO E RESTAURANDO O NÍVEL DE SEGURANÇA DO TRÁFEGO DA WEB

Dependendo das suas necessidades atuais, você pode selecionar um dos níveis de segurança do tráfego da Web predefinidos ou configurar você mesmo o Antivírus da Web.

Ao configurar o Antivírus da Web, você pode restaurar os valores recomendados a qualquer momento. Essas configurações são consideradas ideais, são recomendadas pela Kaspersky Lab e estão agrupadas no nível de segurança **Recomendado**.

- *Para alterar o nível de segurança do tráfego da Web:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
  3. À direita da janela, na seção **Nível de segurança**, defina o nível de segurança necessário ou clique no botão **Configurações** para modificar as configurações manualmente.

  Se você modificar as configurações manualmente, o nome do nível de segurança será alterado para **Personalizado**.

- *Para restaurar o nível de segurança do tráfego da Web padrão:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
  3. Clique no botão **Nível padrão** na seção **Nível de segurança** à direita da janela.

ALTERANDO A AÇÃO A SER EXECUTADA COM OBJETOS PERIGOSOS DO TRÁFEGO DA WEB

Se forem detectados objetos infectados, o aplicativo executará a ação selecionada.

O Antivírus da Web sempre bloqueia ações de scripts perigosos e exibe mensagens que informam o usuário sobre a ação executada. Não é possível alterar a ação a ser executada com um script perigoso; você pode apenas desativar a verificação de scripts (consulte a seção "Bloqueando scripts perigosos" na página 81).

- *Para alterar a ação a ser executada com os objetos detectados:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
  3. À direita da janela, na seção **Ação ao detectar ameaça**, selecione a opção desejada.

VERIFICANDO URLS EM PÁGINAS DA WEB

A verificação de páginas da Web quanto à presença de phishing permite evitar *ataques de phishing*. Normalmente, os ataques de phishing consistem em emails de supostas organizações financeiras que contêm URLs dos sites dessas organizações. O email convence o leitor a clicar no URL e inserir informações particulares na janela que é aberta; por exemplo, o número de um cartão bancário ou o login e a senha de uma conta bancária online. Um ataque de phishing pode ser disfarçado, por exemplo, como uma carta de seu banco com um link para o site oficial da instituição. Ao clicar no link, você é direcionado para uma cópia exata do site do banco e pode até ver seu endereço no navegador, embora esteja em um site falso. Desse momento em diante, todas as suas ações no site são rastreadas e podem ser usadas para roubá-lo.

Como os links para sites de phishing podem ser recebidos de outras fontes além dos emails, como mensagens do ICQ, o Antivírus da Web monitora as tentativas de acessar um site de phishing no nível do tráfego da Web e bloqueia o acesso a esses locais.

Além dos bancos de dados do Kaspersky Anti-Virus, a análise heurística (veja a página 81) também pode ser usada para verificar as páginas da Web quanto à presença de phishing.

NESTA SEÇÃO:

ATIVANDO E DESATIVANDO A VERIFICAÇÃO DE URLS

- *Para ativar a verificação de URLs usando os bancos de dados de endereços suspeitos e de phishing:*

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
3. Clique no botão **Configurações** à direita da janela.

   A janela **Antivírus da Web** é aberta.
4. Na guia **Geral**, na seção **Consultor de URLs Kaspersky**, marque as caixas **Verificar se os URLs estão listados no banco de dados de URLs suspeitos** e **Verificar páginas da Web quanto à presença de phishing**.

USANDO O CONSULTOR DE URLS KASPERSKY

O Consultor de URLs Kaspersky é integrado ao Microsoft Internet Explorer, ao Mozilla Firefox e ao Google Chrome como um plug-in.

O Consultor de URLs Kaspersky verifica todos os URLs em uma página da Web para descobrir se eles estão incluídos na lista de URLs suspeitos. Ele também os verifica quanto à presença de phishing, realçando cada um na janela do navegador.

Você pode criar uma lista de sites nos quais todos os URLs devem ser verificados, verificar URLs em todos os sites exceto aqueles incluídos na lista de exclusões, verificar URLs somente em resultados de pesquisas ou especificar categorias de sites com URLs que devem ser verificados.

Você pode configurar o Consultor de URLs Kaspersky na janela de configurações do aplicativo e também na janela de configurações do Consultor de URLs Kaspersky disponível no navegador da Web.

- *Para especificar os sites nos quais todos os URLs devem ser verificados:*

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
3. Clique no botão **Configurações** à direita da janela.
4. A janela **Antivírus da Web** é aberta.
5. Na guia **Navegação Segura**, na seção **Consultor de URLs Kaspersky**, marque a caixa **Verificar URLs**.
6. Selecione os sites nos quais os links devem ser verificados:
   a. Se desejar criar uma lista de sites nos quais todos os URLs devem ser verificados, selecione **Apenas os sites da lista** e clique no botão **Especificar**. Na janela **URLs verificados** que é aberta, crie uma lista de sites a serem verificados.
   b. Se desejar verificar URLs em todos os sites exceto os especificados, selecione **Todos, exceto as exclusões** e clique no botão **Exclusões**. Na janela **Exclusões** que é aberta, crie uma lista de sites nos quais não é necessário verificar URLs.

- *Para verificar URLs somente nos resultados de pesquisas:*

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
3. Clique no botão **Configurações** à direita da janela.
4. A janela **Antivírus da Web** é aberta.
5. Na guia **Navegação Segura**, na seção **Consultor de URLs Kaspersky**, marque a caixa **Verificar URLs** e clique no botão **Configurações**.
6. Na janela **Configurações do Consultor de URLs Kaspersky** que é aberta, na seção **Modo de verificação**, selecione **Apenas os URLs dos resultados da pesquisa**.

- *Para selecionar as categorias de sites com URLs que devem ser verificados:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
  3. Clique no botão **Configurações** à direita da janela.
  4. A janela **Antivírus da Web** é aberta.
  5. Na guia **Navegação Segura**, na seção **Consultor de URLs Kaspersky**, marque a caixa **Verificar URLs** e clique no botão **Configurações**.
  6. Na janela **Configurações do Consultor de URLs Kaspersky** que é aberta, na seção **Categorias de sites**, marque a caixa **Mostrar informações sobre as categorias de conteúdo de sites**.
  7. Na lista de categorias, marque as caixas ao lado das categorias de sites com URLs que devem ser verificados.

- *Para abrir a janela de configurações do Consultor de URLs Kaspersky no navegador da Web,*

  clique no botão com o ícone do Kaspersky Anti-Virus na barra de ferramentas do navegador.

USANDO A ANÁLISE HEURÍSTICA AO TRABALHAR COM O ANTIVÍRUS DA WEB

Para melhorar a eficiência da proteção, você pode usar a *análise heurística* (ou seja, a análise da atividade que um objeto executa no sistema). Essa análise permite detectar novos objetos maliciosos que ainda não estão descritos nos bancos de dados.

Quando o Antivírus da Web está em execução, você pode ativar a análise heurística separadamente para verificar o tráfego da Web e para verificar phishing nas páginas da Web.

- *Para ativar a análise heurística para verificar o tráfego da Web:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
  3. Clique no botão **Configurações** à direita da janela.

     A janela **Antivírus da Web** é aberta.
  4. Na guia **Geral**, na seção **Análise Heurística**, marque a caixa **Usar a Análise Heurística** e defina o nível de detalhamento da verificação.

- *Para ativar a análise heurística para verificar phishing nas páginas da Web:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
  3. Clique no botão **Configurações** à direita da janela.

     A janela **Antivírus da Web** é aberta.
  4. Na guia **Geral**, na seção **Consultor de URLs Kaspersky**, clique no botão **Adicional**.
  5. Na janela **Configurações do Antiphishing** que é aberta, marque a caixa **Usar a Análise Heurística para verificar páginas da Web quanto à presença de phishing** e defina o nível de detalhamento da verificação.

BLOQUEANDO SCRIPTS PERIGOSOS

O Antivírus da Web verifica todos os scripts processados no Microsoft Internet Explorer e também todos os outros scripts WSH (por exemplo, JavaScript, Visual Basic Script, etc.) executados enquanto você trabalha no computador. Se um script representar uma ameaça para o computador, ele será bloqueado.

Para desativar o bloqueio de scripts perigosos:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
3. Clique no botão **Configurações** à direita da janela.

   A janela **Antivírus da Web** é aberta.
4. Na guia **Geral**, na seção **Adicional**, desmarque a caixa **Bloquear scripts perigosos no Microsoft Internet Explorer**.

OTIMIZAÇÃO DA VERIFICAÇÃO

Para melhorar a eficiência de detecção de código malicioso, o Antivírus da Web usa o armazenamento em cache dos fragmentos de objetos recebidos da Internet. Usando o cache, o Antivírus da Web verifica os objetos somente depois que eles são inteiramente recebidos no computador.

O armazenamento em cache aumenta o tempo necessário para processar objetos e passá-los para o usuário para as outras operações. O armazenamento em cache pode gerar problemas ao baixar ou processar objetos grandes, pois a conexão com o cliente HTTP pode atingir o tempo limite.

Você pode solucionar esse problema usando a opção de limitar o armazenamento em cache de fragmentos de objetos recebidos da Internet. Quando um determinado intervalo de tempo expirar, cada fragmento de um objeto é passado para o usuário sem ser verificado. Quando a cópia for concluída, o objeto será inteiramente verificado. Isso permite reduzir o tempo necessário para passar os objetos para o usuário e solucionar o problema de perda de conexão. O nível de segurança da Internet não é reduzido.

Ao aumento das restrições sobre a duração do armazenamento em cache do tráfego da Web melhora a eficiência das verificações de vírus, mas pode tornar o acesso aos objetos mais lento.

Para definir ou remover o limite de tempo de buffer de fragmentos:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
3. Clique no botão **Configurações** à direita da janela.

   A janela **Antivírus da Web** é aberta.
4. Na guia **Geral**, na seção **Adicional**, marque a caixa **Limitar o tempo de cache do tráfego a 1 seg. para otimizar a verificação**.

CRIANDO UMA LISTA DE ENDEREÇOS CONFIÁVEIS

O Antivírus da Web não verifica objetos perigoso no tráfego da Web, se ele vier de URLs confiáveis.

Para criar uma lista de endereços confiáveis:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus da Web**.
3. Clique no botão **Configurações** à direita da janela.

   A janela **Antivírus da Web** é aberta.
4. Na guia **URLs confiáveis**, marque a caixa **Não verificar o tráfego da Web de URLs confiáveis**.
5. Crie uma lista de sites/páginas da Web com conteúdo no qual você confia. Para fazê-lo:
   a. Clique no botão **Adicionar**.

      A janela **Máscara de endereços (URL)** será aberta.
   b. Insira o endereço de um site/uma página da Web ou a máscara de endereços de um site/uma página da Web.
   c. Clique no botão **OK**.

      Um novo registro é exibido na lista de URLs confiáveis.
6. Se necessário, repita as etapas de a até c.

ANTIVÍRUS DE IM

O Antivírus de IM verifica o tráfego de programas de mensagens instantâneas (os chamados *mensageiros da Internet*).

As mensagens instantâneas podem conter links para sites suspeitos e para sites usados por hackers para organizar ataques de phishing. Programas maliciosos usam programas de IM para enviar spam e links para os programas (ou os próprios programas), que roubam números de ID e senhas dos usuários.

O Kaspersky Anti-Virus garante a operação segura de vários aplicativos de mensagens instantâneas, incluindo ICQ, MSN, AIM, Yahoo! Messenger, Jabber, Google Talk, Mail.Ru Agent e IRC.

Alguns programas de IM, como Yahoo! Messenger e Google Talk, usam conexões criptografadas. Para verificar o tráfego gerado por esses programas, é necessário ativar a verificação de conexões criptografadas (veja a página 88).

O Antivírus de IM intercepta as mensagens e as verifica quanto à presença de objetos ou URLs perigosos. Você pode selecionar os tipos de mensagens que devem ser verificados e vários métodos de verificação.

Se forem detectadas ameaças em uma mensagem, o Antivírus de IM substitui a mensagem por um aviso para o usuário.

Os arquivos transferidos pelos programas de mensagens instantâneas são verificados pelo componente Antivírus de Arquivos (na página 68) quando ocorrem tentativas de salvá-los.

NESTA SEÇÃO:

ATIVANDO E DESATIVANDO O ANTIVÍRUS DE IM

Por padrão, o Antivírus de IM está ativado e funciona no modo normal. Se necessário, você pode desativar o Antivírus de IM.

Para desativar o Antivírus de IM:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de IM**.
3. À direita da janela, desmarque a caixa **Ativar Antivírus de IM**.

CRIANDO O ESCOPO DE PROTEÇÃO DO ANTIVÍRUS DE IM

O escopo de proteção consiste nos tipos de mensagens que devem ser verificados. Por padrão, o Kaspersky Anti-Virus verifica as mensagens enviadas e recebidas. Se tiver certeza de que as mensagens enviadas por você não contêm objetos perigosos, você pode desativar a verificação do tráfego de saída.

Para desativar a verificação de mensagens enviadas:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de IM**.
3. À direita da janela, na seção **Escopo de proteção**, selecione a opção **Apenas mensagens recebidas**.

VERIFICANDO URLS EM MENSAGENS DE PROGRAMAS DE IM

Para verificar as mensagens quanto à presença de URLs suspeitos e de phishing:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de IM**.
3. À direita da janela, na seção **Métodos de verificação**, marque as caixas **Verificar se os URLs estão listados no banco de dados de URLs suspeitos** e **Verificar se os URLs estão listados no banco de dados de URLs de phishing**.

USANDO A ANÁLISE HEURÍSTICA AO TRABALHAR COM O ANTIVÍRUS DE IM

Para melhorar a eficiência da proteção, você pode usar a *análise heurística* (ou seja, a análise da atividade que um objeto executa no sistema). Essa análise permite detectar novos objetos maliciosos que ainda não estão descritos nos bancos de dados.

Ao usar a análise heurística, todos os scripts incluídos em mensagens instantâneas são executados em um ambiente protegido. Se as atividades do script forem típicas de objetos maliciosos, provavelmente o objeto será classificado como malicioso ou suspeito. Por padrão, a análise heurística está ativada.

Para ativar a análise heurística:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Antivírus de IM**.
3. À direita da janela, na seção **Métodos de verificação**, marque a caixa **Análise Heurística** e defina o nível de detalhamento de verificação desejado.

DEFESA PROATIVA

A Defesa Proativa protege o computador contra novas ameaças que ainda não foram incluídas nos bancos de dados do Kaspersky Anti-Virus.

O funcionamento da Defesa Proativa se baseia em tecnologias proativas. As tecnologias proativas permitem neutralizar uma nova ameaça antes que ela danifique o computador. Diferentemente das tecnologias responsivas, que analisam o código com base nos registros dos bancos de dados do Kaspersky Anti-Virus, as tecnologias preventivas reconhecem uma nova ameaça no computador por meio da sequência de ações executadas pelo programa. Se, como resultado da análise de atividades, a sequência de ações do aplicativo for considerada suspeita, o Kaspersky Anti-Virus bloqueará a atividade desse aplicativo.

Por exemplo, quando forem detectadas ações como o programa copiar a si mesmo em recursos de rede, na pasta de inicialização ou no Registro do sistema, é muito provável que se trate de um worm.

As sequências de ações perigosas também incluem tentativas de modificar o arquivo HOSTS, a instalação oculta de drivers, etc. Você pode desativar o monitoramento (veja a página 85) de atividades perigosas ou editar suas regras de monitoramento (veja a página 85).

Você pode criar um grupo de aplicativos confiáveis (veja a página 85) para a Defesa Proativa. Você não será notificado sobre as atividades desses aplicativos.

Se o computador executar o Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 7 ou o Microsoft Windows 7 x64, o controle não se aplicará a todos os eventos. Isso se deve a recursos específicos desses sistemas operacionais. Por exemplo, o controle não se aplicará integralmente ao envio de dados por meio de aplicativos confiáveis e às atividades suspeitas do sistema.

NESTA SEÇÃO:

ATIVANDO E DESATIVANDO A DEFESA PROATIVA

Por padrão, a Defesa Proativa está ativada e é executada no modo recomendado pelos especialistas da Kaspersky Lab. Se necessário, você pode desativar a Defesa Proativa.

Para desativar a Defesa Proativa:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Defesa Proativa**.
3. À direita da janela, desmarque a caixa **Ativar Defesa Proativa**.

CRIANDO UM GRUPO DE APLICATIVOS CONFIÁVEIS

Você pode criar um grupo de aplicativos confiáveis cujas atividades não devem ser controladas pela Defesa Proativa. Por padrão, a lista de aplicativos confiáveis inclui aplicativos com assinaturas digitais verificadas e aplicativos confiáveis do banco de dados do Kaspersky Security Network.

Para alterar as configurações do grupo de aplicativos confiáveis:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Defesa Proativa**.
3. À direita da janela, na seção **Aplicativos confiáveis**, execute as seguintes ações:
   - Se desejar que os aplicativos com assinaturas digitais verificadas sejam incluídos no grupo de aplicativos confiáveis, marque a caixa **Aplicativos com assinatura digital**.
   - Se desejar que os aplicativos confiáveis de acordo com o banco de dados do Kaspersky Security Network sejam incluídos no grupo de aplicativos confiáveis, marque a caixa **Confiável no banco de dados do Kaspersky Security Network**.

USANDO A LISTA DE ATIVIDADES PERIGOSAS

Não é possível editar a lista de ações típicas de atividade perigosa. Entretanto, você pode se recusar a controlar um caso selecionado de atividade perigosa.

Para desativar o monitoramento de algumas atividades perigosas:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Defesa Proativa**.
3. Clique no botão **Configurações** à direita da janela.
4. Na janela **Defesa Proativa** que é aberta, desmarque a caixa ao lado do tipo de atividade que você não deseja monitorar.

ALTERANDO A AÇÃO QUE DEVE SER EXECUTADA COM A ATIVIDADE PERIGOSA DE APLICATIVOS

Não é possível editar a lista de ações típicas de atividade perigosa. No entanto, você pode alterar a ação executada pelo Kaspersky Anti-Virus ao detectar atividades perigosas do aplicativo.

Para alterar a ação executada pelo aplicativo da Kaspersky Lab em relação à atividade perigosa de outro aplicativo:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Defesa Proativa**.
3. Clique no botão **Configurações** à direita da janela.
4. Na janela **Defesa Proativa** que é aberta, na coluna **Evento**, selecione o evento cuja regra você deseja editar.
5. Configure o evento selecionado usando os links na seção **Descrição da regra**. Por exemplo:
   a. Clique no link com a ação predefinida e, na janela **Selecionar ação** que é aberta, selecione a ação desejada.
   b. Clique no link **Ativado/Desativado** para indicar se deve ser criado um relatório de execução da operação.

INSPETOR DO SISTEMA

O Inspetor do Sistema coleta dados sobre as ações de aplicativos no computador e fornece informações a outros componentes para aperfeiçoar a proteção.

Com base nas informações coletadas pelo Inspetor do Sistema, o Kaspersky Anti-Virus pode reverter as ações executadas por programas maliciosos.

A reversão de ações executadas por programas maliciosos pode ser iniciada por um dos seguintes componentes de proteção:

- Inspetor do Sistema - com base nos padrões de atividades perigosas;
- Defesa Proativa;
- Antivírus de Arquivos;
- ao executar uma verificação de vírus.

Se forem detectadas eventos suspeitos no sistema, os componentes de proteção do Kaspersky Anti-Virus podem solicitar informações adicionais do Inspetor do Sistema. No modo de proteção interativa do Kaspersky Anti-Virus (consulte a seção "Selecionando um modo de proteção" na página 56), é possível exibir os dados coletados pelo componente Inspetor do Sistema e apresentados como um relatório do histórico de atividades perigosas. Esses dados podem ajudar a decidir sobre a seleção de uma ação na janela de notificações. Quando o componente detecta um programa malicioso, o link para o relatório do Inspetor do Sistema é exibido na parte superior da janela de notificações (veja a página 128), perguntando o que fazer.

NESTA SEÇÃO:

ATIVANDO E DESATIVANDO O INSPETOR DO SISTEMA

Por padrão, o Inspetor do Sistema está ativado e é executado no modo recomendado pelos especialistas da Kaspersky Lab. Se necessário, você pode desativar o Inspetor do Sistema.

É recomendável não desativar o componente, exceto quando absolutamente necessário, pois inevitavelmente isso reduz a eficiência da Defesa Proativa e de outros componentes de proteção que podem solicitar os dados coletados pelo Inspetor do Sistema para identificar a possível ameaça detectada.

Para desativar o Inspetor do Sistema:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Inspetor do Sistema**.
3. À direita da janela, desmarque a caixa **Ativar Inspetor do Sistema**.

USANDO PADRÕES DE ATIVIDADES PERIGOSAS (BSS)

Os padrões de atividades perigosas (BSS – Behavior Stream Signatures) contêm sequências de ações típicas de aplicativos considerados perigosos. Se a atividade de um aplicativo corresponder a um padrão de atividades perigosas, o Kaspersky Anti-Virus executará a ação definida.

Para oferecer proteção em tempo real eficiente, o Kaspersky Anti-Virus adiciona padrões de atividades perigosas que são usadas pelo Inspetor do Sistema durante as atualizações do banco de dados.

Por padrão, quando o Kaspersky Anti-Virus é executado no modo automático, se a atividade de um aplicativo corresponder a um padrão de atividades perigosas, o Inspetor do Sistema moverá o aplicativo para a Quarentena. Ao ser executado no modo interativo, o Inspetor do Sistema pergunta o que fazer. Você pode especificar a ação que deve ser executada pelo componente quando a atividade de um aplicativo corresponder a um padrão de atividades perigosas.

Além da correspondência exata entre atividades de aplicativos e padrões de atividades perigosas, o Inspetor do Sistema também detecta ações que correspondem parcialmente a padrões de atividades perigosas e que são consideradas suspeitas com base na análise heurística. Se forem detectadas atividades suspeitas, o Inspetor do Sistema perguntará o que fazer independentemente do modo de operação.

- *Para selecionar a ação que deve ser executada pelo componente quando a atividade de um aplicativo corresponder a um padrão de atividades perigosas:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Inspetor do Sistema**.
  3. À direita da janela, na seção **Análise Heurística**, marque a caixa **Usar padrões atualizáveis de atividade perigosa (BSS)**.
  4. Clique em **Selecionar ação** e especifique a ação desejada na lista suspensa.

REVERTENDO AS AÇÕES DE UM PROGRAMA MALICIOSO

Você pode usar a opção de reverter as ações executadas por malware no sistema. Para ativar uma reversão, o Inspetor do Sistema registra o histórico de atividades do programa. Você pode limitar o volume de informações armazenadas pelo Inspetor do Sistema para uma reversão.

Por padrão, o Kaspersky Anti-Virus reverte as operações relevantes automaticamente quando os componentes de proteção detectam atividade maliciosa. Ao ser executado no modo interativo, o Inspetor do Sistema pergunta o que fazer. Você pode especificar a ação que deve ser executada se estiver disponível uma reversão de ações executadas por um programa malicioso.

O procedimento de reverter operações de malware afeta um conjunto de dados definido rigidamente. Ele não tem consequências negativas para a integridade do sistema operacional ou dos dados no seu computador.

- *Para selecionar a ação que deve ser executada se estiver disponível uma reversão de ações executadas por um programa malicioso:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Inspetor do Sistema**.
  3. À direita da janela, na seção **Reversão de ações de malware**, escolha **Selecionar ação** e selecione a ação desejada na lista suspensa.

- *Para limitar o volume de informações armazenadas pelo Inspetor do Sistema para uma reversão:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Centro de Proteção**, selecione o componente **Inspetor do Sistema**.
  3. À direita da janela, na seção **Reversão de ações de malware**, marque a caixa **Limitar dados que devem ser armazenados para reversão** e especifique o volume máximo de dados que o Inspetor do Sistema deve armazenar para uma reversão.

PROTEÇÃO DE REDE

As ferramentas e configurações do Kaspersky Anti-Virus garantem em conjunto a segurança e o controle de suas atividades de rede.

As seções a seguir contêm informações detalhadas sobre a verificação de conexões de rede, configurações do servidor proxy e o monitoramento de portas de rede.

NESTA SEÇÃO:

VERIFICAÇÃO DE CONEXÕES CRIPTOGRAFADAS

As conexões que usam os protocolos SSL/TSL protegem o canal de troca de dados na Internet. Os protocolos SSL/TSL permitem identificar as partes que trocam dados usando certificados eletrônicos, codificar os dados transferidos e assegurar sua integridade durante a transferência.

Esses recursos do protocolo são usados por hackers para disseminar programas maliciosos, pois a maioria dos aplicativos antivírus não verifica o tráfego SSL/TSL.

O Kaspersky Anti-Virus verifica as conexões criptografadas usando um certificado da Kaspersky Lab.

Se for detectado um certificado inválido ao conectar-se com o servidor (por exemplo, se o certificado for substituído por um invasor), será exibida uma notificação pop-up com uma solicitação de aceitar ou rejeitar o certificado.

Se tiver certeza de que uma conexão com um site sempre é segura, apesar do certificado inválido, é possível adicionar o site à lista de URLs confiáveis. O Kaspersky Anti-Virus não verificará mais a conexão criptografada com esse site.

Você pode usar o Assistente para Instalação de Certificados para instalar um certificado para verificar conexões criptografadas no modo semi-interativo no Microsoft Internet Explorer, no Mozilla Firefox (se ele não for executado) e no Google Chrome, além de obter instruções sobre como instalar o certificado da Kaspersky Lab para o Opera.

Para ativar a verificação de conexões criptografadas e instalar o certificado da Kaspersky Lab:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione o componente **Rede**.
3. Na janela que é aberta, marque a caixa **Verificar conexões criptografadas**. Quando você ativar essa configuração pela primeira vez, o Assistente para Instalação de Certificados será executado automaticamente.
4. Se o assistente não for iniciado, clique no botão **Instalar certificado**. Será iniciado um Assistente com instruções a serem seguidas para a instalação bem-sucedida do certificado da Kaspersky Lab.

NESTA SEÇÃO:

VERIFICANDO CONEXÕES CRIPTOGRAFADAS NO MOZILLA FIREFOX

O navegador Mozilla Firefox não usa o armazenamento de certificados do Microsoft Windows. Para verificar conexões SSL ao usar o Firefox, você deve instalar o certificado da Kaspersky Lab manualmente.

Você poderá usar o Assistente para Instalação de Certificados, caso o navegador não seja executado.

- *Para instalar o certificado da Kaspersky Lab:*

  1. No menu do navegador, selecione **Ferramentas** → **Configurações**.
  2. Na janela que é aberta, selecione a seção **Adicional**.
  3. Na seção **Certificados**, selecione a guia **Segurança** e clique no botão **Exibir Certificados**.
  4. Na janela que é aberta, selecione a guia **Autoridades** e clique no botão **Restaurar**.
  5. Na janela que é aberta, selecione o arquivo do certificado da Kaspersky Lab. O caminho do arquivo do certificado da Kaspersky Lab é o seguinte: *%AllUsersProfile%\Dados de Aplicativos\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.*
  6. Na janela que é aberta, marque as caixas para selecionar as ações que devem ser verificadas com o certificado instalado. Para exibir as informações do certificado, clique no botão **Exibir**.

- *Para instalar manualmente o certificado da Kaspersky Lab para o Mozilla Firefox versão 3.x:*

  1. No menu do navegador, selecione **Ferramentas** → **Configurações**.
  2. Na janela que é aberta, selecione a seção **Adicional**.
  3. Na guia **Criptografia**, clique no botão **Exibir Certificados**.
  4. Na janela que é aberta, selecione a guia **Autoridades** e clique no botão **Importar**.
  5. Na janela que é aberta, selecione o arquivo do certificado da Kaspersky Lab. O caminho do arquivo do certificado da Kaspersky Lab é o seguinte: *%AllUsersProfile%\Dados de Aplicativos\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.*
  6. Na janela que é aberta, marque as caixas para selecionar as ações que devem ser verificadas com o certificado instalado. Para exibir as informações do certificado, clique no botão **Exibir**.

Se o computador for executado no Microsoft Windows Vista ou no Microsoft Windows 7, o caminho do arquivo do certificado da Kaspersky Lab será o seguinte: *%AllUsersProfile%\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.*

VERIFICANDO CONEXÕES CRIPTOGRAFADAS NO OPERA

O navegador Opera não usa o armazenamento de certificados do Microsoft Windows. Para verificar conexões SSL ao usar o Opera, você deve instalar o certificado da Kaspersky Lab manualmente.

- *Para instalar o certificado da Kaspersky Lab:*

  1. No menu do navegador, selecione **Ferramentas** → **Configurações**.
  2. Na janela que é aberta, selecione a seção **Adicional**.
  3. À esquerda da janela, selecione a guia **Segurança** e clique no botão **Gerenciar Certificados**.
  4. Na janela que é aberta, selecione a guia **Fornecedores** e clique no botão **Importar**.
  5. Na janela que é aberta, selecione o arquivo do certificado da Kaspersky Lab. O caminho do arquivo do certificado da Kaspersky Lab é o seguinte: *%AllUsersProfile%\Dados de Aplicativos\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.*
  6. Na janela que é aberta, clique no botão **Instalar**. O certificado da Kaspersky Lab será instalado. Para exibir as informações do certificado e selecionar as ações para as quais ele será usado, selecione o certificado na lista e clique no botão **Exibir**.

- *Para instalar o certificado da Kaspersky Lab para o Opera versão 9.x:*

  1. No menu do navegador, selecione **Ferramentas** → **Configurações**.
  2. Na janela que é aberta, selecione a seção **Adicional**.
  3. À esquerda da janela, selecione a guia **Segurança** e clique no botão **Gerenciar Certificados**.
  4. Na janela que é aberta, selecione a guia **Autoridades** e clique no botão **Importar**.
  5. Na janela que é aberta, selecione o arquivo do certificado da Kaspersky Lab. O caminho do arquivo do certificado da Kaspersky Lab é o seguinte: *%AllUsersProfile%\Dados de Aplicativos\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.*
  6. Na janela que é aberta, clique no botão **Instalar**. O certificado da Kaspersky Lab será instalado.

Se o computador for executado no Microsoft Windows Vista ou no Microsoft Windows 7, o caminho do arquivo do certificado da Kaspersky Lab será o seguinte: *%AllUsersProfile%\Kaspersky Lab\AVP12\Data\Cert\(fake)Kaspersky Anti-Virus personal root certificate.cer.*

CONFIGURANDO O SERVIDOR PROXY

Se a conexão do computador com a Internet for estabelecida através de um servidor proxy, talvez seja necessário definir suas configurações de conexão. O Kaspersky Anti-Virus usa essas configurações para determinados componentes de proteção e para atualizar os bancos de dados e módulos do aplicativo.

Se a sua rede incluir um servidor proxy que usa uma porta diferente do padrão, adicione o número da porta à lista de portas monitoradas (consulte a seção "Criando uma lista de portas monitoradas" na página 90).

- *Para configurar a conexão com um servidor proxy:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Configurações Avançadas**, selecione o componente **Rede**.
  3. Na seção **Servidor proxy**, clique no botão **Configurações do servidor proxy**.
  4. Na janela **Configurações do servidor proxy** que é aberta, especifique as configurações desejadas para a conexão com um servidor proxy.

CRIANDO UMA LISTA DE PORTAS MONITORADAS

Os componentes de proteção como o Antivírus de Email, o Antivírus da Web e o Antivírus de IM (veja a página 77) monitoram os fluxos de dados transferidos através de protocolos específicos e que passam por determinadas portas TCP abertas no computador. Por exemplo, o Antivírus de Email verifica as informações transferidas por SMTP, enquanto o Antivírus da verifica as informações transferidas por HTTP, HTTPS e FTP.

Você pode ativar o monitoramento de todas as portas ou apenas das portas de rede selecionadas. Se você configurar o produto para monitorar portas selecionadas, será possível criar uma lista de aplicativos para os quais todas as portas serão monitoradas. É recomendável expandir a lista incluindo os aplicativos que recebem ou transferem dados por FTP.

- *Para adicionar uma porta à lista de portas monitoradas:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Rede**.
  3. Na seção **Portas monitoradas**, selecione **Monitorar somente as portas selecionadas** e clique no botão **Selecionar**.

     A janela **Portas de rede** será aberta.
  4. Clique no link **Adicionar** sob a lista de portas na parte superior da janela para abrir a janela **Porta de rede** e insira o número e a descrição da porta.

- *Para excluir uma porta da lista de portas monitoradas:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Rede**.
  3. Na seção **Portas monitoradas**, selecione **Monitorar somente as portas selecionadas** e clique no botão **Selecionar**.

     A janela **Portas de rede** será aberta.
  4. Na lista de portas na parte superior da janela, desmarque a caixa ao lado da descrição da porta que deve ser excluída.

Para criar uma lista de aplicativos para os quais você deseja monitorar todas as portas:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Rede**.
3. Na seção **Portas monitoradas**, selecione **Monitorar somente as portas selecionadas** e clique no botão **Selecionar**.

   A janela **Portas de rede** será aberta.
4. Marque a caixa **Monitorar todas as portas para os aplicativos especificados** e, na lista de aplicativos abaixo, marque as caixas correspondentes aos nomes dos aplicativos para os quais todas as portas devem ser monitoradas.
5. Se o aplicativo desejado não estiver na lista, adicione-o da seguinte maneira:
   a. Clique no link **Adicionar** abaixo da lista de aplicativos para abrir o menu e selecione um item:
      - Para especificar o local do arquivo executável de um aplicativo, selecione **Procurar** e especifique o local do arquivo no computador.
      - Para selecionar um aplicativo na lista de aplicativos em execução no momento, selecione **Aplicativos**. Na janela **Selecionar aplicativo** que é aberta, selecione o aplicativo desejado.

   b. Na janela **Aplicativo**, insira a descrição do aplicativo selecionado.

ZONA CONFIÁVEL

A *zona confiável* consiste em uma lista de objetos que não devem ser monitorados pelo aplicativo. Em outras palavras, é um conjunto de exclusões do escopo de proteção do Kaspersky Anti-Virus.

A zona confiável é criada com base na lista de aplicativos confiáveis (consulte a seção "Criando uma lista de aplicativos confiáveis" na página 92) e em regras de exclusão (consulte a seção "Criando regras de exclusão" na página 92) de acordo com as características dos objetos com os quais você trabalha e os aplicativos instalados no computador. Talvez seja necessário incluir objetos na zona confiável se, por exemplo, o Kaspersky Anti-Virus bloquear o acesso a um objeto ou aplicativo, embora você tenha certeza de que ele é absolutamente inofensivo.

Por exemplo, se você acha que os objetos usados pelo Bloco de Notas do Microsoft Windows são inofensivos e não precisam ser verificados, ou seja, se você confia nesse aplicativo, adicione o Bloco de Notas à lista de aplicativos confiáveis para excluir da verificação os objetos usados por esse processo.

Algumas ações classificadas como perigosas podem ser seguras na estrutura de determinados aplicativos. Por exemplo, os aplicativos que alternam automaticamente o layout do teclado, como o Punto Switcher, normalmente interceptam o texto digitado no teclado. Para considerar as especificidades desses aplicativos e desativar o monitoramento de suas atividades, é recomendável adicioná-los à lista de aplicativos confiáveis.

Quando um aplicativo é adicionado à lista de aplicativos confiáveis, suas atividades de rede e com arquivos (inclusive as suspeitas) não são mais controladas. O mesmo ocorre com suas tentativas de acesso ao Registro do sistema. Ao mesmo tempo, o arquivo executável e o processo do aplicativo confiável são verificados quanto à presença de vírus, como anteriormente. Para excluir completamente um aplicativo da verificação, use as regras de exclusão.

A exclusão de aplicativos confiáveis da verificação evita problemas de compatibilidade do aplicativo com outros programas (por exemplo, a verificação duplicada do tráfego de rede de um computador de terceiros pelo Kaspersky Anti-Virus e por outro aplicativo antivírus), além de melhorar o desempenho do computador, que é crítico ao usar aplicativos de servidor.

Por sua vez, as regras de exclusão da zona confiável garantem a opção de trabalhar com aplicativos legais que podem ser explorados por invasores para danificar o computador ou os dados do usuário. Esses aplicativos não têm recursos maliciosos, mas podem ser usados como componentes auxiliares de um programa malicioso. Esta categoria inclui aplicativos de administração remota, programas de IRC, servidores FTP, diversos utilitários para interromper ou ocultar processos, programas de registro do teclado, programas de quebra de senhas, discadores e outros. Esses aplicativos podem ser bloqueados pelo Kaspersky Anti-Virus. Para evitar o bloqueio, você pode configurar regras de exclusão.

Uma *regra de exclusão* é um conjunto de condições que determinam que um objeto não deve ser verificado pelo Kaspersky Anti-Virus. Em qualquer outro caso, o objeto é verificado por todos os componentes de proteção de acordo com suas respectivas configurações de proteção.

As regras de exclusão da zona confiável podem ser usadas por vários componentes do aplicativo, como o Antivírus de Arquivos (consulte a seção "Antivírus de Arquivos" na página 68), o Antivírus de Email (consulte a seção "Antivírus de Email" na página 73), o Antivírus da Web (consulte a seção "Antivírus da Web" na página 77), ou ao executar tarefas de verificação de vírus.

NESTA SEÇÃO:

CRIANDO UMA LISTA DE APLICATIVOS CONFIÁVEIS

Por padrão, o Kaspersky Anti-Virus verifica os objetos abertos, executados ou salvos pelos processos de todos os programas e monitora a atividade de todos os aplicativos e do tráfego de rede criado por eles. Quando você adiciona um aplicativo à lista de confiáveis, o Kaspersky Anti-Virus o exclui da verificação.

Para adicionar um aplicativo à lista confiável:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Ameaças e Exclusões**.
3. Na seção **Exclusões**, clique no botão **Configurações**.
4. Na janela que é aberta, na guia **Aplicativos confiáveis**, abra o menu de seleção de aplicativos clicando no botão **Adicionar**.
5. No menu que é aberto, selecione um aplicativo da lista **Aplicativos** ou selecione **Procurar** para especificar o caminho dos arquivos executáveis do aplicativo desejado.
6. Na janela **Exclusões do aplicativo** que é aberta, marque as caixas correspondentes aos tipos de atividades do aplicativo que devem ser excluídos da verificação.

CRIANDO REGRAS DE EXCLUSÃO

Se você usar aplicativos reconhecidos pelo Kaspersky Anti-Virus como legais, mas que podem ser usados por invasores para danificar o computador ou os dados do usuário, é recomendável configurar regras de exclusão para eles.

Para criar uma regra de exclusão:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Ameaças e Exclusões**.
3. Na seção **Exclusões**, clique no botão **Configurações**.
4. Na janela que é aberta, na guia **Regras de exclusão**, clique no botão **Adicionar**.
5. Na janela **Regra de exclusão** que é aberta, edite as configurações da regra de exclusão.

DESEMPENHO E COMPATIBILIDADE COM OUTROS APLICATIVOS

O desempenho do Kaspersky Anti-Virus é definido pelo intervalo de ameaças que ele pode detectar, além de seu consumo de energia e de recursos do computador.

O Kaspersky Anti-Virus permite selecionar várias categorias de ameaças (consulte a seção "Selecionando as categorias de ameaças que podem ser detectadas" na página 93) que devem ser detectadas pelo aplicativo.

O consumo de energia é muito importante nos computadores portáteis. Muitas vezes, a verificação do computador quanto à presença de vírus e a atualização dos bancos de dados do Kaspersky Anti-Virus exigem recursos significativos. O modo para laptops do Kaspersky Anti-Virus (consulte a seção "Economia de bateria" na página 93) permite adiar automaticamente tarefas de atualização e verificação programadas ao trabalhar com a bateria, economizando sua carga, enquanto o modo de Verificação Ociosa (consulte a seção "Executando tarefas em segundo plano" na página 94) permite executar tarefas que utilizam muitos recursos quando o computador não está sendo usado.

A utilização de recursos do computador pelo Kaspersky Anti-Virus pode afetar o desempenho de outros aplicativos. Para solucionar problemas de operações simultâneas que aumentam a carga na CPU e nos subsistemas de disco, o

Kaspersky Anti-Virus pode pausar as tarefas de verificação e conceder recursos a outros aplicativos (consulte a seção "Distribuindo os recursos do computador durante a verificação de vírus" na página 94) em execução no computador.

No modo Perfil de Jogo (veja a página 95), o aplicativo desativa automaticamente a exibição de notificações sobre atividades do Kaspersky Anti-Virus ao executar outros aplicativos no modo de tela inteira.

No caso de uma infecção ativa no sistema, o procedimento de desinfecção avançada exige o reinício do computador, o que também pode afetar o desempenho de outros aplicativos. Se necessário, é possível desativar a tecnologia de desinfecção avançada (veja a página 93) para evitar o reinício indesejado do computador.

NESTA SEÇÃO:

SELECIONANDO AS CATEGORIAS DE AMEAÇAS DETECTÁVEIS

As ameaças detectadas pelo Kaspersky Anti-Virus estão divididas em categorias de acordo com vários atributos. O aplicativo sempre procura vírus, cavalos de Troia e ferramentas de utilitários maliciosos. Esses programas podem causar danos significativos ao computador. Para garantir a proteção mais confiável do computador, você pode estender a lista de ameaças detectadas ativando o controle de ações executadas por aplicativos legais que podem ser exploradas por um invasor para danificar o computador e os dados do usuário.

Para selecionar as categorias de ameaças que podem ser detectadas:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Ameaças e Exclusões**.
3. À direita da janela, clique no botão **Configurações** abaixo da lista **A detecção dos seguintes tipos de ameaças está ativada**.
4. Na janela **Ameaças** que é aberta, marque as caixas correspondentes às categorias de ameaças que devem ser detectadas.

ECONOMIA DE BATERIA

Para economizar energia em um computador portátil, as tarefas de verificação de vírus e atualização programada podem ser adiadas. Se necessário, você pode atualizar o Kaspersky Anti-Virus ou iniciar uma verificação de vírus manualmente.

Para ativar o modo de economia de bateria ao trabalhar com a bateria:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Economia de Bateria**.
3. À direita da janela, marque a caixa **Desativar as verificações programadas ao trabalhar com a bateria**.

DESINFECÇÃO AVANÇADA

Os programas maliciosos atuais conseguem invadir os níveis mais baixos de um sistema operacional, o que torna praticamente impossível excluí-los. Se for detectada alguma atividade maliciosa no sistema, o Kaspersky Anti-Virus permitirá que você aplique a tecnologia de Desinfecção Avançada, que elimina a ameaça e a remove do computador.

Quando o procedimento de desinfecção avançada é concluído, o aplicativo reinicia o computador. Depois de reiniciar o computador, é recomendável executar a verificação completa de vírus (consulte a seção "Como executar uma verificação completa do computador quanto à presença de vírus" na página 42).

Para ativar o Kaspersky Anti-Virus para aplicar a tecnologia de Desinfecção Avançada:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Compatibilidade**.
3. Marque a caixa **Ativar Tecnologia de desinfecção avançada**.

DISTRIBUINDO OS RECURSOS DO COMPUTADOR DURANTE A VERIFICAÇÃO DE VÍRUS

A execução de tarefas de verificação aumenta a carga da CPU e dos subsistemas de disco, tornando os outros aplicativos mais lentos. Por padrão, se isso acontecer, o Kaspersky Anti-Virus pausará as tarefas de verificação de vírus e liberará os recursos do sistema para os aplicativos do usuário.

Entretanto, existem vários aplicativos que são iniciados imediatamente quando os recursos da CPU estão disponíveis, sendo executados em segundo plano. Para que a verificação não dependa do desempenho desses aplicativos, os recursos do sistema não devem ser disponibilizados para eles.

Para que o Kaspersky Anti-Virus adie as tarefas de verificação quando elas tornarem outros aplicativos mais lentos:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Compatibilidade**.
3. Marque a caixa **Conceder recursos a outros aplicativos**.

EXECUTANDO TAREFAS EM SEGUNDO PLANO

Para otimizar a carga sobre os recursos do computador, o Kaspersky Anti-Virus executa a verificação periódica de rootkits em segundo plano e as tarefas que utilizam muitos recursos quando o computador está ocioso.

A verificação normal de rootkits é executada enquanto você trabalha no computador. A verificação leva no máximo cinco minutos e envolve uma parcela mínima dos recursos do computador.

Quando o computador está ocioso, as seguintes tarefas podem ser executadas:

- atualização automática dos bancos de dados de antivírus e módulos do programa;
- verificação da memória do sistema, dos objetos de inicialização e da partição do sistema.

As tarefas de Verificação Ociosa serão executadas se o computador tiver sido bloqueado pelo usuário ou se a proteção de tela for exibida na tela por pelo menos cinco minutos.

Se o computador estiver trabalhando com a bateria, nenhuma tarefa será executada, mesmo que o computador esteja ocioso.

Depois que as tarefas são executadas em segundo plano, seu andamento é exibido no Gerenciador de Tarefas (consulte a seção "Gerenciando tarefas de verificação. Gerenciador de Tarefas" na página 63).

NESTA SEÇÃO:

PROCURANDO ROOTKITS EM SEGUNDO PLANO

Por padrão, o Kaspersky Anti-Virus executa a verificação periódica de rootkits. Se necessário, você pode desativar a verificação de rootkits.

- *Para desativar a verificação periódica de rootkits:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Verificação**, selecione a subseção **Configurações Gerais**.
  3. À direita da janela, desmarque a caixa **Executar verificação periódica de rootkits**.

VERIFICAÇÃO OCIOSA

O primeiro estágio da Verificação Ociosa consiste em verificar se os bancos de dados e módulos do aplicativo estão atualizados. Se for necessária uma atualização após a verificação, a tarefa de atualização automática será iniciada. No segundo estágio, o aplicativo verifica a data e o status da última execução da Verificação Ociosa. Se a Verificação Ociosa ainda não tiver sido executada, tiver sido executada mais de sete dias atrás ou tiver sido interrompida, o aplicativo executará a tarefa de verificação da memória do sistema, dos objetos de inicialização e do Registro do sistema.

A Verificação Ociosa é executada no nível profundo de análise heurística, o que aumenta a probabilidade de detecção de ameaças.

Quando o usuário voltar ao trabalho, a tarefa de Verificação Ociosa será interrompida automaticamente. O aplicativo lembra o estágio em que a tarefa foi interrompida para reiniciar a verificação a partir desse ponto no futuro.

Se a execução das tarefas de Verificação Ociosa tiver sido interrompida durante o download do pacote de atualização, a atualização será iniciada do começo da próxima vez.

- *Para desativar o modo de Verificação Ociosa:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Verificação**, selecione a subseção **Configurações Gerais**.
  3. À direita da janela, desmarque a caixa **Executar Verificação Ociosa**.

MODO DE TELA INTEIRA. PERFIL DE JOGO

Determinados programas (especialmente jogos de computador) que são executados no modo de tela inteira são apenas parcialmente compatíveis com alguns recursos do Kaspersky Anti-Virus: por exemplo, as notificações pop-up são totalmente indesejáveis nesse modo. Muitas vezes, esses aplicativos exigem recursos significativos do sistema, de forma que a execução de determinadas tarefas do Kaspersky Anti-Virus pode reduzir seu desempenho.

Para que não seja necessário desativar manualmente as notificações e pausar as tarefas sempre que você executar aplicativos em tela inteira, o Kaspersky Anti-Virus oferece a opção de alterar temporariamente as configurações, usando o perfil de jogo. Quando o perfil de jogo está ativo, ao alternar para o modo de tela inteira, as configurações de todos os componentes do produto são alteradas automaticamente para assegurar o funcionamento ideal do sistema nesse modo. Ao sair do modo de tela inteira, as configurações do produto retornam aos valores iniciais usados antes de entrar nesse modo.

- *Para ativar o perfil de jogo:*

  1. Abra a janela de configurações do aplicativo.
  2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Perfil de Jogo**.
  3. Marque a caixa **Usar Perfil de Jogo** e, na seção **Opções do perfil** abaixo, especifique as configurações de perfil de jogo desejadas.

AUTODEFESA DO KASPERSKY ANTI-VIRUS

Como o Kaspersky Anti-Virus assegura a proteção do computador contra malware, programas maliciosos que invadem seu computador tentam bloquear o Kaspersky Anti-Virus ou até mesmo excluir o aplicativo do computador.

O desempenho estável da defesa do computador é garantido através dos recursos de autodefesa e da proteção contra o controle externo implementados no Kaspersky Anti-Virus.

A autodefesa do Kaspersky Anti-Virus evita a modificação e a exclusão de seus próprios arquivos do disco rígido, de processos na memória e de entradas no Registro do sistema. A proteção contra o controle externo permite bloquear todas as tentativas de controlar serviços de aplicativos remotamente.

Nos computadores que executam sistemas operacionais de 64 bits e o Microsoft Windows Vista, a Autodefesa do Kaspersky Anti-Virus estará disponível apenas para evitar que os arquivos do próprio aplicativo em unidades locais e o Registro do sistema sejam modificados ou excluídos.

NESTA SEÇÃO:

ATIVANDO E DESATIVANDO A AUTODEFESA

Por padrão, a autodefesa do Kaspersky Anti-Virus está ativada. Se necessário, você pode desativar a autodefesa.

Para desativar a autodefesa do Kaspersky Anti-Virus:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Autodefesa**.
3. À direita da janela, desmarque a caixa **Ativar Autodefesa**.

PROTEÇÃO CONTRA O CONTROLE EXTERNO

Por padrão, a proteção contra controle externo está ativada. Se necessário, você pode desativar a proteção.

Ao usar aplicativos de administração remota (como o RemoteAdmin) será necessário adicioná-los à lista de Aplicativos Confiáveis (consulte a seção "Zona confiável" na página 91) quando o Controle de Serviços Externos estiver ativado, além de ativar sua configuração **Não monitorar a atividade de aplicativos**.

Para desativar a proteção contra o controle externo:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Autodefesa**.
3. Na seção **Controle externo**, desmarque a caixa **Desativar controle de serviços externos**.

QUARENTENA E BACKUP

A *Quarentena* é uma área especial que armazena os arquivos possivelmente infectados por vírus e os arquivos que não podem ser desinfetados no momento de sua detecção.

Um arquivo possivelmente infectado pode ser detectado e colocado na Quarentena durante uma verificação de vírus ou pelos componentes Antivírus de Arquivos, Antivírus de Email ou Defesa Proativa.

Os arquivos são colocados na Quarentena nos seguintes casos:

- O código do arquivo lembra uma ameaça conhecida, mas parcialmente modificado, ou tem uma estrutura semelhante à de malware, mas não está registrado no banco de dados. Nesse caso, o arquivo é movido para a Quarentena depois da análise heurística executada pelo Antivírus de Arquivos, pelo Antivírus de Email ou durante a verificação antivírus. A análise heurística raramente gera falsos positivos.
- A sequência de operações executadas por um objeto parece suspeita. Nesse caso, o arquivo é movido para a Quarentena após a análise de seu comportamento pelo componente Defesa Proativa.

Os arquivos da Quarentena não representam uma ameaça. Com o tempo, são descobertas informações sobre novas ameaças e formas de neutralizá-las, o que pode permitir que o Kaspersky Anti-Virus desinfete um arquivo armazenado na Quarentena.

O *armazenamento de Backup* foi criado para armazenar cópias de backup de arquivos que foram excluídos ou modificados durante o processo de desinfecção.

NESTA SEÇÃO:

ARMAZENANDO ARQUIVOS NA QUARENTENA E NO BACKUP

O período máximo padrão de armazenamento de objetos é de 30 dias. Depois disso, os objetos serão excluídos. Você pode cancelar a restrição de tempo ou alterar a duração máxima do armazenamento de objetos.

Além disso, é possível especificar o tamanho máximo da Quarentena e do Backup. Quando ele for atingido, o conteúdo da Quarentena e do Backup será substituído por novos objetos. Por padrão, a restrição do tamanho máximo está desativada.

Para modificar o tempo máximo de armazenamento de objetos:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Relatórios e Armazenamentos**.
3. À direita da janela, na seção **Armazenando objetos da Quarentena e do Backup**, marque a caixa **Armazenar objetos por no máximo** e especifique o período máximo de armazenamento de objetos na Quarentena.

Para configurar o tamanho máximo da Quarentena e do Backup:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Relatórios e Armazenamentos**.
3. À direita da janela, na seção **Armazenando objetos da Quarentena e do Backup**, marque a caixa **Tamanho máximo** e especifique o tamanho máximo da Quarentena e do Backup.

TRABALHANDO COM ARQUIVOS DA QUARENTENA

A Quarentena do Kaspersky Anti-Virus permite executar as seguintes operações:

- colocar na Quarentena os arquivos que você suspeita que estejam infectados;
- verificar os arquivos da Quarentena usando a versão atual dos bancos de dados do Kaspersky Anti-Virus;
- restaurar arquivos nas pastas originais das quais eles foram movidos para a Quarentena;
- excluir os arquivos selecionados da Quarentena;
- enviar arquivos da Quarentena para serem pesquisados pela Kaspersky Lab.

Você pode usar os seguintes métodos para mover um arquivo para a Quarentena:

- usando no botão **Mover para a Quarentena** na janela **Quarentena**;
- usando o menu de contexto do arquivo.

Para mover um arquivo para a Quarentena na janela Quarentena:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, selecione a seção **Quarentena**.
3. Na guia **Quarentena**, clique no botão **Mover para a Quarentena**.
4. Na janela que é aberta, selecione o arquivo que você deseja mover para a Quarentena.

Para mover um arquivo para a Quarentena usando o menu de contexto:

1. Abra o Microsoft Windows Explorer e vá para a pasta que contém o arquivo que você deseja mover para a Quarentena.
2. Clique com o botão direito do mouse para abrir o menu de contexto do arquivo e selecione **Mover para a Quarentena**.

Para verificar um arquivo da Quarentena:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, selecione a seção **Quarentena**.
3. Na guia **Quarentena**, selecione o arquivo que você deseja verificar.
4. Clique no botão **Verificar**.

Para restaurar um objeto da Quarentena:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, selecione a seção **Quarentena**.
3. Na guia **Quarentena**, selecione o arquivo que você deseja restaurar.
4. Clique no botão **Restaurar**.

Para excluir um objeto da Quarentena:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, selecione a seção **Quarentena**.
3. Na guia **Quarentena**, selecione o arquivo que você deseja excluir.
4. Clique com o botão direito do mouse no arquivo para abrir seu menu de contexto e selecione **Excluir**.

Para enviar um objeto da Quarentena à Kaspersky Lab para análise:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, selecione a seção **Quarentena**.
3. Na guia **Quarentena**, selecione o arquivo que você deseja enviar para pesquisa.
4. Clique com o botão direito do mouse para abrir o menu de contexto do arquivo e selecione **Enviar para análise**.

TRABALHANDO COM OBJETOS DO BACKUP

O armazenamento de backup do Kaspersky Anti-Virus permite executar as seguintes operações:

- restaurar arquivos em uma pasta especificada ou na pasta original, na qual o arquivo foi armazenado antes de ser processado pelo Kaspersky Anti-Virus;
- excluir arquivos selecionados ou todos os arquivos do Backup.

Para restaurar um objeto do Backup:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, selecione a seção **Quarentena**.
3. Na guia **Armazenamento**, selecione o arquivo que você deseja restaurar.
4. Clique no botão **Restaurar**.

Para excluir um arquivo do Backup:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, selecione a seção **Quarentena**.
3. Na guia **Armazenamento**, selecione o arquivo que você deseja excluir.
4. Clique com o botão direito do mouse no arquivo para abrir seu menu de contexto e selecione **Excluir**.

Para excluir todos os arquivos do Backup:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, selecione a seção **Quarentena**.
3. Na guia **Armazenamento**, clique no botão **Limpar armazenamento**.

VERIFICANDO ARQUIVOS NA QUARENTENA APÓS UMA ATUALIZAÇÃO

Se o aplicativo verificar um arquivo e não puder determinar exatamente quais programas maliciosos o infectaram, o arquivo será colocado na Quarentena. Depois que os bancos de dados forem atualizados, o Kaspersky Anti-Virus poderá identificar claramente e remover a ameaça. Você pode ativar a verificação automática de objetos em quarentena após cada atualização.

É recomendável exibir os arquivos da Quarentena periodicamente. A verificação pode alterar seus status. Alguns arquivos poderão ser então restaurados para seus locais anteriores e você poderá continuar trabalhando com eles.

Para ativar a verificação dos arquivos da Quarentena após a atualização:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Atualização**, selecione o componente **Configurações de Atualização**.
3. Marque a caixa **Verificar a Quarentena novamente após a atualização** na seção **Adicional**.

FERRAMENTAS ADICIONAIS PARA PROTEGER MELHOR SEU COMPUTADOR

Os seguintes assistentes e ferramentas fornecidos com o Kaspersky Anti-Virus são usados para resolver problemas específicos referentes à segurança do computador:

- O Assistente para Criação do Kaspersky Rescue Disk foi projetado para criar uma imagem do disco ISO e gravar o Kaspersky Rescue Disk em uma mídia removível que permite recuperar a funcionalidade do sistema após um ataque de vírus carregando o aplicativo a partir da mídia removível. O Kaspersky Rescue Disk deve ser usado quando o nível de infecção torna impossível desinfetar o computador usando aplicativos antivírus ou utilitários de remoção de malware.
- O Assistente de Limpeza de Dados Particulares foi criado para procurar e eliminar rastros das atividades de um usuário no sistema e as configurações do sistema operacional que permitem coletar informações sobre as atividades do usuário.
- O Assistente de Restauração do Sistema foi criado para eliminar danos e rastros de objetos de malware do sistema.
- O Assistente de Configuração do Navegador foi criado para analisar e ajustar as configurações do Microsoft Internet Explorer a fim de eliminar suas possíveis vulnerabilidades.

Todos os problemas encontrados pelos Assistentes (exceto o Assistente para Criação do Kaspersky Rescue Disk) são agrupados de acordo com o tipo de perigo que representam para o sistema operacional. A Kaspersky Lab oferece um conjunto de ações para cada grupo de problemas que ajudam a eliminar vulnerabilidades e pontos frágeis nas configurações do sistema. Existem três grupos de problemas e três grupos correspondentes de ações a serem executadas quando eles forem detectados:

- *Ações altamente recomendadas* ajudarão a eliminar problemas que representam uma ameaça de segurança grave. É recomendável executar todas as ações desse grupo imediatamente para eliminar a ameaça.
- *Ações recomendadas* eliminam problemas que representam uma possível ameaça. Também é recomendável executar todas as ações desse grupo para ter o nível ideal de proteção.
- *Ações adicionais* ajudam a reparar danos ao sistema que não representam uma ameaça atual, mas que podem ameaçar a segurança do computador no futuro. A execução dessas ações garante a proteção abrangente do computador. Contudo, em alguns casos, elas podem levar à exclusão das configurações do usuário (como cookies).

NESTA SEÇÃO:

LIMPEZA DE DADOS PARTICULARES

Ao trabalhar com o computador, as ações do usuário são registradas no sistema. Os dados salvos incluem as consultas de pesquisa inseridas por usuários e os sites visitados, os programas executados, os arquivos abertos e salvos, o log de eventos do sistema Microsoft Windows, os arquivos temporários, etc.

Todas essas fontes de informações sobre as atividades do usuário podem conter dados confidenciais (incluindo senhas) e podem estar disponíveis para serem analisadas por invasores. Frequentemente, o usuário não tem conhecimento suficiente para evitar que informações dessas fontes sejam roubadas.

O Kaspersky Anti-Virus inclui o Assistente de limpeza de dados particulares. Este Assistente procura rastros de atividades do usuário no sistema, além de configurações do sistema operacional que contribuem para o armazenamento de informações sobre as atividades do usuário.

Lembre-se de que os dados relacionados à atividade do usuário no sistema são acumulados continuamente. A execução de qualquer arquivo ou a abertura de qualquer documento são registradas. O log do sistema Microsoft Windows registra vários eventos que ocorrem no sistema. Por isso, a execução repetida do Assistente de Limpeza de Dados Particulares pode detectar rastros de atividades que não foram apagados pela execução anterior do Assistente. Alguns arquivos, como o arquivo de log do Microsoft Windows, podem estar em uso pelo sistema enquanto o Assistente tenta excluí-los. Para excluir esses arquivos, o Assistente solicitará que você reinicie o sistema. Entretanto, ao reiniciar, esses arquivos podem ser recriados e detectados novamente como rastros de atividades.

O Assistente consiste em uma série de telas (etapas) nas quais você pode navegar usando os botões **Voltar** e **Avançar**. Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**. Para interromper o Assistente em qualquer estágio, clique no botão **Cancelar**.

Para remover rastros de atividades do usuário do sistema:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, selecione a seção **Ferramentas**.
3. Na janela que é aberta, na seção **Limpeza de Dados Particulares**, clique no botão **Iniciar**.

Vamos revisar as etapas do Assistente mais detalhadamente.

Etapa 1. Iniciando o Assistente

Confirme se a opção **Executar diagnóstico de rastros de atividades do usuário** está selecionada e clique no botão **Avançar** para iniciar o Assistente.

Etapa 2. Pesquisa de sinais de atividade

Este assistente pesquisa rastros de atividades de malware no computador. A verificação pode levar algum tempo. Quando a pesquisa for concluída, o Assistente continuará automaticamente na próxima etapa.

Etapa 3. Selecionando ações de Limpeza de Dados Particulares

Ao concluir a pesquisa, o Assistente exibe os rastros de atividades detectados e as ações sugeridas para eliminá-los.

Para exibir as ações em um grupo, clique no ícone **+** à esquerda do nome do grupo.

Para fazer o Assistente executar uma determinada ação, marque a caixa à esquerda da descrição da ação correspondente. Por padrão, o Assistente executa todas as ações recomendadas e altamente recomendadas. Se não desejar executar uma determinada ação, desmarque a caixa ao lado dela.

É altamente recomendável não desmarcar as caixas selecionadas por padrão, pois isso pode deixar o computador vulnerável a ameaças.

Depois de definir o conjunto de ações que serão executadas pelo Assistente, clique no botão **Avançar**.

Etapa 4. Limpeza de Dados Particulares

O Assistente executará as ações selecionadas na etapa anterior. A eliminação dos rastros de atividades pode levar algum tempo. Para limpar determinados rastros de atividades, talvez seja necessário reiniciar; se for o caso, o Assistente o notificará.

Quando a limpeza for concluída, o Assistente continuará automaticamente na próxima etapa.

Etapa 5. Conclusão do Assistente

Se desejar limpar os rastros de atividades do usuário automaticamente sempre que o Kaspersky Anti-Virus concluir seu trabalho, na última tela do Assistente, marque a caixa **Limpar rastros de atividades sempre ao sair do Kaspersky Anti-Virus**. Se desejar remover os rastros de atividades manualmente usando o Assistente, não marque essa caixa.

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

CONFIGURANDO UM NAVEGADOR PARA TRABALHAR COM SEGURANÇA

Em determinadas situações, o navegador Microsoft Internet Explorer exige análise e configuração especiais, pois alguns valores selecionados pelo usuário ou definidos por padrão podem gerar problemas de segurança.

Seguem alguns exemplos dos objetos e parâmetros usados no navegador e suas associações a possíveis ameaças de segurança:

- **Cache do Microsoft Internet Explorer**. O cache armazena dados baixados da Internet, de forma que o usuário não precise baixá-los novamente. Isso diminui o tempo de download de páginas da Web e reduz o tráfego da Internet. Além disso, o cache contém dados confidenciais e possibilita descobrir os sites que o usuário visitou. Alguns objetos de malware examinam o cache ao verificar o disco e os invasores podem obter, por exemplo, os endereços de email do usuário. É recomendável limpar o cache sempre que você fechar o navegador para melhorar a proteção.
- **Exibição de extensões de tipos de arquivos conhecidos**. Para editar os nomes de arquivos de forma conveniente, você pode desativar a exibição de suas extensões. Contudo, às vezes é útil ver a extensão do arquivo. Os nomes de arquivo de vários objetos maliciosos contêm combinações de símbolos que simulam uma extensão de arquivo adicional antes da extensão real (por exemplo, exemplo.txt.com). Se a extensão do arquivo real não for exibida, os usuários poderão ver apenas a parte do nome de arquivo com a extensão simulada e, assim, poderão identificar um objeto malicioso como um arquivo inofensivo. Para melhorar a proteção, é recomendável ativar a exibição de arquivos de formatos conhecidos.
- **Lista de sites confiáveis**. Para que alguns sites sejam executados corretamente, você deve adicioná-los à lista de sites confiáveis. Ao mesmo tempo, os objetos maliciosos podem adicionar a esta lista links para os sites criados por invasores.

A configuração do navegador para a Execução Segura pode gerar problemas na exibição de determinados sites (por exemplo, se usarem elementos ActiveX). Esse problema pode ser resolvido adicionando esses sites à zona confiável.

A análise e a configuração do navegador são executadas no Assistente de Configuração do Navegador. O Assistente verifica se as últimas atualizações do navegador estão instaladas e confirma se as configurações atuais do navegador não tornam o sistema vulnerável a explorações maliciosas. Ao concluir o Assistente, será gerado um relatório que pode ser enviado à Kaspersky Lab para análise.

O Assistente consiste em uma série de telas (etapas) nas quais você pode navegar usando os botões **Voltar** e **Avançar**. Para fechar o Assistente ao concluir a tarefa, clique no botão **Concluir**. Para interromper o Assistente em qualquer estágio, clique no botão **Cancelar**.

Feche todas as janelas do Microsoft Internet Explorer antes de iniciar o diagnóstico.

Para configurar o navegador para trabalhar de forma segura:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, selecione a seção **Ferramentas**.
3. Na janela que é aberta, na seção **Configuração do Navegador**, clique no botão **Iniciar**.

Vamos revisar as etapas do Assistente mais detalhadamente.

Etapa 1. Iniciando o Assistente

Confirme se a opção **Executar o diagnóstico do Microsoft Internet Explorer** está selecionada e clique no botão **Avançar** para iniciar o Assistente.

Etapa 2. Análise de configurações do Microsoft Internet Explorer

O assistente analisa as configurações do Microsoft Internet Explorer. A pesquisa de problemas nas configurações do navegador pode levar algum tempo. Quando a pesquisa for concluída, o Assistente continuará automaticamente na próxima etapa.

Etapa 3. Selecionando ações para a configuração do navegador

Ao concluir a pesquisa, o Assistente exibe os problemas detectados e as ações sugeridas para eliminá-los.

Para exibir as ações em um grupo, clique no ícone **+** à esquerda do nome do grupo.

Para fazer o Assistente executar uma determinada ação, marque a caixa à esquerda da descrição da ação correspondente. Por padrão, o Assistente executa todas as ações recomendadas e altamente recomendadas. Se não desejar executar uma determinada ação, desmarque a caixa ao lado dela.

É altamente recomendável não desmarcar as caixas selecionadas por padrão, pois isso pode deixar o computador vulnerável a ameaças.

Depois de definir o conjunto de ações que serão executadas pelo Assistente, clique no botão **Avançar**.

Etapa 4. Configuração do Navegador

O Assistente executará as ações selecionadas na etapa anterior. A configuração do navegador pode levar algum tempo. Quando a configuração for concluída, o Assistente continuará automaticamente na próxima etapa.

Etapa 5. Conclusão do Assistente

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

REVERTENDO AS ALTERAÇÕES EXECUTADAS PELOS ASSISTENTES

É possível reverter algumas alterações feitas ao executar o Assistente de Limpeza de Dados Particulares (consulte a seção "Limpeza de Dados Particulares" na página 100), o Assistente de Restauração do Sistema (consulte a seção "O que fazer se você suspeitar que o computador está infectado" na página 45) e o Assistente de Configuração do Navegador (consulte a seção "Configurando um navegador para trabalhar com segurança" na página 101).

Para reverter as alterações feitas pelos Assistentes:

1. Abra a janela principal do aplicativo e selecione a seção **Ferramentas** na parte inferior da janela.
2. À direita da janela, clique no botão **Iniciar** na seção com o nome do Assistente cujas alterações você deseja reverter:
   - **Limpeza de Dados Particulares** – para reverter as alterações feitas pelo Assistente de Limpeza de Dados Particulares;
   - **Solução de Problemas do Microsoft Windows** – para reverter as ações feitas pelo Assistente de Solução de Problemas do Microsoft Windows;
   - **Configuração do Navegador** – para reverter as alterações feitas pelo Assistente de Configuração do Navegador.

Vejamos de forma mais detalhada as etapas dos Assistentes ao reverter alterações.

Etapa 1. Iniciando o Assistente

Selecione **Reverter alterações** e clique no botão **Avançar**.

Etapa 2. Procurar alterações

O Assistente procura as alterações feitas anteriormente e que podem ser revertidas. Quando a pesquisa for concluída, o Assistente continuará automaticamente na próxima etapa.

Etapa 3. Selecionar alterações que devem ser revertidas

Quando a pesquisa for concluída, o Assistente o informará sobre as alterações encontradas.

Para que o assistente reverta uma ação executada anteriormente, marque a caixa à esquerda do nome da ação.

Depois de selecionar as ações que você deseja reverter, clique no botão **Avançar**.

Etapa 4. Revertendo alterações

O Assistente reverte as ações selecionadas na etapa anterior. Quando as alterações forem revertidas, o Assistente continuará automaticamente na etapa seguinte.

Etapa 5. Conclusão do Assistente

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

RELATÓRIOS

Os eventos que ocorrem durante a operação dos componentes de proteção ou enquanto as tarefas do Kaspersky Anti-Virus são executadas são registrados em relatórios.

NESTA SEÇÃO:

CRIANDO UM RELATÓRIO PARA O COMPONENTE DE PROTEÇÃO SELECIONADO

Você pode obter um relatório detalhado dos eventos ocorridos durante a operação de cada componente do Kaspersky Anti-Virus ou durante a execução de suas tarefas.

Para trabalhar com os relatórios de forma mais conveniente, você pode alterar a exibição dos dados na tela: agrupar eventos de acordo com diversos parâmetros, selecionar o período do relatório, classificar eventos por coluna ou por importância e ocultar colunas.

Para criar um relatório de determinada tarefa ou determinado componente de proteção:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela, clique no link **Relatórios**.
3. Na janela **Relatórios** que é aberta, clique no botão **Relatório detalhado**.
4. À esquerda da janela **Relatório detalhado** que é aberta, selecione o componente ou a tarefa para o qual deve ser criado um relatório. Ao selecionar o item **Centro de Proteção**, é criado um relatório de todos os componentes de proteção.

FILTRAGEM DE DADOS

Você pode filtrar os eventos dos relatórios do Kaspersky Anti-Virus por um ou vários valores nas colunas do relatório, além de definir condições complexas de filtragem de dados.

Para filtrar os eventos de acordo com seus valores:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela, clique no link **Relatórios**.
3. Na janela **Relatórios** que é aberta, clique no botão **Relatório detalhado**.
4. À direita da janela **Relatório detalhado** que é aberta, mova o ponteiro do mouse para o canto superior esquerdo do cabeçalho da coluna e clique nele para abrir o menu do filtro.
5. Selecione o valor que deve ser usado para filtrar dados no menu do filtro.
6. Repita o procedimento para outra coluna, se necessário.

Para especificar uma condição complexa de filtragem:

1. Abra a janela principal do aplicativo.
2. Clique no link **Relatórios** na parte superior da janela para abrir a janela de relatórios.
3. Na janela que é aberta, na guia **Relatório**, clique no botão **Relatório detalhado**.
4. À direita da janela **Relatório detalhado** que é aberta, clique com o botão direito do mouse na coluna do relatório apropriada para exibir o menu de contexto correspondente e selecione **Personalizado**.
5. Na janela **Filtro personalizado** que é aberta, defina as configurações de filtragem:
   a. Defina os limites da consulta à direita da janela.
   b. À esquerda da janela, na lista suspensa **Condição**, selecione as condições de consulta desejadas (por exemplo, é maior ou menor, igual ou diferente do valor especificado como limite de consulta).
   c. Se necessário, adicione uma segunda condição usando as operações lógicas de conjunção (AND lógico) ou disjunção (OR lógico). Se deseja que sua consulta de dados atenda às duas condições especificadas, selecione **E**. Se apenas uma das duas condições for necessária, selecione **OU**.

PESQUISA DE EVENTOS

Você pode pesquisar em um relatório o evento desejado usando uma palavra-chave na linha de pesquisa ou na janela de pesquisa especial.

Para localizar um evento usando a linha de pesquisa:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela, clique no link **Relatórios**.
3. Na janela **Relatórios** que é aberta, clique no botão **Relatório detalhado**.
4. Insira a palavra-chave na linha de pesquisa à direita da janela **Relatório detalhado** que é aberta.

Para localizar um evento usando a janela de pesquisa:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela, clique no link **Relatórios**.
3. Na janela **Relatórios** que é aberta, clique no botão **Relatório detalhado**.
4. À direita da janela **Relatório detalhado** que é aberta, clique com o botão direito do mouse no cabeçalho da coluna apropriada para exibir o menu de contexto correspondente e selecione **Pesquisar**.
5. Especifique os critérios de pesquisa na janela **Pesquisar** que é aberta:
   a. No campo **Texto**, insira uma palavra-chave para a pesquisa.
   b. Na lista suspensa **Coluna**, selecione o nome da coluna na qual deve ser pesquisada a palavra-chave especificada.
   c. Se necessário, marque as caixas correspondentes às configurações de pesquisa adicionais.
6. Inicie a pesquisa usando um dos seguintes métodos:
   - Se desejar localizar um evento que atenda aos critérios de pesquisa especificados e esteja depois daquele que você realçou na lista, clique no botão **Localizar próximo**.
   - Se desejar localizar todos os eventos que atendam aos critérios de pesquisa especificados, clique no botão **Marcar tudo**.

SALVANDO UM RELATÓRIO EM ARQUIVO

O relatório obtido pode ser gravado em um arquivo de texto.

Para salvar o relatório em arquivo:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela, clique no link **Relatórios**.
3. Na janela **Relatórios** que é aberta, clique no botão **Relatório detalhado**.
4. Na janela **Relatório detalhado** que é aberta, crie o relatório desejado e clique no link **Salvar** para selecionar um local para o arquivo que você deseja salvar.
5. Na janela que é aberta, selecione a pasta na qual você deseja salvar o arquivo de relatório e insira o nome do arquivo.

ARMAZENANDO RELATÓRIOS

O período máximo de armazenamento de relatórios é de 30 dias. Depois disso, os relatórios serão excluídos. Você pode cancelar a restrição de tempo ou alterar a duração máxima do armazenamento de relatórios.

Além disso, também é possível definir o tamanho máximo dos arquivos de relatório. Por padrão, o tamanho máximo é 1024 MB. Quando ele for atingido, o conteúdo do arquivo será substituído por novos registros. Você pode cancelar os limites impostos sobre o tamanho do relatório ou inserir outro valor.

Para modificar o tempo máximo de armazenamento de relatórios:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Relatórios e Armazenamentos**.
3. À direita da janela, na seção **Armazenando relatórios**, marque a caixa **Armazenar relatórios por no máximo** e especifique o período máximo de armazenamento de relatórios.

Para configurar o tamanho máximo dos arquivos de relatório:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Relatórios e Armazenamentos**.
3. À direita da janela, na seção **Armazenando relatórios**, marque a caixa **Tamanho máximo de arquivo** e especifique o tamanho máximo dos arquivos de relatório.

LIMPANDO OS RELATÓRIOS DO APLICATIVO

Você pode limpar os relatórios que contêm dados que não são mais necessários.

Para limpar os relatórios *do aplicativo:*

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Relatórios e Armazenamentos**.
3. À direita da janela, na seção **Limpar relatórios**, clique no botão **Limpar**.
4. Na janela **Limpando relatórios** que é aberta, marque as caixas dos relatórios que você deseja limpar.

GRAVANDO EVENTOS NÃO CRÍTICOS NO RELATÓRIO

Por padrão, o produto não adiciona eventos não críticos ou eventos do Registro e do sistema de arquivos aos relatórios. Você pode adicionar registros desse eventos ao relatório.

Para adicionar eventos não críticos ao relatório:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Relatórios e Armazenamentos**.
3. À direita da janela, desmarque a caixa **Registrar eventos não-críticos**.

CONFIGURANDO A NOTIFICAÇÃO DE DISPONIBILIDADE DE RELATÓRIOS

Você pode criar uma programação de acordo com a qual o Kaspersky Anti-Virus o lembrará sobre a disponibilidade de um relatório.

Para configurar a notificação de conclusão de um relatório:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela, clique no link **Relatórios**.
3. Na janela **Relatórios** que é aberta, clique no botão  .
4. Na janela **Notificações** que é aberta, especifique as configurações da programação.

EXIBIÇÃO DO APLICATIVO. GERENCIANDO OS ELEMENTOS ATIVOS DA INTERFACE

O Kaspersky Anti-Virus permite ajustar as configurações de exibição de texto na tela de login do Microsoft Windows e dos elementos ativos da interface (o ícone do aplicativo na área de notificação da barra de tarefas, janelas de notificação e mensagens pop-up).

NESTA SEÇÃO:

TRANSLUCIDEZ DAS JANELAS DE NOTIFICAÇÕES

Para tornar as janelas de notificações translúcidas:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Aparência**.
3. Na seção **Ícone na área de notificação da barra de tarefas**, desmarque a caixa **Habilitar janelas semi-transparentes**.

ANIMAÇÃO DO ÍCONE DO APLICATIVO NA ÁREA DE NOTIFICAÇÃO

A animação do ícone do aplicativo é exibida na área de notificação ao executar uma atualização ou uma verificação.

Por padrão, a animação do ícone do aplicativo na área de notificação está ativada.

Para desativar a animação do ícone do aplicativo:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Aparência**.
3. Na seção **Ícone na área de notificação da barra de tarefas**, desmarque a caixa **Ícone animado na barra de ferramentas ao executar tarefas**.

TEXTO NA TELA DE LOGIN DO MICROSOFT WINDOWS

Por padrão, se o Kaspersky Anti-Virus estiver ativado e protegendo seu computador, o texto "Protegido pela Kaspersky Lab" será exibido na tela de login durante o carregamento do Microsoft Windows.

O texto "Protegido pela Kaspersky Lab" será exibido somente no Microsoft Windows XP.

Para ativar a exibição desse texto durante o carregamento do Microsoft Windows:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Aparência**.
3. Na seção **Ícone na área de notificação da barra de tarefas**, desmarque a caixa **Mostrar "Protegido pela Kaspersky Lab" na tela de logon do Microsoft Windows**.

NOTIFICAÇÕES

Por padrão, se ocorrerem eventos durante sua operação, o Kaspersky Anti-Virus o notificará. Se for necessário selecionar outras ações, serão exibidas janelas de notificação na tela (consulte a seção "Janelas de notificação e mensagens pop-up" na página 30). O aplicativo notifica sobre eventos que não exigem a seleção de uma ação por meio de sinais de áudio, emails e mensagens pop-up na área de notificação da barra de tarefas (consulte a seção "Janelas de notificação e mensagens pop-up" na página 30).

O Kaspersky Anti-Virus compreende o Agente de Notícias (na página 33) usado pela Kaspersky Lab para notificá-lo sobre notícias diversas. Se você não desejar receber notícias, poderá desativar sua entrega.

NESTA SEÇÃO:

ATIVANDO E DESATIVANDO AS NOTIFICAÇÕES

Por padrão, o Kaspersky Anti-Virus usa vários métodos para notificá-lo sobre todos os eventos importantes relacionados à operação do aplicativo (consulte a seção "Configurando o método de notificação" na página 108). É possível desativar a entrega de notificações.

Independentemente da entrega de notificações estar ativada ou desativada, as informações sobre eventos ocorridos durante a operação do Kaspersky Anti-Virus são registradas em um relatório de operação do aplicativo (veja a página 103).

A desativação da entrega de notificações não afeta a exibição das janelas de notificação. Para minimizar o número de janelas de notificação exibidas na tela, use o modo de proteção automática (consulte a seção "Selecionando um modo de proteção" na página 56).

Para desativar a entrega de notificações:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Notificações**.
3. À direita da janela, desmarque a caixa **Ativar notificações de eventos**.

CONFIGURANDO O MÉTODO DE NOTIFICAÇÃO

O aplicativo notifica sobre eventos usando os seguintes métodos:

- mensagens pop-up na área de notificação da barra de tarefas;
- notificações de áudio;
- mensagens por email.

Você pode configurar um conjunto individual de métodos de entrega de notificações para cada tipo de evento.

Por padrão, as notificações críticas e de falhas de operação do aplicativo são acompanhadas de um sinal de áudio. O esquema de som do Microsoft Windows é usado como fonte dos efeitos sonoros. Você pode modificar o esquema atual ou desativar os sons.

Para que o Kaspersky Anti-Virus o notifique sobre eventos por email, ajuste as configurações de entrega de notificações por email.

Para selecionar os métodos de entrega de notificações para diversos tipos de evento:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Notificações**.
3. À direita da janela, marque a caixa **Ativar notificações de eventos** e clique no botão **Configurações** abaixo da caixa.
4. Na janela **Notificações** que é aberta, marque as caixas de acordo com a forma como deseja ser notificado sobre os diversos eventos: por email, através de mensagens pop-up ou por um sinal de áudio.

Para modificar as configurações de email para a entrega de notificações:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Notificações**.
3. À direita da janela, marque a caixa **Ativar notificações por email** e clique no botão **Configurações**.
4. Na janela **Configurações de notificação por email** que é aberta, especifique as configurações de envio de notificações por email.

Para configurar o esquema de som usado com as notificações:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Notificações**.
3. À direita da janela, desmarque a caixa **Ativar notificações de áudio**.

   Se desejar usar o esquema de som do Microsoft Windows para a notificação de eventos do Kaspersky Anti-Virus, marque a caixa **Usar esquema de som Padrão do Windows**. Se esta caixa estiver desmarcada, será usado o esquema de som das versões anteriores do Kaspersky Anti-Virus.

DESATIVANDO A ENTREGA DE NOTÍCIAS

Para desativar a entrega de notícias na janela de configurações do aplicativo:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Aparência**.
3. À direita da janela, desmarque a caixa **Ativar notificações de notícias**.

KASPERSKY SECURITY NETWORK

Para aumentar a eficiência da proteção do computador, o Kaspersky Anti-Virus usa dados recebidos de usuários de todo o mundo. O Kaspersky Security Network foi criado para coletar esses dados.

O Kaspersky Security Network (KSN) é uma infraestrutura de serviços online que dá acesso à Base de Dados de Conhecimento online da Kaspersky Lab, que contém informações sobre a reputação de arquivos, recursos da Web e software. A utilização de dados do Kaspersky Security Network garante um tempo de resposta menor do Kaspersky Anti-Virus ao encontrar novos tipos de ameaças, melhora o desempenho de alguns componentes de proteção e reduz a possibilidade de falsos positivos.

A participação dos usuários no Kaspersky Security Network permite que a Kaspersky Lab colete informações em tempo real sobre os tipos e fontes de novas ameaças, desenvolva métodos para neutralizá-las e reduza o número de falsos positivos.

Além disso, a participação no Kaspersky Security Network permite que você acesse informações sobre a reputação de diversos aplicativos e sites.

Quando você participa do Kaspersky Security Network, determinadas estatísticas coletadas enquanto o Kaspersky Anti-Virus protege seu computador são enviadas automaticamente para a Kaspersky Lab.

Nenhum dado particular é coletado, processado ou armazenado.

A participação no Kaspersky Security Network é voluntária. Você deve decidir se deseja participar ao instalar o Kaspersky Anti-Virus; contudo, é possível alterar sua decisão posteriormente.

NESTA SEÇÃO:

ATIVANDO E DESATIVANDO A PARTICIPAÇÃO NO KASPERSKY SECURITY NETWORK

Para participar do Kaspersky Security Network:

1. Abra a janela de configurações do aplicativo.
2. À esquerda da janela, na seção **Configurações Avançadas**, selecione a subseção **Feedback**.
3. À direita da janela, marque a caixa **Concordo em participar do programa Kaspersky Security Network**.

VERIFICANDO A CONEXÃO COM O KASPERSKY SECURITY NETWORK

A conexão com o Kaspersky Security Network pode ser perdida devido aos seguintes motivos:

- seu computador não está conectado à Internet;
- você não participa do Kaspersky Security Network;
- sua licença do Kaspersky Anti-Virus é limitada.

Para testar a conexão com o Kaspersky Security Network:

1. Abra a janela principal do aplicativo.
2. Na parte superior da janela, clique no botão **Proteção em nuvem**.
3. À esquerda da janela que é aberta, é exibido o status de conexão com o Kaspersky Security Network.

TESTANDO A OPERAÇÃO DO APLICATIVO

Esta seção fornece informações sobre como garantir que o aplicativo detecte vírus e suas modificações, e execute as ações corretas com eles.

NESTA SEÇÃO:

SOBRE O ARQUIVO DE TESTE DA EICAR

Você pode se certificar de que o aplicativo detecta vírus e desinfeta arquivos infectados usando o *arquivo de teste da EICAR*. O arquivo de teste da EICAR foi desenvolvido pela EICAR (European Institute for Computer Antivirus Research) para testar a funcionalidade de aplicativos antivírus.

O arquivo de teste da EICAR não é um vírus. O arquivo de teste da EICAR não contém nenhum código de programa que possa danificar seu computador. No entanto, uma grande parte dos aplicativos antivírus identifica o arquivo de teste da EICAR como vírus.

O arquivo de teste da EICAR não tem a finalidade de testar a funcionalidade do analisador heurístico ou de procurar malware no nível do sistema (rootkits).

Não use vírus reais para testar a funcionalidade de aplicativos antivírus! Isso pode danificar seu computador.

Não esqueça de reiniciar a proteção antivírus do tráfego da Internet e dos arquivos depois de ter concluído os procedimentos com o arquivo de teste da EICAR.

TESTANDO O FUNCIONAMENTO DO APLICATIVO USANDO O ARQUIVO DE TESTE DA EICAR

Você pode usar o arquivo de teste da EICAR para testar a proteção do tráfego da Internet, a proteção antivírus de arquivos e a verificação do computador.

Não esqueça de reiniciar a proteção antivírus do tráfego da Internet e dos arquivos depois de ter concluído os procedimentos com o arquivo de teste da EICAR.

- *Para testar a proteção do tráfego da Internet usando o arquivo de teste da EICAR:*

  1. Você pode baixar este arquivo de teste do site oficial da EICAR em http://www.eicar.org/anti_virus_test_file.htm.
  2. Tente salvar o arquivo de teste da EICAR em qualquer pasta do computador.

     O Kaspersky Anti-Virus informa que foi detectada uma ameaça no URL solicitado e bloqueia a tentativa de salvar o objeto no computador.
  3. Se necessário, você pode usar vários tipos do arquivo de teste da EICAR (consulte a seção "Sobre os tipos do arquivo de teste da EICAR" na página 112).

- *Para testar a proteção antivírus de arquivos usando o arquivo de teste da EICAR ou uma modificação dele*:

  1. Pause a proteção antivírus do tráfego da Internet e de arquivos no computador.

     Quando a proteção estiver pausada, é recomendável não conectar o computador a redes locais, nem usar dispositivos removíveis para evitar que malwares danifiquem o computador.

2. Você pode baixar este arquivo de teste do site oficial da EICAR em http://www.eicar.org/anti_virus_test_file.htm.
3. Salve o arquivo de teste da EICAR em qualquer pasta do computador.
4. Adicione um dos prefixos ao cabeçalho do arquivo de teste da EICAR (consulte a seção "Sobre os tipos do arquivo de teste da EICAR" na página 112).

   Você pode usar qualquer editor de texto ou hipertexto para fazer isso, por exemplo, o Bloco de Notas. Para abrir o Bloco de Notas, selecione **Iniciar → Todos os programas → Acessórios → Bloco de Notas**.
5. Salve o arquivo resultante com um nome que reflita a modificação do arquivo da EICAR; por exemplo, adicione o prefixo DELE- e salve o arquivo como eicar_dele.com.
6. Reinicie a proteção antivírus do tráfego da Internet e de arquivos no computador.
7. Tente executar o arquivo que você salvou.

   O Kaspersky Anti-Virus o informa sobre uma ameaça detectada no disco rígido do computador e executa a ação especificada nas configurações da proteção antivírus de arquivos.

Para testar a verificação de vírus usando o arquivo de teste da EICAR ou uma modificação dele:

1. Pause a proteção antivírus do tráfego da Internet e de arquivos no computador.

   Quando a proteção estiver pausada, é recomendável não conectar o computador a redes locais, nem usar dispositivos removíveis para evitar que malwares danifiquem o computador.
2. Você pode baixar este arquivo de teste do site oficial da EICAR em http://www.eicar.org/anti_virus_test_file.htm.
3. Adicione um dos prefixos ao cabeçalho do arquivo de teste da EICAR (consulte a seção "Sobre os tipos do arquivo de teste da EICAR" na página 112).

   Você pode usar qualquer editor de texto ou hipertexto para fazer isso, por exemplo, o Bloco de Notas. Para abrir o Bloco de Notas, selecione **Iniciar → Todos os programas → Acessórios → Bloco de Notas**.
4. Salve o arquivo resultante com um nome que reflita a modificação do arquivo de teste da EICAR; por exemplo, adicione o prefixo DELE- e salve o arquivo como eicar_dele.com.
5. Execute a verificação do arquivo que você salvou.

   O Kaspersky Anti-Virus o informa sobre uma ameaça detectada no disco rígido do computador e executa a ação especificada nas configurações da verificação de vírus.
6. Reinicie a proteção antivírus do tráfego da Internet e de arquivos no computador.

SOBRE OS TIPOS DO ARQUIVO DE TESTE DA EICAR

Você pode testar o funcionamento do aplicativo por meio da criação de várias modificações do arquivo de teste da EICAR. O aplicativo detecta o arquivo de teste da EICAR (ou uma modificação dele) e atribui um status a ele de acordo com os resultados da verificação. O aplicativo executará determinadas ações com o arquivo de teste da EICAR se elas tiverem sido selecionadas nas configurações do componente que detectou o arquivo.

A primeira coluna da tabela (veja a tabela a seguir) contém prefixos que podem ser usados ao criar modificações do arquivo de teste da EICAR. A segunda coluna lista todos os status possíveis atribuídos ao arquivo com base nos resultados da verificação executada pelo aplicativo. A terceira coluna indica como o aplicativo processa os arquivos com o status especificado.

Tabela 2. Modificações do arquivo de teste da EICAR

Prefixo	Status do arquivo	Informação de processamento do arquivo
Sem prefixo, vírus de teste padrão.	**Infectado.** O arquivo contém o código de um vírus conhecido. O arquivo não pode ser desinfetado.	O aplicativo identifica este arquivo como contendo um vírus que não pode ser desinfetado. A ação definida para arquivos infectados é aplicada ao arquivo. Por padrão, o aplicativo exibe uma notificação na tela de que não é possível desinfetar o arquivo.

Prefixo	Status do arquivo	Informação de processamento do arquivo
CURE-	**Infectado.** O arquivo contém o código de um vírus conhecido. O arquivo pode ser desinfetado.	O arquivo contém um vírus que pode ser desinfetado ou excluído. O aplicativo desinfeta o arquivo; o texto do corpo do vírus será substituído pela palavra CURE. O aplicativo exibe uma notificação na tela informando que foi detectado um arquivo desinfetado.
DELE-	**Infectado.** O arquivo contém o código de um vírus conhecido. O arquivo não pode ser desinfetado.	O aplicativo identifica o arquivo como um vírus que não pode ser desinfetado e o exclui. O aplicativo exibe uma notificação na tela informando o arquivo desinfetado foi excluído.
WARN-	**Possivelmente infectado**. O arquivo contém o código de um vírus desconhecido. O arquivo não pode ser desinfetado.	É possível que o arquivo esteja infectado. O aplicativo executa a ação definida para arquivos possivelmente infectados com o arquivo. Por padrão, o aplicativo exibe uma notificação na tela informando que foi detectado um arquivo possivelmente infectado.
SUSP-	**Possivelmente infectado.** O arquivo contém o código modificado de um vírus conhecido. O arquivo não pode ser desinfetado.	O aplicativo detectou uma correspondência parcial de uma seção do código do arquivo com uma seção do código de um vírus conhecido. Quando um arquivo possivelmente infectado é detectado, os bancos de dados não contêm uma descrição do código completo do vírus. O aplicativo executa a ação definida para arquivos possivelmente infectados com o arquivo. Por padrão, o aplicativo exibe uma notificação na tela informando que foi detectado um arquivo possivelmente infectado.
CORR-	**Corrompido.**	O aplicativo não verifica este tipo de arquivo porque sua estrutura está danificada (por exemplo, o formato de arquivo é inválido). Você pode encontrar informações de que o arquivo foi processado no relatório de operação do aplicativo.
ERRO-	**Erro de verificação.**	Ocorreu um erro durante a verificação de um arquivo. O aplicativo não pôde acessar o arquivo, pois sua integridade foi violada (por exemplo, não existe um final em um arquivo comprimido com vários volumes) ou não é possível conectá-lo (se o arquivo for verificado em uma unidade de rede). Você pode encontrar informações de que o arquivo foi processado no relatório de operação do aplicativo.

ENTRANDO EM CONTATO COM O SERVIÇO DE SUPORTE TÉCNICO

Esta seção fornece informações sobre como obter suporte técnico e quais as condições necessárias para obter ajuda do Serviço de Suporte Técnico.

NESTA SEÇÃO:

COMO OBTER SUPORTE TÉCNICO

Se você não encontrar uma solução para seu problema na documentação do aplicativo ou em uma das fontes de informações sobre o aplicativo (consulte a seção "Fontes de informações sobre o aplicativo" na página 11), é recomendável entrar em contato com o Serviço de Suporte Técnico da Kaspersky Lab. Os especialistas do Serviço de Suporte Técnico responderão todas as suas dúvidas sobre a instalação e o uso do aplicativo. Se o computador estiver infectado, nossos especialistas o ajudarão a corrigir os problemas causados por malware.

Antes de entrar em contato com o Serviço de Suporte Técnico, leia as regras de suporte (http://support.kaspersky.com/support/rules).

Você pode entrar em contato com o Serviço de Suporte Técnico de uma das seguintes maneiras:

- Por telefone. Este método permite consultar especialistas do nosso Serviço de Suporte Técnico em russo ou internacional.
- Enviando uma consulta da Minha conta Kaspersky no site do Serviço de Suporte Técnico. Este método permite o contato com nossos especialistas usando o formulário de consulta.

Para se qualificar para obter suporte técnico, você deve ser usuário registrado de uma versão comercial do Kaspersky Anti-Virus. O suporte técnico não está disponível para usuários das versões de avaliação do aplicativo.

USANDO O ARQUIVO DE RASTREAMENTO E O SCRIPT DO AVZ

Depois de notificar os especialistas do Serviço de Suporte Técnico sobre um problema ocorrido, eles podem solicitar que você crie um relatório com informações sobre o sistema operacional e o envie para o Serviço de Suporte Técnico. Além disso, os especialistas do Serviço de Suporte Técnico podem solicitar que você crie um *arquivo de rastreamento*. O arquivo de rastreamento permite acompanhar passo a passo o processo de execução dos comandos do aplicativo e descobrir em que estágio o erro ocorreu.

Depois que os especialistas do Serviço de Suporte Técnico analisarem os dados que você enviar, eles poderão criar um script do AVZ e enviá-lo para você. Ao executar os scripts do AVZ, você pode analisar os processos ativos e verificar o sistema quanto à presença de código malicioso, desinfetar/excluir arquivos infectados e criar relatórios com os resultados das verificações do sistema.

CRIANDO UM RELATÓRIO DE ESTADO DO SISTEMA

Para criar um relatório de estado do sistema:

1. Abra a janela principal do aplicativo.
2. Clique no link **Suporte** na parte inferior da janela principal para abrir a janela **Suporte** e siga o link **Ferramentas de Suporte**.
3. Na janela **Ferramentas de Suporte** que é aberta, clique no botão **Criar relatório de estado do sistema**.

O relatório de estado do sistema é criado nos formatos HTML e XML e é salvo no arquivo comprimido sysinfo.zip. Quando as informações tiverem sido coletadas, você poderá exibir o relatório.

Para exibir o relatório:

1. Abra a janela principal do aplicativo.
2. Clique no link **Suporte** na parte inferior da janela principal para abrir a janela **Suporte** e siga o link **Ferramentas de Suporte**.
3. Na janela **Ferramentas de Suporte** que é aberta, clique no botão **Exibir**.
4. Abra o arquivo comprimido sysinfo.zip, que contém os arquivos de relatório.

CRIANDO UM ARQUIVO DE RASTREAMENTO

Para criar o arquivo de rastreamento:

1. Abra a janela principal do aplicativo.
2. Clique no link **Suporte** na parte inferior da janela principal para abrir a janela **Suporte** e siga o link **Ferramentas de Suporte**.
3. Na janela **Ferramentas de Suporte** que é aberta, especifique o nível de rastreamento na lista suspensa da seção **Rastros**.

   É recomendável esclarecer o nível de rastreamento desejado com um especialista do Serviço de Suporte Técnico. Quando não houver orientação do Serviço de Suporte Técnico, é recomendável definir o nível de rastreamento como **500**.
4. Para iniciar o processo de rastreamento, clique no botão **Ativar**.
5. Reconstrua a situação em que o problema ocorreu.
6. Para interromper o processo de rastreamento, clique no botão **Desativar**.

Você pode alternar para o carregamento de resultados de rastreamento (consulte a seção "Enviando arquivos de dados" na página 115) no servidor da Kaspersky Lab.

ENVIANDO ARQUIVOS DE DADOS

Depois de criar os arquivos de rastreamento e o relatório de estado do sistema, você deverá enviá-los aos especialistas do Serviço de Suporte Técnico da Kaspersky Lab.

Você precisará de um número de solicitação para carregar os arquivos de dados no servidor do Serviço de Suporte Técnico. Esse número estará disponível na sua Minha conta Kaspersky no site do Serviço Suporte Técnico, se a sua solicitação estiver ativa.

Para carregar os arquivos de dados no servidor do Serviço de Suporte Técnico:

1. Abra a janela principal do aplicativo.
2. Clique no link **Suporte** na parte inferior da janela principal para abrir a janela **Suporte** e siga o link **Ferramentas de Suporte**.
3. Na janela **Ferramentas de Suporte** que é aberta, na seção **Ações**, clique no botão **Carregar informações para o Serviço de Suporte Técnico no servidor**.

   A janela **Carregando informações no servidor para o Serviço de Suporte Técnico** será aberta.
4. Marque as caixas ao lado dos arquivos de rastreamento que você deseja enviar ao Serviço de Suporte Técnico e clique no botão **Enviar**.

   A janela **Número da solicitação** será aberta.
5. Especifique o número atribuído à sua solicitação entrando em contato com o Serviço de Suporte Técnico através da Minha Conta Kaspersky e clique no botão **OK**.

Os arquivos de dados selecionados são compactados e enviados ao servidor do Serviço de Suporte Técnico.

Se, por algum motivo, não for possível entrar em contato com o Serviço de Suporte Técnico, os arquivos de dados poderão ser armazenados no seu computador e enviados posteriormente a partir da Minha conta Kaspersky.

Para salvar os arquivos de dados em disco:

1. Abra a janela principal do aplicativo.
2. Clique no link **Suporte** na parte inferior da janela principal para abrir a janela **Suporte** e siga o link **Ferramentas de Suporte**.
3. Na janela **Ferramentas de Suporte** que é aberta, na seção **Ações**, clique no botão **Carregar informações para o Serviço de Suporte Técnico no servidor**.

   A janela **Carregando informações no servidor para o Serviço de Suporte Técnico** será aberta.
4. Marque as caixas ao lado dos arquivos de rastreamento que você deseja enviar ao Serviço de Suporte Técnico e clique no botão **Enviar**.

   A janela **Número da solicitação** será aberta.
5. Clique no botão **Cancelar** e, na janela que é aberta, confirme a gravação dos arquivos em disco clicando no botão **Sim**.

   A janela para gravação do arquivo comprimido será aberta.
6. Especifique o nome do arquivo comprimido e confirme a gravação.

O arquivo comprimido criado pode ser enviado ao Serviço de Suporte Técnico a partir da Minha conta Kaspersky.

EXECUÇÃO DO SCRIPT DO AVZ

Não é recomendável alterar o texto de um script do AVZ recebido dos especialistas da Kaspersky Lab. Se ocorrerem problemas durante a execução do script, entre em contato com o Serviço de Suporte Técnico (consulte a seção "Como obter suporte técnico" na página 114).

Para executar o script do AVZ:

1. Abra a janela principal do aplicativo.
2. Clique no link **Suporte** na parte inferior da janela principal para abrir a janela **Suporte** e siga o link **Ferramentas de Suporte**.
3. Na janela **Ferramentas de Suporte** que é aberta, clique no botão **Executar script do AVZ**.

Se o script for executado com êxito, o Assistente será fechado. Se ocorrer um erro durante a execução do script, o Assistente exibirá uma mensagem correspondente.

SUPORTE TÉCNICO POR TELEFONE

Se ocorrer um problema urgente, você poderá ligar para os especialistas do Serviço de Suporte Técnico (http://suporte.kasperskyamericas.com/usuarios-domesticos/env%C3%ADe-um-caso-de-suporte).

Antes de entrar em contato com o Serviço de Suporte Técnico, você deve coletar informações (http://support.kaspersky.com/support/details) sobre o computador e os aplicativos antivírus instalados. Assim, nossos especialistas poderão ajudá-lo mais rapidamente.

OBTENDO SUPORTE TÉCNICO ATRAVÉS DA MINHA CONTA KASPERSKY

Minha conta Kaspersky é sua área pessoal (https://my.kaspersky.com/en/index.html?LANG=pt) no site do Serviço de Suporte Técnico.

Para obter acesso à Minha conta Kaspersky, execute o procedimento de registro na página de registro (https://my.kaspersky.com/en/registration?LANG=pt). Insira seu endereço de email e uma senha para entrar na Minha conta Kaspersky.

Na Minha conta Kaspersky, você pode executar as seguintes ações:

- entrar em contato com o Serviço de Suporte Técnico e o Laboratório de Vírus;
- entrar em contato com o Serviço de Suporte Técnico sem usar o email;
- rastrear o status das suas solicitações em tempo real;
- exibir um histórico detalhado de suas solicitações para o Serviço de Suporte Técnico;
- receber uma cópia do arquivo de chave, caso ele tenha sido perdido ou removido.

Suporte técnico por email

Você pode enviar uma solicitação online para o Serviço de Suporte Técnico em russo, inglês, alemão, francês ou espanhol.

Você deve especificar os seguintes dados nos campos do formulário de solicitação online:

- tipo de solicitação;
- nome do aplicativo e número da versão;
- descrição da solicitação;
- ID do cliente e senha;
- endereço de email.

Um especialista do Serviço de Suporte Técnico envia uma resposta à sua pergunta para a Minha conta Kaspersky e para o endereço de email especificado na solicitação online.

Solicitação online para o Laboratório de Vírus

Algumas solicitações devem ser enviadas para o Laboratório de Vírus e não para o Serviço de Suporte Técnico.

Você pode enviar os seguintes tipos de solicitações para o Laboratório de Vírus:

- *Programa malicioso desconhecido* – você suspeita que um arquivo contém um vírus, mas o Kaspersky Anti-Virus não o identificou como infectado.

  Os especialistas do Laboratório de Vírus analisam o código malicioso enviado. Se detectarem um vírus desconhecido, eles adicionarão uma descrição correspondente ao banco de dados, que se tornará disponível ao atualizar os aplicativos antivírus.

- *Falso positivo* – o Kaspersky Anti-Virus classifica um arquivo como vírus, mas você tem certeza de que o arquivo não é um vírus.

- *Solicitação de descrição de programa malicioso* – você deseja receber a descrição de um vírus detectado pelo Kaspersky Anti-Virus usando o nome do vírus.

Também é possível enviar solicitações ao Laboratório de Vírus da página com o formulário de solicitação (http://support.kaspersky.com/virlab/helpdesk.html?LANG=pt) sem estar registrado na Minha conta Kaspersky. Nessa página, não é necessário especificar o código de ativação do aplicativo.

APÊNDICE

Esta seção fornece informações que complementam o texto da documentação.

NESTA SEÇÃO:

TRABALHANDO COM O APLICATIVO NA LINHA DE COMANDO

Você pode trabalhar com o Kaspersky Anti-Virus na linha de comando. É possível executar as seguintes operações:

- ativar o aplicativo;
- iniciar e interromper o aplicativo;
- iniciar e interromper componentes do aplicativo;
- iniciar e interromper as tarefas;
- obter informações sobre o status atual dos componentes e das tarefas, além de suas estatísticas;
- iniciar e interromper tarefas de verificação de vírus;
- verificar os objetos selecionados;
- atualizar os bancos de dados e módulos do software, reverter atualizações;
- exportar e importar configurações de segurança;
- abrir os arquivos de ajuda usando a sintaxe geral da linha de comando e de comandos individuais.

Sintaxe do prompt de comando:

```
avp.com <comando> [opções]
```

Acesse o aplicativo na linha de comando a partir da pasta de instalação do aplicativo ou especificando o caminho completo de avp.com.

A lista de comandos usados para controlar o aplicativo e seus componentes é fornecida na tabela a seguir.

START	Inicia um componente ou uma tarefa.
STOP	Interrompe um componente ou uma tarefa. O comando poderá ser executado somente se a senha atribuída através da interface do Kaspersky Anti-Virus for inserida.
STATUS	Exibe o status atual do componente ou da tarefa na tela.
STATISTICS	Exibe estatísticas do componente ou da tarefa na tela.
HELP	Exibe a lista de comandos e informações sobre a sintaxe de comandos.
SCAN	Verifica objetos quanto à presença de vírus.
UPDATE	Inicia a atualização do aplicativo.
ROLLBACK	Reverte para a última atualização do Kaspersky Anti-Virus. O comando poderá ser executado somente se a senha atribuída através da interface do Kaspersky Anti-Virus for inserida.

EXIT	Fecha o aplicativo. O comando poderá ser executado somente se a senha atribuída através da interface do aplicativo for inserida.
IMPORT	Importa as configurações de proteção do aplicativo. O comando poderá ser executado somente se a senha atribuída através da interface do Kaspersky Anti-Virus for inserida.
EXPORT	Exporta as configurações de proteção do aplicativo.

Cada comando exige seu próprio conjunto específico de configurações.

NESTA SEÇÃO:

ATIVANDO O APLICATIVO

É possível ativar o Kaspersky Anti-Virus usando um arquivo de chave.

Sintaxe do comando:

```
avp.com ADDKEY <nome_do_arquivo)>
```

A tabela a seguir descreve as configurações de execução do comando.

<nome_do_arquivo>	Nome do arquivo de chave do aplicativo com a extensão *.key.

Exemplo:

```
avp.com ADDKEY 1AA111A1.key
```

INICIANDO O APLICATIVO

Sintaxe do comando:

```
avp.com
```

INTERROMPENDO O APLICATIVO

Sintaxe do comando:

```
avp.com EXIT /password=<sua_senha>
```

A descrição dos parâmetros é fornecida na tabela a seguir.

<sua_senha>	Senha do aplicativo especificada na interface.

Este comando não será aceito sem uma senha.

GERENCIANDO COMPONENTES E TAREFAS DO APLICATIVO

Sintaxe do comando:

```
avp.com <comando> <perfil|nome_da_tarefa> [/R[A]:<arquivo_de_relatório>]
avp.com STOP <profile|nome_da_tarefa> /password=<sua_senha>
[/R[A]:<arquivo_de_relatório>]
```

A tabela a seguir fornece as descrições de comandos e configurações.

<comando>	Você pode gerenciar as tarefas e os componentes do Kaspersky Anti-Virus a partir do prompt de comando, com os seguintes comandos: START – inicia uma tarefa ou um componente de proteção. STOP – interrompe uma tarefa ou um componente de proteção. STATUS – exibe o status atual da tarefa ou do componente de proteção. STATISTICS – exibe na tela as estatísticas da tarefa ou do componente de proteção. O comando STOP não será aceito sem uma senha.
<perfil|nome_da_tarefa>	Você pode especificar qualquer componente de proteção, módulo dos componentes, tarefa de verificação por demanda ou de atualização do Kaspersky Anti-Virus como valor da configuração **<perfil>** (os valores padrão usados pelo aplicativo são mostrados na tabela a seguir). Você pode especificar o nome de qualquer tarefa de atualização ou verificação por demanda como valor da configuração **<nome_da_tarefa>**.
<sua_senha>	Senha do aplicativo especificada na interface.
/R[A]:<arquivo_de_relatório>	**/R:<arquivo_de_relatório>** – registra somente os eventos importantes no relatório. **/RA:<arquivo_de_relatório>** – registra todos os eventos no relatório. Você pode usar um caminho absoluto ou relativo para o arquivo. Se a configuração não for definida, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.

Na configuração **<perfil>**, especifique um dos valores fornecidos na tabela a seguir.

RTP	Todos os componentes de proteção. O comando **avp.com START RTP** executa todos os componentes de proteção, se a proteção tiver sido totalmente desativada. Se o componente tiver sido desativado usando o comando **STOP** no prompt de comando, ele não será iniciado pelo comando **avp.com START RTP**. Para iniciá-lo, execute o comando **avp.com START <perfil>** com o nome do componente de proteção específico inserido em **<perfil>**; por exemplo, **avp.com START FM**.
pdm	Defesa Proativa.
FM	Antivírus de Arquivos.
EM	Antivírus de Email.
WM	Antivírus da Web. Valores dos subcomponentes do Antivírus da Web: **httpscan (HTTP)** – verifica o tráfego HTTP; **sc** – verifica scripts.
IM	Antivírus de IM.
Updater	Atualização.

Rollback	Reversão da última atualização.
Scan_My_Computer	Verificação.
Scan_Objects	Verificação de Objetos.
Scan_Quarantine	Verificação da Quarentena.
Scan_Startup (STARTUP)	Verificação de Objetos de Inicialização.
Scan_Vulnerabilities (SECURITY)	Verificação de Vulnerabilidades.

Os componentes e tarefas iniciados no prompt de comando são executados com as configurações definidas na interface do aplicativo.

Exemplos:

- *Para ativar o Antivírus de Arquivos:*

```
avp.com START FM
```

- *Para interromper a verificação do computador:*

```
avp.com STOP Scan_My_Computer /password=<sua_senha>
```

VERIFICAÇÃO DE VÍRUS

Em geral, a execução da verificação de vírus em uma determinada área e o processamento de objetos maliciosos no prompt de comando tem uma aparência semelhante à seguinte:

```
avp.com SCAN [<objeto verificado>] [<ação>] [<tipos de arquivos>] [<exclusões>]
[<arquivo de configuração>] [<configurações relatório>] [<configurações avançadas>]
```

Para verificar objetos, você também pode usar as tarefas criadas no aplicativo, iniciando-as na linha de comando. A tarefa será executada com as configurações especificadas na interface do Kaspersky Anti-Virus.

A descrição dos parâmetros é fornecida na tabela a seguir.

<objeto a ser verificado> – este parâmetro fornece a lista de objetos que serão verificados quanto à presença de código malicioso. Ele pode incluir vários valores da lista fornecida separados por espaços.	
<arquivos>	Lista dos caminhos de arquivos e pastas que devem ser verificados. Você pode inserir um caminho absoluto ou relativo para o arquivo. Os itens da lista são separados por um espaço. Comentários: • se o nome do objeto contiver um espaço, será necessário colocá-lo entre aspas; • se for feita uma referência a uma pasta específica, todos os arquivos da pasta serão verificados.
/MEMORY	Objetos da RAM.
/STARTUP	Objetos de inicialização.
/MAIL	Caixas de correio.
/REMDRIVES	Todas as unidades de mídia removíveis.
/FIXDRIVES	Todas as unidades internas.
/NETDRIVES	Todas as unidades de rede.

/QUARANTINE	Objetos da Quarentena.
/ALL	Verificação completa do computador.
/@:<filelist.lst>	Caminho para um arquivo que contém uma lista de objetos e catálogos a serem verificados. Você pode inserir um caminho absoluto ou relativo para o arquivo com a lista. Mesmo que contenha espaços, o caminho deverá ser indicado sem aspas. O arquivo com a lista de objetos deve estar em formato de texto. Cada objeto de verificação deve estar listado em uma linha separada. É recomendável especificar os caminhos absolutos dos objetos a serem verificados. Ao especificar um caminho relativo, é necessário especificar o caminho relativo ao arquivo executável de um aplicativo e não ao arquivo com a lista de objetos a serem verificados.
<ação> – este parâmetro determina que ações serão executadas com objetos maliciosos detectados durante a verificação. Se este parâmetro não for definido, a ação padrão será aquela com o valor **/i8**. Ao trabalhar no modo automático, o Kaspersky Anti-Virus aplica automaticamente a ação recomendada pelos especialistas da Kaspersky Lab ao detectar objetos perigosos. Uma ação que corresponda ao valor do parâmetro **<ação>** será ignorada.	
/i0	Não é tomada nenhuma ação em relação ao objeto; suas informações são registradas no relatório.
/i1	Neutraliza objetos infectados e, se a desinfecção falhar, os ignora.
/i2	Desinfeta os objetos infectados, ignora se a desinfecção falhar; não exclui objetos infectados de objetos compostos; exclui objetos compostos infectados com cabeçalhos executáveis (arquivos comprimidos sfx).
/i3	Desinfeta os objetos infectados, ignora se a desinfecção falhar; exclui completamente todos os objetos compostos, se não for possível excluir os arquivos incorporados infectados.
/i4	Exclui os objetos infectados. Exclui completamente todos os objetos compostos, se não for possível excluir as partes infectadas.
/i8	Pergunta o que fazer se for detectado um objeto infectado.
/i9	Pergunta o que fazer no final da verificação.
<tipos_de_arquivos> – este parâmetro define os tipos de arquivos que estarão sujeitos à verificação antivírus. Por padrão, se esse parâmetro não for definido, apenas os arquivos que podem ser infectados por conteúdo serão verificados.	
/fe	Verifica somente os arquivos que podem ser infectados de acordo com sua extensão.
/fi	Verifica somente os arquivos que podem ser infectados de acordo com seu conteúdo.
/fa	Verifica todos os arquivos.
<exclusões> – este parâmetro define os objetos excluídos da verificação. Ele pode incluir vários valores da lista fornecida separados por espaços.	
-e:a	Não verifica arquivos comprimidos.
-e:b	Não verifica bancos de dados de email.
-e:m	Não verifica emails em texto sem formatação.
-e:<máscara_arquivos>	Não verifica objetos que correspondem à máscara.

-e:<segundos>	Ignora objetos cujo tempo de verificação ultrapassa o tempo especificado no parâmetro **<segundos>**.
-es:<tamanho>	Ignora objetos cujo tamanho (em MB) excede o valor especificado na configuração **<tamanho>**. Esta configuração estará disponível apenas para arquivos compostos (como arquivos comprimidos).
<arquivo de configuração> – define o caminho do arquivo de configuração que contém as configurações de verificação do aplicativo. O arquivo de configuração está no formato de texto e contém o conjunto de parâmetros da linha de comando para a verificação antivírus. Você pode inserir um caminho absoluto ou relativo para o arquivo. Se este parâmetro não for definido, serão usados os valores definidos na interface do aplicativo.	
/C:<nome_do_arquivo>	Usa os valores das configurações especificadas no arquivo **<nome_do_arquivo>**.
<configurações relatório> – este parâmetro determina o formato do relatório de resultados da verificação. Você pode usar um caminho absoluto ou relativo para o arquivo. Se a configuração não for definida, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.	
/R:<arquivo_de_relatório>	Registra apenas os eventos importantes nesse arquivo.
/RA:<arquivo_de_relatório>	Registra todos os eventos nesse arquivo.
<configurações avançadas> – configurações que definem o uso das tecnologias de verificação antivírus.	
/iChecker=<on|off>	Ativa/desativa o uso da tecnologia iChecker.
/iSwift=<on|off>	Ativa/desativa o uso da tecnologia iSwift.

Exemplos:

- *Iniciar a verificação da memória, dos programas de inicialização, das caixas de correio, dos diretórios de Meus Documentos e Arquivos de Programas e do arquivo test.exe:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and Settings\All Users\Meus documentos" "C:\Arquivos de programas" "C:\Downloads\test.exe"
```

- *Verificar os objetos listados no arquivo object2scan.txt. usando o arquivo de configuração scan_setting.txt para o trabalho. Usar o arquivo de configuração scan_settings.txt. Ao concluir a verificação, criar um relatório de todos os eventos:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

Um exemplo de arquivo de configuração:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt /RA:scan.log
```

ATUALIZANDO O APLICATIVO

A sintaxe para atualizar os módulos do Kaspersky Anti-Virus e os bancos de dados do aplicativo da linha de comando é a seguinte:

```
avp.com UPDATE [<fonte_de_atualização>] [/R[A]:<arquivo_de_relatório>]
[/C:<nome_do_arquivo>]
```

A descrição dos parâmetros é fornecida na tabela a seguir.

<fonte_de_atualização>	Servidor HTTP ou FTP ou pasta de rede para baixar as atualizações. O valor do parâmetro pode estar no formato de um caminho completo para uma fonte de atualização ou um URL. Se não for selecionado um caminho, a fonte da atualização será obtida da configurações de atualização do aplicativo.
/R[A]:<arquivo_de_relatório>	**/R:<arquivo_de_relatório>** – registra somente os eventos importantes no relatório. **/RA:<arquivo_de_relatório>** – registra todos os eventos no relatório. Você pode usar um caminho absoluto ou relativo para o arquivo. Se a configuração não for definida, os resultados da verificação serão exibidos na tela e todos os eventos

	serão mostrados.
/C:<nome_do_arquivo>	Caminho do arquivo de configuração da atualização do Kaspersky Anti-Virus. O arquivo de configuração está no formato de texto sem formatação e contém uma lista de parâmetros da linha de comando para a atualização do aplicativo. Você pode inserir um caminho absoluto ou relativo para o arquivo. Se esse parâmetro não for definido, serão usados os valores definidos na interface do aplicativo.

Exemplos:

- *Atualizar os bancos de dados do aplicativo e registrar todos os eventos no relatório:*

```
avp.com UPDATE /RA:avbases_upd.txt
```

- *Atualizar os módulos do Kaspersky Anti-Virus usando as configurações do arquivo de configuração updateapp.ini:*

```
avp.com UPDATE /C:updateapp.ini
```

Um exemplo de arquivo de configuração:

```
"ftp://meu_servidor/kav updates" /RA:avbases_upd.txt
```

REVERTENDO A ÚLTIMA ATUALIZAÇÃO

Sintaxe do comando:

```
avp.com ROLLBACK [/R[A]:<arquivo_de_relatório>][/password=<sua_senha>]
```

A descrição dos parâmetros é fornecida na tabela a seguir.

/R[A]:<arquivo_de_relatório>	**/R:<arquivo_de_relatório>** – registra somente os eventos importantes no relatório. **/RA:<arquivo_de_relatório>** – registra todos os eventos no relatório. Você pode usar um caminho absoluto ou relativo para o arquivo. Se a configuração não for definida, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.
<sua_senha>	Senha do aplicativo especificada na interface.

Este comando não será aceito sem uma senha.

Exemplo:

```
avp.com ROLLBACK /RA:rollback.txt /password=<sua_senha>
```

EXPORTANDO AS CONFIGURAÇÕES DE PROTEÇÃO

Sintaxe do comando:

```
avp.com EXPORT <perfil> <nome_do_arquivo>
```

A tabela a seguir descreve as configurações de execução do comando.

<perfil>	Componente ou tarefa cujas configurações estão sendo exportadas. Para a configuração **<perfil>**, você pode usar qualquer valor listado na seção da Ajuda "Gerenciando componentes e tarefas do aplicativo".
<nome_do_arquivo>	Caminho do arquivo para o qual as configurações do Kaspersky Anti-Virus estão sendo exportadas. É possível especificar um caminho absoluto ou relativo. Se nenhum formato for especificado, o arquivo de configuração será salvo no formato binário (DAT) e poderá ser usado posteriormente para exportar as configurações do aplicativo para outros computadores. O arquivo de configuração também pode ser gravado como um arquivo de texto. Para fazê-lo, digite a extensão .txt no nome do arquivo. Não é possível importar configurações de proteção de um arquivo de texto. Este arquivo pode ser usado somente para especificar as principais configurações de operação do Kaspersky Anti-Virus.

Exemplo:

```
avp.com EXPORT RTP c:\settings.dat
```

IMPORTANDO AS CONFIGURAÇÕES DE PROTEÇÃO

Sintaxe do comando:

```
avp.com IMPORT <nome_do_arquivo> [/password=<sua_senha>]
```

A tabela a seguir descreve as configurações de execução do comando.

<nome_do_arquivo>	Caminho do arquivo do qual as configurações do Kaspersky Anti-Virus são importadas. É possível especificar um caminho absoluto ou relativo.
<sua_senha>	Senha do Kaspersky Anti-Virus especificada na interface do aplicativo. Os parâmetros de segurança podem ser importados somente de um arquivo binário.

Este comando não será aceito sem uma senha.

Exemplo:

```
avp.com IMPORT c:\ settings.dat /password=<sua_senha>
```

CRIANDO UM ARQUIVO DE RASTREAMENTO

A criação do arquivo de rastreamento pode ser necessária no caso de problemas de operação do Kaspersky Anti-Virus. Isso ajudará os especialistas de Suporte Técnico a diagnosticar os problemas com mais precisão.

É recomendável criar arquivos de rastreamento apenas para a solução de um problema específico. A ativação normal do rastreamento pode tornar o computador lento e sobrecarregar o disco rígido.

Sintaxe do comando:

```
avp.com TRACE [file] [on|off] [<nível_de_rastreamento>]
```

A descrição dos parâmetros é fornecida na tabela a seguir.

[on|off]	Ativa/desativa a criação do arquivo de rastreamento.
[file]	Saída do rastreamento em arquivo.
<nível_de_rastreamento>	O valor desta configuração pode ser de 0 (nível mínimo, apenas mensagens críticas) a 700 (nível máximo, todas as mensagens). O Suporte Técnico o informará sobre o nível de rastreamento necessário quando você entrar em contato. Se o nível não for especificado, é recomendável configurá-lo como 500.

Exemplos:

- *Para desativar a criação do arquivo de rastreamento:*

```
avp.com TRACE file off
```

- *Para criar um arquivo de rastreamento para enviar ao Suporte Técnico com um nível de rastreamento máximo de 500:*

```
avp.com TRACE file on 500
```

EXIBINDO A AJUDA

O comando a seguir é usado para exibir a ajuda da sintaxe da linha de comando:

```
avp.com [ /? | HELP ]
```

Você pode usar um dos seguintes comandos para exibir informações de ajuda da sintaxe de um comando específico:

```
avp.com <comando> /?
avp.com HELP <comando>
```

CÓDIGOS DE RETORNO DA LINHA DE COMANDO

Esta seção descreve os códigos de retorno da linha de comando (veja a tabela a seguir). Os códigos gerais podem ser retornados por qualquer comando da linha de comando. Os códigos de retorno incluem códigos gerais e códigos específicos de um determinado tipo de tarefa.

CÓDIGOS DE RETORNO GERAIS	
0	Operação concluída com êxito.
1	Valor de configuração inválido.
2	Erro desconhecido.
3	Erro ao concluir a tarefa.
4	Tarefa cancelada.
CÓDIGOS DE RETORNO DA TAREFA DE VERIFICAÇÃO DE VÍRUS	
101	Todos os objetos perigosos foram processados.
102	Objetos perigosos detectados.

LISTA DE NOTIFICAÇÕES DO KASPERSKY ANTI-VIRUS

Esta seção fornece informações sobre as notificações que podem ser exibidas na tela pelo Kaspersky Anti-Virus.

NESTA SEÇÃO:

NOTIFICAÇÕES EM QUALQUER MODO DE PROTEÇÃO

Esta seção fornece informações sobre as notificações que são exibidas nos modos de proteção interativa e automática (consulte a seção "Selecionando um modo de proteção" na página 56).

NESTA SEÇÃO:

NEUTRALIZAÇÃO ESPECIAL NECESSÁRIA

Ao detectar uma ameaça ativa no sistema (por exemplo, um processo malicioso na RAM ou em objetos de inicialização), será exibida uma notificação na tela solicitando a confirmação de um procedimento especial de desinfecção avançada.

A notificação fornece as seguintes informações:

- Descrição da ameaça.
- Tipo de ameaça e nome do objeto malicioso conforme listado na Enciclopédia de Vírus da Kaspersky Lab.

  O ícone é exibido ao lado do nome do objeto malicioso. Ao clicar no ícone, é aberta uma janela com informações sobre o objeto. Ao clicar no link www.securelist.com nesta janela, você é direcionado para o site da Enciclopédia de Vírus e pode obter informações mais detalhadas sobre a ameaça imposta pelo objeto.
- Nome do arquivo do objeto malicioso, incluindo seu caminho.

Você pode selecionar uma das seguintes ações:

- **Sim, desinfetar ao reiniciar** – executa o procedimento de desinfecção especial (recomendável).

  Enquanto a desinfecção está em andamento, todos os aplicativos são bloqueados, exceto os confiáveis. Quando a desinfecção for concluída, o sistema operacional será reiniciado; assim, é recomendável salvar as alterações feitas e fechar todos os aplicativos antes de iniciar a desinfecção. Depois de reiniciar o computador, é recomendável executar uma verificação completa de vírus.
- **Não executar** – o objeto ou o processo detectado será processado de acordo com a ação selecionada.

Para aplicar a ação selecionada automaticamente sempre que essa situação ocorrer novamente, marque a caixa **Aplicar a todos os objetos**.

UNIDADE REMOVÍVEL CONECTADA

Quando uma unidade removível é conectada ao computador, é exibida uma notificação na tela.

Você pode selecionar uma das seguintes ações:

- **Verificação Rápida** – verifica apenas os arquivos armazenados na unidade removível que podem representar uma possível ameaça.
- **Verificação Completa** – verifica todos os arquivos armazenados na unidade removível.
- **Não verificar** – não verifica a unidade removível.

Para aplicar a ação selecionada a todas as unidades removíveis que podem ser conectadas no futuro, marque a caixa **Nesses casos, sempre executar**.

CERTIFICADO NÃO CONFIÁVEL DETECTADO

O Kaspersky Anti-Virus verifica a segurança da conexão estabelecida com o protocolo SSL usando um certificado instalado. Se um certificado inválido for detectado ao tentar a conexão com o servidor (por exemplo, se o certificado for substituído por um invasor), será exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- descrição da ameaça;
- um link para exibir o certificado;
- causas prováveis do erro;
- o URL do recurso da Web.

Você pode selecionar uma das seguintes ações:

- **Sim, aceitar o certificado não confiável** – dá prosseguimento à conexão com o recurso da Web.
- **Negar o certificado** – interrompe a conexão com o site.

FOI DETECTADO UM APLICATIVO QUE PODE SER EXPLORADO POR UM INVASOR PARA DANIFICAR O COMPUTADOR OU OS DADOS DO USUÁRIO

Quando o Monitor de Atividade detecta um aplicativo que pode ser explorado por um invasor para danificar o computador ou os dados do usuário, é exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- Descrição da ameaça.
- O tipo e o nome do aplicativo que pode ser explorado por um invasor para danificar o computador ou os dados do usuário.

  O ícone é exibido ao lado do nome do aplicativo. Ao clicar no ícone, é aberta uma janela com informações sobre o aplicativo.
- ID do processo e nome do arquivo do aplicativo, incluindo seu caminho.
- Link para a janela com o log de emergência do aplicativo.

Você pode selecionar uma das seguintes ações:

- **Permitir** – permite a execução do aplicativo.
- **Quarentena** – fecha o aplicativo e move o arquivo do aplicativo para a Quarentena, onde ele não representa nenhuma ameaça à segurança do computador.

  Talvez o status do objeto mude com outras verificações da Quarentena. Por exemplo, o objeto pode ser identificado como infectado e ser processado usando um banco de dados atualizado. Caso contrário, pode ser atribuído a ele o status *não infectado* e ele pode ser restaurado.

O status de um arquivo movido para a Quarentena pode ser alterado para *não infectado* em uma próxima verificação, mas não antes de três dias após ele ser movido para a Quarentena.

- **Encerrar o aplicativo** – interromper a execução do aplicativo.
- **Adicionar às exclusões** – sempre permitir que o aplicativo execute essas ações no futuro.

ARQUIVO DA QUARENTENA NÃO INFECTADO

Por padrão, o Kaspersky Anti-Virus verifica os arquivos em quarentena após cada atualização dos bancos de dados. Se a verificação de um arquivo da Quarentena mostrar que ele não está infectado, será exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- uma recomendação de restaurar o arquivos da Quarentena;
- o nome do arquivo, incluindo o caminho da pasta na qual ele foi armazenado antes de ser movido para a Quarentena.

Você pode selecionar uma das seguintes ações:

- **Restaurar** – restaura o arquivo, movendo-o da Quarentena para a pasta na qual ele foi armazenado antes de ser movido para a Quarentena.
- **Cancelar** – deixa o arquivo na Quarentena.

LANÇAMENTO DE NOVA VERSÃO DO PRODUTO

Quando uma nova versão do Kaspersky Anti-Virus é lançada e está disponível para download nos servidores da Kaspersky Lab, é exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- um link para a janela com informações detalhadas sobre a versão recém-lançada do aplicativo;
- o tamanho do pacote de instalação.

Você pode selecionar uma das seguintes ações:

- **Sim, baixar** – baixa o pacote de instalação da nova versão do aplicativo na pasta selecionada.
- **Não** – cancela o download do pacote de instalação.

Se você não desejar que a notificação sobre novas versões do aplicativo seja exibida na tela no futuro, marque a caixa **Não lembrar-me dessa atualização**.

LANÇAMENTO DE ATUALIZAÇÃO TÉCNICA

Quando uma atualização técnica do Kaspersky Anti-Virus é lançada e está disponível para download nos servidores da Kaspersky Lab, é exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- o número da versão do aplicativo instalada no computador;
- o número da versão do aplicativo após a atualização técnica esperada;
- um link para a janela com informações detalhadas sobre a atualização técnica;
- o tamanho do arquivo de atualização.

Você pode selecionar uma das seguintes ações:

- **Sim, baixar** – baixa o arquivo de atualização na pasta selecionada.
- **Não** – cancela o download da atualização. Esta opção estará disponível se a caixa **Não lembrar-me dessa atualização** estiver marcada (veja a seguir).
- **Não, lembre-me mais tarde** – cancela o download imediato e recebe uma notificação da atualização posteriormente. Esta opção estará disponível se a caixa **Não lembrar-me dessa atualização** estiver desmarcada (veja a seguir).

Se você não desejar que a notificação sobre novas versões do aplicativo seja exibida na tela no futuro, marque a caixa **Não lembrar-me dessa atualização**.

ATUALIZAÇÃO TÉCNICA BAIXADA

Quando o download da atualização técnica do Kaspersky Anti-Virus dos servidores da Kaspersky Lab for concluído, será exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- o número da versão do aplicativo após a atualização técnica;
- um link para o arquivo de atualização.

Você pode selecionar uma das seguintes ações:

- **Sim, instalar** – instala a atualização.

  Depois que a atualização for instalada, será necessário reiniciar o sistema operacional.

- **Adiar instalação** – cancela a instalação para executá-la posteriormente.

ATUALIZAÇÃO TÉCNICA BAIXADA NÃO INSTALADA

Quando uma atualização técnica do Kaspersky Anti-Virus é baixado mas não é instalado no computador, é exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- o número da versão do aplicativo após a atualização técnica;
- um link para o arquivo de atualização.

Você pode selecionar uma das seguintes ações:

- **Sim, instalar** – instala a atualização.

  Depois que a atualização for instalada, será necessário reiniciar o sistema operacional.

- **Adiar instalação** – cancela a instalação para executá-la posteriormente.

Se você não desejar que a notificação sobre esta atualização seja exibida na tela no futuro, marque a caixa **Não perguntar até que haja uma nova versão disponível**.

LICENÇA EXPIRADA

Quando a licença de avaliação expirar, o Kaspersky Anti-Virus exibirá uma notificação na tela.

A notificação fornece as seguintes informações:

- a duração do período de avaliação;
- informações sobre o resultado da operação do aplicativo (pode incluir um link para obter mais detalhes).

Você pode selecionar uma das seguintes ações:

- **Sim, comprar** – ao selecionar esta opção, é aberta uma janela do navegador e carregada a página da Loja Virtual, na qual é possível comprar a licença comercial.
- **Cancelar** – interrompe o uso do aplicativo. Se você selecionar esta opção, o aplicativo interromperá a execução de todas as suas funções principais (verificação de vírus, atualização, proteção em tempo real, etc.).

É RECOMENDÁVEL ATUALIZAR OS BANCOS DE DADOS ANTES DA VERIFICAÇÃO

Se você iniciar tarefas de verificação antes ou durante a primeira atualização dos bancos de dados, será exibida uma notificação na tela.

A notificação contém uma recomendação de atualizar os bancos de dados ou aguardar a conclusão da atualização antes da verificação.

Você pode selecionar uma das seguintes ações:

- **Atualizar bancos de dados antes da verificação** – inicia a atualização dos bancos de dados, após a qual a tarefa de verificação será iniciada automaticamente. Esta opção de ação não estará disponível se você tiver iniciado a tarefa de verificação antes da primeira atualização dos bancos de dados.
- **Iniciar verificação após atualização** – aguarda a conclusão da atualização dos bancos de dados e inicia a tarefa de verificação automaticamente. Esta opção de ação não estará disponível se você tiver iniciado a tarefa de verificação durante a primeira atualização dos bancos de dados.
- **Iniciar verificação agora** – inicia a tarefa de verificação sem aguardar a conclusão da atualização dos bancos de dados.

NOTIFICAÇÕES NO MODO DE PROTEÇÃO INTERATIVA

Esta seção fornece informações sobre as notificações que são exibidas no modo de proteção interativa (consulte a seção "Selecionando um modo de proteção" na página 56).

NESTA SEÇÃO:

OBJETO SUSPEITO/MALICIOSO DETECTADO

Enquanto o Antivírus de Arquivos, o Antivírus de Email ou uma verificação de vírus estiverem em execução, será exibida uma notificação na tela se algum dos seguintes objetos for detectado:

- objeto malicioso;
- objeto que contém o código de um vírus desconhecido;
- objeto que contém o código modificado de um vírus desconhecido.

A notificação fornece as seguintes informações:

- Descrição da ameaça.
- Tipo de ameaça e nome do objeto malicioso conforme listado na Enciclopédia de Vírus da Kaspersky Lab.

  O ícone é exibido ao lado do nome do objeto malicioso. Ao clicar no ícone, é aberta uma janela com informações sobre o objeto. Ao clicar no link www.securelist.com nesta janela, você é direcionado para o site da Enciclopédia de Vírus e pode obter informações mais detalhadas sobre a ameaça imposta pelo objeto.
- Nome do arquivo do objeto malicioso, incluindo seu caminho.

Você pode selecionar uma das seguintes respostas ao objeto:

- **Desinfetar** – tenta desinfetar o objeto malicioso. Esta opção é recomendável quando a ameaça é desconhecida.

  Antes de desinfetar o objeto, é criada uma cópia de backup dele.

- **Quarentena** – move o objeto para a Quarentena, onde ele não representa uma ameaça ao computador. Esta opção é recomendável quando a ameaça e as formas de desinfetar o objeto são desconhecidas.

  Talvez o status do objeto mude com outras verificações da Quarentena. Por exemplo, o objeto pode ser identificado como infectado e ser processado usando um banco de dados atualizado. Caso contrário, pode ser atribuído a ele o status *não infectado* e ele pode ser restaurado.

  O status de um arquivo movido para a Quarentena pode ser alterado para *não infectado* em uma próxima verificação, mas não antes de três dias após ele ser movido para a Quarentena.

- **Excluir** – exclui o objeto. Antes de excluir o objeto, é criada uma cópia de backup dele.

- **Ignorar/Bloquear** – bloqueia o acesso ao objeto, mas não executa nenhuma ação com ele; simplesmente registra suas informações em um relatório.

  Você pode retornar ao processamento de objetos ignorados na janela do relatório. Contudo, não é possível adiar o processamento de objetos detectados em emails.

Para aplicar a ação selecionada a todas as ameaças do mesmo tipo detectadas na sessão atual de um componente ou uma tarefa de proteção, marque a caixa **Aplicar a todos os objetos**. A sessão atual é o período entre o início do componente até ele ser desativado ou o Kaspersky Anti-Virus ser reiniciado, ou o período entre o início e a conclusão de uma verificação de vírus.

Se tiver certeza de que o objeto detectado não é malicioso, é recomendável adicioná-lo à zona confiável para evitar que o programa gere falsos positivos repetidamente quando você usar o objeto.

VULNERABILIDADE DETECTADA

Será exibida uma notificação na tela se for detectada uma vulnerabilidade.

A notificação contém as seguintes informações:

- Descrições da vulnerabilidade.
- O nome da vulnerabilidade conforme listado na Enciclopédia de Vírus da Kaspersky Lab.

  O ícone é exibido ao lado do nome. Ao clicar no ícone, é aberta uma janela com informações sobre a vulnerabilidade. Ao clicar em www.securelist.com na janela, você é direcionado para o site da Enciclopédia de Vírus, na qual é possível obter informações mais detalhadas sobre a vulnerabilidade.
- Nome do arquivo do objeto vulnerável, incluindo seu caminho.

Você pode selecionar uma das seguintes respostas ao objeto:

- **Sim, corrigir** – elimina a vulnerabilidade.
- **Ignorar** – não executa nenhuma ação com o objeto vulnerável.

ATIVIDADE PERIGOSA DETECTADA NO SISTEMA

Quando a Defesa Proativa detecta a atividade perigosa de um aplicativo no sistema, é exibida uma notificação pop-up.

A notificação contém as seguintes informações:

- Descrição da ameaça.
- Tipo de ameaça e nome do objeto malicioso conforme listado na Enciclopédia de Vírus da Kaspersky Lab.

  O ícone é exibido ao lado do nome do objeto malicioso. Ao clicar no ícone, é aberta uma janela com informações sobre o objeto. Ao clicar no link www.securelist.com nesta janela, você é direcionado para o site da Enciclopédia de Vírus e pode obter informações mais detalhadas sobre a ameaça imposta pelo objeto.
- ID do processo e nome do arquivo do aplicativo, incluindo seu caminho.

Você pode selecionar uma das seguintes ações:

- **Permitir** – permite a execução do aplicativo.
- **Quarentena** – fecha o aplicativo e move o arquivo do aplicativo para a Quarentena, onde ele não representa nenhuma ameaça à segurança do computador.

  Talvez o status do objeto mude com outras verificações da Quarentena. Por exemplo, o objeto pode ser identificado como infectado e ser processado usando um banco de dados atualizado. Caso contrário, pode ser atribuído a ele o status *não infectado* e ele pode ser restaurado.

  O status de um arquivo movido para a Quarentena pode ser alterado para *não infectado* em uma próxima verificação, mas não antes de três dias após ele ser movido para a Quarentena.

- **Encerrar o aplicativo** – interromper a execução do aplicativo.
- **Adicionar às exclusões** – sempre permitir que o aplicativo execute essas ações no futuro.

Se tiver certeza de que o programa detectado não é perigoso, é recomendável adicioná-lo à zona confiável, para evitar que o Kaspersky Anti-Virus repita falsos positivos ao detectá-lo.

REVERTER AS ALTERAÇÕES FEITAS PELO APLICATIVO QUE PODE SER EXPLORADO POR UM INVASOR PARA DANIFICAR O COMPUTADOR OU OS DADOS DO USUÁRIO

É recomendável reverter (descartar) as alterações feitas pelo aplicativo que pode ser explorado por um invasor para danificar o computador ou os dados do usuário. Quando esse aplicativo cessa suas atividades, é exibida uma notificação na tela solicitando a reversão das alterações.

A notificação fornece as seguintes informações:

- Solicitação da reversão das alterações feitas pelo aplicativo que pode ser explorado por um invasor para danificar o computador ou os dados do usuário.
- Tipo e nome do aplicativo.

  O ícone é exibido ao lado do nome do aplicativo. Ao clicar no ícone, é aberta uma janela com informações sobre o aplicativo.

- ID do processo e nome do arquivo do aplicativo, incluindo seu caminho.

Você pode selecionar uma das seguintes ações:

- **Ignorar** – cancela a reversão de alterações.
- **Sim, reverter** – reverte as alterações feitas pelo aplicativo.

APLICATIVO MALICIOSO DETECTADO

Quando o Inspetor do Sistema detecta um aplicativo cujo comportamento corresponde inteiramente às atividades de aplicativos maliciosos, é exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- Descrição da ameaça.
- Tipo e nome do aplicativo malicioso.

  O ícone é exibido ao lado do nome do aplicativo. Ao clicar no ícone, é aberta uma janela com informações sobre o aplicativo.

- ID do processo e nome do arquivo do aplicativo, incluindo seu caminho.
- Link para a janela com o log de emergência do aplicativo.

Você pode selecionar uma das seguintes ações:

- **Permitir** – permite a execução do aplicativo.
- **Quarentena** – fecha o aplicativo e move o arquivo do aplicativo para a Quarentena, onde ele não representa nenhuma ameaça à segurança do computador.

Talvez o status do objeto mude com outras verificações da Quarentena. Por exemplo, o objeto pode ser identificado como infectado e ser processado usando um banco de dados atualizado. Caso contrário, pode ser atribuído a ele o status *não infectado* e ele pode ser restaurado.

O status de um arquivo movido para a Quarentena pode ser alterado para *não infectado* em uma próxima verificação, mas não antes de três dias após ele ser movido para a Quarentena.

- **Encerrar o aplicativo** – interromper a execução do aplicativo.
- **Adicionar às exclusões** – sempre permitir que o aplicativo execute essas ações no futuro.

FOI DETECTADO UM APLICATIVO QUE PODE SER EXPLORADO POR INVASORES

Se o Antivírus de Arquivos, o Antivírus de Email ou a tarefa de verificação de vírus detectar um aplicativo que pode ser explorado por invasores, será exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- Descrição da ameaça.
- Tipo de ameaça e nome do objeto conforme listado na Enciclopédia de Vírus da Kaspersky Lab.

  O ícone é exibido ao lado do nome do objeto. Ao clicar no ícone, é aberta uma janela com informações sobre o objeto. Ao clicar no link www.securelist.com na janela, você pode ir para o site da Enciclopédia de Vírus e obter mais detalhes.
- Nome do arquivo do objeto, incluindo seu caminho.

Você pode selecionar uma das seguintes respostas ao objeto:

- **Quarentena** – move o objeto para a Quarentena, onde ele não representa uma ameaça ao computador. Esta opção é recomendável quando a ameaça e as formas de desinfetar o objeto são desconhecidas.

  Talvez o status do objeto mude com outras verificações da Quarentena. Por exemplo, o objeto pode ser identificado como infectado e ser processado usando um banco de dados atualizado. Caso contrário, pode ser atribuído a ele o status *não infectado* e ele pode ser restaurado.

  O status de um arquivo movido para a Quarentena pode ser alterado para *não infectado* em uma próxima verificação, mas não antes de três dias após ele ser movido para a Quarentena.
- **Excluir** – exclui o objeto. Antes de excluir o objeto, é criada uma cópia de backup dele.
- **Excluir arquivo comprimido** - exclui o arquivo comprimido protegido por senha.
- **Ignorar/Bloquear** – bloqueia o acesso ao objeto, mas não executa nenhuma ação com ele; simplesmente registra suas informações em um relatório.

  Você pode retornar ao processamento de objetos ignorados na janela do relatório. Contudo, não é possível adiar o processamento de objetos detectados em emails.
- **Adicionar às exclusões** - cria uma regra de exclusão para este tipo de ameaça.

Para aplicar a ação selecionada a todas as ameaças do mesmo tipo detectadas na sessão atual de um componente ou uma tarefa de proteção, marque a caixa **Aplicar a todos os objetos**. A sessão atual é o período entre o início do componente até ele ser desativado ou o Kaspersky Anti-Virus ser reiniciado, ou o período entre o início e a conclusão de uma verificação de vírus.

Se tiver certeza de que o objeto detectado não é malicioso, é recomendável adicioná-lo à zona confiável para evitar que o programa gere falsos positivos repetidamente quando você usar o objeto.

LINK SUSPEITO/MALICIOSO DETECTADO

Quando o Kaspersky Anti-Virus detecta uma tentativa de ir para um site com conteúdo suspeito ou malicioso, uma notificação é exibida na tela.

A notificação fornece as seguintes informações:

- descrição da ameaça;
- o nome do aplicativo (navegador) com o qual o site foi carregado;
- o URL do site ou da página da Web com conteúdo suspeito ou malicioso.

Você pode selecionar uma das seguintes ações:

- **Permitir** – continua o download do site.
- **Bloquear** – bloqueia o download do site.

Para aplicar a ação selecionada a todos os sites com ameaças do mesmo tipo detectadas na sessão atual de um componente de proteção, marque a caixa **Aplicar a todos os objetos**. A sessão atual consiste no período desde o momento em que ele foi iniciado até o momento em que foi fechado ou o Kaspersky Anti-Virus foi reiniciado.

OBJETO PERIGOSO DETECTADO NO TRÁFEGO

Quando o Antivírus da Web detecta um objeto malicioso no tráfego, é exibida uma notificação especial na tela.

A notificação contém as seguintes informações:

- Uma descrição da ameaça ou das ações executadas pelo aplicativo.
- Nome do aplicativo que executa a ação.
- Tipo de ameaça e nome do objeto malicioso conforme listado na Enciclopédia de Vírus da Kaspersky Lab.

  O ícone  é exibido ao lado do nome do objeto malicioso. Ao clicar no ícone, é aberta uma janela com informações sobre o objeto. Ao clicar no link www.securelist.com nesta janela, você é direcionado para o site da Enciclopédia de Vírus e pode obter informações mais detalhadas sobre a ameaça imposta pelo objeto.
- Local do objeto (URL).

Você pode selecionar uma das seguintes ações:

- **Permitir** – continua o download do objeto.
- **Bloquear** – bloqueia o download do objeto do recurso da Web.

Para aplicar a ação selecionada a todas as ameaças do mesmo tipo detectadas na sessão atual de um componente ou uma tarefa de proteção, marque a caixa **Aplicar a todos os objetos**. A sessão atual consiste no período desde o momento em que ele foi iniciado até o momento em que foi fechado ou o Kaspersky Anti-Virus foi reiniciado.

TENTATIVA DE ACESSO A UM SITE DE PHISHING DETECTADA

Quando o Kaspersky Anti-Virus detecta uma tentativa de acessar um site que é ou que pode ser um site de phishing, é exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- descrição da ameaça;
- o URL do site.

Você pode selecionar uma das seguintes ações:

- **Permitir** – continua o download do site.
- **Bloquear** – bloqueia o download do site.

Para aplicar a ação selecionada a todos os sites com ameaças do mesmo tipo detectadas na sessão atual do Kaspersky Anti-Virus, marque a caixa **Aplicar a todos os objetos**. A sessão atual consiste no período desde o momento em que ele foi iniciado até o momento em que foi fechado ou o Kaspersky Anti-Virus foi reiniciado.

TENTATIVA DE ACESSO AO REGISTRO DO SISTEMA DETECTADA

Quando a Defesa Proativa detecta uma tentativa de acessar as chaves do Registro do sistema, é exibida uma notificação pop-up.

A notificação fornece as seguintes informações:

- a chave do Registro que está sendo acessada;
- o nome do arquivo do processo que iniciou a tentativa de acesso às chaves do Registro, incluindo seu caminho.

Você pode selecionar uma das seguintes ações:

- **Permitir** – permite a execução da ação perigosa uma vez;
- **Bloquear** – bloqueia a ação perigosa uma vez.

Para aplicar a ação selecionada a cada tentativa de obter acesso às chaves do Registro, marque a caixa **Criar uma regra**.

Se tiver certeza de que nenhuma atividade do aplicativo que tentou acessar as chaves do Registro do sistema é perigosa, adicione o aplicativo à lista de aplicativos confiáveis.

O OBJETO NÃO PODE SER DESINFETADO

Em alguns casos, não é possível desinfetar um objeto; por exemplo, se o arquivo estiver tão danificado que o aplicativo não consegue remover o código malicioso e restaurar sua integridade. Além disso, o procedimento de desinfecção não pode ser aplicado a diversos tipos de objetos malicioso, como os cavalos de Troia. Se não for possível desinfetar um objeto, será exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- Descrição da ameaça.
- Tipo de ameaça e nome do objeto malicioso conforme listado na Enciclopédia de Vírus da Kaspersky Lab.

  O ícone é exibido ao lado do nome do objeto malicioso. Ao clicar no ícone, é aberta uma janela com informações sobre o objeto. Ao clicar no link www.securelist.com nesta janela, você é direcionado para o site da Enciclopédia de Vírus e pode obter informações mais detalhadas sobre a ameaça imposta pelo objeto.
- Nome do arquivo do objeto malicioso, incluindo seu caminho.

Você pode selecionar uma das seguintes ações:

- **Excluir** – exclui o objeto. Antes de excluir o objeto, é criada uma cópia de backup dele.
- **Ignorar/Bloquear** – bloqueia o acesso ao objeto, mas não executa nenhuma ação com ele; simplesmente registra suas informações em um relatório.

  Você pode retornar ao processamento de objetos ignorados na janela do relatório. Contudo, não é possível adiar o processamento de objetos detectados em emails.
- **Adicionar às exclusões** - cria uma regra de exclusão para este tipo de ameaça.

Para aplicar a ação selecionada a todas as ameaças do mesmo tipo detectadas na sessão atual de um componente ou uma tarefa de proteção, marque a caixa **Aplicar a todos os objetos**. A sessão atual é o período entre o início do componente até ele ser desativado ou o Kaspersky Anti-Virus ser reiniciado, ou o período entre o início e a conclusão de uma verificação de vírus.

PROCESSO OCULTO DETECTADO

Se a Defesa Proativa detectar um processo oculto no sistema, será exibida uma notificação na tela.

A notificação fornece as seguintes informações:

- Descrição da ameaça.
- Tipo e nome da ameaça conforme listado na Enciclopédia de Vírus da Kaspersky Lab.

  O ícone é exibido ao lado do nome. Ao clicar no ícone, é aberta uma janela com informações sobre a ameaça. Ao clicar em www.securelist.com na janela, você é direcionado para o site da Enciclopédia de Vírus, na qual é possível obter informações mais detalhadas sobre a ameaça.
- Nome do arquivo do processo, incluindo seu caminho.

Você pode selecionar uma das seguintes ações:

- **Quarentena** – fecha o processo e move seu arquivo para a Quarentena, onde ele não representa nenhuma ameaça à segurança do computador.

  Talvez o status do objeto mude com outras verificações da Quarentena. Por exemplo, o objeto pode ser identificado como infectado e ser processado usando um banco de dados atualizado. Caso contrário, pode ser atribuído a ele o status *não infectado* e ele pode ser restaurado.

  > O status de um arquivo movido para a Quarentena pode ser alterado para *não infectado* em uma próxima verificação, mas não antes de três dias após ele ser movido para a Quarentena.
- **Encerrar** – interrompe o processo.
- **Permitir** – permite a execução do processo.

Para aplicar a ação selecionada a todas as ameaças do mesmo tipo detectadas na sessão atual da Defesa Proativa, marque a caixa **Aplicar a todos**. A sessão atual consiste no período desde o momento em que ele foi iniciado até o momento em que foi fechado ou o Kaspersky Anti-Virus foi reiniciado.

Se tiver certeza de que o processo detectado não é perigoso, é recomendável adicioná-lo à zona confiável para evitar que o Kaspersky Anti-Virus repita falsos positivos ao detectá-lo.

GLOSSÁRIO

A

Analisador heurístico

Uma tecnologia criada para detectar ameaças que não podem ser identificadas usando os bancos de dados do aplicativo da Kaspersky Lab. Permite detectar objetos suspeitos de infecção por um vírus desconhecido ou por uma nova modificação de vírus conhecidos.

O analisador heurístico detecta até 92% das ameaças. Esse mecanismo é bastante eficiente e raramente produz falsos positivos.

Os arquivos detectados pelo analisador heurístico são considerados suspeitos.

Aplicativo incompatível

Aplicativo antivírus de outro desenvolvedor ou aplicativo da Kaspersky Lab que não dá suporte ao gerenciamento por meio do Kaspersky Anti-Virus.

Arquivo compactado

Um arquivo comprimido que contém um programa de descompactação e instruções para sua execução pelo sistema operacional.

Arquivo comprimido

Arquivo que "contêm" um ou vários outros objetos que também podem ser arquivos comprimidos.

Arquivo de chave

Um arquivo com a extensão KEY que é sua "chave" pessoal, necessário para a operação do aplicativo da Kaspersky Lab. Um arquivo de chave será fornecido com o produto, se você o comprar dos distribuidores da Kaspersky Lab, ou enviado por email, se você comprar o produto online.

Ativando o aplicativo

Alterna o aplicativo para o modo totalmente funcional. O usuário precisa de uma licença para ativar o aplicativo.

Atualização

Procedimento de substituição/adição de novos arquivos (bancos de dados ou módulos do aplicativo) recuperados dos servidores de atualização da Kaspersky Lab.

Atualização dos bancos de dados

Uma das funções executadas pelos aplicativos da Kaspersky Lab que permitem manter a proteção atualizada. Ao fazê-lo, os bancos de dados são baixados dos servidores de atualização da Kaspersky Lab para o computador e são conectados automaticamente ao aplicativo.

Atualizações disponíveis

Um conjunto de atualizações dos módulos do aplicativo da Kaspersky Lab que inclui as atualizações críticas acumuladas por um determinado período e as alterações da arquitetura do aplicativo.

Atualizações urgentes

Atualizações críticas dos módulos do aplicativo da Kaspersky Lab.

B

Banco de dados de endereços da Web suspeitos

Lista de endereços da Web cujo conteúdo pode ser considerado como possivelmente perigoso. A lista foi criada pelos especialistas da Kaspersky Lab. Ela é atualizada periodicamente, sendo incluída no pacote do aplicativo da Kaspersky Lab.

BANCO DE DADOS DE ENDEREÇOS DE PHISHING

Lista de endereços da Web definidos pelos especialistas da Kaspersky Lab como endereços de phishing. O banco de dados é atualizado periodicamente e faz parte do aplicativo da Kaspersky Lab.

BANCOS DE DADOS

Bancos de dados criados pelos especialistas da Kaspersky Lab, que contêm descrições detalhadas de todas as ameaças atuais à segurança do computador, além dos métodos usados para sua detecção e desinfecção. Esses bancos de dados são atualizados pela Kaspersky Lab constantemente conforme surgem novas ameaças.

BLOQUEIO DE UM OBJETO

Negação de acesso de aplicativos externos a um objeto. Um objeto bloqueado não pode ser lido, executado, alterado ou excluído.

C

CABEÇALHO

Informações no início de um arquivo ou uma mensagem que compreendem dados de nível inferior sobre o processamento e o status do arquivo (ou mensagem). Particularmente, o cabeçalho dos emails contém dados como informações sobre o remetente e o destinatário, além da data.

CERTIFICADO DO SERVIDOR DE ADMINISTRAÇÃO

Um certificado que permite a autenticação do Servidor de Administração ao conectar o Console de Administração a ele e ao trocar dados com os computadores dos usuários. O certificado do Servidor de Administração é criado ao instalar o Servidor de Administração e armazenado na pasta %ALLUSERSPROFILE%\Application Data\KasperskyLab\adminkit\1093\cert.

CONFIGURAÇÕES DA TAREFA

Configurações do aplicativo que são específicas de cada tipo de tarefa.

CONFIGURAÇÕES DO APLICATIVO

Configurações do aplicativo que são comuns a todos os tipos de tarefa, regulando a operação do aplicativo como um todo, como as configurações de desempenho do aplicativo, as configurações de relatórios e as configurações de armazenamento no backup.

CONTADOR DE SURTO DE VÍRUS

Um modelo baseado no qual é gerada a notificação sobre surtos de vírus. Um contador de surto de vírus inclui uma combinação de configurações que determinam o limite da atividade de vírus, sua forma de disseminação e o texto das mensagens enviadas.

D

DESINFECÇÃO DE OBJETOS

Um método usado para processar objetos infectados que resulta na recuperação completa ou parcial dos dados, ou na decisão de que os objetos não podem ser desinfetados. Os objetos são desinfetados usando os registros do banco de dados. Parte dos dados pode ser perdida durante a desinfecção.

DESINFECÇÃO DE OBJETOS AO REINICIAR

Método de processamento de objetos infectados que estão sendo usados por outros aplicativos no momento da desinfecção. Consiste em criar uma cópia do objeto infectado, desinfetar a cópia criada e substituir o objeto original infectado pela cópia desinfetada na próxima reinicialização do sistema.

DESPEJO DA MEMÓRIA

Conteúdo da memória de trabalho de um processo ou de toda a RAM do sistema em um momento especificado.

DNS (SERVIÇO DE NOMES DE DOMÍNIO)

Um sistema distribuído para converter o nome de um host (um computador ou outro dispositivo de rede) em um endereço IP. O DNS funciona em redes TCP/IP. Em situações específicas, o DNS também pode armazenar e processar

solicitações reversas e determinar o nome de um host por seu endereço IP (registro PTR). Normalmente, a resolução de nomes DNS é executada pelos aplicativos de rede, não pelos usuários.

E

ESTADO DE PROTEÇÃO

O status atual da proteção que resume o nível de segurança do computador.

EXCLUSÃO

Uma exclusão é um objeto excluído da verificação pelo aplicativo da Kaspersky Lab. Você pode excluir da verificação arquivos de determinados formatos, máscaras de arquivos, uma determinada área (por exemplo, uma pasta ou um programa), processos de aplicativos ou objetos por tipo de ameaça, de acordo com a classificação da Enciclopédia de Vírus. A cada tarefa pode ser atribuído um conjunto de exclusões.

EXCLUSÃO DE UM OBJETO

Método de processamento de objetos que os exclui fisicamente de seu local original (disco rígido, pasta, recurso de rede). É recomendável aplicar esse método a objetos perigosos que, por algum motivo, não podem ser desinfetados.

F

FALSO POSITIVO

Uma situação em que o aplicativo da Kaspersky Lab considera um objeto não infectado como infectado devido à semelhança de seu código com o de um vírus.

FLUXOS NTFS ALTERNATIVOS

Fluxos de dados NTFS (fluxos de dados alternativos) criados para conter informações de arquivos ou atributos adicionais.

Cada arquivo do sistema de arquivos NTFS é um conjunto de fluxos. Um deles armazena o conteúdo do arquivo que poderá ser exibido ao abrir o arquivo; os outros fluxos (os chamados alternativos) foram criados para conter metainformações e assegurar, por exemplo, a compatibilidade do NTFS com outros sistemas, como um sistema de arquivos mais antigo da Macintosh chamado HFS (Hierarchical File System). Os fluxos podem ser criados, excluídos e armazenados separadamente, renomeados e até mesmo executados como um processo.

Os fluxos alternativos podem ser usados por invasores para transferir dados ocultamente ou para roubá-los de um computador.

G

GATEWAY DUPLO

Computador equipado com dois adaptadores de rede (cada um conectado a uma rede diferente) que transferem dados de uma rede para outra.

I

INSTALAÇÃO USANDO UM SCRIPT DE LOGON

Um método de instalação remota dos aplicativos da Kaspersky Lab que permite atribuir a inicialização da tarefa de instalação remota a uma conta de usuário individual (ou a várias contas de usuário). O registro de um usuário em um domínio leva a uma tentativa de instalar o aplicativo no computador cliente no qual o usuário foi registrado. Esse método é recomendável para a instalação dos aplicativos em computadores que executam sistemas operacionais Microsoft Windows 98/ME.

INTERCEPTADOR

Subcomponente do aplicativo responsável pela verificação de tipos específicos de email. O conjunto de interceptadores específicos à sua instalação depende da função e da combinação de funções para as quais o aplicativo está sendo implantado.

IP (PROTOCOLO IP)

O protocolo básico da Internet, usado sem alterações desde seu desenvolvimento, em 1974. Executa as operações básicas de transmissão de dados de um computador para outro e serve como base para protocolos de nível superior, como o TCP e o UDP. Gerencia a conexão e o processamento de erros. Tecnologias como a NAT e as máscaras possibilitam ocultar muitas redes particulares usando um pequeno número de endereços IP (ou até mesmo um endereço). Assim, é possível atender à demanda cada vez maior de crescimento da Internet usando o espaço relativamente restrito de endereços IPv4.

K

KASPERSKY SECURITY NETWORK

O Kaspersky Security Network (KSN) é uma infraestrutura de serviços online que dá acesso à Base de Dados de Conhecimento online da Kaspersky Lab, que contém informações sobre a reputação de arquivos, recursos da Web e software. A utilização de dados do Kaspersky Security Network garante um tempo de resposta menor do Kaspersky Anti-Virus ao encontrar novos tipos de ameaças, melhora o desempenho de alguns componentes de proteção e reduz a possibilidade de falsos positivos.

L

LICENÇA ADICIONAL

Uma licença que foi adicionada para a operação do aplicativo da Kaspersky Lab, mas que ainda não foi ativada. A licença adicional entra em vigor quando a licença ativa expira.

LICENÇA ATIVA

A licença usada no momento para a operação de um aplicativo da Kaspersky Lab. A licença define a data de expiração da funcionalidade completa e a política de licenças do aplicativo. O aplicativo não pode ter mais de uma licença com o status ativo.

LIMITE DE ATIVIDADE DE VÍRUS

O nível máximo permitido de um tipo de evento específico durante um período definido que, quando excedido, será considerado como atividade excessiva de vírus e ameaça de um surto de vírus. Esse recurso é muito importante durante os surtos de vírus e permite que um administrador reaja de forma oportuna às ameaças de surtos de vírus emergentes.

LISTA DE ENDEREÇOS DA WEB A SEREM VERIFICADOS

Uma lista de máscaras e endereços de recursos da Web que são obrigatoriamente verificados quanto à presença de objetos maliciosos pelo aplicativo da Kaspersky Lab.

LISTA DE URLS BLOQUEADOS

Uma lista de máscaras e endereços de recursos da Web cujo acesso é bloqueado pelo aplicativo da Kaspersky Lab. A lista de endereços é criada pelo usuário durante a configuração do aplicativo.

LISTA DE URLS CONFIÁVEIS

Uma lista de máscaras e endereços de recursos da Web em cujo conteúdo o usuário confia. O aplicativo da Kaspersky Lab não verifica as páginas da Web que correspondem aos itens da lista quanto à presença de objetos maliciosos.

LISTA DE URLS PERMITIDOS

Uma lista de máscaras e endereços de recursos da Web cujo acesso não é bloqueado pelo aplicativo da Kaspersky Lab. A lista de endereços é criada pelo usuário durante a configuração do aplicativo.

LISTA NEGRA DE ARQUIVOS DE CHAVE

Um banco de dados que contém informações sobre arquivos de chave da Kaspersky Lab contidos na lista negra. O conteúdo do arquivo da lista negra é atualizado juntamente com os bancos de dados do produto.

M

MÁSCARA DE ARQUIVOS

Representação de um nome de arquivo e extensão usando curingas. Os dois curingas padrão usados em máscaras de arquivos são * e ?, onde * representa qualquer número de caracteres e ? representa qualquer caractere. Com esses curingas, você pode representar qualquer arquivo. O nome e a extensão do arquivo sempre são separados por um ponto.

MÁSCARA DE SUB-REDE

A máscara de sub-rede (também conhecida como máscara de rede) e o endereço de rede determinam os endereços dos computadores em uma rede.

MENSAGEM OBSCENA

Email que contém linguagem ofensiva.

MENSAGEM SUSPEITA

Uma mensagem que não pode ser considerada spam com certeza, mas que parece suspeita quando verificada (por exemplo, determinados tipos de correspondência e mensagens publicitárias).

MODELO DE NOTIFICAÇÃO

Um modelo baseado no qual é gerada a notificação sobre objetos infectados detectados pela verificação. Um modelo de notificação inclui uma combinação de configurações que regulam o modo de notificação, o meio de distribuição e o texto das mensagens que devem ser enviadas.

MÓDULOS DO APLICATIVO

Arquivos fornecidos no pacote de instalação da Kaspersky Lab, responsáveis pela execução de suas principais tarefas. Um módulo executável específico corresponde a cada tipo de tarefa executada pelo aplicativo (proteção em tempo real, verificação por demanda, atualizações). Ao executar uma verificação completa do computador na janela principal, você inicia a execução do módulo dessa tarefa.

MOVIMENTAÇÃO DE OBJETOS PARA A QUARENTENA

Método de processamento de um objeto possivelmente infectado através do bloqueio do acesso ao arquivo e sua movimentação do seu local original para a pasta Quarentena, na qual o objeto é salvo em formato criptografado, o que elimina a ameaça de infecção.

N

NÍVEL DE GRAVIDADE DO EVENTO

Descrição de um evento registrada durante a operação do aplicativo da Kaspersky Lab. Existem quatro níveis de gravidade:

Evento crítico.

Falha funcional.

Aviso.

Mensagem informativa.

Eventos do mesmo tipo podem ter diferentes níveis de gravidade, dependendo da situação em que o evento ocorreu.

NÍVEL DE SEGURANÇA

O nível de segurança é definido como uma configuração predefinida do componente.

NÍVEL RECOMENDADO

O nível de segurança baseado nas configurações do aplicativo recomendadas pelos especialistas da Kaspersky Lab e que fornecem um nível ideal de proteção do computador. Esse nível é definido para ser usado por padrão.

O

OBJETO INFECTADO

Objeto que contém um código malicioso. É detectado quando uma seção do código do objeto corresponde integralmente a uma seção do código de uma ameaça conhecida. A Kaspersky Lab não recomenda usar esses objetos, pois eles podem infectar o computador.

OBJETO MONITORADO

Um arquivo transferido pelos protocolos HTTP, FTP ou SMTP através do firewall e enviado para a verificação por um aplicativo da Kaspersky Lab.

OBJETO OLE

Um objeto anexado ou incorporado a outro arquivo. O aplicativo da Kaspersky Lab permite verificar vírus em objetos OLE. Por exemplo, se você inserir uma tabela do Microsoft Office Excel em um documento do Microsoft Office Word, a tabela será verificada como um objeto OLE.

OBJETO PERIGOSO

Um objeto que contém um vírus. É recomendável não acessar esses objetos, pois isso poderia resultar na infecção do computador. Quando um objeto infectado é detectado, é recomendável desinfetá-lo usando um dos aplicativos da Kaspersky Lab ou, caso a desinfecção não seja possível, excluí-lo.

OBJETO POSSIVELMENTE INFECTADO

Um objeto que, devido à sua estrutura ou ao seu formato, pode ser usado por invasores como um "contêiner" para armazenar e distribuir um objeto malicioso. Normalmente, são arquivos executáveis, por exemplo, arquivos com as extensões COM, EXE, DLL, etc. O risco de infiltração de código malicioso nesses arquivos é bastante alto.

OBJETO POSSIVELMENTE INFECTADO

Um objeto que contém o código de um vírus conhecido modificado ou um código que parece o código de um vírus, mas que ainda não é conhecido pela Kaspersky Lab. Arquivos possivelmente infectados são detectados usando o analisador heurístico.

OBJETO SUSPEITO

Um objeto que contém o código de um vírus conhecido modificado ou um código que parece o código de um vírus, mas que ainda não é conhecido pela Kaspersky Lab. Os objetos suspeitos são detectados usando o analisador heurístico.

OBJETOS DE INICIALIZAÇÃO

Conjunto de programas necessários para iniciar e operar corretamente o sistema operacional e os softwares instalados no computador. Esses objetos são executados sempre que o sistema operacional é iniciado. Existem vírus capazes de infectar esses objetos de forma específica, o que pode levar, por exemplo, ao bloqueio da inicialização do sistema operacional.

P

PACOTE DE ATUALIZAÇÃO

Pacote de arquivos para a atualização do software. É baixado da Internet e instalado no computador.

PERÍODO DE VALIDADE DA LICENÇA

O período durante o qual você pode usar todos os recursos de seu aplicativo da Kaspersky Lab. Em geral, o período de validade da licença é de um ano a partir da data de instalação. Após a expiração da licença, a funcionalidade do aplicativo é reduzida. Você não poderá atualizar os bancos de dados do aplicativo.

PHISHING

Um tipo de fraude da Internet que consiste no envio de emails com o objetivo de roubar informações confidenciais; normalmente, dados financeiros diversos.

PORTA DE ENTRADA/SAÍDA

Usada processadores (como os da Intel) para a troca de dados com componentes de hardware. A porta de entrada/saída está associada a um determinado componente de hardware e permite seu endereçamento por aplicativos para a troca de dados.

PORTA DE HARDWARE

Soquete em um componente de hardware de um computador no qual é possível conectar um cabo ou plugue (porta LPT, porta serial, porta USB).

PORTA DE REDE

Um parâmetro TCP e UDP que determina o destino dos pacotes de dados no formato IP que são transmitidos para um host pela rede e possibilita que vários programas em execução em um único host recebam dados de forma independente. Cada programa processa os dados recebidos por uma determinada porta (às vezes se faz referência a isso dizendo que o programa "escuta" àquela porta).

Para alguns protocolos de rede comuns, geralmente existem números de porta padrão (por exemplo, geralmente os servidores Web recebem solicitações HTTP na porta TCP 80); no entanto, em geral, um programa pode usar qualquer protocolo em qualquer porta. Os valores possíveis são: 1 a 65535.

PROCESSO CONFIÁVEL

O processo de um programa cujas operações com arquivos não são monitoradas pelo aplicativo da Kaspersky Lab no modo de proteção em tempo real. Em outras palavras, os objetos executados, abertos ou salvos pelos processos confiáveis não serão verificados.

PROTEÇÃO EM TEMPO REAL

Modo de operação do aplicativo no qual os objetos são verificados em tempo real quanto à presença de código maliciosos.

O aplicativo intercepta todas as tentativas de abrir qualquer objeto (leitura, gravação ou execução) e verifica o objeto quanto à presença de ameaças. Os objetos não infectados são disponibilizados para o usuário; os objetos que contêm ameaças ou que são suspeitos de contê-las são processados de acordo com as configurações da tarefa (são desinfetados, excluídos ou colocados na Quarentena).

PROTOCOLO

Um conjunto de regras claramente definido e padronizado que define a interação entre um cliente e um servidor. Protocolos conhecidos e os serviços associados a eles incluem o HTTP (WWW), o FTP e o NNTP (notícias).

Q

QUARENTENA

Uma pasta específica na qual são colocados todos os objetos possivelmente infectados detectados durante as verificações ou pela proteção em tempo real.

R

RASTROS

Execução do aplicativo no modo de depuração; depois que cada comando é executado, o aplicativo é interrompido e o resultado da etapa é exibido.

RESTAURAÇÃO

Movimentação de um objeto original da Quarentena ou do backup para a pasta na qual ele se encontrava originalmente, antes de ser movido para a Quarentena, desinfetado ou excluído, ou para uma outra pasta especificada pelo usuário.

ROOTKIT

Um aplicativo ou um conjunto de aplicativos desenvolvidos para mascarar rastros de um invasor ou um malware no sistema.

Em sistemas baseados em Windows, rootkit normalmente significa um programa que invade o sistema e intercepta suas funções (API do Windows). Primeiro, a interceptação e modificação de funções de APIs de nível inferior permite que esse programa mascare sua presença no sistema de forma bastante sofisticada. Além disso, como regra, um rootkit pode mascarar a presença de qualquer processo, pasta e arquivo no disco, e de chaves do Registro, se estiverem descritos na configuração do rootkit. Vários rootkits instalam seus próprios drivers e serviços no sistema (eles também são "invisíveis").

S

SCRIPT

Um pequeno programa de computador ou uma parte independente de um programa (função) que, como regra, foi desenvolvida para executar uma pequena tarefa específica. É usado com mais frequência com programas incorporados no hipertexto. Os scripts são executados, por exemplo, quando você abre um determinado site.

Se a proteção em tempo real estiver ativada, o aplicativo controlará a execução de scripts, os interceptará e verificará a presença de vírus. Dependendo dos resultados da verificação, você poderá bloquear ou permitir a execução do script.

SERVIDOR PROXY

Um serviço de rede de computadores que permite aos usuários fazer solicitações indiretas a outros serviços de rede. Primeiro, um usuário se conecta a um servidor proxy e solicita um recurso (por exemplo, um arquivo) localizado em outro servidor. Em seguida, o servidor proxy se conecta ao servidor especificado e obtém o recurso ou retorna o recurso de seu próprio cache (se o proxy tiver seu próprio cache). Em alguns casos, uma solicitação do usuário ou uma resposta do servidor pode ser modificada pelo servidor proxy.

SERVIDORES DE ATUALIZAÇÃO DA KASPERSKY LAB

Uma lista de servidores HTTP e FTP da Kaspersky Lab a partir dos quais o aplicativo baixa atualizações dos bancos de dados e módulos do aplicativo para o seu computador.

SETOR DE INICIALIZAÇÃO DO DISCO

O setor de inicialização é uma área específica no disco rígido, disquete ou outro dispositivo de armazenamento de dados do computador. Ele contém informações sobre o sistema de arquivos do disco e um programa de carregamento de inicialização responsável por iniciar o sistema operacional.

Existem diversos vírus que infectam os setores de inicialização, os chamados vírus de inicialização. O aplicativo da Kaspersky Lab permite verificar os setores de inicialização quanto à presença de vírus e desinfetá-los, caso seja detectada uma infecção.

SOCKS

Protocolo de servidor proxy que permite estabelecer uma conexão ponto a ponto entre computadores em redes internas e externas.

SURTO DE VÍRUS

Uma série de tentativas deliberadas de infectar um computador com vírus.

T

TAREFA

As funções executadas pelo aplicativo da Kaspersky Lab são implementadas como tarefas, como: Proteção em tempo real, Verificação completa do computador, Atualização do banco de dados.

TECNOLOGIA ICHECKER

O iChecker é uma tecnologia que aumenta a velocidade das verificações antivírus por meio da exclusão de objetos que permaneceram inalterados desde a última verificação, desde que os parâmetros de verificação (as configurações e o banco de dados de antivírus) não tenham mudado. As informações de cada arquivo são armazenadas em um banco de dados especial. Essa tecnologia é usada nos modos de proteção em tempo real e de verificação por demanda.

Por exemplo, você tem um arquivo comprimido que foi verificado pelo aplicativo da Kaspersky Lab e ao qual foi atribuído o status não infectado. Na próxima verificação, o aplicativo vai ignorar esse arquivo comprimido, a menos que ele tenha sido modificado ou que as configurações de verificação tenham sido alteradas. Se você alterou o conteúdo do arquivo comprimido, adicionando um novo objeto a ele, modificou as configurações de verificação ou atualizou o banco de dados de antivírus, o arquivo comprimido será verificado novamente.

Limitações da tecnologia iChecker:

essa tecnologia não funciona com arquivos grandes, pois é mais rápido verificar o arquivo que analisar se ele foi modificado desde sua última verificação;

a tecnologia dá suporte a um número limitado de formatos (EXE, DLL, LNK, TTF, INF, SYS, COM, CHM, ZIP, RAR).

V

VERIFICAÇÃO DO TRÁFEGO

Verificação em tempo real dos objetos transmitidos por todos os protocolos (por exemplo, HTTP, FTP, etc.) que usa informações da versão mais recente do banco de dados.

VÍRUS DE INICIALIZAÇÃO

Um vírus que infecta os setores de inicialização do disco rígido de um computador. O vírus faz o sistema carregá-lo na memória durante a reinicialização e direcionar o controle para o código do vírus em vez do código do carregamento de inicialização original.

VÍRUS DESCONHECIDO

Um novo vírus sobre o qual não há informações nos bancos de dados. Em geral, os vírus desconhecidos são detectados pelo aplicativo em objetos usando o analisador heurístico, e esses objetos são classificados como possivelmente infectados.

KASPERSKY LAB ZAO

O software da Kaspersky Lab é conhecido internacionalmente por sua proteção contra vírus, malware, spam, ataques de rede e de hackers, além de outras ameaças.

Em 2008, a Kaspersky Lab foi classificada como um dos quatro principais fornecedores de soluções de software de segurança de informações para o usuário final (IDC Worldwide Endpoint Security Revenue by Vendor). A Kaspersky Lab é o desenvolvedor de sistemas de proteção de computadores preferido dos usuários domésticos na Rússia, de acordo com a pesquisa da "TGI-Russia 2009".

A Kaspersky Lab foi fundada na Rússia em 1997. Atualmente, é um grupo internacional de empresas sediado em Moscou, com cinco divisões regionais que gerenciam as atividades da empresa na Rússia, na Europa Ocidental e Oriental, no Oriente Médio, na África, nas Américas do Norte e do Sul, no Japão, na China e em outros países da região do Pacífico Asiático. A empresa emprega mais de 2.000 especialistas qualificados.

Produtos. Os produtos da Kaspersky Lab oferecem proteção para todos os tipos de sistemas: de computadores domésticos a grandes redes corporativas.

A linha de produtos pessoais inclui aplicativos antivírus para computadores desktop, laptop e portáteis, além de smartphones e outros dispositivos móveis.

A Kaspersky Lab fornece aplicativos e serviços para proteger estações de trabalho, servidores de arquivos e de email, gateways de email e firewalls. Usadas em conjunto com o sistema de gerenciamento centralizado da Kaspersky Lab, essas soluções garantem a proteção automatizada eficiente de empresas e organizações contra as ameaças de computadores. Os produtos da Kaspersky Lab são certificados pelos principais laboratórios de testes, são compatíveis com os softwares de diversos fornecedores de aplicativos para computadores e são otimizados para a execução em várias plataformas de hardware.

Os analistas de vírus da Kaspersky Lab trabalham 24 horas por dia. Todos os dias, eles descobrem milhares de novas ameaças de computador, criam ferramentas para detectá-las e desinfetá-las, e as incluem nos bancos de dados usados pelos aplicativos da Kaspersky Lab. *O banco de dados do antivírus da Kaspersky Lab é atualizado a cada hora* e o *banco de dados do antispam*, *a cada cinco minutos*.

Tecnologias. Várias tecnologias que agora são parte integrante de modernas ferramentas antivírus foram originalmente desenvolvidas pela Kaspersky Lab. Não é uma simples coincidência o fato de que diversos outros desenvolvedores usam o kernel do Kaspersky Anti-Virus em seus produtos, como: 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), ZyXEL Communications (Taiwan). Muitas das tecnologias inovadoras da empresa são patenteadas.

Realizações. Ao longo dos anos, a Kaspersky Lab recebeu centenas de prêmios por seus serviços no combate às ameaças de computador. Por exemplo, em 2010, o Kaspersky Anti-Virus recebeu vários prêmios Advanced+ após uma série de testes realizados pela AV-Comparatives, um renomado laboratório de antivírus austríaco. Mas a principal realização da Kaspersky Lab é a fidelidade de seus usuários em todo o mundo. Os produtos e as tecnologias da empresa protegem mais de 300 milhões de usuários, e seus clientes corporativos somam mais de 200.000.

Site oficial da Kaspersky Lab:	http://brazil.kaspersky.com
Enciclopédia de vírus:	http://www.securelist.com
Laboratório de antivírus:	newvirus@kaspersky.com (somente para o envio de arquivos possivelmente infectados no formato comprimido) http://support.kaspersky.com/virlab/helpdesk.html?LANG=pt (para consultas endereçadas aos analistas de vírus)
Fórum da Kaspersky Lab na Web:	http://forum.kaspersky.com/index.php?showforum=87

INFORMAÇÕES SOBRE CÓDIGO DE TERCEIROS

As informações sobre códigos de terceiros estão contidas em um arquivo chamado legal_notices.txt e armazenado na pasta de instalação do aplicativo.

ÍNDICE

A

B

C

D

E

L

N

O

P

Q

R

T

V

Z