KASPERSKY LAB

Kaspersky® Anti-Virus 6.0

MANUAL DO USUÁRIO

KASPERSKY ANTI-VIRUS 6.0

Manual do Usuário

http://www.kaspersky.com

Data de revisão: Janeiro de 2007

Sumário

CAPÍTULO 1. AMEAÇAS À SEGURANÇA DOS COMPUTADORES

Com a rápida evolução da tecnologia da informação e sua penetração em várias áreas, cresce também o número e a variedade de crimes associados à violação de informações.

Os chamados criminosos virtuais têm grande interesse nas atividades de instituições governamentais e empresas privadas. Eles tentam roubar e divulgar informações confidenciais, causando danos à reputação das empresas, interferindo na continuidade dos negócios e podem prejudicar os recursos de informações das organizações. Essas ações podem causar sérios danos aos ativos tangíveis e intangíveis das empresas.

Não são apenas as grandes empresas que correm riscos; usuários individuais também podem ser atacados. Os criminosos podem acessar dados pessoais (por exemplo, números e senhas de contas bancárias e de cartões de crédito) ou causar o mal funcionamento de um computador. Alguns tipos de ataques podem permitir o acesso completo do computador pelos hackers, que podem então usá-lo como parte de uma “rede de zumbis”, ou seja, uma rede de computadores infectados que atacam servidores, enviam spams, coletam informações confidenciais e disseminam novos vírus e cavalos de Tróia.

No mundo de hoje, as informações são amplamente reconhecidas como ativos valiosos que devem ser protegidos. Ao mesmo tempo, essas informações devem estar acessíveis para aqueles que realmente precisam delas (por exemplo, funcionários, clientes e parceiros de uma empresa). Conseqüentemente, existe a necessidade de criar um sistema de segurança de informações abrangente, que deve considerar todas as fontes de ameaças possíveis, sejam elas humanas, geradas pelo homem ou desastres naturais, e usar uma variedade completa de medidas defensivas nos níveis físico, administrativo e de software.

1.1. Fontes de ameaças

Um indivíduo, um grupo de pessoas ou um fenômeno não relacionado à atividade humana podem representar uma ameaça à segurança das informações. Assim, todas as fontes de ameaças podem ser classificadas em três grupos:

- **O fator humano**. Este grupo de ameaças refere-se às ações de pessoas com acesso autorizado ou não às informações. As ameaças desse grupo podem ser divididas em:
    - *Externas*, incluindo criminosos virtuais, hackers, golpistas da Internet, parceiros inescrupulosos e organizações criminosas.
    - *Internas*, incluindo ações de funcionários da empresas e usuários de PCs domésticos. As ações executadas por este grupo podem ser deliberadas ou acidentais.
- **O fator tecnológico**. Este grupo de ameaças está relacionado com problemas técnicos; o uso de software e hardware obsoletos ou de má qualidade para o processamento das informações. Isso pode resultar em falhas nos equipamentos e, freqüentemente, na perda de dados.
- **O fator de desastres naturais**. Este grupo de ameaças inclui toda a variedade de eventos provocados pela natureza e outros que independem da atividade humana.

  Essas três fontes de ameaças precisam ser consideradas no desenvolvimento de um sistema de proteção à segurança de dados. Este Manual do Usuário enfoca a área diretamente vinculada à especialidade da Kaspersky Lab, as ameaças externas que envolvem atividade humana.

1.2. Como as ameaças se disseminam

O desenvolvimento das ferramentas de comunicação e das tecnologias de computação ampliam as oportunidades para os hackers disseminarem ameaças. Vamos examiná-las mais detalhadamente:

A Internet

A Internet é única porque não pertence a ninguém e não tem fronteiras. Sob vários aspectos, isso promoveu o desenvolvimento dos recursos da Web e a troca de informações. Atualmente, qualquer pessoa pode acessar dados na Internet ou criar sua própria página na Web.

Entretanto, esses vários recursos da rede mundial também permitem que hackers cometam crimes virtuais, dificultando sua detecção e punição.

Os hackers inserem vírus e outros programas mal-intencionados nos sites, disfarçados como interessantes programas gratuitos. Além disso, scripts que são executados automaticamente ao abrir uma página da Web podem executar ações perigosas no seu computador, incluindo a

modificação do Registro do sistema, o roubo de dados pessoais e a instalação de software mal-intencionado.

Usando tecnologias de rede, os hackers conseguem atacar servidores corporativos e PCs remotos. Esses ataques podem ocasionar o mal funcionamento de componentes do sistema ou viabilizar o acesso total dos hackers ao sistema e, conseqüentemente, às informações armazenadas nele. Eles também podem usá-los como parte de uma rede de zumbis.

Por fim, a possibilidade de usar cartões de crédito e dinheiro eletrônico pela Internet, em páginas de lojas, leilões e instituições bancárias, tornou os golpes on-line cada vez mais comuns.

Intranet

A intranet é sua rede interna, destinada à troca de informações dentro de uma empresa ou em uma rede doméstica. A intranet é um ambiente comum no qual todos os computadores da rede podem armazenar, trocar e acessar informações. Isso significa que, no caso de infecção de um dos computadores da rede, todos os demais correm um sério risco. Para evitar situações como essa, é necessário proteger tanto os limites da rede como também cada um dos computadores.

E-mail

Como a grande maioria dos computadores possui programas de e-mail instalados, e os programas mal-intencionados exploram o conteúdo dos catálogos de endereços eletrônicos, geralmente essa é a condição ideal para a disseminação desses programas. O usuário de um computador infectado pode, sem se dar conta, enviar e-mails infectados para seus amigos ou colegas de trabalho que, por sua vez, enviariam mais e-mails infectados. Por exemplo, é comum que documentos em arquivos infectados passem desapercebido quando distribuídos com informações comerciais através de um sistema de e-mail interno da empresa. Quando isso ocorre, um grande número de pessoas é infectado. Podem ser centenas ou milhares de funcionários da empresa, junto com possivelmente dezenas de milhares de assinantes.

Além da ameaça dos programas mal-intencionados, existe o problema dos e-mails indesejados ou spams. Embora não representem uma ameaça direta a um computador, os spams sobrecarregam os servidores de e-mail, consomem largura de banda, enchem a caixa de correio do usuário e interferem na produtividade, causando prejuízos financeiros.

Além disso, os hackers começaram a usar programas que enviam e-mails em massa e métodos de engenharia social para convencer os usuários a abrirem e-mails ou clicarem em links para determinados sites. Assim, os recursos de filtragem de spam são valiosos por diversos motivos: para interromper os e-mails indesejados, para combater novos

tipos de golpes on-line, como o phishing, para interromper a disseminação de programas mal-intencionados.

Mídia de armazenamento removível

As mídias removíveis (disquetes, CDs/DVDs e unidades flash USB) são muito usadas no armazenamento e na transmissão de informações.

A abertura de um arquivo que contém código mal-intencionado armazenado em um dispositivo de armazenamento removível pode danificar os dados armazenados no computador local e disseminar o vírus para outras unidades do computador ou para outros computadores da rede.

1.3. Tipos de ameaças

Atualmente, existe um grande número de ameaças à segurança dos computadores. Esta seção examinará as ameaças bloqueadas pelo Kaspersky Anti-Virus.

Worms

Esta categoria de programas mal-intencionados se dissemina amplamente através da exploração de vulnerabilidades nos sistemas operacionais dos computadores. A classe recebeu esse nome em alusão à forma como os worms (vermes) passam de um computador para outro, por meio de redes e e-mails. Esse recurso permite que os worms se disseminem muito rapidamente.

Os worms entram no computador, buscam endereços de rede de outros computadores e enviam um grande volume de cópias automáticas de si mesmos para esses endereços. Além disso, freqüentemente os worms utilizam dados contidos nos catálogos de endereços dos programas de e-mail. Às vezes, alguns desses programas mal-intencionados criam arquivos de trabalho nos discos do sistema, mas eles podem ser executados sem nenhum recurso do sistema além da RAM.

Vírus

Os vírus são programas que infectam outros arquivos, agregando seu próprio código a eles de maneira a controlar os arquivos infectados quando eles são abertos. Esta definição simples explica a principal ação de um vírus, a *infecção*.

Cavalos de Tróia

Os cavalos de Tróia são programas que executam ações não-autorizadas em computadores, como excluir informações em unidades, travar o sistema, roubar informações confidenciais e assim por diante.

Essa classe de programas mal-intencionados não se constitui em vírus, no sentido tradicional da palavra, pois eles não infectam outros computadores ou dados. Os cavalos de Tróia não conseguem invadir um computador e são disseminados por hackers, que os disfarçam como software comum. Os danos causados por eles podem exceder em muito os ataques de vírus tradicionais.

Atualmente, os worms são o tipo mais comum de programa mal-intencionado utilizado para danificar dados de computadores, seguidos dos vírus e cavalos de Tróia. Alguns programas mal-intencionados combinam recursos de duas ou até três dessas classes.

Adware

Os adwares consistem em programas incluídos no software sem o conhecimento do usuário, com o objetivo de exibir anúncios. Geralmente, o adware vem incorporado a um software distribuído gratuitamente. Os anúncios são apresentados na interface do programa. Freqüentemente, esses programas também coletam dados pessoais do usuário e os enviam para o desenvolvedor, alteram as configurações do navegador (a página inicial, páginas de busca, níveis de segurança, etc.) e geram um tráfego que não pode ser controlado pelo usuário. Tudo isso pode levar a violações de segurança e acarretar prejuízos financeiros diretos.

Spyware

Estes softwares coletam informações sobre um determinado usuário ou organização, sem o conhecimento dos mesmos. Freqüentemente, os spywares não são detectados. Em geral, o objetivo do spyware é:

- controlar as ações do usuário em um computador;
- coletar informações sobre o conteúdo do seu disco rígido. Nesses casos, geralmente isso envolve a verificação de vários diretórios e do Registro do sistema para compilar uma lista dos softwares instalados no computador;
- coletar informações sobre a qualidade da conexão, largura de banda, velocidade do modem, etc.

Riskware

O riskware inclui softwares que não possuem recursos mal-intencionados, mas que poderiam fazer parte do ambiente de desenvolvimento de programas mal-intencionados ou ser usados por hackers como componentes auxiliares desses programas. Essa categoria de programas inclui programas com backdoors e vunlerabilidades, além de utilitários de administração remota, programas que interferem no layout do teclado, clientes IRC, servidores FTP e utilitários multifuncionais que interrompem processos ou ocultam suas operações.

Um outro tipo de programa mal-intencionado semelhante aos adwares, spywares e riskwares são os programas que se conectam ao navegador da Internet e redirecionam o tráfego. O navegador abrirá sites diferentes dos pretendidos.

Piadas

Os softwares de piadas não causam danos diretos, mas exibem mensagens informando que houve ou que haverá algum dano, sob determinadas condições. Freqüentemente, esses programas advertem o usuário sobre perigos inexistentes, como mensagens que avisam sobre a formatação do disco rígido (embora isso não ocorra realmente) ou a detecção de vírus em arquivos não infectados.

Rootkits

São utilitários usados para disfarçar a atividade mal-intencionada. Eles encobrem programas mal-intencionados, evitando que sejam detectados por programas antivírus. Os rootkits modificam funções básicas do sistema operacional do computador, ocultando sua própria existência e as ações executadas pelo hacker no computador infectado.

Outros programas perigosos

Estes programas são criados, por exemplo, para configurar ataques DoS a servidores remotos, invadir outros computadores e programas que fazem parte do ambiente de desenvolvimento de programas mal-intencionados. Esses programas incluem ferramentas de hackers, construtores de vírus, programas de varredura de vulnerabilidades, programas para a violação de senhas e outros tipos de programas para invadir os recursos da rede ou penetrar em um sistema.

Ataques de hackers

Os ataques de hackers podem ser iniciados por hackers ou por programas mal-intencionados. Eles visam o roubo de informações residentes de um computador remoto, provocando o mal funcionamento do sistema ou controlando todos os recursos do mesmo.

Alguns tipos de golpes on-line

O **phishing** é um golpe on-line que utiliza o envio de e-mails em massa para roubar informações confidenciais do usuário, geralmente de natureza financeira. Os e-mails de phishing são criados para reproduzir, da melhor forma possível, e-mails informativos de instituições bancárias e de empresas conhecidas. Esses e-mails contêm links para sites falsos criados por hackers para simular o site legítimo da organização. Nesse site, é solicitado que o usuário informe, por exemplo, o número do seu cartão de crédito e outras informações confidenciais.

Discadores para sites "pay-per-use" – tipo de golpe on-line que faz uso não-autorizado de serviços da Internet do tipo "pay-per-use", que geralmente são sites de cunho pornográfico. O discador instalado pelos hackers inicia uma conexão por modem entre o computador e o número do serviço pago. Freqüentemente, esses números cobram taxas muito caras e o usuário é obrigado a pagar enormes contas telefônicas.

Publicidade invasiva

Inclui janelas pop-up e banners de anúncios que são abertos ao usar o navegador da Internet. Em geral, as informações nessas janelas não trazem qualquer benefício ao usuário. Elas atraem a atenção do usuário e consomem largura de banda.

Spam

O spam consiste em e-mails indesejados anônimos, incluindo vários tipos de conteúdo: anúncios, mensagens políticas, solicitações de ajuda, e-mails que solicitam o investimento de uma grande soma em dinheiro ou a participação em esquemas do tipo pirâmide, e-mails direcionados para o roubo de senhas e números de cartão de crédito e e-mails que devem ser enviados para amigos (as chamadas correntes).

O Kaspersky Anti-Virus usa dois métodos para detectar e bloquear esses tipos de ameaças:

- *Reativo* – este método pesquisa arquivos mal-intencionados usando um banco de dados de assinaturas de ameaças atualizado periodicamente.
- *Proativo* – diferente da proteção reativa, esse método não se baseia na análise de código, mas no comportamento do sistema. Seu objetivo é detectar novas ameaças ainda não definidas nas assinaturas.

Utilizando esses dois métodos, o Kaspersky Anti-Virus oferece proteção abrangente para o seu computador contra ameaças novas e conhecidas.

1.4. Sinais de infecção

Há vários sinais que indicam que um computador foi infectado. Os eventos a seguir podem indicar que um computador esteja infectado por um vírus:

- Mensagens ou imagens inesperadas aparecem na tela ou sons não usuais são tocados;
- A bandeja do CD/DVD-ROM abre e fecha inesperadamente;
- O computador inicia um programa arbitrariamente, sem que você tenha solicitado;

- Surgem na tela avisos pop-up sobre um programa que está tentando acessar a Internet, mesmo que você não o tenha iniciado;

Também há vários outros sinais de infecção de vírus por meio de e-mails:

- Amigos ou conhecidos comentam sobre mensagens que você nunca enviou;
- Sua caixa de entrada possui um grande número de mensagens sem cabeçalhos ou endereços do remetente.

É importante observar que esses sinais podem ter outros motivos, que não vírus. Por exemplo, no caso dos e-mails, as mensagens infectadas podem ter sido enviadas com seu endereço para resposta, mas não do seu computador.

Há também outras indicações indiretas de que seu computador está infectado:

- O computador congela ou trava freqüentemente;
- Os programas demoram para ser carregados;
- Você não consegue inicializar o sistema operacional;
- Arquivos e pastas desaparecem, ou seu conteúdo é deturpado;
- O disco rígido é acessado com freqüência (as luzes piscam);
- O navegador da Web (por exemplo, o Microsoft Internet Explorer) congela ou tem um comportamento inesperado (por exemplo, você não consegue fechar a janela do programa).

Em 90% dos casos, esses sintomas indiretos são causados por mal funcionamento de hardware ou software. Apesar de esses sintomas raramente indicarem a infecção do computador, é recomendável que, ao detectá-los, você execute uma verificação completa do computador (consulte 5.2 na p. 54) com as configurações no nível **recomendado**.

1.5. O que fazer ao suspeitar de uma infecção

Se você notar algum tipo de comportamento suspeito no seu computador...

1. Não entre em pânico! Esta é a regra de ouro: ela pode evitar que você perca dados importantes e preocupações desnecessárias.
2. Desconecte o computador da Internet ou da rede local, se for o caso.
3. Se não for possível inicializar o computador do disco rígido (o computador exibe uma mensagem de erro quando é ligado), tente

reinicializá-lo no modo de segurança ou usando o disco de inicialização de emergência do sistema operacional, criado na sua instalação.

4. Antes de qualquer coisa, faça o backup do seu trabalho em uma mídia de armazenamento removível (disquete, CD/DVD, unidade flash, etc.).
5. Instale o Kaspersky Anti-Virus, caso ainda o não tenha feito. Consulte a seção Capítulo 3 na página 29.
6. Atualize as assinaturas de ameaças do programa e os módulos do aplicativo (consulte 5.5 na p. 56). Se possível, baixe as atualizações na Internet usando um outro computador não-infectado, por exemplo, de um amigo, em uma lan house ou no trabalho. É melhor usar outro computador, pois ao conectar um computador infectado à Internet, é possível que o vírus envie informações importantes para hackers ou dissemine o vírus para os endereços de seu catálogo de endereços. Por isso, se suspeitar que o computador está com vírus, desconecte-o imediatamente da Internet. Você também pode obter atualizações das assinaturas de ameaças em disquete junto à Kaspersky Lab ou seus distribuidores, e usá-las para fazer as atualizações.
7. Selecione o nível de segurança recomendado pelos especialistas da Kaspersky Lab.
8. Inicie uma verificação completa do computador (consulte 5.2 na p. 54).

1.6. Evitando infecções

Nem mesmo as medidas mais confiáveis e ponderadas garantem 100% de proteção contra vírus e cavalos de Tróia mas, seguindo este conjunto de regras, você reduzirá significativamente a probabilidade de ataques de vírus e o nível dos possíveis danos.

As regras básicas de segurança são discutidas no restante deste capítulo.

Regra nº 1: *Use software antivírus e programas de segurança da Internet*. Para fazê-lo:

- Instale o Kaspersky Anti-Virus assim que possível.
- Atualize regularmente (consulte 5.5 na p. 56) as assinaturas de ameaças do programa. No caso de surtos de vírus, atualize as assinaturas várias vezes por dia. Nessas situações, a Kaspersky Lab atualiza imediatamente as assinaturas de ameaças em seus servidores.
- Selecione as configurações de segurança recomendadas pela Kaspersky Lab para o seu computador. Você estará sempre protegido, desde o

momento em que liga o computador, dificultando a infecção do mesmo por vírus.

- Selecione as configurações de verificação completa recomendadas pela Kaspersky Lab e programe verificações pelo menos uma vez por semana.

Regra nº 2: *Cuidado ao copiar dados novos para o seu computador*:

- Verifique todas as unidades de armazenamento removíveis, por exemplo disquetes, CD/DVDs e unidades flash, quanto à presença de vírus antes de usá-las (consulte 5.4 na p. 55).
- Cuidado com os e-mails. Não abra arquivos que estão anexados aos e-mails, a menos que tenha certeza de que foram enviados a você, mesmo que tenham sido enviados por conhecidos.
- Cuidado com as informações obtidas pela Internet. Se algum site sugerir a instalação de um novo programa, certifique-se de que ele possui um certificado de segurança.
- Se estiver copiando um arquivo executável da Internet ou da rede local, verifique-o usando o Kaspersky Anti-Virus.
- Use seu bom-senso ao visitar sites da Web. Muitos sites estão infectados por vírus de script ou worms da Internet perigosos.

Regra nº 3: *Preste muita atenção às informações divulgadas pela Kaspersky Lab*.

Na maioria dos casos, a Kaspersky Lab divulga um novo surto de vírus muito antes do seu pico. A probabilidade de infecção nesse caso é pequena. Se você tiver baixado as atualizações das assinaturas de ameaças, terá bastante tempo para se proteger do novo vírus.

Regra nº 4: *Não confie em boatos sobre vírus*, como programas fictícios e e-mails sobre ameaças de infecção.

Regra nº 5: *Use o Windows Update* e instale as atualizações do sistema operacional Windows periodicamente.

Regra nº 6: *Compre software original de distribuidores autorizados*.

Regra nº 7: *Limite o número de pessoas autorizadas a usar o seu computador*.

Regra nº 8: *Reduza os riscos das conseqüências desagradáveis de uma possível infecção*:

- Faça backup dos dados regularmente. No caso de perda de dados, o sistema poderá ser restaurado rapidamente, se você tiver cópias de backup. Guarde os disquetes, CDs, unidades flash e outras mídias de armazenamento de distribuição com software e informações importantes em um local seguro.

- Crie um Disco de Recuperação (consulte 14.10 na p. 191) que possibilite a inicialização, usando um sistema operacional limpo.

Regra nº 9: *Confira periodicamente a lista de programas instalados no computador*. Para fazê-lo, abra **Adicionar ou Remover Programas** no **Painel de Controle** ou examine o diretório **Arquivos de Programas** e o diretório de inicialização. Assim, é possível descobrir softwares que foram instalados no computador sem o seu conhecimento, por exemplo, enquanto você usava a Internet ou instalava um outro programa. Quase sempre, é possível que esses programa sejam perigosos.

CAPÍTULO 2. KASPERSKY ANTI-VIRUS 6.0

O Kaspersky Anti-Virus 6.0 representa uma nova geração de produtos de segurança de dados.

O que realmente diferencia o Kaspersky Anti-Virus 6.0 dos outros softwares, até mesmo de outros produtos da Kaspersky Lab, é sua abordagem multifacetada à segurança de dados.

2.1. Novidades do Kaspersky Anti-Virus 6.0

O Kaspersky Anti-Virus 6.0 (chamado “Kaspersky Anti-Virus” ou “o programa”) utiliza uma nova abordagem à segurança de dados. A principal característica do programa é que ele combina e aprimora visivelmente os recursos existentes em todos os produtos da empresa em uma única solução de segurança. O programa oferece proteção contra vírus e ameaças desconhecidas.

Não é mais necessário instalar vários produtos no computador para obter segurança total. Basta simplesmente instalar o Kaspersky Anti-Virus 6.0.

Sua proteção abrangente protege todos os canais de dados de entrada e de saída. Todos os componentes do programa possuem configurações flexíveis que permitem que o Kaspersky Anti-Virus se adapte às necessidades de cada usuário. A configuração de todo o programa pode ser feita em um único local.

Vamos examinar os novos recursos do Kaspersky Anti-Virus.

Novos recursos de proteção

- O Kaspersky Anti-Virus o protege de programas mal-intencionados conhecidos e de programas que ainda não foram descobertos. A Defesa Proativa (consulte Capítulo 10 na p. 113) é a principal vantagem do programa. Ela analisa o comportamento dos aplicativos instalados no computador, monitorando as alterações do Registro do sistema, controlando as macros e combatendo ameaças ocultas. O componente usa um analisador heurístico para detectar e registrar vários tipos de atividade mal-intencionada; assim, as ações executadas por programas mal-intencionados podem ser revertidas e o sistema pode ser restaurado a seu estado anterior.

- A tecnologia do Antivírus de Arquivos foi aprimorada: agora você pode diminuir a carga no processador central e nos sub-sistemas dos discos, e aumentar a velocidade da verificação de arquivos. O iChecker™ e o iSwift™ ajudam a conseguir isso. Esse método evita que o aplicativo repita a verificação dos mesmos arquivos.
- Agora, o processo de verificação é executado em segundo plano, permitindo que o usuário continue usando o computador. Se houver uma concorrência pelos recursos do sistema, a verificação de vírus será interrompida até que a operação do usuário seja concluída; então, ela continuará do ponto onde parou.
- As áreas críticas do computador, cuja infecção afetaria seriamente a qualidade ou a segurança dos dados, possuem sua própria tarefa. Ela pode ser configurada para ser executada sempre que o sistema é iniciado.
- Foram feitos avanços importantes na proteção dos e-mails do usuário contra programas mal-intencionados. O programa verifica e-mails contendo vírus nos seguintes protocolos:
    - IMAP, SMTP, POP3, independentemente do programa de e-mail utilizado
    - NNTP, independentemente do programa de e-mail
    - Independentemente do protocolo (MAPI, HTTP), ao usar plug-ins para o Microsoft Office Outlook e o The Bat!
- Existem plug-ins específicos disponíveis para os programas de e-mail mais comuns, como o Outlook, o Microsoft Outlook Express e o The Bat!. Eles inserem a proteção de e-mails contra vírus diretamente no programa de e-mail.
- A função de notificação do usuário (consulte 14.11.1 na p. 195) foi ampliada para determinados eventos de proteção. Você pode selecionar o método de notificação, como e-mail, notificações sonoras ou mensagens pop-up, além de registrar o evento em log.
- Agora, o programa consegue verificar o tráfego enviado pelo protocolo SSL.
- Foram acrescentados ao programa recursos de autodefesa, incluindo a proteção contra acesso remoto não autorizado de serviços antivírus e proteção das configurações do programa por senha. Esses recursos ajudam a evitar que programas mal-intencionados, hackers e usuários não autorizados desabilitem a proteção.

- Foi adicionada a opção de criar um disco de recuperação. Com esse disco, você pode reiniciar o sistema operacional após um ataque de vírus e verificá-lo quanto à presença de objetos mal-intencionados.

Recursos da nova interface do programa

- A nova interface do Kaspersky Anti-Virus torna as funções do programa claras e fáceis de usar. Você também pode mudar a aparência do programa usando seus próprios elementos gráficos e esquemas de cores.
- Durante sua utilização, o programa fornece dicas: o Kaspersky Anti-Virus exibe mensagens informativas sobre o nível de proteção, acompanha sua operação com dicas, e inclui uma seção de Ajuda completa.

Novos recursos de atualização do programa

- Esta versão do aplicativo inaugura o procedimento de atualização aprimorada: o Kaspersky Anti-Virus verifica automaticamente os pacotes de atualização na fonte. Ao detectar novas atualizações, o programa as baixa e instala no computador.
- O programa baixa as atualizações de maneira incremental, ignorando os arquivos que já foram baixados. Isso diminui o tráfego de download de atualizações em até 90%.
- As atualizações são baixadas da fonte mais rápida.
- Você pode escolher não usar um servidor proxy, baixando as atualizações do programa de uma fonte local. Isso reduz significativamente o tráfego no servidor proxy.
- O programa possui um recurso de reversão da atualização que permite retornar para a versão anterior das assinaturas se, por exemplo, as assinaturas de ameaças forem danificadas ou se houver um erro na cópia.
- Foi adicionado um recurso para a distribuição de atualizações de uma pasta local, de forma que outros computadores da rede tenham acesso a elas economizando largura de banda.

2.2. Os elementos da defesa do Kaspersky Anti-Virus

A proteção do Kaspersky Anti-Virus foi criada tendo em mente as fontes de ameaças. Em outras palavras, um componente separado do programa lida com cada ameaça, monitorando-a e tomando as medidas necessárias para evitar

seus efeitos mal-intencionados sobre os dados do usuário. Isso torna o sistema flexível, com opções amigáveis para que cada componente se ajuste às necessidades de um usuário específico ou de uma empresa como um todo.

O Kaspersky Anti-Virus inclui:

- Componentes de proteção (consulte 2.2.1 na p. 23), que fornecem uma defesa abrangente de todos os canais para transmissão e troca de dados no computador.
- Tarefas de verificação de vírus (consulte 2.2.2 na página 24) que verificam vírus na memória e no sistema de arquivos do computador, como arquivos individuais, pastas, discos ou regiões.
- Ferramentas de suporte (consulte 2.2.3 na página 25) que dão suporte para o programa e ampliam sua funcionalidade.

2.2.1. Componentes de proteção

Estes componentes de proteção protegem seu computador em tempo real:

Antivírus de Arquivos

Um sistema de arquivos pode conter vírus e outros programas perigosos. Os programas mal-intencionados podem permanecer inativos no sistema de arquivos durante anos sem aparecer, depois de serem copiados de um disquete ou da Internet. Contudo, basta utilizar o arquivo infectado para ativar o vírus instantaneamente.

Antivírus de Arquivos é o componente que monitora o sistema de arquivos do computador. Ele verifica todos os arquivos que podem ser abertos, executados ou salvos no computador e em todas as unidades de disco conectadas. O programa intercepta todas as tentativas de acessar arquivos e os verifica quanto à presença de vírus conhecidos. Se, por algum motivo, não for possível desinfectar um arquivo, ele será excluído e uma cópia do mesmo será salva no Backup (consulte 14.2 na p. 171) ou ele será movido para a Quarentena (consulte 14.1 na p. 167).

Antivírus de E-Mail

Os e-mails são amplamente usados pelos hackers para disseminar programas mal-intencionados, sendo um dos métodos mais comuns de disseminação de worms. Por isso, é extremamente importante monitorar todos os e-mails.

O componente *Antivírus de E-Mail* verifica todos os e-mails enviados e recebidos no computador. Ele analisa os e-mails com relação a programas mal-intencionados, concedendo acesso ao destinatário somente se o e-mail estiver livre de objetos perigosos.

Antivírus da Web

Ao abrir vários sites da Internet, você corre o risco de infectar o computador com vírus que serão instalados por scripts que estão nos sites, além de poder baixar um objeto perigoso.

O *Antivírus da Web* foi criado especificamente para combater esses perigos, interceptando e bloqueando os scripts de sites, se eles representarem uma ameaça, e monitorando extensivamente todo o tráfego HTTP.

Defesa Proativa

A cada dia surgem mais e mais programas mal-intencionados. Eles estão se tornando mais complexos, combinando vários tipos, e os métodos usados para se disseminarem estão se tornando cada vez mais difíceis de detectar.

Para detectar um novo programa mal-intencionado antes que ele possa causar danos, a Kaspersky Lab desenvolveu um componente específico, a *Defesa Proativa*. Ele foi criado para monitorar e analisar o comportamento de todos os programas instalados no computador. O Kaspersky Anti-Virus decide, com base nas ações do programa, se ele é possivelmente perigoso. A Defesa Proativa protege o computador dos vírus conhecidos e de vírus novos que ainda não foram descobertos.

2.2.2. Tarefas de verificação de vírus

Além de monitorar constantemente todos os possíveis caminhos de programas mal-intencionados, é extremamente importante fazer a verificação de vírus periodicamente no computador. Isso é necessário para detectar programas mal-intencionados que não foram descobertos antes pelo programa porque, por exemplo, ele estava definido com um nível de segurança muito baixo.

O Kaspersky Anti-Virus configura, por padrão, três tarefas de verificação de vírus:

Áreas críticas

Verifica todas as áreas críticas do computador quanto à presença de vírus. Estão incluídos: a memória do sistema, os programas carregados na inicialização, os setores de inicialização do disco rígido e os diretórios do sistema *Windows*. Essa tarefa tem como objetivo detectar vírus ativos rapidamente sem verificar todo o computador.

Meu Computador

Verifica vírus no computador com uma inspeção completa de todas as unidades de disco, da memória e dos arquivos.

Objetos de inicialização

Verifica vírus em todos os programas carregados automaticamente na inicialização, além da RAM e dos setores de inicialização dos discos rígidos.

Há também a opção de criar outras tarefas de verificação de vírus e criar uma programação para elas. Por exemplo, é possível criar uma tarefa de verificação semanal dos bancos de dados de e-mail ou uma tarefa de verificação de vírus na pasta **Meus Documentos**.

2.2.3. Ferramentas de programas

O Kaspersky Anti-Virus inclui várias ferramentas de suporte criadas para oferecer suporte a software em tempo real, expandindo os recursos do programa e o auxiliando no decorrer do trabalho.

Atualização

Para estar preparado para um ataque de hackers ou para excluir um vírus ou qualquer outro programa perigoso, o Kaspersky Anti-Virus precisa ser mantido atualizado. O componente *Atualização* foi criado para fazer exatamente isso. Ele é responsável pela atualização das assinaturas de ameaças e dos módulos internos do Kaspersky Anti-Virus.

O recurso de Distribuição de atualizações permite salvar atualizações do banco de dados de assinaturas de ameaças e drivers de rede, além dos módulos do aplicativo recuperados dos servidores da Kaspersky Lab, para depois conceder acesso a eles a outros computadores de forma a economizar largura de banda.

Arquivos de dados

A atualização de cada componente de segurança, tarefa de pesquisa de vírus e do programa cria um relatório enquanto é executada. Os relatórios contêm informações sobre as operações executadas e seus resultados. Utilizando o recurso *Relatórios*, você ficará sempre atualizado sobre o funcionamento de todos os componentes do Kaspersky Anti-Virus. Se houver problemas, os relatórios poderão ser enviados para a Kaspersky Lab para que nossos especialistas estudem a situação mais detalhadamente e o ajudem o mais rápido possível.

O Kaspersky Anti-Virus envia todos os arquivos suspeitos de serem perigosos para uma área específica de *Quarentena*, onde são armazenados em formato criptografado para evitar a infecção do computador. Você pode verificar esses objetos quanto à presença de vírus, restaurá-los em seus locais anteriores, excluí-los ou adicionar arquivos manualmente à Quarentena. Os arquivos que não estiverem infectados após a conclusão da verificação de vírus serão automaticamente restaurados em seus locais anteriores.

A área de *Backup* mantém cópias dos arquivos desinfectados e excluídos pelo programa. Essas cópias são criadas caso seja necessário restaurar os arquivos ou se você precisar das informações sobre a infecção. Essas cópias de backup também são armazenadas em formato criptografado para evitar outras infecções.

Você pode restaurar manualmente um arquivo do Backup no local original e excluir a cópia.

Disco de Recuperação

O Kaspersky Anti-Virus pode criar um Disco de Recuperação que fornece um plano de backup caso os arquivos do sistema sejam danificados por um ataque de vírus e seja impossível inicializar o sistema operacional. Nesse caso, usando o Disco de Recuperação, você pode inicializar o computador e restaurar o sistema à condição anterior à ação mal-intencionada.

Suporte

Todos os usuários registrados do Kaspersky Anti-Virus têm acesso à nossa equipe de Suporte Técnico. Para saber onde você pode obter suporte técnico, use o recurso *Suporte*.

Usando os links, é possível acessar o fórum de usuários da Kaspersky Lab e navegar por uma lista de perguntas freqüentes com respostas que podem ajudá-lo a resolver seu problema. Você também pode enviar um relatório de erros ou perguntas sobre o funcionamento do programa ao Suporte Técnico preenchendo um formulário on-line.

Também é possível acessar o Suporte Técnico on-line e, claro, nossos funcionários estarão sempre prontos para ajudá-lo com o Kaspersky Anti-Virus por telefone.

2.3. Requisitos de hardware e software do sistema

Para que o Kaspersky Anti-Virus 6.0 seja executado corretamente, seu computador deve atender a estes requisitos mínimos:

Requisitos gerais:

- 50 MB de espaço livre no disco rígido
- Unidade de CD-ROM (para instalar o Kaspersky Anti-Virus 6.0 de um CD de instalação)

- Microsoft Internet Explorer 5.5 ou superior (para atualizar as assinaturas de ameaças e módulos do programa pela Internet)
- Microsoft Windows Installer 2.0

Microsoft Windows 98, Microsoft Windows Me, Microsoft Windows NT Workstation 4.0 (Service Pack 6a):

- Processador Intel Pentium 300 MHz ou mais rápido (ou compatível)
- 64 MB de RAM

Microsoft Windows 98, Microsoft Windows Me, Microsoft Windows NT Workstation 4.0 (Service Pack 6a), Microsoft Windows 2000 Professional (Service Pack 2 ou superior), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 1 ou superior), Microsoft Windows XP Professional x64 Edition:

- Processador Intel Pentium 300 MHz ou mais rápido (ou compatível)
- 128 MB de RAM

Microsoft Windows Vista, Microsoft Windows Vista x64:

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

2.4. Pacotes de software

Você pode adquirir a vestão do Kaspersky Anti-Virus na caixa junto a nossos revendedores ou baixá-la de lojas da Internet, inclusive na seção **eStore** em www.kaspersky.com.

Se comprar a versão do programa na caixa, o pacote incluirá:

- Um envelope lacrado contendo um CD de instalação com os arquivos do programa
- Um Manual do Usuário
- O código de ativação do produto, em anexo ao envelope do CD de instalação
- O Contrato de Licença do Usuário Final (EULA)

Antes de abrir o lacre do envelope do disco de instalação, leia atentamente todo o EULA.

Se você comprou o Kaspersky Anti-Virus em uma loja on-line, copie o produto do site da Kaspersky Lab (**Downloads** → **Product Downloads**). Você pode baixar o Manual do Usuário na seção **Downloads** → **Documentation**.

Você receberá um código de ativação por e-mail após o recebimento do pagamento.

O Contrato de Licença do Usuário Final é um contrato legal entre você e a Kaspersky Lab que especifica os termos segundo os quais você pode usar o software que adquiriu.

Leia todo o EULA atentamente.

Se você não concordar com os termos do EULA, poderá retornar o produto na caixa para o revendedor de quem o comprou e será reembolsado da quantia paga pelo programa. Nesse caso, o envelope lacrado com o disco de instalação ainda deverá estar lacrado.

Ao abrir o disco de instalação lacrado, você aceita todos os termos do EULA.

2.5. Suporte para usuários registrados

A Kaspersky Lab fornece vários serviços que tornam o Kaspersky Anti-Virus mais efetivo para seus usuários registrados.

Ao ativar o programa, você se torna um usuário registrado e terá os seguintes serviços disponíveis até que a licença expire:

- Novas versões do programa gratuitamente
- Consultoria sobre questões relativas à instalação, configuração e funcionamento do programa, por telefone e por e-mail
- Notificações sobre novas versões de produtos da Kaspersky Lab e novos vírus (esses serviços se destinam a usuários que assinarem as mensagens de notícias da Kaspersky Lab)

A Kaspersky Lab não fornece suporte técnico relativo ao uso e funcionamento do sistema operacional ou de quaisquer produtos que não sejam de sua propriedade.

CAPÍTULO 3. INSTALANDO O KASPERSKY ANTI-VIRUS 6.0

Você pode instalar o Kaspersky Anti-Virus no computador total ou parcialmente.

Se escolher a instalação parcial, você poderá selecionar os componentes a serem instalados ou instalar automaticamente apenas os componentes antivírus (consulte a Etapa 9 do procedimento de instalação). É possível instalar os outros componentes do programa posteriormente, mas o disco de instalação será necessário para fazê-lo. É recomendável copiar o disco de instalação no disco rígido.

O aplicativo pode ser instalado das maneiras a seguir:

- Usando o assistente para instalação (consulte 3.1 na p. 29)
- Do prompt de comando (consulte 3.3 na p. 39)

3.1. Procedimento de instalação usando o Assistente para Instalação

Antes de iniciar a instalação do Kaspersky Anti-Virus, é recomendável fechar todos os outros aplicativos.

Para instalar o Kaspersky Anti-Virus no computador, abra o arquivo do Windows Installer do CD de instalação.

Observação:
A instalação do programa por meio de um pacote de instalação baixado pela Internet é igual à instalação a partir de um CD de instalação.

Um assistente para instalação do programa será aberto. Cada janela contém um conjunto de botões para navegar pelo processo de instalação. Segue uma breve explicação sobre suas funções:

- **Avançar** – aceita uma ação e avança para a próxima etapa da instalação.

- **Voltar** – volta para a etapa anterior da instalação.
- **Cancelar** – cancela a instalação do produto.
- **Concluir** – conclui o procedimento de instalação do programa.

Vamos examinar as etapas do procedimento de instalação mais detalhadamente.

Etapa 1. Verificando as condições do sistema necessárias para instalar o Kaspersky Anti-Virus

Antes de o programa ser instalado no computador, a instalação verifica o computador quando ao sistema operacional e os pacotes de serviços necessários para instalar o Kaspersky Anti-Virus. Também são verificados os outros programas necessários e se os seus direitos de usuário permitem a instalação de software.

Se algum desses requisitos não for atendido, o programa exibirá uma mensagem informando-o. É recomendável instalar os programas e os pacotes de serviços necessários através do **Windows Update** antes de instalar o Kaspersky Anti-Virus.

Etapa 2. Janela de boas-vindas da instalação

Se o sistema atender a todos os requisitos, uma janela de instalação com informações sobre como iniciar a instalação do Kaspersky Anti-Virus aparecerá ao abrir o arquivo de instalação.

Para continuar a instalação, clique no botão **Avançar**. Você pode cancelar a instalação clicando em **Cancelar**.

Etapa 3. Exibindo o Contrato de Licença do Usuário Final

A janela a seguir contém o Contrato de Licença do Usuário Final entre você e a Kaspersky Lab. Leia-o atentamente e, se concordar com todos os termos do contrato, selecione **Eu aceito os termos do Contrato de Licença** e clique no botão **Avançar**. A instalação continuará.

Etapa 4. Selecionando uma pasta de instalação

O próximo estágio da instalação do Kaspersky Anti-Virus determina o local onde o programa será instalado no computador. O caminho padrão é o seguinte: **<Unidade>\Arquivos de Programas\Kaspersky Lab\Kaspersky Anti-Virus 6.0**.

Você pode especificar outra pasta clicando no botão **Procurar** e selecionando-a na janela de seleção de pastas ou inserindo o caminho para a pasta no campo disponível.

Lembre-se de que, se você inserir o nome completo da pasta de instalação manualmente, ele não poderá exceder 200 caracteres, nem conter caracteres especiais.

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

Etapa 5. Selecionando um tipo de instalação

Neste estágio, selecione as partes do programa que deseja instalar no computador. Existem três opções:

Completa. Se você selecionar esta opção, todos os serviços do Kaspersky Anti-Virus serão instalados.

Personalizada. Se você selecionar esta opção, poderá selecionar os componentes do programa que deseja instalar. Para saber mais, consulte a Etapa 6. .

Para selecionar um tipo de instalação, clique no botão apropriado.

Etapa 6. Selecionando os componentes do programa a serem instalados

Você verá esta etapa somente se selecionar o tipo de instalação **Personalizada**.

Se você selecionou a instalação Personalizada, poderá escolher os componentes do Kaspersky Anti-Virus que deseja instalar. Por padrão, todos os componentes estão selecionados.

Para selecionar os componentes que deseja instalar, clique com o botão direito do mouse no ícone ao lado do nome de um componente e selecione **Será instalado no disco rígido local** no menu de contexto. Você encontrará mais informações sobre a proteção que um componente selecionado fornece e quanto espaço em disco é necessário para sua instalação na parte inferior da janela de instalação do programa.

Se não desejar instalar um componente, selecione **Todo o recurso estará indisponível** no menu de contexto. Lembre-se de que, ao escolher não instalar um componente, você se priva da proteção contra vários programas perigosos.

Depois de selecionar os componentes que deseja instalar, clique em **Avançar**. Para fazer a lista retornar aos programas padrão a serem instalados, clique em **Redefinir**.

Etapa 7. Pesquisando outros programas antivírus

Neste estágio, a instalação pesquisa outros produtos antivírus instalados no computador, incluindo produtos da Kaspersky Lab, que poderiam gerar problemas de compatibilidade com o Kaspersky Anti-Virus.

A instalação exibirá na tela uma lista desses programas detectados. O programa perguntará se deseja desinstalá-los antes de continuar a instalação.

Você pode selecionar a desinstalação manual ou automática na lista de aplicativos antivírus detectados.

Se a lista de programas antivírus contiver o Kaspersky Anti-Virus® Personal ou o Kaspersky Anti-Virus® Personal Pro, é recomendável salvar a chave de licença usada por eles antes de excluí-los, pois você poderá usá-la como chave de licença do Kaspersky Anti-Virus 6.0. Também é recomendável salvar os objetos da Quarentena e do Backup. Esses objetos serão movidos automaticamente para a Quarentena e o Backup do Kaspersky Anti-Virus 6.0 e você poderá continuar trabalhando com eles.

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

Etapa 8. Concluindo a instalação do programa

Neste estágio, o programa solicitará que você conclua a instalação do programa no computador. Você pode decidir se deseja usar configurações de proteção ou assinaturas de ameaças de uma versão anterior do Kaspersky Anti-Virus (por exemplo, se você instalou a versão beta e está instalando agora a versão comercial).

Vamos examinar mais detalhadamente como usar as opções descritas acima.

Se você tiver instalado anteriormente outra versão ou compilação do Kaspersky Anti-Virus no computador e tiver salvado as assinaturas de ameaças ao desinstalá-la, poderá usá-las na versão atual. Para fazê-lo, marque ☑ **Assinaturas de ameaças**. As assinaturas de ameaças incluídas com o programa de instalação não serão copiadas para o computador.

Para usar as configurações de proteção definidas e salvas em uma versão anterior, marque ☑ **Configurações de proteção**.

É recomendável não desmarcar ☑ **Habilitar Autodefesa antes da instalação** ao instalar o Kaspersky Anti-Virus 6.0 pela primeira vez. Ao habilitar os módulos de proteção, você poderá reverter a instalação corretamente, se ocorrerem erros na instalação do programa. Se estiver reinstalando o programa, é recomendável desmarcar esta caixa de seleção.

Se o aplicativo for instalado remotamente por meio da **Área de Trabalho Remota do Windows**, é recommendável marcar ☑ **Habilitar Autodefesa antes da instalação**. Caso contrário, talvez o procedimento de instalação não

seja concluído corretamente.

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

Etapa 9. Lendo informações importantes sobre o programa

Neste estágio, a instalação pergunta se você deseja examinar informações importantes sobre o programa antes de começar com o Kaspersky Anti-Virus. Esta caixa de diálogo contém os recursos básicos do Kaspersky Anti-Virus, com algumas informações sobre como ele funciona.

Para continuar na próxima etapa, clique no botão **Avançar**.

Etapa 10. Concluindo o procedimento de instalação

A janela **Instalação concluída** contém informações sobre como concluir o processo de instalação do Kaspersky Anti-Virus.

Se a instalação for concluída com êxito, uma mensagem na tela solicitará que você reinicie o computador. Depois de reiniciar o sistema, o Assistente para Instalação do Kaspersky Anti-Virus será iniciado automaticamente.

Se não for necessário reiniciar o sistema para concluir a instalação, clique em **Avançar** para continuar no Assistente para Instalação.

3.2. Assistente para Instalação

O Assistente para Instalação do Kaspersky Anti-Virus 6.0 é iniciado depois de o programa ter concluído a instalação. Ele foi criado para ajudá-lo a definir as configurações iniciais do programa para se ajustarem aos recursos e usos do computador.

A interface do Assistente para Instalação foi criada como um Assistente do Windows padrão e consiste em uma série de etapas pelas quais você pode se mover usando os botões **Voltar** e **Avançar**, ou concluir, usando o botão **Concluir.** O botão **Cancelar** interromperá o Assistente a qualquer momento.

Você pode ignorar este estágio de configurações iniciais ao instalar o programa, fechando a janela do Assistente. No futuro, você poderá executá-lo novamente a partir da interface do programa, se restaurar as configurações padrão do Kaspersky Anti-Virus (consulte 6.6 na p. 77).

3.2.1. Usando objetos salvos na Versão 5.0

Esta janela do assistente será exibida ao instalar o aplicativo sobre o Kaspersky Anti-Virus 5.0. Será solicitado que você selecione os dados usados pela verão

5.0 que deseja importar para a versão 6.0. Podem estar incluídos os arquivos da quarentena ou do backup, ou as configurações de proteção.

Para usar esses dados na Versão 6.0, marque as caixas desejadas.

3.2.2. Ativando o programa

Você pode ativar o programa instalando uma chave de licença. O Kaspersky Anti-Virus verifica o contrato de licença e determina sua data de expiração.

A chave de licença contém as informações do sistema necessárias para o funcionamento de todos os recursos do programa e outras informações:

- Informações de suporte (que fornecem suporte ao programa e onde é possível obtê-lo)
- Nome, número e data de expiração de sua licença

Aviso!

É necessário ter uma conexão com a Internet para ativar o programa. Se você não estiver conectado à Internet durante a instalação, poderá ativar o programa posteriormente a partir da interface do programa (consulte 14.5 na p. 183).

Selecionando um método de ativação do programa

Existem várias opções de ativação do programa, dependendo de você ter uma chave de licença do Kaspersky Anti-Virus ou precisar obter uma do servidor da Kaspersky Lab:

- **Ativar usando o código de ativação**. Selecione esta opção de ativação se tiver comprado a versão completa do programa e recebido um código de ativação. Com esse código, você receberá uma chave de licença que fornece acesso completo a todos os recursos do programa até a expiração da licença.
- **Ativar versão de teste.** Selecione esta opção de ativação se desejar instalar a versão de teste do programa antes de decidir comprar a versão comercial. Será fornecida uma chave de licença gratuita com um período de teste limitado.
- **Aplicar chave de licença existente**. Ativa o aplicativo usando o arquivo da chave de licença do Kaspersky Anti-Virus 6.0, obtido anteriormente.
- **Ativar mais tarde**. Se você escolher esta opção, o estágio de ativação será ignorado. O Kaspersky Anti-Virus 6.0 será instalado no computador e você terá acesso a todos os recursos do programa, exceto as atualizações (é

possível atualizar as assinaturas de ameaças somente depois de instalar o programa).

As duas primeiras opções de ativação utilizam um servidor Web da Kaspersky Lab, o que exige uma conexão com a Internet. Antes da ativação, edite suas configurações de rede (consulte 13.4.3 na p. 161) na janela que é aberta ao clicar em **Configurações da LAN**, se necessário. Para obter informações mais detalhadas sobre a configuração da rede, entre em contato com o administrador do sistema ou seu provedor.

Inserindo o código de ativação

Para ativar o programa, insira o código de ativação fornecido ao comprar o programa. O código de ativação deve ser inserido usando caracteres latinos.

Insira suas informações pessoais na parte inferior da janela: nome completo, endereço de e-mail, país e cidade de residência. Essas informações poderão ser solicitadas para identificar um usuário registrado, caso uma chave seja perdida ou roubada. Se isso ocorrer, você poderá obter uma nova chave de licença com as informações pessoais.

Obtendo uma chave de licença

O Assistente para Instalação se conecta aos servidores da Kaspersky Lab e envia seus dados de registro (o código de ativação e as informações pessoais) para inspeção.

Se o código de ativação passar na inspeção, o Assistente receberá o arquivo da chave de licença. Se você instalar a versão de demonstração do programa, o Assistente para Instalação receberá o arquivo da chave de teste sem um código de ativação.

O arquivo recebido será instalado automaticamente e você verá uma janela de conclusão da ativação com informações detalhadas sobre a licença.

Se o código de ativação não passar na inspeção, uma mensagem informativa será exibida na tela. Se isso ocorrer, entre em contato com os fornecedores do software de quem você comprou o programa para obter mais informações.

Selecionando o arquivo da chave de licença

Se você possuir um arquivo de chave de licença do Kaspersky Anti-Virus 6.0, o Assistente perguntará se deseja instalá-lo. Se desejar, use o botão **Procurar** e selecione o caminho do arquivo da chave com a extensão *.key* na janela de seleção de arquivos.

Depois de ter instalado a chave com êxito, você verá informações sobre a licença na parte inferior da janela: nome do proprietário do software, número da licença, tipo de licença (completo, teste beta, demonstração, etc.) e a data de expiração da licença.

Concluindo a ativação do programa

O Assistente para Instalação o informará que a ativação do programa foi bem-sucedida. Também serão exibidas informações sobre a chave de licença instalada: nome do proprietário do software, número da licença, tipo de licença (completo, teste beta, demonstração, etc.) e a data de expiração da licença.

3.2.3. Selecionando um modo de segurança

Nesta janela, o Assistente para Instalação solicitará que você selecione o modo de segurança no qual o programa funcionará:

Básico. Esta é a configuração padrão, criada para usuários que não têm muita experiência com computadores ou com software antivírus. Define todos os componentes do programa com seus níveis de segurança recomendados e apenas informa o usuário sobre eventos perigosos, como a detecção de código mal-intencionado ou ações perigosas que estão sendo executados.

Interativo. Este modo fornece uma defesa mais personalizada dos dados do seu computador que a do modo básico. Ele controla as tentativas de alterar as configurações do sistema e atividades suspeitas no sistema.

Todas as atividades listadas poderiam ser indícios de programas mal-intencionados ou de atividade padrão de alguns dos programas que você usa no computador. Será necessário decidir caso a caso se essas atividades devem ser permitidas ou bloqueadas.

Se optar por este modo, especifique quando ele deve ser usado:

- **Habilitar Proteção do Registro** – solicita a decisão do usuário no caso de detectar tentativas de alterar chaves do Registro do sistema.

  Se o aplicativo for instalado em um computador que executa o Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista ou Microsoft Windows Vista x64, as configurações do modo interativo listadas a seguir não estarão disponíveis.

- **Habilitar Controle de integridade do aplicativo** – solicita que o usuário confirme as ações executadas quando forem carregados módulos nos aplicativos monitorados.

- **Habilitar Defesa Proativa Estendida** – habilita a análise de todas as atividades suspeitas no sistema, incluindo a abertura de navegadores com configurações da linha de comando, o

carregamento em processos de programas e ganchos de janelas (essas configurações estão desabilitadas por padrão).

3.2.4. Configurando a atualização

A segurança do computador depende diretamente da atualização periódica das assinaturas de ameaças e dos módulos do programa. Nesta janela, o Assistente para Instalação solicita que você selecione um modo de atualização do programa e que configure uma programação.

- **Automaticamente**. O Kaspersky Anti-Virus verifica os pacotes de atualização na fonte em intervalos definidos. É possível definir as verificações de forma que sejam mais freqüentes durante os surtos de vírus e menos freqüentes quando eles terminarem. Ao detectar novas atualizações, o programa as baixa e instala no computador. Essa é a configuração padrão.
- **Cada 1 dia(s)**.As atualizações serão executadas automaticamente de acordo com a programação criada. Você pode configurar a programação clicando em **Alterar**.
- **Manualmente**. Se escolher esta opção, você mesmo executará as atualizações do produto.

Observe que as assinaturas de ameaças e os módulos do programa incluídos com o software podem estar desatualizados ao instalar o programa. Por isso, é recomendável baixar as atualizações mais recentes do programa. Para fazê-lo, clique em **Atualizar agora**. Em seguida, o Kaspersky Anti-Virus baixará as atualizações necessárias dos servidores de atualização e as instalará no computador.

Se desejar configurar as atualizações (configurar propriedades da rede, selecionar o recurso do qual as atualizações serão baixadas ou selecionar o servidor de atualização mais próximo), clique em **Configurações**.

3.2.5. Configurando uma programação de verificação de vírus

A verificação de objetos mal-intencionados em áreas selecionadas do computador é uma das principais etapas da proteção do mesmo.

Ao instalar o Kaspersky Anti-Virus, três tarefas de verificação de vírus padrão são criadas. Nesta janela, o Mestre de Configurações solicita que você escolha uma configuração para a tarefa de verificação:

Verificar objetos de inicialização

Por padrão, o Kaspersky Anti-Virus verifica automaticamente os objetos de inicialização ao ser iniciado. Você pode editar as configurações da programação em outra janela, clicando em **Alterar**.

Verificar áreas críticas

Para verificar automaticamente as áreas críticas do computador (memória do sistema, objetos de inicialização, setores de inicialização, pastas do sistema do Windows) quanto à presença de vírus, marque a caixa apropriada. Você pode configurar a programação clicando em **Alterar**.

A configuração padrão dessa verificação automática é desabilitada.

Verificação completa do computador

Para que uma verificação completa de vírus no seu computador seja executada automaticamente, marque a caixa apropriada. Você pode configurar a programação clicando em **Alterar**.

A configuração padrão para a execução programada dessa tarefa é desabilitada. Contudo, é recomendável executar uma verificação completa de vírus no computador imediatamente após a instalação do programa.

3.2.6. Restringindo o acesso ao programa

Como várias pessoas com diferentes níveis de experiência com computadores podem usar um computador pessoal e vários programas mal-intencionados podem desabilitar a proteção, existe a opção de proteger o acesso ao Kaspersky Anti-Virus por senha. O uso de uma senha pode proteger o programa de tentativas não-autorizadas de desabilitar a proteção ou alterar as configurações.

Para habilitar a proteção por senha, marque **Habilitar proteção por senha** e preencha os campos **Senha** e **Confirmar senha**.

Selecione a seguir a área na qual deseja aplicar a proteção por senha:

- **Todas as operações (exceto notificações de eventos perigosos)**. Solicita a senha se o usuário tenta executar qualquer ação no programa, exceto pelas respostas a notificações sobre a detecção de objetos perigosos.
- **Operações selecionadas:**
  - **Ao salvar configurações do programa** - solicita a senha quando um usuário tenta salvar alterações das configurações do programa.
  - **Ao sair do programa** - solicita a senha se um usuário tentar fechar o programa.
  - **Ao interromper/pausar componentes de proteção ou tarefas de verificação de vírus** – solicita a senha se o usuário tentar pausar ou

desabilitar completamente qualquer componente de proteção ou tarefa de verificação de vírus.

3.2.7. Controle de integridade do aplicativo

Neste estágio, o assistente do Kaspersky Anti-Virus analisará os aplicativos instalados no computador (arquivos de bibliotecas dinâmicas, assinaturas de fabricação digital), contará os arquivos de soma de verificação dos aplicativos e criará uma lista de programas confiáveis com relação à segurança de vírus. Por exemplo, essa lista incluirá automaticamente todos os arquivos assinados digitalmente pela Microsoft.

No futuro, o Kaspersky Anti-Virus usará as informações obtidas ao analisar a estrutura dos aplicativos para evitar que códigos mal-intencionados sejam incorporados em módulos de aplicativos.

A análise dos aplicativos instalados no seu computador pode levar algum tempo.

3.2.8. Concluindo o Assistente para Instalação

A última janela do Assistente perguntará se você deseja reiniciar o computador para concluir a instalação do programa. Reinicie para que alguns dos drivers de serviços do Kaspersky Anti-Virus sejam registrados corretamente.

Você pode aguardar para reiniciar mas, se o fizer, alguns componentes do programa não funcionarão.

3.3. Instalando o programa do prompt de comando

Para instalar o Kaspersky Anti-Virus 6.0, insira o seguinte no prompt de comando:

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

O Assistente para Instalação será iniciado (consulte 3.1 na p. 29). Depois que o programa for instalado, reinicie o computador.

Você também pode usar um dos seguintes métodos para instalar o aplicativo.

Para instalar o aplicativo em segundo plano, sem reiniciar o computador (o computador deve ser reiniciado manualmente após a instalação), digite:

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

Para instalar o aplicativo em segundo plano e reiniciar o computador, digite:

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

3.4. Atualizando da versão 5.0 para a versão 6.0

Se o Kaspersky Anti-Virus 5.0 Personal ou o Kaspersky Anti-Virus 5.0 Personal Pro estiver instalado no computador, você poderá atualizá-lo para o Kaspersky Anti-Virus 6.0.

Depois de iniciar o programa de instalação do Kaspersky Anti-Virus 6.0, você terá a opção de desintalar a versão 5.0 instalada. Depois que o processo de desinstalação for concluído, reinicie o computador e a instalação da versão 6.0 será executada.

Aviso!

Ao atualizar o Kaspersky Anti-Virus 5.0 para a versão 6.0 de uma pasta de rede protegida por senha, a versão 5.0 será desinstalada e o computador será reiniciado sem instalar a versão 6.0 do aplicativo. Isso se deve ao fato de o programa de instalação não possuir privilégios de acesso à pasta de rede. Para resolver este problema, execute a instalação de uma pasta local.

CAPÍTULO 4. INTERFACE DO PROGRAMA

A interface do Kaspersky Anti-Virus é direta e amigável. Este capítulo aborda seus recursos básicos:

- Ícone da bandeja do sistema (consulte 4.1 na página 41)
- Menu de contexto (consulte 4.2 na página 42)
- Janela principal (consulte 4.3 na página 43)
- Janela de configurações do programa (consulte 4.4 na página 46)

Além da interface principal do programa, existem plug-ins para os seguintes aplicativos:

- Microsoft Office Outlook;
- The Bat!;
- Microsoft Windows Explorer.

Os plug-ins ampliam a funcionalidade desses programas, tornando possível gerenciar e configurar o Kaspersky Anti-Virus nas suas interfaces.

4.1. Ícone da bandeja do sistema

Logo após a instalação do Kaspersky Anti-Virus, o ícone do programa será exibido na bandeja do sistema.

O ícone é um indicador das funções do Kaspersky Anti-Virus. Ele reflete o status da proteção e mostra várias funções básicas executadas pelo programa.

Se o ícone estiver ativo  (colorido), seu computador estará protegido. Se o ícone estiver inativo  (preto e branco), sua proteção estará totalmente parada ou vários componentes de proteção (consulte 2.2.1 na p. 23) estarão pausados.

O ícone do Kaspersky Anti-Virus muda dependendo da operação em execução:

 Os e-mails estão sendo verificados.

 Os scripts estão sendo verificados.

Um arquivo que você ou algum programa está abrindo, salvando ou executando está sendo verificado.

As assinaturas de ameaças e módulos do Kaspersky Anti-Virus estão sendo atualizados.

Ocorreu um erro em algum componente do Kaspersky Anti-Virus.

O ícone também dá acesso aos principais itens da interface do programa: o menu de contexto (consulte 4.2 na página 42) e a janela principal (consulte 4.3 na página 43).

Para abrir o menu de contexto, clique com o botão direito do mouse no ícone do programa.

Para abrir a janela principal do Kaspersky Anti-Virus na seção **Proteção** (a primeira tela padrão ao abrir o programa), clique duas vezes no ícone do programa. Se você clicar uma vez, a janela principal será aberta na seção que estava ativa quando foi fechada pela última vez.

4.2. O menu de contexto

Você pode executar tarefas de proteção básicas a partir do menu de contexto (consulte a fig. 1).

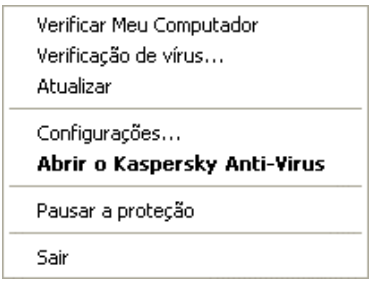


Figura 1. O menu de contexto

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

Verificar Meu Computador – inicia uma verificação completa de objetos perigosos no computador. Os arquivos em todas as unidades, incluindo mídias de armazenamento removíveis, serão verificados.

Verificação de vírus... – seleciona objetos e inicia sua verificação quanto à presença de vírus. A lista padrão contém vários arquivos, como a pasta **Meus Documentos**, a pasta Inicialização, bancos de dados de e-mail,

todas as unidades do computador, etc. Você pode completar a lista, selecionar arquivos para serem verificados e iniciar verificações de vírus.

Atualização – baixa atualizações de módulos do programa e assinaturas de ameaças e os instala no computador.

Ativar – ativa o programa. Este item de menu estará disponível somente se o programa não estiver ativado.

Configurações... – exibe e configura o Kaspersky Anti-Virus.

Abrir o Kaspersky Anti-Virus – abre a janela principal do programa (consulte 4.3 na página 43).

Pausar a Proteção / Reiniciar a Proteção – desabilita temporariamente ou habilita os componentes de proteção (consulte 2.2.1 na p. 23). Este item do menu não afeta tarefas de atualização do programa ou de verificação de vírus.

Sair – fecha o Kaspersky Anti-Virus.

Se uma tarefa de pesquisa de vírus estiver em execução, o menu de contexto exibirá seu nome com um medidor de porcentagem de andamento. Ao selecionar a tarefa, você poderá abrir a janela de relatório para exibir os resultados de desempenho atuais.

4.3. Janela principal do programa

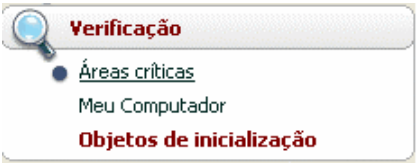
A janela principal do Kaspersky Anti-Virus (veja a fig. 2) oferece uma interface direta e amigável para você gerenciar o programa. Ela pode ser dividida em duas partes:

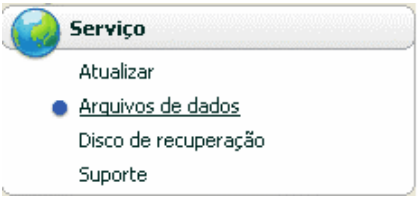
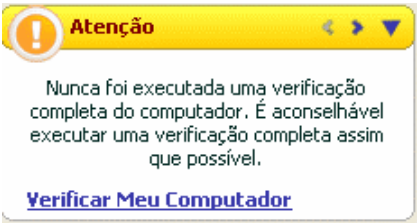
- à esquerda da janela, o painel de navegação o orienta de maneira rápida e fácil para qualquer componente, o desempenho da tarefa de verificação de vírus ou as ferramentas de suporte do programa;
- à direita da janela, o painel informativo contém informações sobre o componente de proteção selecionado à esquerda e exibe as configurações de cada um deles, fornecendo ferramentas para executar verificações de vírus, trabalhar com arquivos em quarentena e cópias de backup, gerenciar chaves de licença, etc.

Figura 2. Janela principal do Kaspersky Anti-Virus

Ao selecionar uma seção ou componente à esquerda da janela, você encontrará informações correspondentes à direita.

Agora, vamos examinar mais detalhadamente os elementos no painel de navegação da janela principal.

Seção da janela principal	Finalidade
Essencialmente, esta janela o informa sobre o status de proteção do seu computador. A seção **Proteção** foi criada exatamente para isso.  	Aqui, você encontrará informações gerais sobre as operações do Kaspersky Anti-Virus, sendo possível verificar se todos os componentes estão sendo executados corretamente e examinar as estatísticas gerais. Você também pode habilitar/desabilitar os componentes de proteção. Para exibir as estatísticas e configurações de um componente de proteção específico, basta selecionar o nome do componente sobre o qual deseja informações na seção **Proteção**.
Para verificar programas ou arquivos mal-intencionados no computador, use a seção **Verificação** específica na janela principal.  	Esta seção contém uma lista de objetos que podem ser verificados quanto à presença de vírus. Também é possível criar tarefas de verificação de vírus nesta seção, que será exibida no painel de navegação. Este recurso torna o início das verificações de vírus muito mais simples. As tarefas mais comuns e mais importantes são incluídas nesta seção. Elas incluem tarefas de verificação de vírus em áreas críticas, em programas de inicialização e a verificação completa do computador.

A seção **Serviço** inclui recursos adicionais do Kaspersky Anti-Virus. 	Aqui, você pode atualizar o programa, exibir relatórios sobre o desempenho dos componentes do Kaspersky Anti-Virus, trabalhar com objetos em quarentena e cópias de backup, examinar informações de suporte técnico, criar um Disco de Recuperação e gerenciar chaves de licença.
A seção de **comentários e dicas** o acompanha durante o uso do aplicativo. 	Esta seção fornece dicas de como elevar o nível de segurança do computador. Você também encontrará comentários sobre o desempenho atual do aplicativo e suas configurações. Os links nesta seção o orientam na execução das ações recomendadas para uma determinada seção ou para exibir informações mais detalhadas.

Cada elemento do painel de navegação é acompanhado por um menu de contexto específico. O menu contém pontos para as ferramentas e componentes de proteção que ajudam o usuário na sua rápida configuração, gerenciamento e na exibição de relatórios. Existe um item de menu adicional para tarefas de verificação de vírus e de atualização que permite que você crie sua própria tarefa modificando uma cópia de uma tarefa selecionada.

Você pode mudar a aparência do programa criando e usando seus próprios elementos gráficos e esquemas de cores.

4.4. Janela de configurações do programa

Você pode abrir a janela de configurações do Kaspersky Anti-Virus a partir da janela principal (consulte 4.3 na página 43). Para fazê-lo, clique em Configurações na parte superior da janela.

A janela de configurações (veja a fig. 3) tem uma aparência semelhante à da janela principal:

- à esquerda da janela, você tem acesso rápido e fácil às configurações de cada componente do programa, das tarefas de pesquisa de vírus e das ferramentas do programa;
- à direita da janela, existe uma lista detalhada de configurações do item selecionado à esquerda.

Ao selecionar qualquer seção, componente ou tarefa à esquerda da janela de configurações, a parte direita exibirá suas configurações básicas. Para definir as configurações avançadas, você pode abrir janelas de configurações de segundo e terceiro níveis, clicando nos botões correspondentes. É possível obter uma descrição detalhada das configurações do programa nas seções apropriadas do Manual do Usuário.

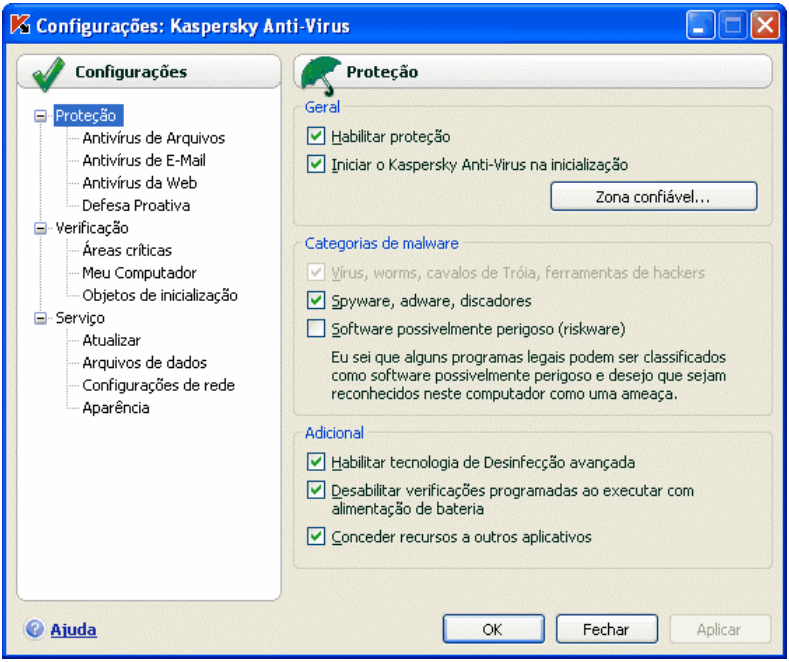


Figura 3. Janela de configurações do Kaspersky Anti-Virus

CAPÍTULO 5. INTRODUÇÃO

Uma das principais metas da Kaspersky Lab na criação do Kaspersky Anti-Virus é o fornecimento de uma configuração ótima para cada opção do programa. Isso possibilita que um usuário com qualquer nível de experiência em informática proteja rapidamente seu computador imediatamente após a instalação.

Contudo, os detalhes de configuração do computador ou os trabalhos para os quais você o utiliza podem ter seus requisitos específicos. Por isso, é recomendável executar uma configuração preliminar para atingir a proteção personalizada mais flexível para o computador.

Para tornar mais fácil começar, combinamos todos os estágios preliminares de configuração em um Assistente para Instalação (consulte 3.2 na p. 33) que é iniciado assim que o programa é instalado. Seguindo as instruções do Assistente, você pode ativar o programa, configurar as atualizações e verificações de vírus, além de proteger o acesso ao programa por senha.

Depois de instalar e iniciar o programa, é recomendável executar as seguintes etapas:

- Verifique o status de proteção atual (consulte 5.1 na página 48) para certificar-se de que o Kaspersky Anti-Virus está sendo executado no nível apropriado.
- Atualize o programa (consulte 5.5 na página 56) se o Assistente para Instalação não o fizer automaticamente depois de instalar o programa.
- Verifique o computador (consulte 5.2 na página 54) quanto à presença de vírus.

5.1. Qual é o status de proteção do computador?

Informações complexas sobre a proteção do computador são fornecidas na janela principal do programa, na seção **Proteção**. O *status de proteção atual* do computador e as *estatísticas gerais de desempenho* do programa são exibidos aqui.

O **status de proteção do computador** exibe o status atual da proteção do computador usando indicadores especiais (consulte 5.1.1 na página 49). As estatísticas (consulte 5.1.2 na página 52) analisam a sessão atual do programa.

5.1.1. Indicadores de proteção

O **status de proteção** é determinado por três indicadores que refletem aspectos diversos da proteção do computador a qualquer momento e que mostram problemas nas configurações e no desempenho do programa.

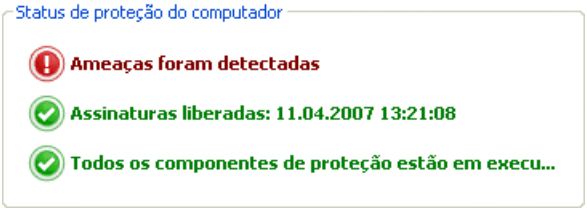


Figura 4. Indicadores que refletem o status de proteção do computador

Cada indicador tem três aparências possíveis:

– *a situação é normal*; o indicador mostra que a proteção do computador está adequada e que não há problemas na configuração ou no desempenho do programa.

– *existem um ou mais desvios* no desempenho do Kaspersky Anti-Virus com relação ao nível recomendado, o que poderia afetar a segurança das informações. Preste atenção às ações recomendadas pela Kaspersky Lab, fornecidas em links.

– *o status de segurança do computador é crítico*. Siga rigorosamente as recomendações para aprimorar a proteção do computador. São fornecidos links para as ações recomendadas.

Agora, vamos examinar os indicadores de proteção e as situações indicadas por cada um deles mais detalhadamente.

O primeiro indicador reflete a situação de arquivos e programas mal-intencionados no computador. Os três valores deste indicador significam o seguinte:

Nenhuma ameaça detectada

O Kaspersky Anti-Virus não detectou nenhum arquivo ou programa perigoso no computador.

Todas as ameaças foram neutralizadas

O Kaspersky Anti-Virus neutralizou todos os arquivos e

programas infectados e excluiu os que não puderam ser neutralizados.

Ataque de hacker bloqueado

O Kaspersky Anti-Virus detectou e bloqueou uma tentativa de ataque de rede.

Foram detectadas ameaças

Existe risco de infecção no computador. O Kaspersky Anti-Virus detectou programas mal-intencionados (vírus, cavalos de Tróia, worms, etc.) que devem ser neutralizados. Para fazê-lo, use o link Neutralizar tudo. Clique no link Detalhes para ver informações mais detalhadas sobre os objetos mal-intencionados.

Reinicie o computador

Para processar os arquivos ou programas mal-intencionados, é necessário reiniciar o computador. Salve e feche todos os arquivos com os quais está trabalhando e use o link Reiniciar computador.

O segundo indicador mostra a eficiência da proteção do computador. O indicador assume um dos seguintes valores:

Assinaturas liberadas: (data, hora)

O aplicativo e as assinaturas de ameaças usadas pelo Kaspersky Anti-Virus são as versões mais recentes.

As assinaturas estão desatualizadas

As assinaturas de ameaças e os módulos internos do Kaspersky Anti-Virus não foram atualizados por vários dias. Você está correndo o risco de infectar o computador com novos programas mal-intencionados que apareceram desde a última atualização do programa. É recomendável atualizar o Kaspersky Anti-Virus. Para fazê-lo, use o link Atualização.

Reinicie o computador

Reinicie o sistema para que o programa seja executado corretamente. Salve e feche todos os arquivos com os quais está trabalhando e use o link Reiniciar computador.

As assinaturas estão obsoletas

O Kaspersky Anti-Virus não foi atualizado por algum tempo. Os dados correm um grande risco. Atualize o programa assim que possível. Para fazê-lo, use o link Atualização.

As assinaturas estão corrompidas ou parcialmente corrompidas

Os arquivos de assinaturas de ameaças estão total ou parcialmente danificados. Se isso ocorrer, é recomendável executar as atualizações do programa novamente. Se a mesma mensagem de erro aparecer novamente, entre em contato com o Serviço de Suporte Técnico da Kaspersky Lab.

O terceiro indicador mostra a funcionalidade atual do programa. O indicador assume um dos seguintes valores:

Todos os componentes de proteção estão em execução

O Kaspersky Anti-Virus está protegendo o computador em todos os canais pelos quais programas mal-intencionados poderiam entrar. Todos os componentes de proteção estão habilitados.

A proteção não está instalada

Quando o Kaspersky Anti-Virus foi instalado, nenhum dos componentes de monitoramento foi instalado. Isso significa que você pode apenas verificar vírus. Para obter segurança máxima, instale os componentes de proteção no computador.

Alguns componentes de proteção estão pausados

Um ou vários componentes de proteção foram pausados. Para restaurar o componente inativo, selecione-o na lista e clique em ▶.

Todos os componentes de proteção estão pausados

Todos os componentes de proteção foram pausados. Para restaurá-los, selecione **Continuar proteção** no menu de contexto, clicando no ícone da bandeja do sistema.

Alguns componentes de proteção estão desabilitados

Um ou vários componentes de proteção foram parados. Isso poderia levar à infecção do computador e à perda de dados. É fortemente recomendável habilitá-la. Para fazê-lo, selecione um componente inativo na lista e clique em ▶.

Todos os componentes de proteção estão desabilitados

A proteção está totalmente desabilitada. Nenhum componente está em execução. Para restaurá-los, selecione **Continuar proteção** no menu de contexto, clicando no ícone da bandeja do sistema.

Alguns componentes de proteção tiveram mal funcionamento

Um ou mais componentes do Kaspersky Anti-Virus têm erros internos. Se isso ocorrer, é recomendável habilitar o componente ou reiniciar o computador, pois é possível que os drivers dos componentes precisem ser registrados depois de serem atualizados.

5.1.2. Status dos componentes do Kaspersky Anti-Virus

Para determinar como o Kaspersky Anti-Virus protege o sistema de arquivos, os e-mails, o tráfego HTTP e outras áreas pelas quais programas perigosos poderiam invadir seu computador, ou para exibir o andamento de uma tarefa de verificação de vírus ou atualização de assinaturas de ameaças, abra a seção correspondente na janela principal do programa.

Por exemplo, para exibir o status atual do Antivírus de Arquivos, selecione **Antivírus de Arquivos** à esquerda da janela principal ou, para ver se você está protegido contra novos vírus, selecione **Defesa Proativa**. O painel direito exibirá um resumo das informações sobre o funcionamento do componente.

Para os componentes de proteção, o painel direito contém a **barra de status**, a caixa **Status** e a caixa **Estatísticas**.

Para o componente Antivírus de Arquivos, a *barra de status* aparece da seguinte maneira:

- *Antivírus de Arquivos: em execução* – a proteção de arquivos está ativa para o nível selecionado (consulte 7.1 na p. 80).
- *Antivírus de Arquivos: em pausa* - o Antivírus de Arquivos está desabilitado por um determinado período. O componente continuará seu funcionamento automaticamente depois que o período atribuído expirar ou depois que o programa for reiniciado. Você também pode reiniciar a proteção de arquivos manualmente, clicando no botão ▶ localizado na barra de status.

- *Antivírus de Arquivos: interrompido* – o componente foi interrompido pelo usuário. Você pode reiniciar a proteção de arquivos manualmente, clicando no botão ▶ localizado na barra de status.
- *Antivírus de Arquivos: não executando* – por algum motivo, a proteção de arquivos não está disponível. Por exemplo, se você não tiver uma chave de licença do programa.
- *Antivírus de Arquivos: desabilitado (erro)* – o componente encontrou um erro. Se isso ocorrer, entre em contato com o Suporte Técnico da Kaspersky Lab.

Se o componente contiver vários módulos, a seção **Status** mostrará informações sobre os status de cada um. Para os recursos que não possuem módulos individuais, são exibidos o status, nível de segurança e, para alguns recursos, a resposta a programas perigosos.

Não há uma caixa **Status** para tarefas de verificação de vírus e atualização. A caixa **Configurações** relaciona o nível de segurança e a ação aplicada a programas perigosos nas tarefas de verificação de vírus e o modo de execução nas atualizações.

A caixa **Estatísticas** contém informações sobre o funcionamento dos componentes de proteção, atualizações ou tarefas de verificação de vírus.

5.1.3. Estatísticas de desempenho do programa

As **estatísticas do programa** podem ser encontradas na caixa **Estatísticas** da seção **Proteção**, na janela principal do programa, e exibem informações gerais sobre a proteção do computador, registradas a partir da instalação do Kaspersky Anti-Virus.

Figura 5. A caixa de estatísticas gerais do programa

Você pode clicar em qualquer lugar na caixa para exibir um relatório com informações detalhadas. As guias exibem:

- Informações sobre objetos encontrados (consulte 14.3.2 na página 177) e o status atribuído a eles
- Log de eventos (consulte 14.3.3 na página 177)

- Estatísticas gerais de verificação (consulte 14.3.4 na página 178) do computador
- Configurações de operação do programa (consulte 14.3.5 na página 179)

5.2. Como verificar seu computador quanto à presença de vírus

Após a instalação, o aplicativo certamente o informará por meio de um aviso específico na parte inferior esquerda da janela que o computador ainda não foi verificado e recomendará que você execute uma verificação de vírus imediatamente.

O Kaspersky Anti-Virus inclui uma tarefa de verificação de vírus no computador localizada na seção **Verificação** da janela principal do programa.

Depois de selecionar a tarefa chamada **Meu Computador**, o painel direito exibirá o seguinte: as estatísticas da verificação mais recente do computador; as configurações da tarefa; o nível de proteção selecionado e as ações que serão executadas para objetos perigosos.

Para verificar programas mal-intencionados no computador,

Clique no botão **Verificação** à direita da tela.

Como resultado, o programa começará a verificar o computador e os detalhes serão mostrados em uma janela específica. Ao clicar no botão **Fechar**, a janela com informações sobre o andamento da instalação será oculta. Isso não interromperá a verificação.

5.3. Como verificar áreas críticas do computador

Existem áreas no computador que são críticas com relação à segurança. Elas são alvos de programas mal-intencionados que visam danificar o sistema operacional, processador, memória, etc.

É extremamente importante proteger essas áreas críticas para assegurar que o computador continue funcionando. Existe uma tarefa de verificação de vírus específica para essas áreas, localizada na janela principal do programa, na seção **Verificação**.

Depois de selecionar a tarefa chamada **Áreas críticas**, o painel direito da janela principal exibirá o seguinte: as estatísticas da verificação mais recente dessas

áreas; as configurações da tarefa; o nível de proteção selecionado e as ações que serão aplicadas às ameaças de segurança. Aqui, você também pode selecionar as áreas críticas que deseja verificar e iniciar imediatamente a verificação nessas áreas.

Para verificar programas mal-intencionados nas áreas críticas do computador,

Clique no botão **Verificação** à direita da tela.

Ao fazê-lo, será iniciada uma verificação das áreas selecionadas e os detalhes serão mostrados em uma janela específica. Ao clicar no botão **Fechar**, a janela com informações sobre o andamento da instalação será oculta. Isso não interromperá a verificação.

5.4. Como verificar vírus em um arquivo, uma pasta ou um disco

Às vezes, é necessário verificar vírus em objetos individuais e não em todo o computador: por exemplo, um disco rígido portátil ou um memory stick usado para transferir arquivos entre os computadores do escritório e de casa. Você pode selecionar um objeto para ser verificado com as ferramentas padrão do sistema operacional Windows (por exemplo, na janela do programa **Explorer** ou na **Área de Trabalho**, etc.).

Para verificar um objeto,

Coloque o cursor sobre o nome do objeto selecionado, abra o menu de contexto do Windows clicando com o botão direito do mouse e selecione **Verificar vírus** (veja a fig. 6).

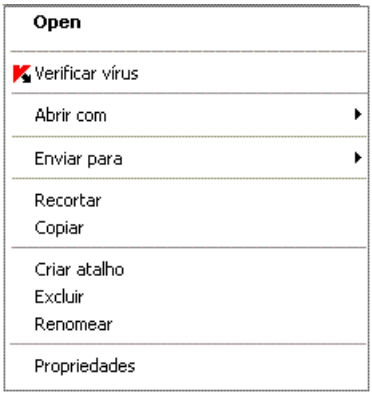


Figura 6. Verificando um objeto selecionado usando um menu de contexto padrão do Windows

Será iniciada então uma verificação do objeto selecionado e os detalhes serão mostrados em uma janela específica. Ao clicar no botão **Fechar**, a janela com informações sobre o andamento da instalação será oculta. Isso não interromperá a verificação.

5.5. Como atualizar o programa

A Kaspersky Lab atualiza as assinaturas de ameaças e os módulos internos do Kaspersky Anti-Virus usando servidores de atualização dedicados.

Os *servidores de atualização da Kaspersky Lab* são os sites da Kaspersky Lab na Internet, onde são armazenadas as atualizações do programa.

Aviso!

Para atualizar o Kaspersky Anti-Virus, será necessária uma conexão com a Internet.

Por padrão, o Kaspersky Anti-Virus verifica automaticamente as atualizações nos servidores da Kaspersky Lab. Se o servidor tiver as atualizações mais recentes, o Kaspersky Anti-Virus as baixará e instalará no modo silencioso.

Para atualizar o Kaspersky Anti-Virus manualmente,

selecione o componente **Atualização** na seção **Serviço** da janela principal do programa e clique no botão **Atualizar agora!** à direita da janela.

Como resultado, o Kaspersky Anti-Virus começará o processo de atualização e exibirá os detalhes em uma janela específica.

5.6. O que fazer se a proteção não for executada

Se houver problemas ou erros no funcionamento de qualquer componente de proteção, verifique seu status. Se o status do componente for *não executando* ou *erro de operação*, tente reiniciar o Kaspersky Anti-Virus.

Se o problema não for resolvido depois que você reiniciar o computador, é recomendável corrigir os possíveis erros usando o programa de reversão do aplicativo (consulte Capítulo 16 na p. 218).

Se o procedimento de restauração do aplicativo não ajudar, entre em contato com o Suporte Técnico da Kaspersky Lab. Pode ser necessário salvar um relatório sobre a operação do componente ou de todo o aplicativo em um arquivo e enviá-lo para o Suporte Técnico para investigação.

Para salvar o relatório em um arquivo:

1. Selecione o componente na seção **Proteção** da janela principal do programa e clique em qualquer local da caixa **Estatísticas**.
2. Clique no botão **Salvar como** e, na janela que é aberta, especifique o nome do arquivo para o relatório de desempenho do componente.

Para salvar um relatório de todos os componentes do Kaspersky Anti-Virus de uma vez (componentes de proteção, tarefas de verificação de vírus, recursos de suporte):

1. Selecione a seção **Proteção** na janela principal do programa e clique em qualquer local da caixa **Estatísticas**.

   ou

   Clique em Todos os relatórios na janela de relatório de qualquer componente. Em seguida, a guia **Relatórios** relacionará os relatórios de todos os componentes do programa.
2. Clique no botão **Salvar como** e, na janela que é aberta, especifique o nome do arquivo do relatório de operação do programa.

CAPÍTULO 6. SISTEMA DE GERENCIAMENTO DA PROTEÇÃO

O Kaspersky Anti-Virus permite gerenciar várias tarefas de segurança do computador:

- Habilitar, desabilitar e pausar (consulte 6.1 na página58) o programa
- Definir os tipos de programas perigosos (consulte 6.2 na página 63) dos quais o Kaspersky Anti-Virus protegerá seu computador
- Criar uma lista de exclusões (consulte 6.3 na página 64) para a proteção
- Criar suas próprias tarefas de atualização e verificação de vírus (consulte 6.4 na página 74)
- Configurar uma programação de verificação de vírus (consulte 6.5 na página 75)
- Configurar a energia da proteção antivírus (consulte 6.6 na p. 77)

6.1. Interrompendo e reiniciando a proteção do computador

Por padrão, o Kaspersky Anti-Virus é aberto na inicialização e protege o computador durante todo o tempo em que você o utiliza. As palavras *Kaspersky Anti-Virus 6.0* no canto superior direito da tela indicam que a proteção está ativa. Todos os componentes de proteção (consulte 2.2 na p. 22) estão sendo executados.

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

Aviso!

A Kaspersky Lab recomenda enfaticamente que você **não desabilite a proteção**, pois isso poderia levar à infecção do computador e à conseqüente perda de dados.

Observe que, nesse caso, a proteção é discutida no contexto dos componentes de proteção. Desabilitar ou pausar os componentes de proteção não afeta o desempenho das tarefas de verificação de vírus ou atualizações do programa.

6.1.1. Pausando a proteção

Pausar a proteção significa desabilitar temporariamente todos os componentes que monitoram os arquivos no computador, os e-mails enviados e recebidos, os scripts executáveis, o comportamento dos aplicativos.

Para pausar a operação do Kaspersky Anti-Virus:

1. Selecione **Pausar proteção** no menu de contexto do programa (consulte 4.2 na página 42).
2. Na janela Pausar proteção que é aberta (veja a fig. 7), selecione em quanto tempo deseja que a proteção volte a funcionar:
   - **Em <intervalo de tempo>** - a proteção será habilitada após este período. Para selecionar um período, use o menu suspenso.
   - **Na próxima reinicialização do programa** – a proteção será reiniciada se você abrir o programa no Menu Iniciar ou após reiniciar o computador (desde que o programa esteja definido para iniciar ao ligar o computador; consulte 6.1.5 na página 62).
   - **Somente por solicitação do usuário** – a proteção será interrompida até que você mesmo a inicie. Para habilitar a proteção, selecione **Continuar proteção** no menu de contexto do programa.

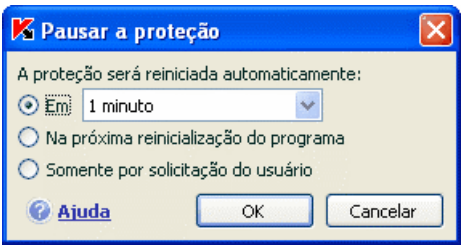


Figura 7. Janela Pausar proteção

Dica:
Você também pode interromper a proteção do computador por meio de um dos seguintes métodos:

- Clique no botão na seção **Proteção**.
- Selecione **Sair** no menu de contexto.

Se você pausar a proteção, todos os componentes de proteção ficarão pausados. Isso é indicado por:

- Nomes inativos (cinza) dos componentes desabilitados na seção Proteção da janela principal.
- Ícone inativo (cinza) na bandeja do sistema.
- O terceiro indicador de proteção (consulte 5.1.1 na página 49) no computador, que mostra que **Nenhum componente de proteção está habilitado**.

6.1.2. Interrompendo a proteção

Interromper a proteção significa desabilitar totalmente os componentes de proteção. As verificações de vírus e atualizações continuam funcionando neste modo.

Se a proteção for interrompida, ela só poderá ser reiniciada pelo usuário: os componentes de proteção não continuarão automaticamente depois da reinicialização do sistema ou do programa. Lembre-se que se, de alguma forma, o Kaspersky Anti-Virus estiver em conflito com outros programas instalados no computador, você poderá pausar componentes individuais ou criar uma lista de exclusões (consulte 6.3 na página 64).

Para interromper toda a proteção:

1. Abra a janela principal do Kaspersky Anti-Virus.
2. Selecione a seção **Proteção** e clique em **Configurações**.
3. Na janela de configurações do programa, desmarque **Habilitar proteção**.

Após desabilitar a proteção, todos os componentes de proteção serão interrompidos. Isso é indicado por:

- Nomes inativos (cinza) dos componentes desabilitados na seção Proteção da janela principal.
- Ícone inativo (cinza) na bandeja do sistema.

- O terceiro indicador de proteção (consulte 5.1.1 na página 49) no computador, que mostra que  **Todos os componentes de proteção estão desabilitados**.

6.1.3. Pausando / interrompendo serviços de proteção, verificações de vírus e tarefas de atualização

Existem várias maneiras de interromper um componente de proteção, verificação de vírus ou atualização. Antes de fazê-lo, é estritamente recomendável estabelecer o motivo da interrupção. É provável que o problema possa ser resolvido de outra maneira, por exemplo, alterando o nível de segurança. Se, por exemplo, você estiver trabalhando com um banco de dados que certamente não contém vírus, simplesmente adicione seus arquivos como uma exclusão (consulte 6.3 na página 64).

Para pausar componentes de proteção, verificações de vírus e tarefas de atualização:

Selecione o componente ou a tarefa à esquerda da janela principal e clique no botão ❚❚ na barra de status.

O status do componente/tarefa mudará para ***em pausa***. O componente ou a tarefa ficará em pausa até que você o reinicie, clicando no botão ▶.

Ao pausar o componente ou a tarefa, as estatísticas da sessão atual do Kaspersky Anti-Virus são salvas e continuarão sendo registradas após a atualização do componente.

Para interromper componentes de proteção, verificações de vírus e tarefas de atualização:

Clique no botão ■ na barra de status. Você também pode interromper componentes de proteção na janela de configurações do programa, desmarcando ☑ **Habilitar <nome do componente>** na seção **Geral** do componente.

O status do componente/tarefa mudará para *interrompido (desabilitado)*. O componente ou a tarefa será interrompido até que você o habilite, clicando no botão ▶. Para tarefas de atualização e verificação de vírus, você poderá escolher dentre as seguintes opções: continuar a tarefa que foi interrompida ou reiniciá-la do início.

Ao interromper uma tarefa ou um componente em tempo real, todas as estatísticas do trabalho anterior serão limpas e, quando o componente for iniciado, serão substituídas.

6.1.4. Restaurando a proteção no computador

Se, em algum momento, você pausou ou interrompeu a proteção no computador, será possível reiniciá-la usando um dos seguintes métodos:

- *No menu de contexto*.

  Para fazê-lo, selecione **Reiniciar proteção**.

- *Na janela principal do programa*.

  Para fazê-lo, clique no botão ▶ na barra de status, na seção **Proteção** da janela principal.

O status de proteção muda imediatamente para ***em execução***. O ícone do programa na bandeja do sistema fica ativo (colorido). O terceiro indicador de proteção (consulte 5.1.1 na página 49) também informará que **Todos os componentes de proteção estão em execução**.

6.1.5. Desligando o programa

Se for necessário desligar o Kaspersky Anti-Virus, selecione **Sair** no menu de contexto do programa (consulte 4.2 na página 42). Isso fechará o programa, deixando seu computador desprotegido.

Se as conexões de rede que o programa monitora estiverem ativas no computador, ao fechá-lo, aparecerá um aviso na tela informando que essas conexões serão interrompidas. Isso é necessário para que o programa seja desligado corretamente. As conexões são encerradas automaticamente depois de dez segundos ou clicando no botão **Sim**. A maioria das conexões será reiniciada automaticamente após um breve período.

Observe que, se você estiver baixando um arquivo sem um gerenciador de download, quando a conexão for encerrada, a transferência do arquivo será perdida. Será necessário baixar o arquivo novamente.

Você pode optar por não interromper as conexões, clicando no botão **Não** na janela de aviso. Se o fizer, o programa continuará em execução.

Após fechar o programa, você pode habilitar a proteção do computador novamente abrindo o Kaspersky Anti-Virus (**Iniciar** → **Programas** → **Kaspersky Anti-Virus 6.0** → **Kaspersky Anti-Virus 6.0**).

Também será possível reiniciar a proteção automaticamente depois de reiniciar o sistema operacional. Para habilitar este recurso, selecione a seção **Proteção** na janela de configurações do programa e marque ☑ **Iniciar o Kaspersky Anti-Virus na inicialização**.

6.2. Tipos de programas que serão monitorados

O Kaspersky Anti-Virus o protege de vários tipos de programas mal-intencionados. Independentemente das configurações, o programa sempre verifica e neutraliza os vírus, cavalos de Tróia e ferramentas de hackers. Esses programas podem causar danos significativos ao computador. Para tornar o computador mais seguro, você pode expandir a lista de ameaças que o programa detectará, fazendo-o monitorar outros tipos de programas perigosos.

Para escolher os programas mal-intencionado dos quais o Kaspersky Anti-Virus o protegerá, selecione a seção **Proteção** na janela de configurações do programa (consulte 4.4 na página 46).

A caixa **Categorias de malware** contém os tipos de ameaças:

- **Vírus, worms, cavalos de Tróia, ferramentas de hackers**. Esse grupo combina as categorias mais comuns e perigosas de programas mal-intencionados. Este é o nível de segurança mínimo admissível. Por recomendação dos especialistas da Kaspersky Lab, o Kaspersky Anti-Virus sempre monitora esta categoria de programas mal-intencionados.
- **Spyware, adware, discadores**. Esse grupo inclui softwares possivelmente perigosos que poderiam causar inconveniências ao usuário ou resultar em danos significativos.
- **Software possivelmente perigoso (riskware)**. Este grupo inclui programas que não são mal-intencionados ou perigosos. Contudo, em determinadas situações, eles poderiam ser usados para danificar o seu computador.

Os grupos listados acima compreendem toda a variedade de ameaças que o programa detecta ao verificar objetos.

Se todos os grupos forem selecionados, o Kaspersky Anti-Virus fornecerá a proteção antivírus mais completa possível para o computador. Se o segundo e o terceiro grupos forem desabilitados, o programa o protegerá apenas dos programas mal-intencionados mais comuns.

A Kaspersky Lab não recomenda desabilitar o monitoramento do segundo grupo. Se o Kaspersky Anti-Virus classificar um programa que você não considera perigoso como um programa possivelmente perogoso, é recomendável criar uma exclusão para ele (consulte 6.3 na p. 64).

6.3. Criando uma zona confiável

Uma *zona confiável* consiste em uma lista de objetos, criada pelo usuário, que não serão monitorados pelo Kaspersky Anti-Virus. Em outras palavras, é um conjunto de programas excluídos da proteção.

O usuário cria uma zona de proteção com base nas propriedades dos arquivos usados e nos programas instalados no computador. Poderá ser necessário criar uma lista de exclusões se, por exemplo, o Kaspersky Anti-Virus bloquear o acesso a um objeto ou programa e você tiver certeza de que ele é absolutamente seguro.

Você pode excluir da verificação arquivos de determinados formatos, usar uma máscara de arquivos ou excluir uma determinada área (por exemplo, uma pasta ou um programa), processos de programas ou objetos, de acordo com a classificação da Enciclopédia de Vírus (o status que o programa atribui aos objetos durante uma verificação).

Aviso!

Os objetos excluídos não são verificados quando o disco ou a pasta em que se localizam é verificado. Contudo, se você selecionar esse objeto especificamente, a regra de exclusão não será aplicada.

Para criar uma lista de exclusões,

1. Abra a janela de configurações do Kaspersky Anti-Virus e selecione a seção **Proteção**.
2. Clique no botão **Zona confiável** na seção **Geral**.
3. Configure as regras de exclusão para objetos e crie uma lista de aplicativos confiáveis na janela que é aberta (veja a fig. 8).

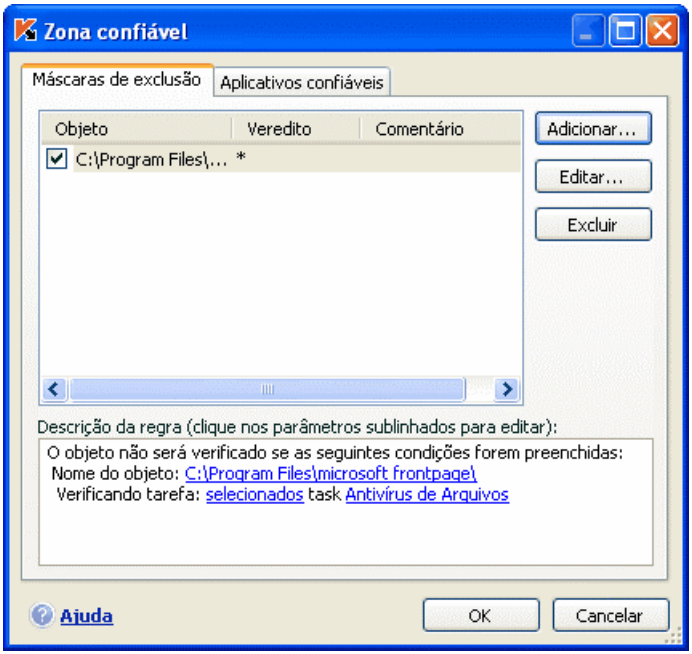


Figura 8. Criando uma zona confiável

6.3.1. Regras de exclusão

As regras de exclusão são conjuntos de condições que o Kaspersky Anti-Virus usa para saber que não deve verificar um objeto.

Você pode excluir da verificação arquivos com determinados formatos, usar uma máscara de arquivos ou excluir uma determinada área, como uma pasta ou um programa, processos de programas ou objetos, de acordo com sua classificação na Enciclopédia de Vírus.

A *classificação* é o status que o Kaspersky Anti-Virus atribui a um objeto durante a verificação. Um status é atribuído com base na classificação de programas mal-intencionados e possivelmente perigosos encontrados na Enciclopédia de Vírus da Kaspersky Lab.

O software possivelmente perigoso não tem função mal-intencionada, mas pode ser usado como componente auxiliar de um código mal-intencionado, pois contém falhas e erros. Essa categoria inclui, por exemplo, programas de administração remota, clientes IRC, servidores FTP, utilitários multifuncionais para interromper processos ou ocultá-los, registradores de uso do teclado, macros de senha, discadores automáticos, etc. Esses programas não são

classificados como vírus. Eles podem ser divididos em vários tipos, por exemplo, Adware, Piadas, Riskware, etc. (para obter mais informações sobre programas potencialmente perigosos detectados pelo Kaspersky Anti-Virus, consulte a Enciclopédia de Vírus (em inglês) em www.viruslist.com). Depois da verificação, esses programas podem ser bloqueados. Como vários deles são muito comuns, você tem a opção de excluí-los da verificação. Para fazê-lo, adicione o nome ou a máscara do objeto à zona confiável usando a classificação da Enciclopédia de Vírus.

Por exemplo, imagine que você usa um programa de Administração Remota freqüentemente no seu trabalho. Trata-se de um sistema de acesso remoto com o qual você pode trabalhar de um computador remoto. O Kaspersky Anti-Virus considera este tipo de atividade de aplicativo como possivelmente perigoso e pode bloqueá-lo. Para impedir que o aplicativo seja bloqueado, crie uma regra de exclusão que especifica not-a-virus:RemoteAdmin.Win32.RAdmin.22 como classificação.

Ao adicionar uma exclusão, será criada uma regra que vários componentes do programa (Antivírus de Arquivos, Antivírus de E-Mail, Defesa Proativa) e tarefas de verificação de vírus podem usar posteriormente. É possível criar regras de exclusão em uma janela específica que pode ser aberta da janela de configurações do programa, do aviso sobre a detecção do objeto e da janela de relatório.

*Para adicionar exclusões na guia **Máscara de Exclusões**:*

1. Clique no botão **Adicionar** na guia **Máscara de exclusões**.
2. Na janela que é aberta (veja a fig. 9), clique no tipo de exclusão na seção **Propriedades**:

   Objeto – exclusão das verificações de um determinado objeto, diretório ou arquivos que correspondem a uma determinada máscara.

   Veredito – exclusão de um objeto das verificações com base em seu status na classificação da Enciclopédia de Vírus.

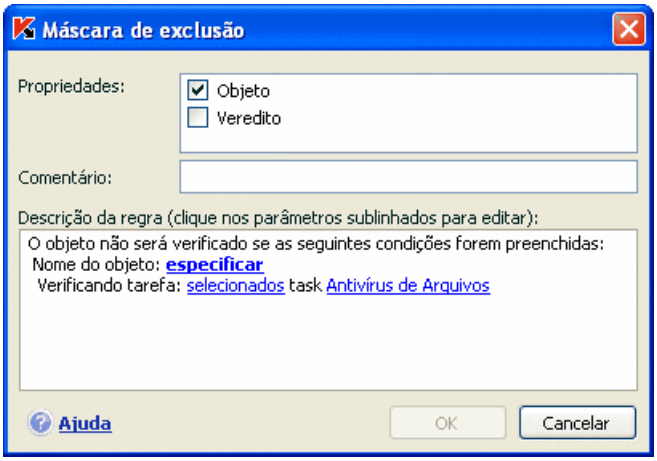


Figura 9. Criando uma regra de exclusão

Se você marcar as duas caixas de uma vez, será criada uma regra para aquele objeto com uma determinada classificação da Enciclopédia de Vírus. Nesse caso, as seguintes regras se aplicam:

- Se você especificar um determinado arquivo como **Objeto** e um determinado status na seção **Veredito**, o arquivo especificado será uma exclusão somente se for classificado como sendo a ameaça selecionada durante a verificação.
- Se você selecionar uma área ou pasta como **Objeto** e o status (ou máscara) como **Veredito**, os objetos com esse status serão excluídos da verificação somente nessa área ou pasta.

3. Atribua valores aos tipos de exclusão selecionados. Para fazê-lo, clique na seção **Descrição da regra** no link de especificação localizado ao lado do tipo de exclusão:
   - Para o tipo **Objeto**, insira seu nome na janela que é aberta (pode ser um arquivo, um diretório específico ou uma máscara de arquivos (consulte A.2 na p. 227). Marque ☑ **Incluir subpastas** para que o objeto (arquivo, máscara de arquivos, pasta) seja excluído recursivamente da verificação. Por exemplo, se você atribuir **C:\Arquivos de Programas\winword.exe** como uma exclusão e marcar a opção de subpastas, o arquivo **winword.exe** será excluído da verificação se for encontrado em qualquer subpasta de **C:\Arquivos de Programas**.

- Insira o nome completo da ameaça que deseja excluir das verificações, como mostrado na Enciclopédia de Vírus, ou use uma máscara para o **Veredito** (consulte A.3 na p. 226).

  Para algumas classificações, você pode atribuir condições avançadas para a aplicação de regras no campo **Configurações avançadas**. Na maioria dos casos, o programa preenche esse campo automaticamente quando você adiciona uma regra de exclusão em um aviso de Defesa Proativa.

  Você pode adicionar configurações avançadas aos seguintes vereditos, entre outros:

  - *Invasor* (se insere nos processos do programa). Para esse veredito, você pode fornecer o nome, máscara ou caminho completo do objeto que está sendo inserido (por exemplo, um arquivo .dll) como uma condição de exclusão adicional.
  - *Abertura do navegador da Internet*. Para esse veredito, você pode listar configurações de abertura do navegador como configurações de exclusão adicionais. Por exemplo, você bloqueou a abertura de navegadores com determinadas configurações na análise de atividade de aplicativos da Defesa Proativa. Contudo, deseja que o navegador possa ser aberto no domínio *www.kaspersky.com* com um link do Microsoft Office Outlook como uma regra de exclusão. Para fazê-lo, selecione o Outlook como **Objeto** da exclusão e *Iniciando navegador da Internet* como **Veredito**, e insira uma máscara de domínio permitida no campo **Configurações avançadas**.

4. Defina quais componentes do Kaspersky Anti-Virus usarão esta regra. Se qualquer estiver selecionado, a regra se aplicará a todos os componentes. Se desejar restringir a regra a um ou a vários componentes, clique em qualquer, que mudará para selecionado. Na janela que é aberta, marque as caixas dos componentes aos quais deseja que essa regra de exclusão se aplique.

Para criar uma regra de exclusão a partir de um aviso do programa informando que foi detectado um objeto perigoso:

1. Use o link Adicionar à zona confiável na janela da notificação (veja a fig. 10).

Figura 10. Notificação de detecção de objeto perigoso

2. Na janela que é aberta, verifique se todas as configurações das regras de exclusão correspondem às suas necessidades. O programa preencherá o nome do objeto e o tipo de ameaça automaticamente, com base nas informações contidas na notificação. Para criar a regra, clique em **OK**.

Para criar uma regra de exclusão na janela de relatório:

1. Selecione o objeto no relatório que você deseja adicionar às exclusões.
2. Abra o menu de contexto e selecione **Adicionar à zona confiável** (veja a fig. 11).
3. A janela de configurações da exclusão será aberta. Verifique se todas as configurações das regras de exclusão correspondem às suas necessidades. O programa preencherá o nome do objeto e o tipo de ameaça automaticamente com base nas informações do relatório. Para criar a regra, clique em **OK**.

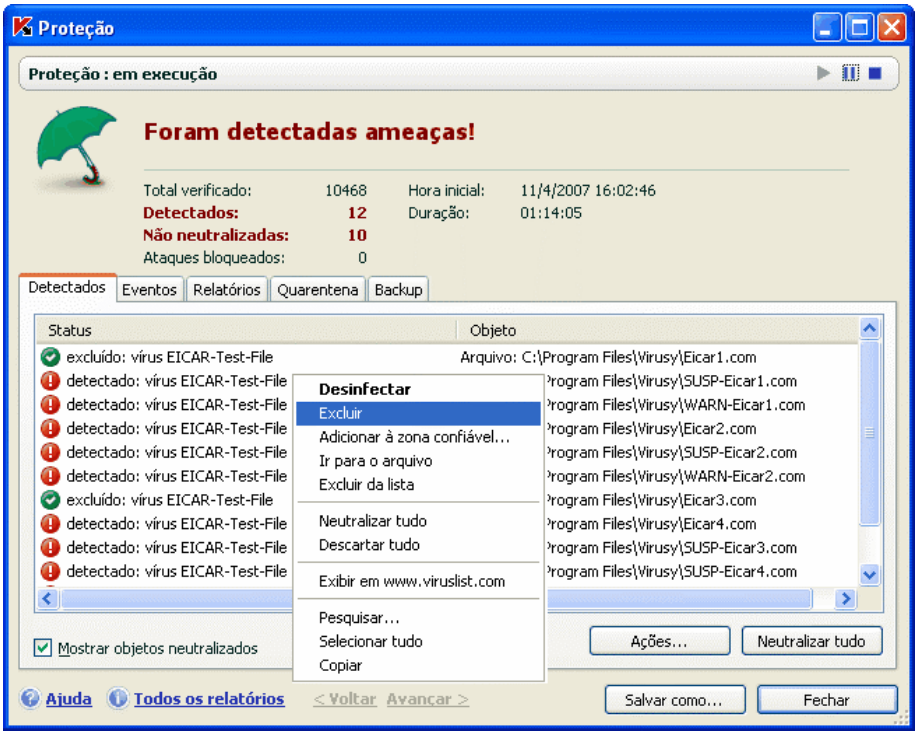


Figura 11. Criando uma regra de exclusão em um relatório

6.3.2. Aplicativos confiáveis

Você poderá excluir aplicativos confiáveis da verificação no Kaspersky Anti-Virus somente se ele estiver instalado em um computador que executa o Microsoft Windows NT 4.0/2000/XP/Vista.

O Kaspersky Anti-Virus pode criar uma lista de aplicativos confiáveis, cujos arquivos e atividade de rede não precisam ser monitorados, considerados suspeitos, etc.

Por exemplo, você acha que os objetos e processos usados pelo Bloco de Notas do Windows são seguros e não precisam ser verificados. Para excluir os objetos usados por esse processo da verificação, adicione o Bloco de Notas à lista de aplicativos confiáveis. Contudo, o arquivo executável e o processo do aplicativo confiável serão verificados quanto à presença de vírus, como anteriormente. Para excluir totalmente o aplicativo da verificação, use regras de exclusão (consulte 6.3.1 na p. 65).

Além disso, algumas ações classificadas como perigosas são perfeitamente normais para vários programas. Por exemplo, programas de alternância de layout do teclado interceptam normalmente o texto digitado no teclado. Para acomodar esses programas e interromper o monitoramento de sua atividade, é recomendável adicioná-los à lista de aplicativos confiáveis.

A exclusão de aplicativos confiáveis também resolve possíveis conflitos de compatibilidade entre o Kaspersky Anti-Virus e outros aplicativos (por exemplo, o tráfego de rede de outro computador que já foi verificado pelo aplicativo antivírus) e pode aumentar a produtividade do computador, o que é especialmente importante ao usar aplicativos de servidor.

Por padrão, o Kaspersky Anti-Virus verifica objetos abertos, executados ou salvos pelos processos de todos os programas e monitora a atividade de todos os programas e do tráfego de rede criado por eles.

Você pode criar uma lista de aplicativos confiáveis na guia **Aplicativos confiáveis** específica (veja a Figura 12). Por padrão, essa lista contém a relação dos aplicativos que não serão monitorados com base nas recomendações da Kaspersky Lab ao instalar o Kaspersky Anti-Virus. Se você não confiar em um aplicativo da lista, desmarque a caixa de seleção correspondente. É possível editar a lista usando os botões **Adicionar**, **Editar** e **Excluir** à direita.

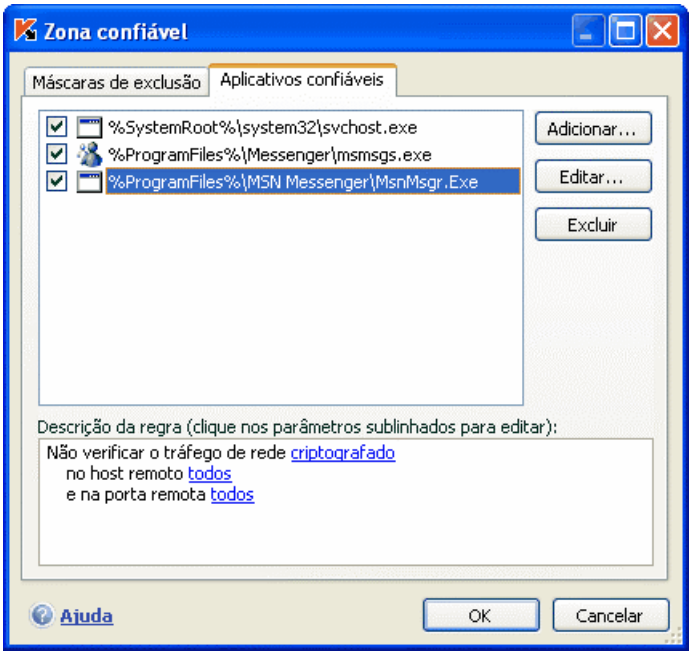


Figura 12. Lista de aplicativos confiáveis

Para adicionar um programa à lista de aplicativos confiáveis:

1. Clique no botão **Adicionar** à direita da janela.
2. Na janela **Aplicativo confiável** (veja a fig. 13) que é aberta, selecione o aplicativo usando o botão **Procurar**. Um menu de contexto será aberto e, ao clicar em **Procurar**, você poderá ir para a janela de seleção de arquivos e selecionar o caminho do arquivo executável ou, ao clicar em **Aplicativos**, poderá ir para uma lista de aplicativos em execução no momento e selecioná-los conforme necessário.

Figura 13. Adicionando um aplicativo à lista de aplicativos confiáveis

Ao selecionar um programa, o Kaspersky Anti-Virus registra os atributos internos do arquivo executável e os usa para identificar o programa confiável durante as verificações.

O caminho do arquivo é inserido automaticamente quando você seleciona seu nome.

3. Especifique as ações executadas por esse processo que o não serão monitoradas:

   Não verificar arquivos abertos – exclui da verificação todos os arquivos processados pelo aplicativo confiável.

   Não restringir a atividade de aplicativos – exclui do monitoramento da Defesa Proativa todas as atividades suspeitas ou semelhantes que o aplicativo confiável executa.

   Não restringir o acesso ao Registro – exclui da verificação os acessos ao Registro do sistema iniciados pelo aplicativo confiável.

   Não verificar o tráfego da rede – exclui das verificações de vírus e spam o tráfego de rede iniciado pelo aplicativo confiável. Você pode excluir da verificação todo o tráfego de rede do aplicativo ou o tráfego criptografado (SSL). Para fazê-lo, clique no link tudo. Ele mudará para criptografado. Além disso, você pode restringir a exclusão atribuindo uma porta/host remoto. Para criar uma restrição, clique em qualquer, que mudará para selecionados, e insira um valor para a porta/host remoto.

6.4. Iniciando tarefas de verificação de vírus e atualização em outra conta do usuário

Observe que este recurso não está disponível no Microsoft Windows 98/ME.

O Kaspersky Anti-Virus 6.0 possui um recurso que permite iniciar tarefas de verificação usando outra conta de usuário. Por padrão, esse recurso está desabilitado e as tarefas são executadas na conta com a qual você entrou no sistema.

Este recurso é útil se, por exemplo, você precisa de direitos de acesso a um determinado objeto durante uma verificação. Ao usá-lo, você pode configurar tarefas para serem executadas como um usuário que possui os privilégios necessários.

As atualizações do produto podem ser feitas de uma fonte à qual você não tem acesso (por exemplo, a pasta de atualização da rede) ou direitos de usuário autorizado para um servidor proxy. Você pode usar esse recurso para executar a Atualização com outra conta que possua esses direitos.

Para configurar uma tarefa de verificação que é iniciada com outra conta de usuário:

1. Selecione o nome da tarefa na seção **Verificação (Serviço)** da janela principal e use o link Configurações para abrir a janela de configurações da tarefa.
2. Clique no botão **Personalizar** na janela de configurações da tarefa e vá para a guia **Adicional** na janela que é aberta (veja a fig. 14).

Para habilitar este recurso, marque ☑ **Executar essa tarefa como**. Insira os dados de login com os quais deseja iniciar a tarefa, como: nome de usuário e senha.

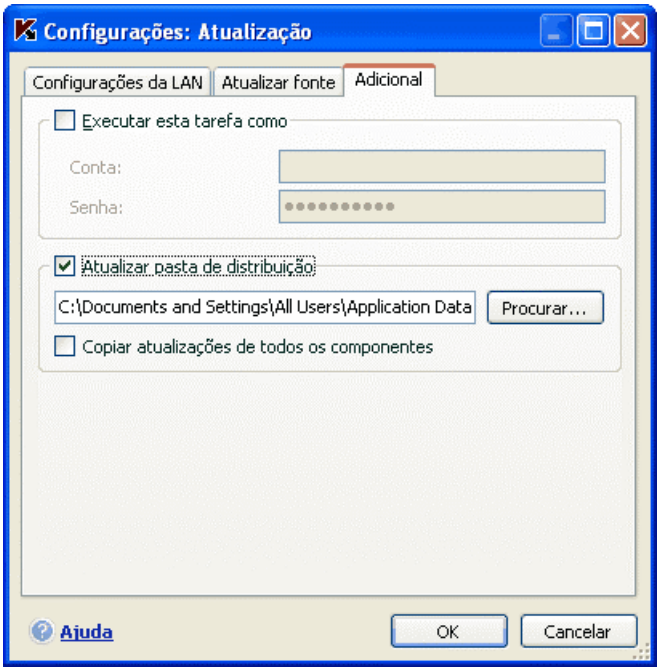


Figura 14. Configurando uma tarefa de atualização em outro perfil

6.5. Configurando programações de verificação de vírus e atualização

Você pode executar tarrefas de atualização e verificação de vírus manualmente or automaticalmente usando uma programação.

As verificações de vírus pré-instaladas com o aplicativo são iniciadas automaticamente de acordo com uma programação selecionada. De forma semelhante, a programação é desativada para as tarefas de atualização criadas durante a instalação. A Atualização é executada automaticamente conforme as atualizações são lançadas nos servidores da Kaspersky Lab.

Para alterar as configurações da programação, selecione o nome da tarefa na janela principal do programa, na seção **Verificação** (para verificações de vírus) ou na seção **Serviço** (para tarefas de atualização), e abra a janela de configurações clicando em Configurações.

Para que as tarefas sejam iniciadas de acordo com uma programação, marque a caixa de início automático de tarefas na seção **Modo de execução**. Você pode editar o horário para iniciar a tarefa de verificação na janela **Programação** (veja a fig. Figura 15) que é aberta ao clicar em **Alterar**.

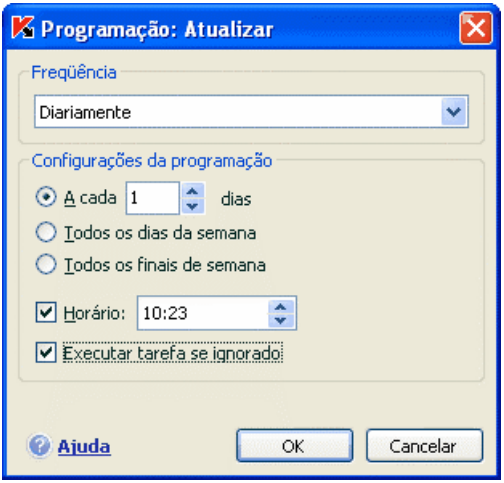


Figura 15. Configurando uma programação de tarefas

A etapa mais importante é determinar a freqüência com que a tarefa é iniciada. É possível selecionar uma das seguintes opções:

- **Em uma hora especificada**. A tarefa será executada uma vez, no dia e na hora especificados.
- **Ao iniciar o programa**. A tarefa será iniciada sempre que o Kaspersky Anti-Virus for executado.
- **Após cada atualização**. A tarefa é iniciada após cada atualização da assinatura de ameaças (se aplica somente a tarefas de verificação de vírus).
- **Em minutos**. O intervalo entre as verificações será um número de minutos, não maior que 59. Especifique os minutos entre as verificações nas configurações da programação.
- **Em horas**. O intervalo entre as verificações é calculado em horas. Insira o número de horas nas configurações de programação: **A cada *n*horas** e insira o valor de *n*. Por exemplo, insira **A cada 1 hora** se desejar que a tarefa seja executada a cada hora.
- **Diária** – o período entre as verificações é calculado em dias. Especifique com que freqüência a verificação deve ser executada nas configurações de programação:

- Selecione a opção **A cada *n* dias** e insira o valor de *n*. Insira *A cada 2 dias*, se desejar executar a verificação em dias alternados.
- Selecione **Todos os dias da semana**, se desejar que a verificação seja executada diariamente, de segunda a sexta-feira.
- Selecione **Todos os finais de semana** para que a tarefa seja executada somente aos sábados e domingos.

  Além da freqüência, especifique a hora em que a tarefa de verificação será executada no campo **Hora**.

Semanal – a tarefa de verificação será executada em determinados dias da semana. Se você selecionar esta opção, marque os dias da semana nos quais deseja que a verificação seja executada nas configurações de programação. Insira também a hora na qual a tarefa de verificação será executada no campo *Hora*.

Mensal – a tarefa de verificação será executada uma vez por mês, no dia e na hora especificados.

Se, por algum motivo, a tarefa de verificação for ignorada (por exemplo, se o computador não estava ligado naquela hora), você poderá configurar a tarefa que foi perdida para ser iniciada automaticamente assim que possível. Para fazê-lo, marque **Executar a tarefa se ignorado** na janela da programação.

6.6. Opções de energia

Para preservar a bateria do seu laptop e reduzir a carga nos subsistemas do processador central e do disco, você pode adiar as verificações de vírus:

- Como às vezes as verificações de vírus e atualizações do programa exigem recursos consideráveis e podem levar algum tempo, é recomendável desabilitar a programação dessas tarefas, o que ajuda a economizar bateria. Se necessário, você mesmo pode atualizar o programa (consulte 5.5 na p. 56) ou iniciar uma verificação de vírus. Para usar o recurso de economia de bateria, marque **Desabilitar verificações programadas ao executar com alimentação de bateria**.
- As verificações de vírus aumentam a carga nos subsistemas do processador central e do disco, fazendo os outros programas serem executados mais lentamente. Por padrão, se ocorrer essa situação, o programa pausará as verificações de vírus e liberará os recursos do sistema para os aplicativos do usuário.

  Entretanto, há vários programas que podem ser iniciados assim que os recursos do processador forem liberados e executados em segundo plano. Para que as verificações de vírus não dependam do

funcionamento desses programas, desmarque **Conceder recursos a outros aplicativos**.

Observe que esta configuração pode ser definida individualmente para cada tarefa de verificação de vírus. Se você escolher esta opção, a configuração de uma tarefa específica terá uma prioridade superior.

Para configurar a energia das tarefas de verificação de vírus:

Selecione a seção **Proteção** da janela principal do programa e clique no link Configurações. Configure a energia na caixa **Avançado** (veja a figura 16).

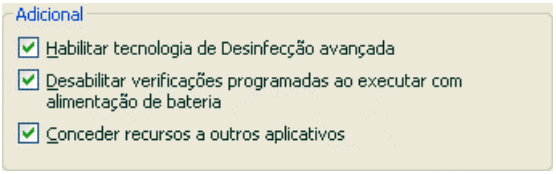


Figura 16. Opções de energia

6.7. Tecnologia de Desinfecção Avançada

Os programas mal-intencionados atuais conseguem invadir os níveis mais baixos de um sistema operacional, o que torna praticamente impossível excluí-los. O Kaspersky Anti-Virus 6.0 pergunta se você deseja executar a Tecnologia de Desinfecção Avançada quando ele detecta uma ameaça atualmente ativa no sistema. Ela neutralizará a ameaça e a excluirá do computador.

Após este procedimento, será necessário reiniciar o computador. Depois disso, é recomendável executar uma verificação completa de vírus (consulte 5.2 na p. 54). Para usar a Tecnologia de Desinfecção Avançada, marque **Habilitar Tecnologia de Desinfecção Avançada**.

Para habilitar/desabilitar a Tecnologia de Desinfecção Avançada:

Selecione a seção **Proteção** da janela principal do programa e clique no link Configurações. Configure a energia na caixa **Avançado** (veja a figura 16).

CAPÍTULO 7. ANTIVÍRUS DE ARQUIVOS

O componente do Kaspersky Anti-Virus que protege os arquivos do computador contra infecção é chamado *Antivírus de Arquivos*. Ele é carregado ao iniciar o sistema operacional, sendo executado na RAM do computador, e verifica todos os arquivos abertos, salvos ou executados.

A atividade do componente é indicada pelo ícone do Kaspersky Anti-Virus na bandeja do sistema, que tem a seguinte aparência  sempre que um arquivo está sendo verificado.

Por padrão, o Antivírus de Arquivos verifica somente *arquivos novos ou modificados*, ou seja, apenas os arquivos que foram adicionados ou alterados desde a verificação anterior. Os arquivos são verificados usando o seguinte algoritmo:

1. Cada arquivo usado pelo usuário ou por um programa é interceptado pelo recurso.
2. O Antivírus de Arquivos verifica as informações do arquivo interceptado nos bancos de dados do iCheckerTM e do iSwiftTM. A decisão de verificar o arquivo ou não se baseia nas informações recuperadas.

O processo de verificação inclui as seguintes etapas:

1. O arquivo é analisado quando à presença de vírus. Os objetos mal-intencionados são detectados por comparação com as *assinaturas de ameaças*, que contêm descrições de todos os programas mal-intencionados, ameaças e ataques de rede conhecidos até o momento e os métodos para neutralizá-los.
2. Depois da análise, existem três medidas a serem tomadas:
    a. Se for detectado um código mal-intencionado no arquivo, o Antivírus de Arquivos bloqueará o arquivo, colocará uma cópia do mesmo no *Backup* e tentará neutralizar o arquivo. Se o arquivo for desinfectado com êxito, ele ficará disponível novamente. Caso contrário, o arquivo será excluído.
    b. Se for detectado em um arquivo um código que parece ser mal-intencionado, mas sem garantias disso, o arquivo será submetido à desinfecção e enviado para a *Quarentena*.
    c. Se nenhum código mal-intencionado for descoberto no arquivo, ele será restaurado imediatamente.

7.1. Selecionando um nível de segurança de arquivos

O Antivírus de Arquivos protege os arquivos que você está usando em um dos seguintes níveis (veja a fig. 17):

Alto – o nível com o monitoramento mais abrangente dos arquivos abertos, salvos ou executados.

Recomendado – a Kaspersky Lab recomenda este nível de configuração. As seguintes categorias de objetos serão verificadas:

- Programas e arquivos por conteúdo
- Objetos novos e modificados desde a última verificação
- Objetos OLE incorporados

Baixo – o nível com configurações que permitem usar tranqüilamente aplicativos que exigem recursos significativos do sistema, pois o escopo dos arquivos verificados é menor.

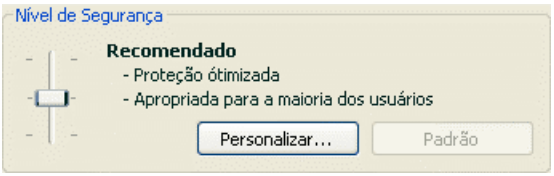


Figura 17. Nível de segurança do Antivírus de Arquivos

A configuração padrão do Antivírus de Arquivos é **Recomendado**.

Você pode aumentar ou diminuir o nível de proteção dos arquivos usados selecionando o nível desejado ou alterando as configurações do nível atual.

Para alterar o nível de segurança:

Ajuste os controles deslizantes. Ao ajustar o nível de segurança, você define a taxa da velocidade de verificação com relação ao número total de arquivos verificados: quanto menos arquivos verificados quanto à presença de vírus, maior a velocidade de verificação.

Se nenhum dos níveis de segurança de arquivos definidos atender às suas necessidades, você poderá personalizar as configurações de proteção. Para fazê-lo, selecione o nível mais próximo do necessário como ponto inicial e edite suas configurações. Nesse caso, o nível será definido como **Personalizado**. Vamos examinar um exemplo de quando os níveis de segurança de arquivos definidos pelo usuário seriam úteis.

Exemplo:

O trabalho que você executa no computador usa muitos tipos de arquivos, alguns dos quais podem ser bastante grandes. Você não deseja correr o risco de ignorar algum arquivo na verificação devido ao seu tamanho ou extensão, mesmo que isso afete de alguma forma a produtividade do computador.

Dica para selecionar um nível:

Com base nos dados fornecidos, é possível concluir que você tem um risco bastante alto de ser infectado por um programa mal-intencionado. O tamanho e o tipo dos arquivos usados é bem variado e ignorá-los na verificação colocaria seus dados em risco. Você deseja verificar os arquivos que utiliza por conteúdo, não por extensão.

É recomendável iniciar com o nível de segurança **Recomendado** e fazer as seguintes alterações: remova a restrição sobre os tamanhos dos arquivos verificados e otimize a operação do Antivírus de Arquivos verificando apenas arquivos novos e modificados. Assim, a verificação não ocupará tantos recursos do sistema e você poderá usar outros aplicativos tranqüilamente.

Para modificar as configurações de um nível de segurança:

Clique no botão **Personalizar** na janela de configurações do Antivírus de Arquivos. Edite as configurações do Antivírus de Arquivos na janela que é aberta e clique em **OK**.

Como resultado, será criado um quarto nível de segurança, **Personalizado**, que contém as configurações de proteção definidas.

7.2. Configurando o Antivírus de Arquivos

Suas configurações determinam como o Antivírus de Arquivos defenderá o seu computador. Elas podem ser divididas nos seguintes grupos:

- Configurações que definem os tipos de arquivos (consulte 7.2.1 na p. 82) que deverão ser verificados quanto à presença de vírus
- Configurações que definem o escopo da proteção (consulte 7.2.2 na p. 85)
- Configurações que definem como o programa responderá a objetos perigosos (consulte 7.2.5 na p. 89).

- Configurações adicionais do Antivírus de Arquivos (consulte 7.2.3 na p. 86)

As seções a seguir abordarão esses grupos detalhadamente.

7.2.1. Definindo os tipos de arquivos que serão verificados

Ao selecionar os tipos de arquivos que serão verificados, você estabelece quais os formatos e tamanhos de arquivo, e quais as unidades que, ao serem abertos, executados ou salvos, serão verificados quanto à presença de vírus.

Para facilitar a configuração, todos os arquivos estão divididos em dois grupos: *simples* e *compostos*. Os arquivos simples, por exemplo, arquivos .txt, não contêm nenhum objeto. Os objetos compostos podem incluir vários objetos, sendo que cada um deles também pode conter outros objetos. Existem vários exemplos: arquivos comprimidos, arquivos contendo macros, planilhas, e-mails com anexos, etc.

Os tipos de arquivos verificados são definidos na seção **Tipos de arquivos** (veja a Figura 18). Selecione uma das três opções:

- **Verificar todos os arquivos**. Com esta opção selecionada, todos os objetos do sistema de arquivos que forem abertos, executados ou salvos serão verificados, sem exceções.
- **Verificar programas e documentos (por conteúdo)**. Se você selecionar este grupo de arquivos, o Antivírus de Arquivos verificará apenas os arquivos possivelmente infectados; aqueles nos quais um vírus poderia ser incorporado.

> Observação:
>
> Há vários formatos de arquivos que têm um risco bem menor de conter código mal-intencionado infiltrado e, conseqüentemente, de estar ativados. Um exemplo são os arquivos .txt.
>
> Por outro lado, há formatos de arquivos que contêm ou podem conter código executável. Por exemplo, os formatos .exe, .dll ou .doc. O risco de infiltração e ativação de código mal-intencionado nesses arquivos é bastante alto.

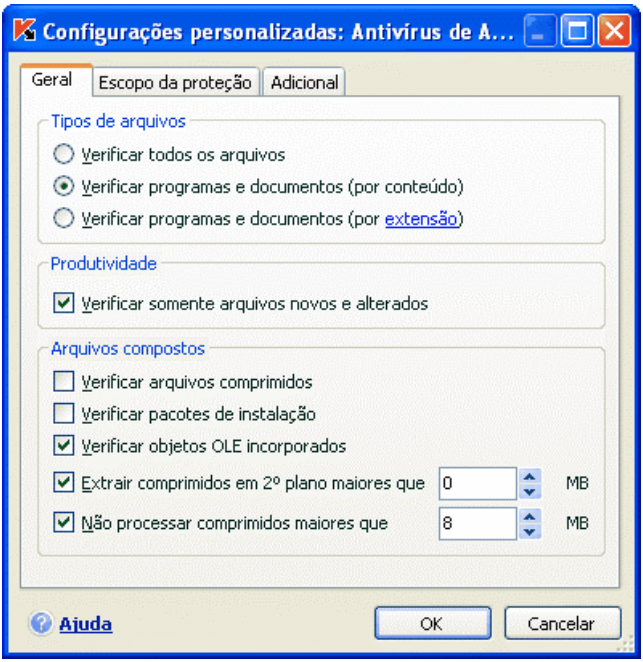


Figura 18. Selecionando os tipos de arquivos verificados quanto à presença de vírus

Antes de pesquisar vírus em um arquivo, seu cabeçalho interno é analisado com relação ao formato do arquivo (txt, doc, exe, etc.). Se a análise mostrar que o formato do arquivo não pode ser infectado, ele não será verificado quanto à presença de vírus e retornará imediatamente ao usuário. Se o formato do arquivo puder ser infectado, ele será verificado quanto à presença de vírus.

Verificar programas e documentos (por extensão). Se você selecionar esta opção, o Antivírus de Arquivos verificará apenas os arquivos possivelmente infectados, mas o formato do arquivo será determinado pela extensão do nome do arquivo. Usando o link extensão, você pode analisar uma lista de extensões de arquivos (consulte A.1 na p. 224) que são verificados com essa opção.

Dica:

Não esqueça que alguém pode enviar para o seu computador um vírus com uma extensão (por exemplo, .txt) que, na verdade, é um arquivo executável renomeado como .txt. Se você selecionar **Verificar programas e documentos (por extensão)**, a verificação ignoraria esse arquivo. Mas se a opção **Verificar programas e documentos (por conteúdo)** estiver selecionada, a extensão será ignorada, e a análise dos cabeçalhos do arquivo descobrirá que o arquivo é, na verdade, um arquivo .exe. O Antivírus de Arquivos verificaria o arquivo quanto à presença de vírus.

Na seção **Produtividade**, você pode especificar a verificação de vírus apenas nos arquivos novos e modificados. Esse modo reduz visivelmente o tempo de verificação e aumenta a velocidade de operação do programa. Para selecionar este modo, marque **Verificar somente arquivos novos e modificados**. Esse modo se aplica a arquivos simples e compostos.

Na seção **Arquivos compostos**, especifique os arquivos compostos que devem ser verificados quanto à presença de vírus:

- **Verificar arquivos comprimidos** – verifica arquivos comprimidos .zip, .cab, .rar e .arj.
- **Verificar pacotes de instalação** – verifica arquivos comprimidos de extração automática quanto à presença de vírus.
- **Verificar objetos OLE incorporados** – verifica objetos incorporados em arquivos (por exemplo, planilhas do Excel ou macros incorporadas em um arquivo do Microsoft Word, anexos de e-mail, etc.).

Você pode selecionar e verificar todos os arquivos ou somente os novos, para cada tipo de arquivo composto. Para fazê-lo, clique no link ao lado do nome do objeto para alternar seu valor. Se a seção **Produtividade** tiver sido configurada para verificar somente arquivos novos e modificados, você não poderá selecionar o tipo de arquivos compostos que serão verificados.

Para especificar os arquivos compostos que não devem ser verificados quanto à presença de vírus, use as seguintes configurações:

- **Extrair arquivos comprimidos em segundo plano se maiores que... MB**. Se o tamanho de um objeto composto exceder esta restrição, o programa o verificará como um único objeto (analisando o cabeçalho) e o retornará para o usuário. Os objetos contidos nele serão verificados posteriormente. Se esta opção não estiver marcada, o acesso a arquivos maiores que o tamanho indicado será bloqueado até que tenham sido verificados.
- **Não processar arquivos comprimidos maiores que MB**. Com esta opção marcada, arquivos maiores que o tamanho especificado serão ignorados na verificação.

7.2.2. Definindo o escopo da proteção

Por padrão, o Antivírus de Arquivos verifica todos os arquivos usados, independentemente de onde estão armazenados, seja em um disco rígido, um CD/DVD-ROM ou uma unidade flash.

Você pode limitar o escopo da proteção. Para fazê-lo:

1. Selecione **Antivírus de Arquivos** na janela principal e vá para a janela de configurações do componente clicando em Configurações.
2. Clique no botão **Personalizar** e selecione a guia **Escopo de proteção** (veja a fig. 19) na janela que é aberta.

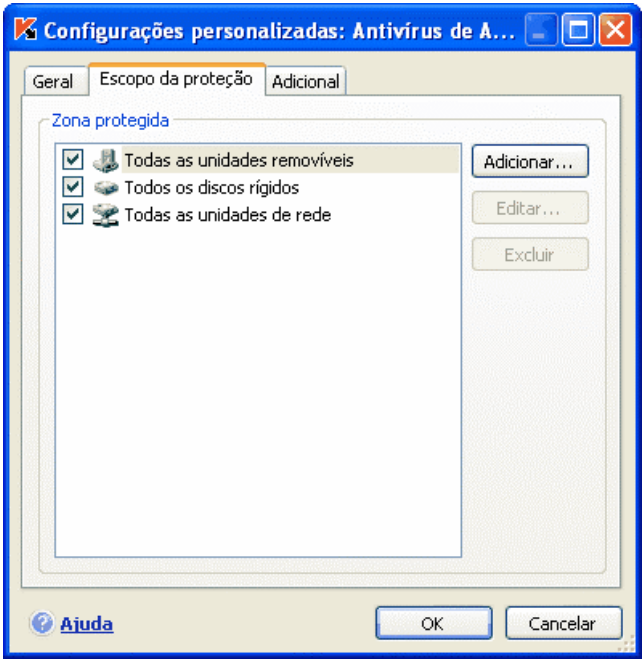


Figura 19. Criando uma zona de proteção

A guia exibe uma lista de objetos que serão verificados pelo Antivírus de Arquivos. Por padrão, a proteção é habilitada para todos os objetos em discos rígidos, mídia removível e unidades de rede conectadas ao seu computador. É possível acrescentar itens e editar a lista usando os botões **Adicionar, Editar** e **Excluir**.

Se desejar proteger menos objetos, você pode fazê-lo usando os seguintes métodos:

- Especifique somente as pastas, unidades e arquivos que precisam ser protegidos.
- Crie uma lista de objetos que não precisam ser protegidos.
- Combine os dois métodos anteriores; crie um escopo de proteção que exclua vários objetos.

Você pode usar máscaras ao adicionar objetos para verificação. Observe que só é possível inserir máscaras com caminhos de objetos absolutos:

- **C:\dir*.***, **C:\dir*** ou **C:\dir** - todos os arquivos na pasta *C:\dir*
- **C:\dir*.exe** - todos os arquivos com a extensão *.exe* na pasta *C:\dir*
- **C:\dir*.ex?** – todos os arquivos com a extensão *.ex?* na pasta *C:\dir* , onde ? representa qualquer caractere
- **C:\dir\teste** - somente o arquivo *C:\dir\teste*

Para que a verificação seja executada recursivamente, marque **Incluir subpastas**.

Aviso!

Lembre-se de que o Antivírus de Arquivos verificará apenas os arquivos incluídos no escopo de proteção criado. Os arquivos que não estão incluídos nesse escopo estarão disponíveis para uso sem serem verificados. Isso aumenta o risco de infecção no seu computador.

7.2.3. Definindo as configurações avançadas

Nas configurações adicionais do Antivírus de Arquivos, você pode especificar o modo de verificação do sistema de arquivos e configurar as condições para pausar o componente temporariamente.

Para definir configurações adicionais do Antivírus de Arquivos:

1. Selecione **Antivírus de Arquivos** na janela principal e vá para a janela de configurações do componente clicando no link Configurações.
2. Clique no botão **Personalizar** e selecione a guia **Adicional** na janela que é aberta (veja a Figura 20).

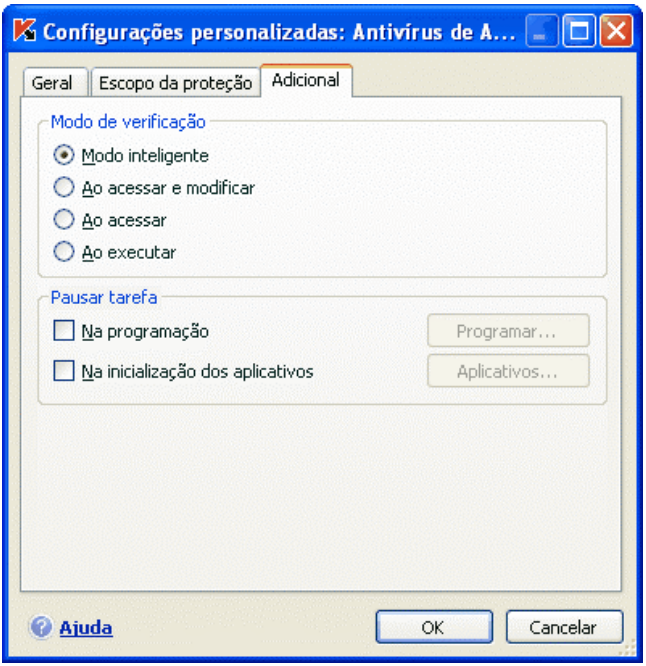


Figura 20. Definindo as configurações adicionais do Antivírus de Arquivos

O modo de verificação de arquivos determina as condições de processamento do Antivírus de Arquivos. Você tem as seguintes opções:

- **Modo inteligente**. Este modo tem como objetivo acelerar o processamento de arquivos e retorná-los para o usuário. Quando está selecionado, a decisão de verificação se baseia na análise das operações executadas com o arquivo.

  Por exemplo, ao usar um arquivo do Microsoft Office, o Kaspersky Anti-Virus o verifica quando é aberto pela primeira vez e fechado pela última vez. Todas as operações intermediárias que substituem o arquivo não são verificadas.

  O modo inteligente é o padrão.

- **Ao acessar e modificar** – o Antivírus de Arquivos verifica os arquivos quando são abertos ou editados.

- **Ao acessar** – verifica os arquivos apenas ao tentar abri-los.

- **Ao executar** – verifica os arquivos apenas ao tentar executá-los.

Pode ser necessário pausar o Antivírus de Arquivos ao executar tarefas que exigem recursos significativos do sistema operacional. Para diminuir a carga e assegurar que o usuário tenha novamente acesso aos arquivos rapidamente, é recomendável configurar que o componente seja desabilitado em uma determinada hora ou enquanto determinados programas estão em uso.

Para pausar o componente por um determinado período, marque **Na programação** e, na janela que é aberta (veja a Figura 8), clique em **Programação** para atribuir um período para desabilitar e reiniciar o componente. Para fazê-lo, insira um valor no formato HH:MM nos campos correspondentes.

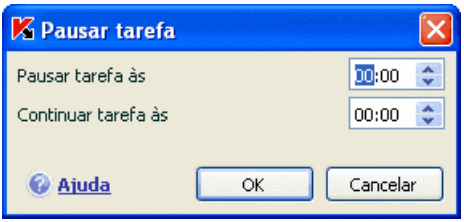


Figura 21. Pausando o componente

Para desabilitar o componente ao trabalhar com programas que exigem recursos significativos, marque **Ao inicializar aplicativos** e edite a lista de programas na janela que é aberta (veja Figura 22) clicando em **Aplicativos**.

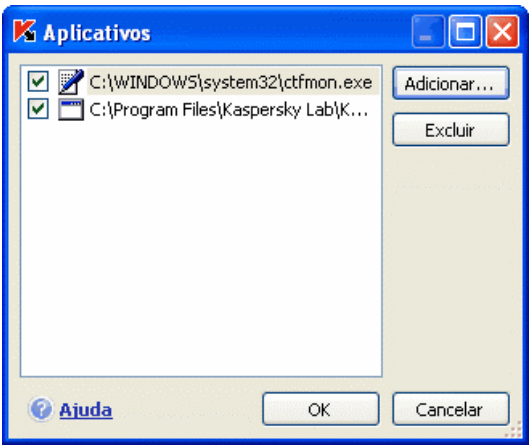


Figura 22. Criando uma lista de aplicativos

Para adicionar um aplicativo à lista, use o botão **Adicionar**. Um menu de contexto será aberto e, ao clicar em **Procurar**, você poderá ir para a janela de

seleção de arquivos padrão e selecionar arquivo executável do aplicativo a ser adicionado. Ou vá para a lista de aplicativos em execução no item **Aplicativos** e selecione o desejado.

Para excluir um aplicativo, selecione-o em uma lista e clique em **Excluir**.

Você pode desabilitar temporariamente a pausa no Antivírus de Arquivos ao usar um aplicativo específico. Para fazê-lo, desmarque o nome do aplicativo. Não é necessário excluí-lo da lista.

7.2.4. Restaurando as configurações padrão do Antivírus de Arquivos

Ao configurar o Antivírus de Arquivos, você sempre pode retornar às configurações de desempenho padrão. A Kaspersky Lab as considera ideais e as combinou no nível de segurança **Recomendado**.

Para restaurar as configurações padrão do Antivírus de Arquivos:

1. Selecione **Antivírus de Arquivos** na janela principal e vá para a janela de configurações do componente clicando em Configurações.
2. Clique no botão **Padrão** na seção **Nível de segurança**.

Se você modificou a lista de objetos incluídos na zona protegida ao configurar o Antivírus de Arquivos, o programa perguntará se deseja salvar essa lista para usar no futuro, ao restaurar as configurações iniciais. Para salvar a lista de objetos, marque **Zona de proteção** na janela **Restaurar configurações** que é aberta.

7.2.5. Selecionando ações para objetos

Se o Antivírus de Arquivos descobrir ou suspeitar de uma infecção em um arquivo ao verificá-lo quanto à presença de vírus, as próximas etapas do programa dependerão do status do objeto e da ação selecionada.

O Antivírus de Arquivos pode rotular um objeto com um dos seguintes status:

- Status de programa mal-intencionado (por exemplo, *vírus, cavalo de Tróia*).
- *Possivelmente infectado*, quando a verificação não consegue determinar se o objeto está infectado. Isso significa que o programa detectou no arquivo uma seqüência de código de um vírus desconhecido ou de código modificado de um vírus conhecido.

Por padrão, todos os arquivos infectados estão sujeitos à desinfecção e, se estiverem possivelmente infectados, serão enviados para a Quarentena.

Para editar uma ação para um objeto:

selecione **Antivírus de Arquivos** na janela principal e vá para a janela de configurações do componente clicando em Configurações. Todas as ações possíveis são exibidas nas seções apropriadas (veja a fig. 23).

Figura 23. Possíveis ações do Antivírus de Arquivos para objetos perigosos

Se a ação selecionada for	Ao detectar um objeto perigoso
Perguntar o que fazer	O Antivírus de Arquivos emite uma mensagem de aviso com informações sobre o programa mal-intencionado que infectou, ou possivelmente infectou, o arquivo e permite que você escolha o que fazer. A opção pode variar dependendo do status do objeto.
Bloquear o acesso	O Antivírus de Arquivos bloqueia o acesso ao objeto. Essas informações são registradas no relatório (consulte 14.3 na p. 173). Posteriormente, você pode tentar desinfectar esse objeto.
Bloquear o acesso **Desinfectar**	O Antivírus de Arquivos bloqueará o acesso ao objeto e tentará desinfectá-lo. Se a desinfecção falhar, será atribuído o status de *possivelmente infectado* ao arquivo e ele será movido para a Quarentena (consulte 14.1 na p. 167). Essas informações são registradas no relatório. Posteriormente, você pode tentar desinfectar esse objeto.
Bloquear o acesso	O Antivírus de Arquivos bloqueará o acesso ao objeto e tentará desinfectá-

Se a ação selecionada for	Ao detectar um objeto perigoso
☑ **Desinfectar** ☑ **Excluir se a desinfecção falhar**	lo. Se a desinfecção for bem-sucedida, ele será restaurado para uso normal. Se o objeto não puder ser desinfectado, ele será excluído. Uma cópia do objeto será armazenada no Backup (consulte 14.2 na p. 171).
◉ **Bloquear o acesso** ☑ **Desinfectar** ☑ **Excluir**	O Antivírus de Arquivos bloqueará o acesso ao objeto e o excluirá.

Ao desinfectar ou excluir um objeto, o Kaspersky Anti-Virus cria uma cópia do mesmo e a envia para o Backup, caso seja necessário restaurar o objeto ou surja uma oportunidade de neutralizá-lo.

7.3. Desinfecção adiada

Se você selecionar ◉ **Bloquear o acesso** como ação para programas mal-intencionados, os objetos não serão neutralizados e o acesso a eles será bloqueado.

Se as ações selecionadas forem

◉ **Bloquear o acesso**
☑ **Desinfectar**

todos os objetos não neutralizados também serão bloqueados.

Para obter novamente o acesso a objetos bloqueados, eles devem ser desinfectados. Para fazê-lo:

1. Selecione **Antivírus de Arquivos** na janela principal do programa e clique em qualquer local da caixa **Estatísticas**.
2. Selecione os objetos que o interessam na guia **Detectados** e clique no botão **Ações** ⟶ **Neutralizar tudo**.

Os arquivos desinfectados com êxito serão retornados ao usuário. Os que não puderem ser neutralizados, poderão ser *excluídos* ou *ignorados*. No último caso, o acesso ao arquivo será restaurado. Contudo, isso aumenta significativamente o risco de infecção no seu computador. É altamente recomendável não ignorar objetos mal-intencionados.

CAPÍTULO 8. ANTIVÍRUS DE E-MAIL

O *Antivírus de E-Mail* é o componente do Kaspersky Anti-Virus que evita que os e-mails enviados e recebidos transfiram objetos perigosos. Ele é executado na inicialização do sistema operacional, fica ativo na memória do sistema e verifica todos os e-mails nos protocolos POP3, SMTP, IMAP, MAPI[1] e NNTP, além da criptografia de POP3 e IMAP (SSL).

A atividade do componente é indicada pelo ícone do Kaspersky Anti-Virus na bandeja do sistema, que tem a seguinte aparência  sempre que um e-mail está sendo verificado.

A configuração padrão do Antivírus de E-Mail é a seguinte:

1. O Antivírus de E-Mail intercepta todos os e-mails enviados ou recebidos pelo usuário.
2. O e-mail é dividido em partes: cabeçalhos, corpo e anexos do e-mail.
3. São verificados objetos perigosos no corpo e nos anexos do e-mail (incluindo anexos OLE). Os objetos mal-intencionados são detectados usando as *assinaturas de ameaças* incluídas no programa e com o algoritmo heurístico. As assinaturas contêm descrições de todos os programas mal-intencionados conhecidos até o momento e os métodos para neutralizá-los. O algoritmo heurístico pode detectar novos vírus que ainda não fazem parte das assinaturas de ameaças.
4. Depois da verificação de vírus, você poderá tomar as seguintes medidas:
    - Se o corpo ou os anexos do e-mail contiverem código mal-intencionado, o Antivírus de E-Mail bloqueará o e-mail, colocará uma cópia do objeto infectado no *Backup* e tentará desinfectar o objeto. Se a desinfecção for bem-sucedida, o e-mail será disponibilizado para o usuário novamente. Caso contrário, o objeto infectado no e-mail será excluído. Depois da verificação antivírus, um texto específico é inserido na linha de assunto do e-mail, informando que o mesmo foi processado pelo Kaspersky Anti-Virus.

[1] Os e-mails enviados com MAPI são verificados usando um plug-in específico para o Microsoft Office Outlook e o The Bat!

- Se for detectado, no corpo ou em um anexo, um código que parece ser mal-intencionado, mas sem garantias disso, a parte suspeita do e-mail será enviada para a *Quarentena*.
- Se nenhum código mal-intencionado for descoberto no e-mail, ele será disponibilizado imediatamente para o usuário.

É fornecido um plug-in específico (consulte 8.2.2 na p. 98) para o Microsoft Outlook que permite configurar a verificação de e-mails de maneira mais precisa.

Se você usar o The Bat!, o Kaspersky Anti-Virus poderá ser usado em conjunto com outros aplicativos antivírus. As regras para o processamento do tráfego de e-mail (consulte 8.2.3 na p. 100) são configuradas diretamente no The Bat! e sobrepõem as configurações de proteção de e-mail do Kaspersky Anti-Virus.

Ao trabalhar com outros programas de e-mail, incluindo Outlook Express, Mozilla Thunderbird, Eudora, Incredimail, o Antivírus de E-Mail verifica os e-mails nos protocolos SMTP, POP3, IMAP, MAPI e NNTP.

8.1. Selecionando um nível de proteção de e-mails

O Kaspersky Anti-Virus protege seus e-mails em um dos seguintes níveis (veja a fig. 24):

Alto – o nível com o monitoramento mais abrangente dos e-mails enviados e recebidos. O programa verifica anexos de e-mail detalhadamente, incluindo arquivos comprimidos, independentemente do tempo gasto na verificação.

Recomendado – os especialistas da Kaspersky recomendam este nível. São verificados os mesmos objetos que no nível **Alto**, com exceção dos anexos ou dos e-mails que levarem mais de três minutos para serem verificados.

Baixo – o nível com configurações que permitem usar tranqüilamente aplicativos que consomem muitos recursos, pois o escopo de verificação de e-mails é limitado. Neste nível, apenas os e-mails recebidos são verificados, ou seja, os arquivos comprimidos e objetos (e-mails) em anexo não serão verificados, se essa verificação demorar mais de três minutos. Este nível é recomendado se você tiver outro software de proteção de e-mails instalado no computador.

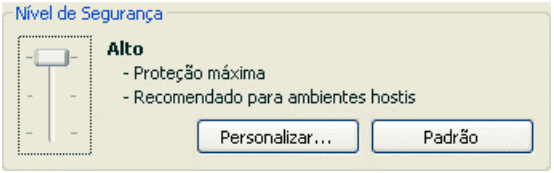


Figura 24. Selecionando um nível de segurança de e-mail

Por padrão, o nível de segurança de e-mail é definido como **Recomendado**.

Você pode aumentar ou reduzir o nível de segurança de e-mail, selecionando o nível desejado ou editando as configurações do nível atual.

Para alterar o nível de segurança:

Ajuste os controles deslizantes. Ao alterar o nível de segurança, você define a taxa da velocidade de verificação com relação ao número total de objetos verificados: quanto menos objetos de e-mail forem verificados quanto à presença de objetos perigosos, maior a velocidade de verificação.

Se nenhum dos níveis pré-instalados atender às suas necessidades, você poderá editar suas configurações. Se o fizer, o nível será definido como **Personalizado**. Vamos examinar um exemplo de quando os níveis de segurança de e-mail definidos pelo usuário seriam úteis.

Exemplo:

O computador está fora da rede local e usa uma conexão discada com a Internet. Você usa o Outlook Express como programa de e-mail para receber e enviar e-mails, e usa um serviço de e-mail gratuito. Por vários motivos, seus e-mails contêm anexos com arquivos comprimidos. Qual a melhor maneira de proteger seu computador de infecções por e-mail?

Dica para selecionar um nível:

Analisando sua situação, é possível concluir que você tem um alto risco de infecção por e-mail, no cenário descrito, pois não há uma proteção centralizada de e-mail e por usar uma conexão discada.

É recomendável usar inicialmente o nível de segurança **Alto**, com as seguintes alterações: reduza o tempo de verificação de anexos, por exemplo, para 1-2 minutos. A maioria dos anexos de arquivos comprimidos será verificada quanto à presença de vírus e a velocidade de processamento não será muito comprometida.

Para modificar um nível de segurança pré-instalado:

Clique no botão **Personalizar** na janela de configurações do Antivírus de E-Mail. Edite as configurações de proteção de e-mail na janela que é aberta e clique em **OK**.

8.2. Configurando o Antivírus de E-Mail

Uma série de configurações controla a maneira como seus e-mails são verificados. Elas podem ser divididas nos seguintes grupos:

- Configurações que definem o grupo de e-mails protegidos (consulte 8.2.1 na p. 96)
- Configurações de verificação de e-mail do Microsoft Outlook (consulte 8.2.2 na p. 98) e do The Bat! (consulte 8.2.3 na p. 100)

  Aviso!

  Esta versão do Kaspersky Anti-Virus não fornece plug-ins do Antivírus de E-Mail para programas de e-mail de 64 bits.

- configurações que definem ações para objetos de e-mail perigosos (consulte 8.2.4 na p. 102)

As seções a seguir examinam estas configurações detalhadamente.

8.2.1. Selecionando um grupo de e-mails protegidos

O Antivírus de E-Mail permite selecionar exatamente que grupo de e-mails deve ser verificados quanto à presença de objetos perigosos.

Por padrão, o componente protege os e-mails no nível de segurança **Recomendado**, que inclui a verificação de e-mails enviados e recebidos. Quando você começa a trabalhar no programa pela primeira vez, é recomendável verificar os e-mails enviados, pois é possível que haja worms no computador que usam o e-mail para se distribuírem. Isso ajudará a evitar a possibilidade de enviar e-mails infectados em massa sem monitoramento do seu computador.

Se você estiver certo de que os e-mails que você está enviando não contêm objetos perigosos, poderá desabilitar a verificação de e-mails enviados. Para fazê-lo:

1. Selecione **Antivírus de E-Mail** na janela principal e vá para a janela de configurações do componente clicando em Configurações. Clique no botão **Personalizar** na janela de configurações do Antivírus de E-Mail.
2. Na janela de configurações personalizadas do Antivírus de E-Mail que é aberta (veja a fig.), selecione **E-mail recebido** na seção **Escopo**.

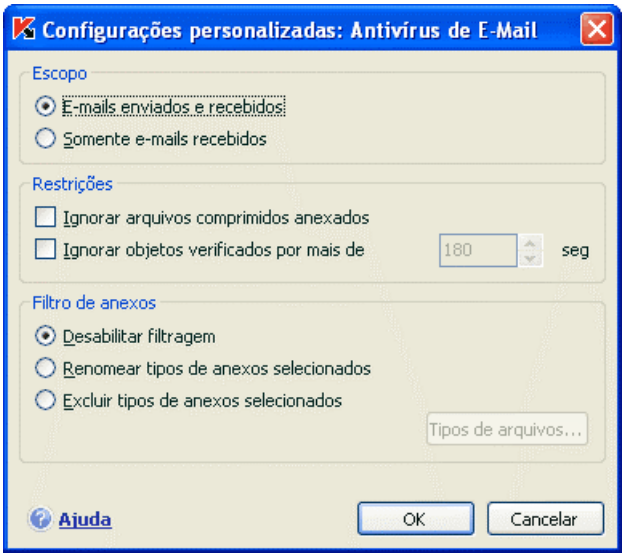


Figura 25. Configurações do Antivírus de E-Mail

Além de selecionar um grupo de e-mails, você pode especificar que os anexos de arquivos comprimidos devem ser verificados e também definir o tempo máximo para a verificação de um objeto de e-mail. Essas configurações são definidas na seção **Restrições**.

Se o computador não estiver protegido por nenhum software de rede local e acessar a Internet sem usar um servidor proxy ou um firewall, é recomendável **não desabilitar** a verificação de anexos de arquivos comprimidos e não definir um limite de tempo para a verificação.

Se estiver trabalhando em um ambiente protegido, poderá alterar as restrições de tempo da verificação para aumentar a velocidade de verificação dos e-mails.

Você pode configurar as condições de filtragem dos objetos conectados a um e-mail na seção **Filtro de anexos**:

- **Desabilitar filtragem** – não usa filtragem adicional de anexos.
- **Renomear tipos de anexos selecionados** – filtra um determinado formato de anexo e substitui o último caractere do nome do arquivo por

um sublinhado. Você pode selecionar o tipo de arquivo clicando no botão Tipos de arquivos.

Excluir tipos de anexos selecionados – filtra e exclui um determinado formato de anexo. Você pode selecionar o tipo de arquivo clicando no botão Tipos de arquivos.

Você pode obter mais informações sobre tipos de anexos filtrados na seção A.1 na p. 224.

Ao usar o filtro, você aumenta a segurança do computador, pois freqüentemente os programas mal-intencionados se disseminam por e-mail como anexos. Ao renomear ou excluir determinados tipos de anexos, você protege o computador de anexos abertos automaticamente quando uma mensagem é recebida.

8.2.2. Configurando o processamento de e-mail no Microsoft Office Outlook

Se você usar o Outlook como programa de e-mail, poderá definir configurações personalizadas para as verificações de vírus.

Um plug-in específico é instalado no Outlook ao instalar o Kaspersky Anti-Virus. Ele pode acessar as configurações do Antivírus de E-Mail rapidamente e também definir o tempo máximo de verificação de objetos perigosos em e-mails individuais.

Aviso!

Esta versão do Kaspersky Anti-Virus não fornece plug-ins do Antivírus de E-Mail para o Microsoft Office Outlook de 64 bits.

O plug-in é fornecido na forma de uma guia **Antivírus de E-Mail** específica, localizada sob **Serviço** → **Opções** (veja a fig. 26).

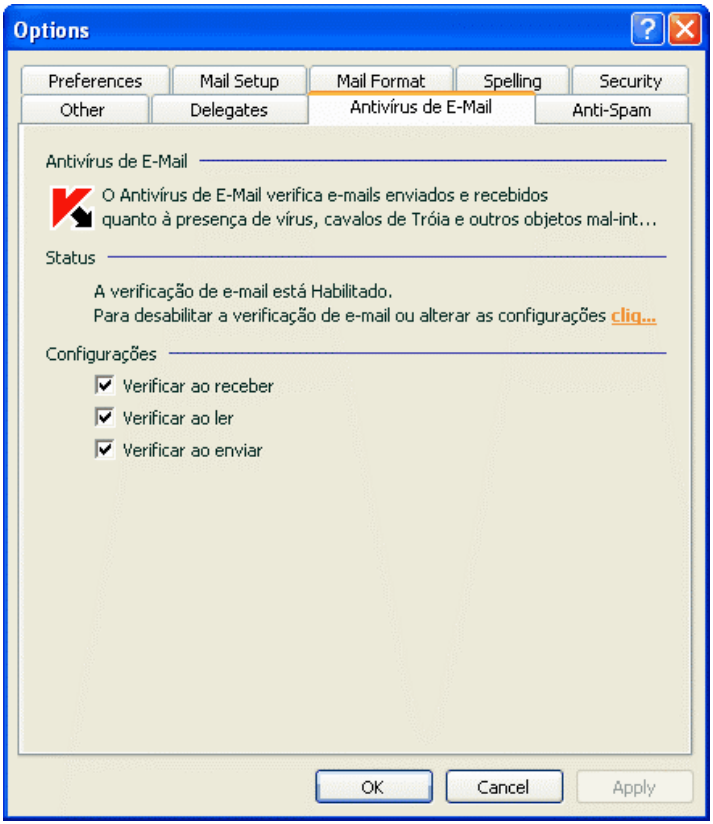


Figura 26. Configurando o Antivírus de E-Mail no Microsoft Outlook

Selecione um modo de verificação de e-mail:

- **Verificar ao receber** – analisa cada e-mail que entra na sua Caixa de Entrada.
- **Verificar ao ler** – verifica o e-mail quando você o abre para lê-lo.
- **Verificar ao enviar** – verifica vírus em cada e-mail, ao enviá-lo.

Aviso!

Se você usar o Outlook para conectar seu serviço de e-mail no IMAP, é recomendável não usar o modo **Verificar ao receber**. Habilitar esse modo fará os e-mails serem copiados para o computador local quando enviados para o servidor e, conseqüentemente, a principal vantagem do IMAP será perdida: a criação de menos tráfego e o tratamento de e-mails indesejados no servidor sem copiá-los para o computador do usuário.

A medida que será tomada com relação a objetos de e-mail perigosos é definida nas configurações do Antivírus de E-Mail, que podem ser acessadas por meio do link clique aqui na seção Status.

8.2.3. Configurando a verificação de e-mail no The Bat!

As ações tomadas com relação a objetos de e-mail infectados no The Bat! são definidas pelas ferramentas do próprio programa.

Aviso!

As configurações do Antivírus de E-Mail que determinam se os e-mails enviados e recebidos são verificados, assim como as ações com relação a objetos de e-mail perigosos e exclusões são ignoradas. A única coisa que o The Bat! considera é a verificação de anexos com arquivos comprimidos e os limites de tempo da verificação de e-mails (consulte 8.2.1 na p. 96).

O plug-in do Antivírus de E-Mail para a versão de 64 bits do Microsoft Office Outlook não está disponível nesta versão do Kaspersky Anti-Virus.

Para configurar as regras de proteção de e-mail no The Bat!:

1. Selecione **Preferences** no menu **Options** do programa de e-mail.
2. Selecione **Protection** na árvore de configurações.

As configurações de proteção exibidas (veja a fig. Figura 27) estendem-se a todos os módulos antivírus instalados no computador que dá suporte ao The Bat!

Você deve decidir:

- O grupo de e-mails que será verificado quanto à presença de vírus (recebidos, enviados)
- Em que momento os objetos de e-mail serão verificados quanto à presença de vírus (ao abrir um e-mail ou antes de salvá-lo no disco)

- As ações executadas pelo programa de e-mail quando objetos perigosos são detectados em e-mails. Por exemplo, você poderia selecionar:

  Try to cure infected parts – tenta neutralizar o objeto de e-mail infectado e, se isso não for possível, o objeto permanecerá no e-mail. O Kaspersky Anti-Virus sempre o informará se um e-mail estiver infectado. Mas, mesmo que você selecione **Excluir** na janela de aviso do Antivírus de E-Mail, o objeto permanecerá no e-mail, pois a ação selecionada no The Bat! sobrepõe as ações do Antivírus de E-Mail.

  Remove infected parts – exclui o objeto perigoso no e-mail, independentemente de ele estar infectado ou de haver apenas uma suspeita de que esteja infectado.

  Por padrão, o The Bat! coloca todos os objetos de e-mail infectados na pasta Quarentena sem neutralizá-los.

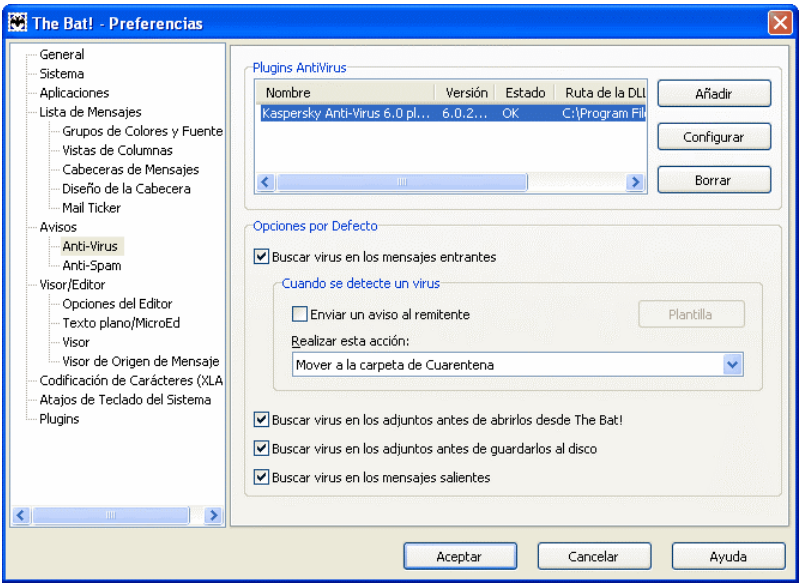


Figura 27. Configurando a verificação de e-mail no The Bat!

Aviso!

O The Bat! não marca os e-mails que contêm objetos perigosos com cabeçalhos específicos.

8.2.4. Restaurando as configurações padrão do Antivírus de E-Mail

Ao configurar o Antivírus de E-Mail, você sempre pode retornar para as configurações de desempenho padrão, consideradas ideais pela Kaspersky Lab, que as combinou no nível de segurança **Recomendado**.

Para restaurar as configurações padrão do Antivírus de E-Mail:

1. Selecione **Antivírus de E-Mail** na janela principal e vá para a janela de configurações do componente clicando em Configurações.
2. Clique no botão **Padrão** na seção **Nível de segurança**.

8.2.5. Selecionando ações para objetos de e-mail perigosos

Se uma verificação mostrar que um e-mail ou alguma de suas partes (corpo, anexo) está infectado ou que há suspeitas disso, as etapas executadas pelo Antivírus de E-Mail dependem do status do objeto e da ação selecionada.

Um dos seguintes status pode ser atribuído ao objeto de e-mail após a verificação:

- Status de programa mal-intencionado (por exemplo, *vírus, cavalo de Tróia*; para obter mais detalhes, consulte 1.1 na p. 9).
- *Possivelmente infectado*, quando a verificação não consegue determinar se o objeto está infectado. Isso significa que o programa detectou no arquivo uma seqüência de código de um vírus desconhecido ou de código modificado de um vírus conhecido.

Por padrão, quando o Antivírus de E-Mail detecta um objeto perigoso ou possivelmente infectado, ele exibe um aviso na tela e solicita ao usuário que selecione uma ação para o objeto.

Para editar uma ação para um objeto:

Abra a janela de configurações do Kaspersky Anti-Virus e selecione **Antivírus de E-Mail**. Todas as ações possíveis para objetos perigosos são relacionadas na caixa **Ação** (veja a fig. 28).

Figura 28. Selecionando ações para objetos de e-mail perigosos

Vamos examinar mais detalhadamente as opções possíveis para o processamento de objetos de e-mail perigosos.

Se a ação selecionada for	Ao detectar um objeto perigoso
Perguntar o que fazer	O Antivírus de E-Mail emitirá uma mensagem de aviso com informações sobre o programa mal-intencionado que infectou (ou possivelmente infectou) o arquivo e permite que você escolha uma das ações a seguir.
Bloquear o acesso	O Antivírus de E-Mail bloqueia o acesso ao objeto. Essas informações são registradas no relatório (consulte 14.3 na p. 173). Posteriormente, você pode tentar desinfectar esse objeto.
Bloquear o acesso **Desinfectar**	O Antivírus de E-Mail bloqueará o acesso ao objeto e tentará desinfectá-lo. Se a desinfecção for bem-sucedida, ele será restaurado para uso normal. Se o objeto não puder ser neutralizado, ele será movido para a Quarentena. Essas informações são registradas no relatório. Posteriormente, você pode tentar desinfectar esse objeto.
Bloquear o acesso	O Antivírus de E-Mail bloqueará o acesso ao objeto e tentará desinfectá-lo. Se a

☑ **Desinfectar** ☑ **Excluir se a desinfecção falhar**[2]	desinfecção for bem-sucedida, ele será restaurado para uso normal. Se o objeto não puder ser desinfectado, ele será excluído. Uma cópia do objeto será armazenada no Backup. Os objetos com o status *possivelmente infectado* serão movidos para a Quarentena.
◉ **Bloquear o acesso** ☐ **Desinfectar** ☑ **Excluir**	Quando o Antivírus de E-Mail detecta um objeto infectado ou possivelmente infectado, ele o exclui sem informar o usuário.

Ao desinfectar ou excluir um objeto, o Kaspersky Anti-Virus cria uma cópia do mesmo e a envia para o Backup (consulte 14.2 na p. 171), antes de tentar neutralizar ou excluir o objeto, caso seja necessário restaurá-lo ou surja uma oportunidade de neutralizá-lo.

[2] Se estiver usando o The Bat! como programa de e-mail, os objetos de e-mail perigosos serão desinfectados ou excluídos quando o Antivírus de E-Mail executar esta ação (dependendo da ação selecionada no The Bat!).

CAPÍTULO 9. ANTIVÍRUS DA WEB

Ao usar a Internet, as informações armazenadas no computador estão abertas à possível infecção por programas perigosos, que podem invadir o computador enquanto você lê um artigo na Internet.

O *Antivírus da Web* é o componente do Kaspersky Anti-Virus que protege o computador durante o uso da Internet. Ele protege as informações que entram no computador via protocolo HTTP e também impede que scripts perigosos sejam carregados no computador.

Aviso!

O Antivírus da Web monitora apenas o tráfego HTTP que passa pelas portas relacionadas na lista de portas monitoradas (consulte 14.7 na p. 186). As portas mais usadas para transmitir e-mails e tráfego HTTP estão listadas no pacote do programa. Se você usa portas que não estão nesta lista, adicione-as para proteger o tráfego que passa por elas.

Se estiver trabalhando em uma rede não protegida ou usando um modem para acessar a Internet, é recomendável usar o Antivírus da Web para proteger-se enquanto usa a Internet. Se o computador for executado em uma rede protegida por um firewall ou por filtros de tráfego HTTP, o Antivírus da Web fornece proteção adicional enquanto você navega na Web.

A atividade do componente é indicada pelo ícone do Kaspersky Anti-Virus na bandeja do sistema, que tem a seguinte aparência  sempre que scripts estão sendo verificados.

Vamos examinar o funcionamento do componente mais detalhadamente.

O Antivírus da Web consiste em dois módulos, que tratam da:

- *Verificação de tráfego* – verifica objetos que entram no computador do usuário via HTTP.
- *Verificação de scripts* – verifica todos os scripts processados pelo Microsoft Internet Explorer e todos os scripts WSH (JavaScript, Visual Basic Script, etc.) que são carregados enquanto o usuário está no computador e na Internet.

  Um plug-in específico para o Microsoft Internet Explorer é instalado como parte da instalação do Kaspersky Anti-Virus. O ícone  na barra de ferramentas Padrão do navegador indica que ele foi instalado. Clicar nele

abre um painel informativo com estatísticas do Antivírus da Web sobre o número de scripts verificados e bloqueados.

O Antivírus da Web protege o tráfego HTTP conforme indicado a seguir:

1. Cada página da Web ou arquivo que pode ser acessado pelo usuário ou por um determinado aplicativo via HTTP é interceptado e analisado pelo Antivírus da Web quanto à presença de código mal-intencionado. Os objetos mal-intencionados são detectados usando as assinaturas de ameaças incluídas no Kaspersky Anti-Virus e o algoritmo heurístico. As assinaturas contêm descrições de todos os programas mal-intencionados conhecidos até o momento e os métodos para neutralizá-los. O algoritmo heurístico pode detectar novos vírus que ainda não fazem parte das assinaturas de ameaças.
2. Depois da análise, as seguintes medidas a serem tomadas estão disponíveis:
    a. Se um objeto ou página da Web contiver código mal-intencionado, o programa bloqueará o acesso a ele e aparecerá uma mensagem na tela, informando que o objeto ou a página estão infectados.
    b. Se o arquivo ou a página da Web não contiver código mal-intencionado, o navegador da Web terá acesso a ele imediatamente.

Os scripts são verificados de acordo com o seguinte algoritmo:

1. O Antivírus da Web intercepta cada script executado em uma página da Web e verifica a presença de código mal-intencionado.
2. Se um script contiver código mal-intencionado, o Antivírus da Web o bloqueará e informará o usuário através de uma notificação pop-up específica.
3. Se nenhum código mal-intencionado for descoberto no script, ele será executado.

9.1. Selecionando o nível de segurança da Web

O Kaspersky Anti-Virus o protege enquanto você usa a Internet em um dos seguintes níveis (veja a Figura 29):

Alto – o nível com o monitoramento mais abrangente de scripts e objetos recebidos via HTTP. O programa executa uma verificação completa de todos os objetos usando o conjunto total de assinaturas de ameaças.

Este nível de proteção é recomendado para ambientes confidenciais, quando nenhuma outra ferramenta de segurança HTTP estiver sendo usada.

Recomendado – este nível verifica os mesmos objetos que o nível **Alto**, mas limita o tempo de cache para fragmentos do arquivo, o que acelera a verificação e retorna os objetos ao usuário mais rapidamente.

Baixo – o nível de segurança com configurações que permitem usar tranqüilamente aplicativos que consomem muitos recursos, pois o escopo dos objetos verificados é menor, usando um conjunto limitado de assinaturas de ameaças. Este nível de segurança é recomendado se você tiver outro software de proteção da Web instalado no computador.

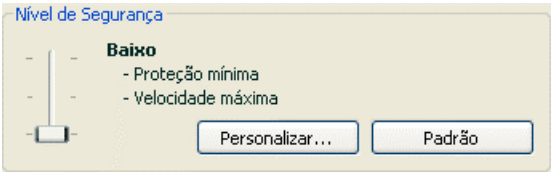


Figura 29. Selecionando um nível de segurança da Web

Por padrão, o nível de proteção é definido como **Recomendado**.

Você pode aumentar ou reduzir o nível de segurança, selecionando o nível desejado ou editando as configurações do nível atual.

Para editar o nível de segurança:

Ajuste os controles deslizantes. Ao alterar o nível de segurança, você define a taxa da velocidade de verificação com relação ao número total de objetos verificados: quanto menos objetos verificados quanto à presença de código mal-intencionado, maior a velocidade de verificação.

Se um nível predefinido não atender às suas necessidades, você poderá criar um nível de segurança **Personalizado**. Vamos examinar um exemplo de quando esse nível seria útil.

Exemplo:

O computador conecta-se com a Internet por um modem. Ele não está em uma rede local corporativa e você não tem proteção antivírus para tráfego HTTP recebido.

Devido ao seu tipo de trabalho, você baixa arquivos grandes da Internet regularmente. A verificação de arquivos como esses normalmente leva um tempo razoável.

Qual a maneira ideal de proteger seu computador de infecções por tráfego HTTP ou por um script?

Dica para selecionar um nível:

A julgar por estas informações básicas, podemos concluir que o computador está sendo executado em um ambiente confidencial e que tem um alto risco de infecção por tráfego HTTP, pois não há uma proteção centralizada da Web e devido ao uso da conexão discada com a Internet.

É recomendável usar o nível de segurança **Alto** como ponto inicial, com as seguintes alterações: é recomendável limitar o tempo de armazenamento de fragmentos de arquivos em cache durante a verificação.

Para modificar um nível de segurança pré-instalado:

clique no botão **Personalizar** na janela de configurações do Antivírus da Web. Na janela que é aberta, edite as configurações de proteção da Web (consulte 9.2 na p. 108) e clique em **OK**.

9.2. Configurando o Antivírus da Web

O Antivírus da Web verifica todos os objetos carregados no computador via HTTP e monitora todos os scripts WSH (JavaScript ou Visual Basic Script, etc.) executados.

Você pode definir várias configurações do Antivírus da Web para aumentar a velocidade de funcionamento do componente, mais especificamente:

- Definir o algoritmo de verificação, selecionando um conjunto completo ou limitado de assinaturas de ameaças
- Criar uma lista de endereços da Web confiáveis

Também é possível selecionar as ações que o Antivírus da Web executará em resposta à descoberta de objetos HTTP perigosos.

As seções a seguir examinam estas configurações detalhadamente.

9.2.1. Configurando um método de verificação

Você pode verificar os dados da Internet usando um dos seguintes algoritmos:

- *Verificação contínua* – este método para a detecção de código mal-intencionado no tráfego de rede verifica os dados em trânsito: conforme o

arquivo é baixado da Internet, o Antivírus da Web verifica as partes do arquivo, liberando o objeto verificado mais rápido para o usuário. Ao mesmo tempo, um conjunto limitado de assinaturas de ameaças é usado para executar verificações contínuas (apenas as ameaças mais ativas), o que reduz significativamente o nível de segurança para usar a Internet.

- *Verificação de buffering* – este método verifica objetos apenas depois de eles terem sido baixados integralmente para o buffer. Após a conclusão da verificação, o programa passa o objeto para o usuário ou o bloqueia.
  Ao usar este tipo de verificação, o conjunto completo de assinaturas de ameaças é usado, o que aumenta o nível de detecção de códigos mal-intencionados. Contudo, o uso desse algoritmo aumenta o tempo de processamento do objeto, tornando a navegação na Web mais lenta: ele também pode gerar problemas ao copiar e processar objetos grandes, pois a conexão com o cliente HTTP pode atingir o tempo limite.
  Uma maneira de resolver este problema é limitar o tempo de armazenamento em cache dos fragmentos de objetos baixados da Internet. Quando o limite de tempo expirar, o usuário receberá a parte baixada do arquivo sem ela ter sido verificada e, assim que o objeto tiver sido totalmente copiado, ele será verificado em sua totalidade. Isto pode fazer o objeto ser entregue ao usuário mais rapidamente e solucionar o problema da interrupção da conexão, sem reduzir a segurança ao usar a Internet.

Para selecionar o algoritmo de verificação que o Antivírus da Web irá usar:

1. Clique no botão **Personalizar** na janela de configurações do Antivírus da Web.
2. Na janela que é aberta (veja a fig. 30), selecione a opção desejada na seção **Método de varradura**.

Por padrão, o Antivírus da Web executa uma verificação de buffering nos os dados da Internet e usa o conjunto completo de assinaturas de ameaças. O tempo de armazenamento de fragmentos de arquivos em cache é de um segundo.

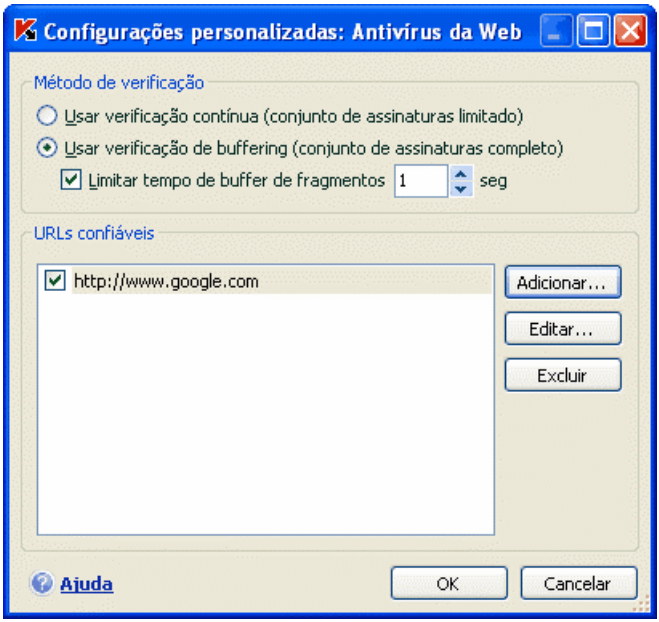


Figura 30. Configurando o Antivírus da Web

Aviso!
Se você tiver problemas ao acessar recursos como o rádio pela Internet, vídeo contínuo ou conferência pela Internet, use a verificação contínua.

9.2.2. Criando uma lista de endereços confiáveis

Você pode criar uma lista de endereços confiáveis, em cujo conteúdo você confia totalmente. O Antivírus da Web não analisará os dados desses endereços quanto à presença de objetos perigosos. Este recurso poderá ser usado quando o Antivírus da Web impedir o download de um determinado arquivo, bloqueando-o.

Para criar uma lista de endereços confiáveis:

1. Clique no botão **Personalizar** na janela de configurações do Antivírus da Web.
2. Na janela que é aberta (veja a fig. 30), crie uma lista de servidores confiáveis na seção **URLs confiáveis**. Para fazê-lo, use os botões à direita da lista.

Ao inserir um endereço confiável, você pode criar máscaras com os seguintes caracteres curinga:

***** – qualquer combinação de caracteres.

Exemplo: Se você criar a máscara ***abc***, nenhuma URL que contém **abc** será verificada. Por exemplo: www.virus.com/download_virus/page_0-9abcdef.html

? – qualquer caractere.

Exemplo: Se você criar a máscara **Patch_123?.com**, as URLs que contêm essa série de caracteres, mais qualquer caractere depois do 3, não serão verificadas. Por exemplo: **Patch_1234.com**. Entretanto, **patch_12345.com** será verificado.

Se um * ou ? fizer parte de uma URL real adicionada à lista, quando você as inserir, use uma barra invertida para substituir o * ou ? que vem em seguida.

Exemplo: Você deseja adicionar esta URL à lista de endereços confiáveis: www.virus.com/download_virus/virus.dll?virus_name=

Para que o Kaspersky Anti-Virus não processe o **?** como um caractere curinga, coloque uma barra invertida (\) antes dele. Então, a URL que você está adicionando à lista de exclusões será a seguinte: www.virus.com/download_virus/virus.dll\?virus_name=

9.2.3. Restaurando as configurações padrão do Antivírus da Web

Ao configurar o Antivírus da Web, você sempre pode retornar para as configurações de desempenho padrão, consideradas ideais pela Kaspersky Lab, que as combinou no nível de segurança **Recomendado**.

Para restaurar as configurações padrão do Antivírus da Web:

1. Selecione **Antivírus da Web** na janela principal e vá para a janela de configurações do componente clicando em Configurações.
2. Clique no botão **Padrão** na seção **Nível de segurança**.

9.2.4. Selecionando respostas para objetos perigosos

Se a análise de um objeto HTTP demonstrar que ele contém código mal-intencionado, a resposta do Antivírus da Web dependerá das ações selecionadas.

Para configurar as reações do Antivírus da Web à detecção de um objeto perigoso:

Abra a janela de configurações do Kaspersky Anti-Virus e selecione **Antivírus da Web**. As possíveis respostas para objetos perigosos estão relacionadas na seção **Ação** (veja a fig. 31).

Por padrão, ao detectar um objeto HTTP perigoso, o Antivírus da Web exibe um aviso na tela e oferece várias opções de ação sobre o objeto.

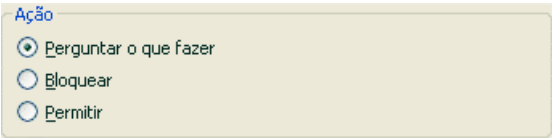


Figura 31. Selecionando ações para scripts perigosos

As opções possíveis para processar objetos HTTP perigosos são as seguintes.

Se a ação selecionada for	Se um objeto perigoso for detectado no tráfego HTTP
Perguntar o que fazer	O Antivírus da Web emitirá uma mensagem de aviso com informações sobre o código mal-intencionado que possivelmente infectou o objeto e lhe dará opções de resposta.
Bloquear	O Antivírus da Web bloqueará o acesso ao objeto e exibirá uma mensagem na tela sobre o bloqueio. Informações semelhantes serão registradas no relatório (consulte 14.3 na p. 173).
Permitir	O Antivírus da Web concederá o acesso ao objeto. Essas informações são registradas no relatório.

O Antivírus da Web sempre bloqueia scripts perigosos e emite mensagens pop-up que informam o usuário sobre a ação executada. Você não pode alterar a resposta a scripts perigosos, além de desabilitar o módulo de verificação do script.

CAPÍTULO 10. DEFESA PROATIVA

Aviso!

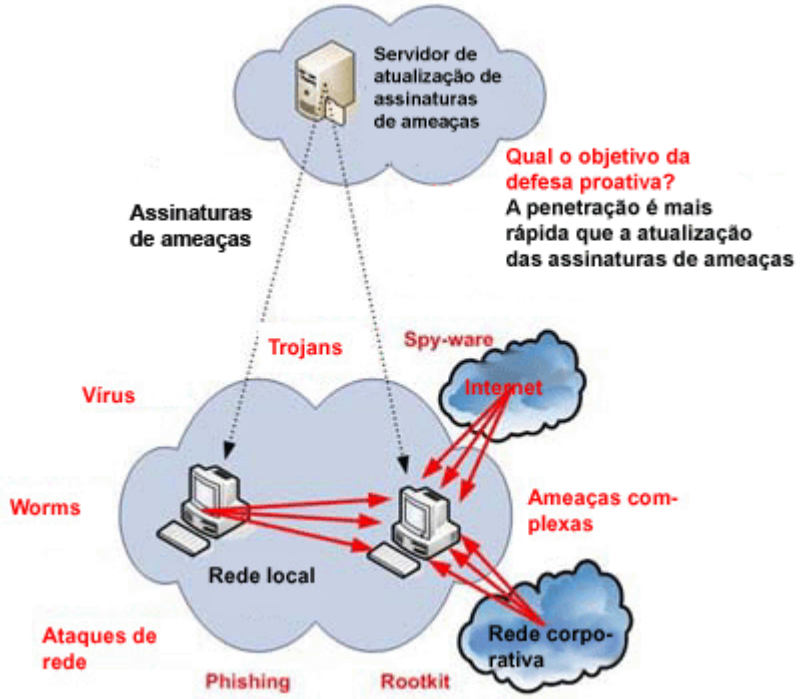
Esta versão do aplicativo não possui o componente de defesa proativa: não há componentes de Defesa Proativa nesta versão do aplicativo (**Controle de integridade do aplicativo** e **Proteção do Microsoft Office**) para computadores que executam o Microsoft Windows XP Professional x64 Edition, o Microsoft Windows Vista ou o Microsoft Windows Vista x64.

O Kaspersky Anti-Virus o protege de ameaças conhecidas e novas, sobre as quais não há informações nas assinaturas de ameaças. Isso é assegurado por um componente desenvolvido especialmente, a *Defesa Proativa*.

A Defesa Proativa se tornou mais necessária na medida em que os programas começaram a se disseminar mais rápido do que é possível lançar atualizações de antivírus para neutralizá-los.

A técnica reativa, na qual se baseia a proteção antivírus, exige que uma nova ameaça infecte pelo menos um computador e precisa de tempo para analisar o código mal-intencionado e adicioná-lo às assinaturas de ameaças e para atualizar o banco de dados nos computadores dos usuários. Até então, a nova ameaça pode ter causado danos enormes.

As tecnologias preventivas fornecidas pela Defesa Proativa do Kaspersky Anti-Virus não exigem tanto tempo quanto a técnica reativa e neutralizam novas ameaças antes que elas danifiquem seu computador. Como isso é feito? Diferentemente das tecnologias reativas, que analisam o código usando um banco de dados de assinaturas de ameaças, as tecnologias preventivas reconhecem uma nova ameaça no computador por meio da seqüência de ações executadas por um determinado programa. A instalação do aplicativo inclui um conjunto de critérios que podem ajudar a determinar a periculosidade da atividade de um programa. Se a análise da atividade determinar que as ações de um determinado programa são suspeitas, o Kaspersky Anti-Virus executará as ações atribuídas pela regra para esse tipo de atividade.



A atividade perigosa é determinada pelo comportamento geral do programa. 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 e, em seguida, enviar várias cópias de si mesmo, é muito provável que se trate de um worm. O comportamento perigoso também inclui:

- Alterações do sistema de arquivos
- Incorporação de módulos em outros processos
- Mascaramento de processos no sistema
- Modificação de determinadas chaves do Registro do sistema do Microsoft Windows

A Defesa Proativa controla e bloqueia todas as operações perigosas. A Defesa Proativa também controla todas as macros executadas em aplicativos do Microsoft Office.

A Defesa Proativa usa um conjunto de regras fornecidas com o aplicativo, além de regras definidas pelo usuário criadas durante o uso do mesmo. Uma *regra* é

um conjunto de critérios que define o comportamento suspeito e como o Kaspersky Anti-Virus deve reagir a ele.

São fornecidas regras individuais para a atividade de aplicativos e para monitorar alterações ao Registro do sistema, macros e programas executados no computador. Você pode alterar as regras conforme queira, adicionando, excluindo ou editando-as. As regras podem bloquear ações ou conceder permissões.

Vamos examinar os algoritmos da Defesa Proativa:

1. Imediatamente depois que o computador é iniciado, a Defesa Proativa analisa os seguintes fatores, usando o conjunto de regras e exclusões:

    - *Ações de cada aplicativo em execução no computador*. A Defesa Proativa grava um histórico de ações executadas em ordem e as compara com seqüências características de atividades perigosas (um banco de dados de tipos de atividades perigosas é fornecido com o programa, sendo atualizado com as assinaturas de ameaças).

    - As *ações de cada macro em VBA executada* são analisadas quanto a sinais de atividade mal-intencionada.

    - A *integridade dos módulos dos programas* instalados no computador, que detecta a substituição de módulos de programas por versões com códigos mal-intencionados incorporados neles.

    - *Cada tentativa de editar o Registro do sistema* (excluindo ou adicionando chaves do Registro do sistema, inserindo valores em chaves em um formato inadmissível ou impedindo que sejam exibidos ou editados, etc.).

2. A análise é realizada usando as regras de permissão e bloqueio da Defesa Proativa.

3. Depois da análise, existem três medidas a serem tomadas:

    - Se a atividade satisfizer às condições da regra de permissão da Defesa Proativa ou não corresponder a nenhuma regra de bloqueio, ela não será bloqueada.

    - Se a atividade for definida como perigosa de acordo com os critérios relevantes, as próximas etapas executadas pelo componente corresponderão às instruções especificadas na regra: geralmente, a atividade é bloqueada. Será exibida uma mensagem na tela especificando o programa perigoso, seu tipo de atividade e um histórico das ações executadas. Aceite a decisão, bloqueie ou permita essa atividade. Você pode criar

uma regra para a atividade e cancelar as ações executadas no sistema.

10.1. Configurações da Defesa Proativa

As categorias de configurações (veja a fig. 32) do componente Defesa Proativa são as seguintes:

- *Se a atividade de aplicativos é monitorada no seu computador*

  Este recurso da Defesa Proativa é habilitado marcando a caixa **Habilitar Verificador de atividade do aplicativo**. Esse modo é habilitado por padrão, o que assegura que as ações de todos os programas abertos no computador serão cuidadosamente controladas e comparadas com uma lista configurável de atividades perigosas. Você pode configurar a ordem de processamento dos aplicativos (consulte 10.1.1 na p. 118) para essa atividade. Também é possível criar exclusões da Defesa Proativa que interrompem a monitoração de aplicativos selecionados.

- *Se o Controle de integridade do aplicativo está habilitado*

  Este recurso é responsável pela integridade dos módulos de aplicativos (bibliotecas de vínculos dinâmicos ou DLLs) instalados no computador, sendo habilitado marcando a caixa **Controle de integridade do aplicativo**. A integridade é controlada pelo monitoramento dos módulos do programa e do próprio programa. Você pode criar regras de controle de integridade para os módulos de qualquer aplicativo. Para fazê-lo, adicione o aplicativo à lista de aplicativos monitorados.

  Este componente da Defesa Proativa não está disponível no Microsoft Windows XP Professional x64 Edition, no Microsoft Windows Vista ou no Microsoft Windows Vista x64.

- *Se as alterações do Registro do sistema são monitoradas*

  Por padrão, **Habilitar Proteção do Registro** está marcado, o que significa que o Kaspersky Anti-Virus analisa todas as tentativas de alterar as chaves do Registro do sistema do Windows.

  Você pode criar suas próprias regras (consulte 0 na p. 131) para monitorar o Registro, dependendo da chave do Registro do Microsoft Windows.

- *Se as macros são verificadas*

O monitoramento de macros VBA no computador é controlado marcando a caixa **Habilitar Proteção do Microsoft Office**, que é marcada por padrão.

Você pode selecionar quais macros são consideradas perigosas e o que fazer com elas (consulte 10.1.3 na p. 125).

Este componente da Defesa Proativa não está disponível no Microsoft Windows XP Professional x64 Edition, no Microsoft Windows Vista ou no Microsoft Windows Vista x64.

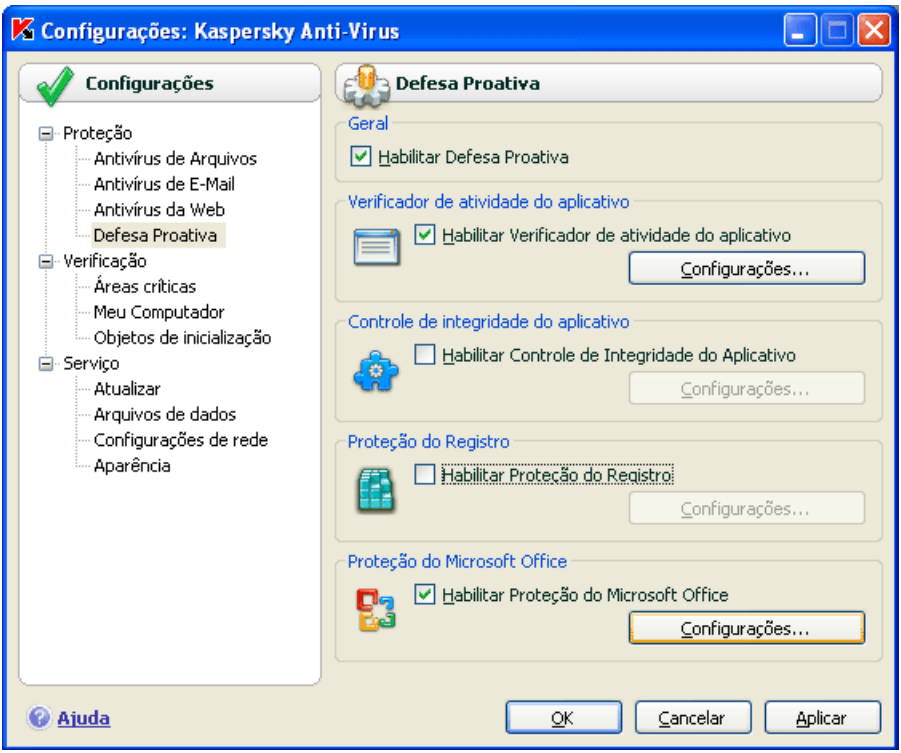


Figura 32. Configurações da Defesa Proativa

É possível configurar exclusões (consulte 6.3.1 na p. 65) para os módulos da Defesa Proativa e criar uma lista de aplicativos confiáveis (consulte 6.3.2 na p. 70).

As seções a seguir examinam estes aspectos mais detalhadamente.

10.1.1. Regras de controle de atividades

Observe que a configuração do controle de aplicativos no Microsoft Windows XP Professional x64 Edition, no Microsoft Windows Vista ou no Microsoft Windows Vista x64 é diferente do processo de configuração em outros sistemas operacionais.
Informações sobre a configuração do controle de atividade nesses sistemas operacionais são fornecidas no final desta seção.

O Kaspersky Anti-Virus monitora a atividade dos aplicativos no computador. O aplicativo inclui um conjunto de descrições de eventos que podem ser consideradas perigosas. Uma regra de monitoramento é criada para cada um desses eventos. Se a atividade de qualquer aplicativo for classificada como um evento perigoso, a Defesa Proativa seguirá rigorosamente as instruções definidas na regra desse evento.

Marque a caixa de seleção **Habilitar Verificador de atividade do aplicativo** se desejar monitorar a atividade dos aplicativos.

Vamos examinar vários tipos de eventos que ocorrem no sistema e que o aplicativo considerará suspeitos:

- *Atividade perigosa (análise de comportamento)*. O Kaspersky Anti-Virus analisa a atividade dos aplicativos instalados no computador e, com base na lista de regras criadas pela Kaspersky Lab, detecta ações perigosas ou suspeitas dos programas. Essas ações incluem, por exemplo, a instalação dissimulada ou a cópia de programas.
- *Abrir o navegador com configurações*. Por meio da análise desse tipo de atividade, é possível detectar tentativas de abrir um navegador com configurações. Essa atividade é característica da abertura de um navegador da Web de um aplicativo com determinadas configurações do prompt de comando: por exemplo, quando você clicar em um link para uma determinada URL em um e-mail de publicidade.
- *Intrusos no processo* – adição de código executável ou criação de um fluxo adicional para o processo de um determinado programa. Esta atividade é amplamente utilizada pelos cavalos de Tróia.
- *Aparição de processos dissimulados (Rootkit)*. O rootkit é um conjunto de programas usados para dissimular programas mal-intencionados e seus processos no sistema. O Kaspersky Anti-Virus analisa o sistema operacional quanto à presença de processos dissimulados.
- *Invasores*. Esta atividade é usada em tentativas de ler senhas e outras informações confidenciais exibidas em caixas de diálogo do sistema operacional. O Kaspersky Anti-Virus rastreará essa atividade, se houver tentativas de interceptar dados transferidos entre o sistema operacional e a caixa de diálogo.

- *Valores suspeitos no Registro*. O Registro do sistema consiste em um banco de dados para armazenar as configurações do usuário e do sistema que controlam a operação do Windows, além dos utilitários instalados no computador. Ao tentar dissimular sua presença no sistema, os programas mal-intencionados copiam valores incorretos nas chaves do Registro. O Kaspersky Anti-Virus analisa as entradas do Registro do sistema quanto à presença de valores suspeitos.
- *Atividade do sistema suspeita*. O programa analisa as ações executadas pelo Microsoft Windows e exclui as atividades suspeitas. Um exemplo de atividade suspeita seria uma violação de integridade, que envolve a modificação de um ou vários módulos de um aplicativo monitorado desde sua última execução.
- *Keyloggers (Registradores de uso do teclado)*. Esta atividade é usada em tentativas de ler senhas e outras informações confidenciais que você inseriu usando o teclado por programas mal-intencionados.
- *Proteção do Gerenciador de Tarefas do Microsoft Windows*. O Kaspersky Anti-Virus protege o Gerenciador de Tarefas da infiltração de módulos mal-intencionados, quando seu objetivo é bloquear o funcionamento do Gerenciador de Tarefas.

A lista de atividades perigosas pode ser ampliada automaticamente pelo processo de atualização do Kaspersky Anti-Virus, mas não pode ser editada pelo usuário. Você pode:

- Desativar o monitoramento de uma atividade desmarcando o ☑ ao lado de seu nome
- Editar a regra usada pela Defesa Proativa ao detectar a atividade perigosa
- Criar uma lista de exclusões (consulte 6.3 na p. 64) relacionando os aplicativos com atividades que você não considera perigosas.

Para configurar o monitoramento de atividades,

1. Abra a janela de configurações do Kaspersky Anti-Virus clicando em Configurações na janela principal do programa.
2. Selecione **Defesa Proativa** na árvore de configurações.
3. Clique no botão **Configurações** na seção **Verificador de atividade do aplicativo**.

Os tipos de atividade monitorados pela Defesa Proativa estão listados na janela **Configurações: Verificador de atividade do aplicativo** (veja a fig. 33).

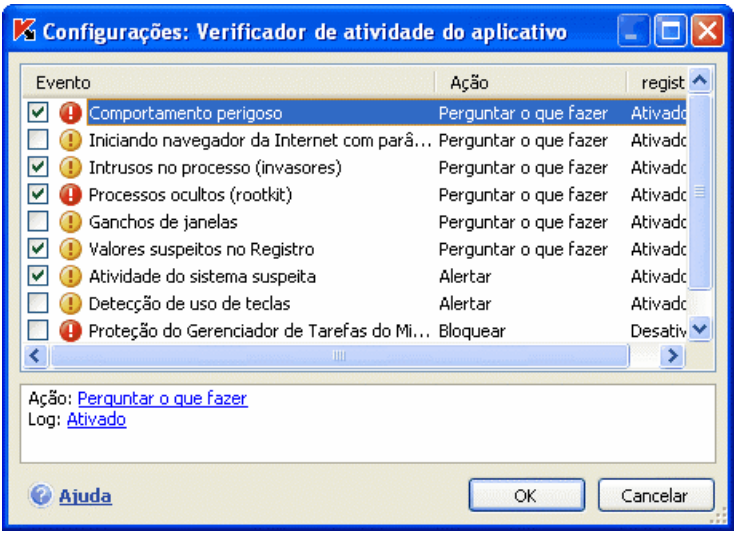


Figura 33. Configurando o controle da atividade de aplicativos

Para editar uma regra de monitoramento de atividade perigosa, selecione-a na lista e atribua a configurações da regra na parte inferior da guia:

- Atribua a resposta da Defesa Proativa à atividade perigosa.
- Você pode atribuir qualquer das seguintes ações como resposta: permitir, perguntar o que fazer e encerrar o processo. Clique no link da ação até que ele chegue ao valor desejado. Além de interromper o processo, você pode colocar o aplicativo que iniciou a atividade perigosa em Quarentena. Para fazê-lo, use o link Ligado / Desligado de acordo com a configuração apropriada. É possível atribuir um período para a freqüência com que a verificação será executada para detectar processos ocultos no sistema.
- Escolha se deseja gerar um relatório sobre a operação executada. Para fazê-lo, clique no link **Log** até ele mostrar Ligado ou Desligado, conforme o desejado.

Para desativar o monitoramento de uma atividade perigosa, desmarque o ☑ ao lado de seu nome na lista.

Especificidades da configuração do controle de atividade de aplicativos do Kaspersky Anti-Virus no Microsoft Windows XP Professional x64 Edition, no Microsoft Windows Vista ou no Microsoft Windows Vista x64:

Se você estiver executando um dos sistemas operacionais listados acima, apenas um tipo de evento do sistema será controlado, a atividade perigosa

(análise de comportamento). Se desejar que o Kaspersky Anti-Virus monitore as modificações das contas de usuário do sistema, além da atividade perigosa, marque a caixa de seleção ☑ **Examinar contas de usuário do sistema** (veja a 34).

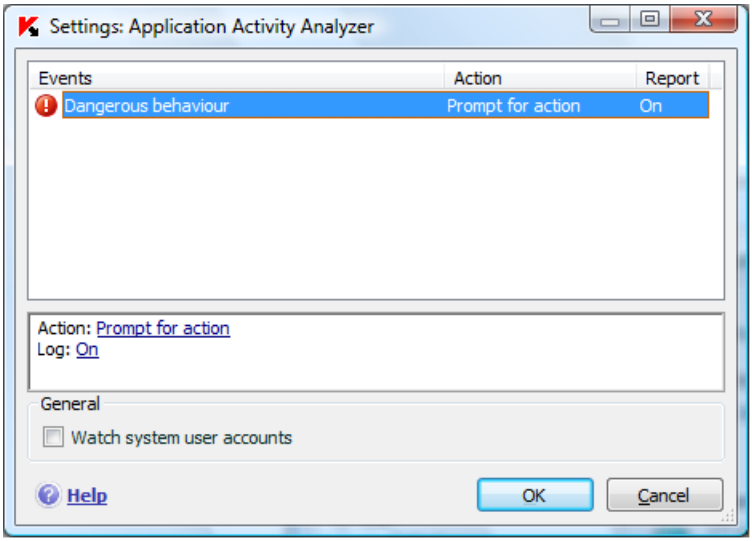


Figura 34. Configurando o controle de integridade de aplicativos no Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista e Microsoft Windows Vista x64

10.1.2. Controle de integridade do aplicativo

Este componente da Defesa Proativa não funciona no Microsoft Windows XP Professional x64 Edition, no Microsoft Windows Vista ou no Microsoft Windows Vista x64.

Existem vários programas críticos para o sistema que poderiam ser usados por programas mal-intencionados em sua distribuição, como navegadores, programas de e-mail, etc. Normalmente, são os aplicativos do sistema e processos usados para acessar a Internet e trabalhar com e-mail e outros documentos. Por isso, esses aplicativos são considerados *críticos* no controle de atividades.

A Defesa Proativa monitora cuidadosamente esses aplicativos críticos, analisando sua atividade e observando outros processos iniciados por eles. O Kaspersky Anti-Virus é fornecido com uma lista de aplicativos críticos e uma

regra de monitoramento criada cada um, controlando a atividade do aplicativo. Você pode adicionar a essa lista outros aplicativos críticos, além de excluir ou editar as regras dos aplicativos da lista fornecida.

Além da lista de aplicativos críticos, existe um conjunto de módulos confiáveis que podem ser abertos em todos os aplicativos controlados. Por exemplo, os módulos assinados digitalmente pela Microsoft Corporation. É altamente improvável que esses módulos sejam mal-intencionados, então não é necessário monitorá-los cuidadosamente, o que, por sua vez, diminui a carga no computador ao usar a Defesa Proativa.

Os componentes com assinaturas da Microsoft são designados automaticamente como aplicativos confiáveis. Se necessário, você pode adicionar ou excluir componentes da lista.

Os processos de monitoramento e sua integridade no sistema são habilitados marcando a caixa **Habilitar Controle de integridade do aplicativo** na janela de configurações da Defesa Proativa: por padrão, a caixa está desmarcada. Se você habilitar este recurso, cada aplicativo ou módulo de aplicativo aberto será verificado com relação à lista de aplicativos críticos e confiáveis. Se o aplicativo estiver na lista de aplicativos críticos, sua atividade será controlada pela Defesa Proativa, de acordo com a regra criada para ele.

Para configurar o Controle de integridade do aplicativo:

1. Abra a janela de configurações do Kaspersky Anti-Virus clicando em Configurações na janela principal do programa.
2. Selecione **Defesa Proativa** na árvore de configurações.
3. Clique no botão **Configurações** na caixa **Controle de integridade do aplicativo**.

Vamos examinar o trabalho com processos críticos e confiáveis mais detalhadamente.

Configurando regras do Controle de integridade do aplicativo

Os *aplicativos críticos* são arquivos executáveis de programas cujo monitoramento é extremamente importante, pois os arquivos mal-intencionados os utilizam para se distribuírem.

Uma lista dos aplicativos críticos foi criada na instalação do aplicativo, sendo mostrada na guia **Aplicativos críticos** (veja a fig. 35): cada aplicativo possui sua própria regra de monitoramento que regula seu comportamento. Você pode editar as regras existentes e criar as suas próprias.

A Defesa Proativa analisa as seguintes operações envolvendo aplicativos críticos: o início deles, a alteração do conteúdo de módulos dos aplicativos e o início de um aplicativo como um processo filho. Você pode selecionar a resposta da Defesa Proativa a cada uma das operações relacionadas (permitir ou bloquear a operação) e também especificar se a atividade será registrada no relatório do componente. As configurações padrão permitem que as operações mais críticas iniciem, editem ou sejam iniciadas como processos filho.

Para adicionar um aplicativo à lista de aplicativos críticos e criar uma regra para ele:

1. Clique em **Adicionar** na guia **Aplicativos críticos**. Um menu de contexto será aberto: clique em **Procurar** para abrir a janela de seleção de arquivos padrão ou clique em **Aplicativos** para ver uma lista dos aplicativos ativos no momento e selecionar um deles, conforme desejado. O novo aplicativo será adicionado ao início da lista e regras de **permissão** (ou seja, todas as atividades serão permitidas) serão criadas para ele, por padrão. Quando esse aplicativo for iniciado pela primeira vez, os módulos que ele acessa serão adicionados à lista e, de forma semelhante, esses módulos receberão regras de **permissão**.

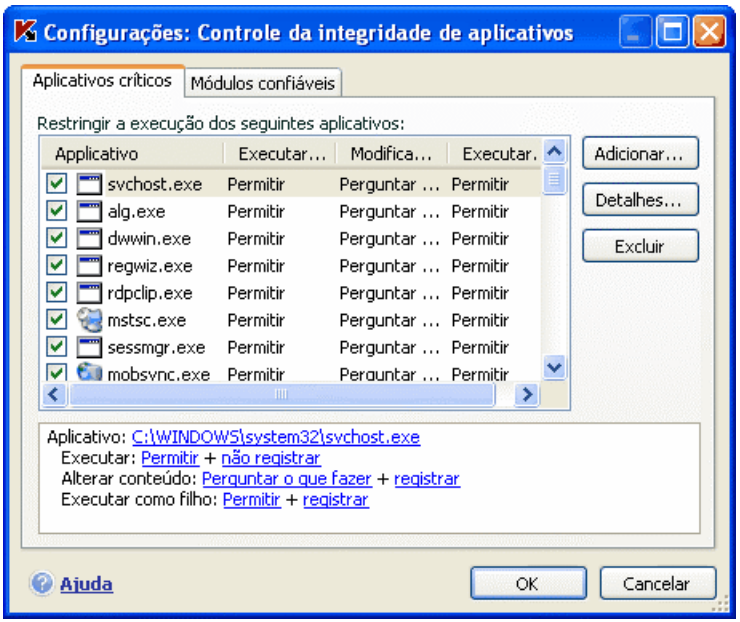


Figura 35. Configurando o Controle de integridade do aplicativo

2. Selecione uma regra na lista e atribua configurações a ela na parte inferior da guia:

- Defina a resposta da Defesa Proativa a tentativas de executar o aplicativo crítico, alterar seu conteúdo ou iniciá-lo como um processo filho.

  Você pode usar qualquer das seguintes ações como resposta: permitir, perguntar o que fazer ou bloquear. Clique no link da ação até que ele chegue ao valor desejado.

- Escolha se deseja gerar um relatório sobre a atividade, clicando em registrar / não registrar.

Para desativar o monitoramento da atividade de um aplicativo, desmarque o ☑ ao lado de seu nome.

Use o botão **Detalhes** para exibir uma lista detalhada de módulos do aplicativo selecionado. A janela **Configurações: módulos do aplicativo** contém uma lista dos módulos usados quando um aplicativo monitorado é iniciado. É possível completar e editar a lista usando os botões **Adicionar** e **Excluir** à direita da janela.

Você também pode permitir que os módulos de qualquer aplicativo controlado sejam carregados, ou pode bloqueá-los. Por padrão, uma regra de permissão é criada para cada módulo. Para modificar a ação, selecione o módulo na lista e clique no botão **Modificar**. Selecione a ação desejada na janela que é aberta.

Observe que o treinamento do Kaspersky Anti-Virus vai da primeira vez em que você executa o aplicativo controlado após a instalação do programa até o encerramento do aplicativo. O processo de treinamento produz uma lista de módulos usados pelo aplicativo. As regras do Controle de integridade serão aplicadas na próxima vez em que o aplicativo for executado.

Criando uma lista de componentes compartilhados

O Kaspersky Anti-Virus inclui uma lista de componentes que podem ser abertos por todos os aplicativos controlados. Você encontrará essa lista na guia **Módulos confiáveis** (veja a fig. 36). Ela inclui módulos usados pelo Kaspersky Anti-Virus e componentes assinados pela Microsoft; o usuário pode adicionar ou remover componentes.

Se você instalar programas no computador, pode assegurar que aqueles com módulos assinados pela Microsoft sejam adicionados automaticamente à lista de módulos confiáveis. Para fazê-lo, marque ☑ **Adicionar automaticamente componentes assinados pela Microsoft Corporation a esta lista**. Então, se um aplicativo controlado tentar abrir o módulo assinado pela Microsoft, a Defesa Proativa permitirá automaticamente que o módulo seja carregado sem ser verificado e ele será adicionado à lista de componentes compartilhados.

Para completar a lista de módulos confiáveis, clique em **Adicionar** e, na janela de seleção de arquivos padrão, selecione o módulo.

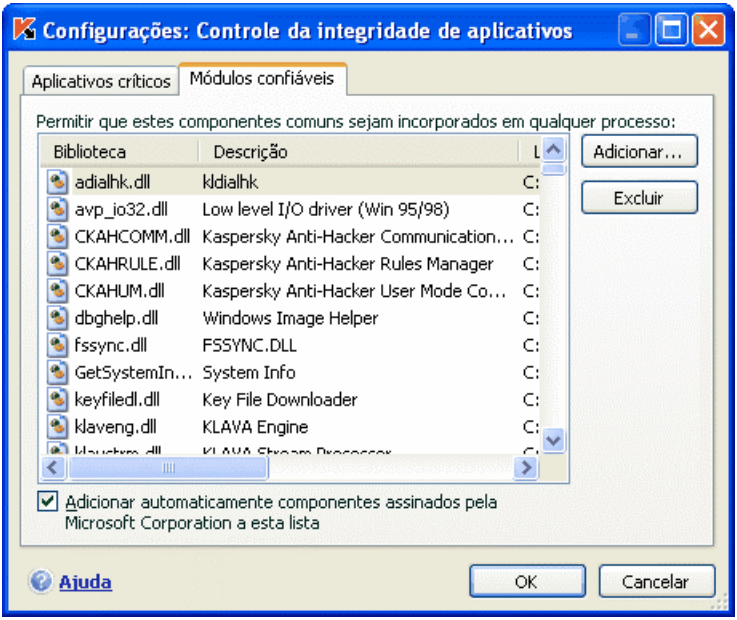


Figura 36. Configurando a lista de módulos confiáveis

10.1.3. Proteção do Microsoft Office

Este componente da Defesa Proativa não funciona no Microsoft Windows XP Professional x64 Edition, no Microsoft Windows Vista ou no Microsoft Windows Vista x64.

Você pode habilitar a verificação e o processamento de macros perigosas executadas no computador marcando ☑ **Habilitar Proteção do Microsoft Office** (veja a fig. 32). Por padrão, a caixa de seleção está marcada e a atividade de cada execução de macro é controlada com relação a comportamentos perigosos. Se for detectada alguma atividade suspeita, a Defesa Proativa permitirá ou bloqueará a macro.

Exemplo:

> A macro *PDFMaker* é um plug-in da barra de ferramentas do Adobe Acrobat no Microsoft Office Word que pode criar um arquivo .pdf a partir de qualquer documento. A Defesa Proativa classifica a incorporação de elementos no software como uma ação perigosa. Se a Proteção do

Microsoft Office estiver habilitada, quando uma macro for carregada, a Defesa Proativa emitirá um aviso na tela, informando que foi detectado um comando de macro perigoso. Você pode escolher encerrar a macro ou permitir que continue.

Você pode configurar as reações do Kaspersky Anti-Virus às macros que executam comportamentos suspeitos. Se tiver certeza de que uma macro não é perigosa ao trabalhar com um arquivo específico, por exemplo, um documento do Microsoft Word, é recomendável criar uma regra de exclusão. Se ocorrer uma correspondência com os termos da regra de exclusão, a ação suspeita executada pela macro não será processada pela Defesa Proativa.

Para configurar a Proteção do Microsoft Office:

1. Abra a janela de configurações do Kaspersky Anti-Virus clicando em Configurações na janela principal do programa.
2. Selecione **Defesa Proativa** na árvore de configurações.
3. Clique no botão **Configurações** na caixa **Proteção do Microsoft Office**.

As regras para o processamento de macros perigosas são configuradas na janela **Proteção do Microsoft Office** (veja a fig. 37). Ela contém regras padrão para comportamentos classificados pela Kaspersky Lab como perigosos. Essas ações de macros perigosas incluem, por exemplo, a incorporação de módulos em programas e a exclusão de arquivos.

Se você não considerar que um comportamento da lista seja perigoso, desmarque a caixa ao lado de seu nome. Por exemplo, talvez freqüentemente você use macros para abrir arquivos (não como somente leitura) e tem certeza de que essa operação não é mal-intencionada.

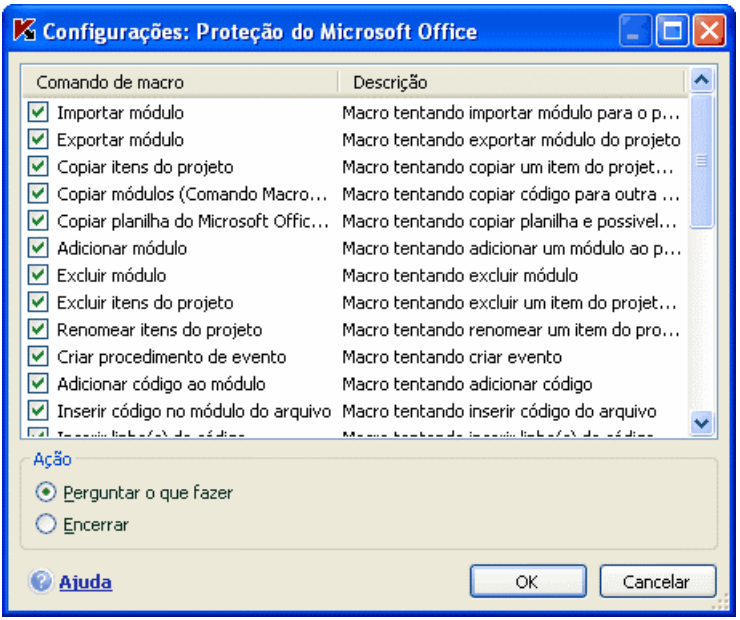


Figura 37. Configurando a Proteção do Microsoft Office

Para que o Kaspersky Anti-Virus não bloqueie a macro:

desmarque a caixa ao lado da ação. O programa não considerará mais este comportamento como perigoso e a Defesa Proativa não o processará.

Por padrão, sempre que o programa detectar uma ação iniciada por uma macro no computador, ele perguntará se você deseja permitir ou bloquear a macro.

Para que o programa bloqueie automaticamente todos os comportamentos perigosos sem perguntar o que fazer:

Na janela com a lista de macros, selecione **Encerrar**.

10.1.4. Proteção do Registro

Um dos objetivos de vários programas mal-intencionados é editar o Registro do sistema do Windows no computador. Podem ser piadas inofensivas ou programas mais mal-intencionados que representam uma ameaça grave ao computador.

Por exemplo, os programas mal-intencionados podem copiar suas informações na chave do Registro que faz os aplicativos abrirem automaticamente na

inicialização. Assim, esses programas serão iniciados na inicialização do sistema operacional.

A Defesa Proativa pode detectar ameaças desconhecidas que tentam editar as chaves do Registro no computador. Você pode habilitá-lo marcando a caixa **Habilitar Proteção do Registro** na janela de configurações da **Defesa Proativa**.

Para configurar o monitoramento do Registro do sistema:

1. Abra a janela de configurações do Kaspersky Anti-Virus clicando em Configurações na janela principal do programa.
2. Selecione **Defesa Proativa** na árvore de configurações.
3. Clique no botão **Configurações** na seção **Proteção do Registro**.

A Kaspersky Lab criou uma lista de regras que controlam as operações nos arquivos do Registro e a incluiu no programa. As operações com arquivos do Registro são categorizadas em grupos lógicos como *Segurança do sistema*, *Segurança da Internet*, etc. Cada um desses grupos lista arquivos do Registro do sistema e regras para trabalhar com eles. Essa lista é atualizada juntamente com o resto do aplicativo.

A janela de configurações da **Proteção do Registro** (veja a fig. 38) exibe a lista completa de regras.

Cada grupo de regras tem uma prioridade de execução que pode ser aumentada ou diminuída, usando os botões **Mover para cima** e **Mover para baixo**. Quanto mais alta a posição do grupo na lista, maior a prioridade atribuída a ele. Se um arquivo do Registro fizer parte de vários grupos, a primeira regra aplicada a ele será a do grupo com a prioridade mais alta.

Você pode parar de usar qualquer grupo de regras das seguintes maneiras:

- Desmarque a caixa ao lado do nome do grupo. Então, o grupo de regras permanecerá na lista, mas não será usado.
- Exclua o grupo de regras da lista. Não é recomendável excluir os grupos criados pela Kaspersky Lab, pois eles contêm uma lista dos arquivos do Registro do sistema mais usados por programas mal-intencionados.

Figura 38. Grupos de chaves do registro controlados

Você pode criar seus próprios grupos de arquivos do Registro do sistema monitorados. Para fazê-lo, clique em **Adicionar** na janela de grupos de arquivos.

Execute as seguintes etapas na janela que é aberta:

1. Insira o nome do novo grupo de chaves do Registro para monitorar as chaves do Registro do sistema no campo **Nome**.
2. Selecione a guia **Chaves** e crie uma lista de arquivos do Registro do sistema que serão incluídos no grupo monitorado (consulte 0 na p. 129) para o qual você deseja criar regras. Pode ser apenas uma ou podem ser várias chaves.
3. Selecione a guia **Regras** e crie uma regra para os arquivos (consulte 0 na p. 131) que se aplicará às chaves selecionadas na guia Chaves. Você pode criar várias regras e definir a ordem na qual elas são aplicadas.

Selecionando chaves do Registro para criar uma regra

O grupo de arquivos criado deve conter pelo menos um arquivo do Registro do sistema. A guia **Chaves** mostra a lista de arquivos aos quais as regras se aplicam.

Para adicionar um arquivo do Registro do sistema:

1. Clique no botão **Adicionar** na janela **Editar grupo** (veja a fig. 39).
2. Na janela que é aberta, selecione o arquivo do Registro ou a pasta de arquivos para os quais deseja criar a regra de monitoramento.
3. Especifique o valor do arquivo ou uma máscara para o grupo de arquivos aos quais deseja aplicar a regra no campo **Valor**.
4. Marque **Incluir subchaves** para que a regra seja aplicada a todos os arquivos anexados ao arquivo do Registro listado.

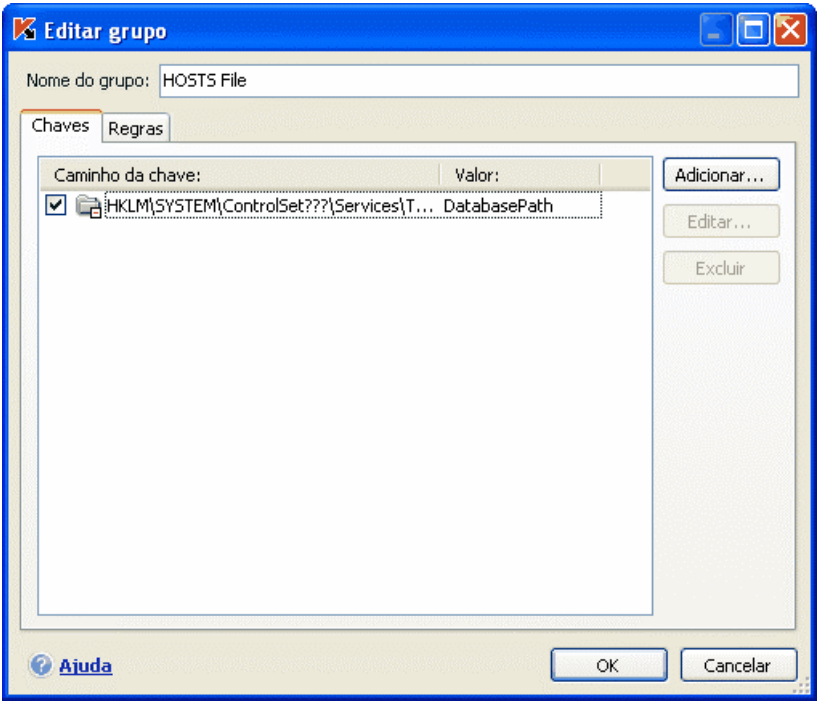


Figura 39. Adicionando chaves do registro controladas

Você só precisa usar máscaras com um asterisco e um ponto de interrogação ao mesmo tempo que o recurso **Incluir subchaves** se os curingas forem usados no nome da chave.

Se você selecionar uma pasta de arquivos do Registro usando uma máscara e especificar um determinado valor para ela, a regra será aplicada a esse valor para qualquer chave no grupo selecionado.

Criando uma regra da Proteção do Registro

Uma regra da Proteção do Registro especifica:

- O programa cujo acesso ao Registro do sistema está sendo monitorado
- A resposta da Defesa Proativa quando um programa tenta executar uma operação com um arquivo do Registro do sistema

Para criar uma regra para os arquivos do Registro do sistema selecionados:

1. Clique em **Nova** na guia **Regras**. A nova regra será adicionada ao início da lista (veja a fig. 40).

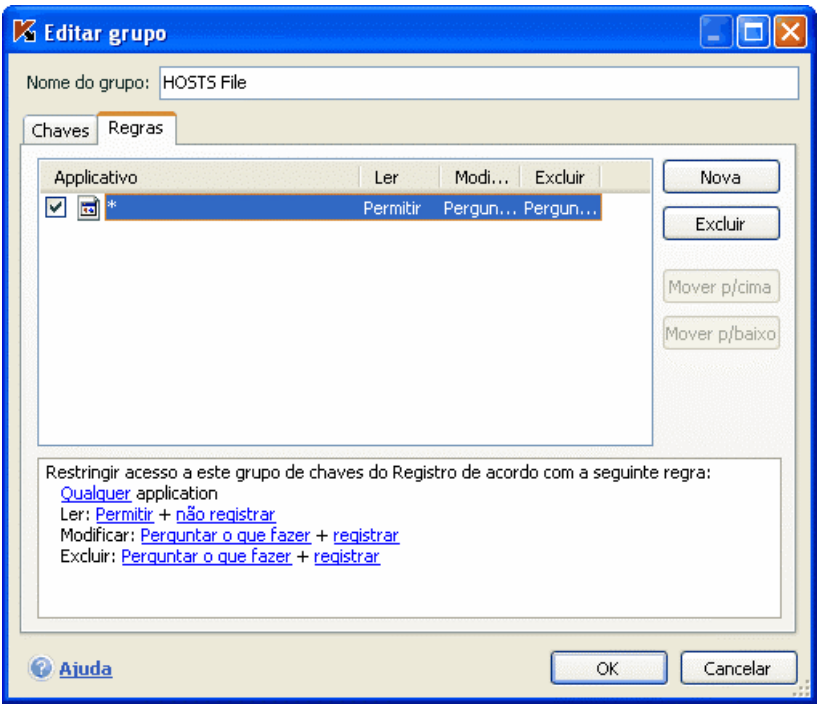


Figura 40. Criando uma regra de monitoramento de chaves do Registro

2. Selecione uma regra na lista e atribua configurações a ela na parte inferior da guia:
    - Especifique o aplicativo.

Por padrão, a regra será criada para qualquer aplicativo. Se desejar que a regra se aplique a um aplicativo específico, clique em qualquer e ele mudará para este. Em seguida, clique no link especificar nome do aplicativo. Um menu de contexto será aberto: clique em **Procurar** para ver a janela de seleção de arquivos padrão ou clique em **Aplicativos** para ver uma lista dos aplicativos abertos e selecionar um deles, conforme desejado.

- Defina a resposta da Defesa Proativa à tentativa do aplicativo selecionado de ler, editar ou excluir arquivos do Registro do sistema.

  Você pode usar qualquer das seguintes ações como resposta: permitir, perguntar o que fazer e bloquear. Clique no link da ação até que ele chegue ao valor desejado.

- Escolha se deseja gerar um relatório sobre a operação executada, clicando no link registrar / não registrar.

Você pode criar várias regras e classificar suas prioridades usando os botões **Mover para cima** e **Mover para baixo**. Quanto mais alta a posição da regra na lista, maior a prioridade atribuída a ela.

Também é possível criar uma regra de *permissão* (ou seja, todas as ações serão permitidas) para um arquivo do Registro do sistema na janela de notificação que informa que o programa está tentando executar uma operação com o arquivo. Para fazê-lo, clique em Criar regra de permissão no aviso e selecione qual será a aplicação da regra na janela que é aberta.

CAPÍTULO 11. VERIFICANDO O COMPUTADOR QUANTO À PRESENÇA DE VÍRUS

Um dos aspectos importantes da proteção do computador é a verificação de vírus em áreas definidas pelo usuário. O Kaspersky Anti-Virus pode verificar itens individuais, arquivos, pastas, discos, dispositivos plug-and-play ou todo o computador. A verificação de vírus impede a disseminação de códigos mal-intencionados não detectados pelos componentes de proteção em tempo real.

O Kaspersky Anti-Virus inclui três tarefas de verificação padrão:

Áreas críticas

Verifica todas as áreas críticas do computador quanto à presença de vírus, incluindo: a memória do sistema, os programas carregados na inicialização, os setores de inicialização no disco rígido e os diretórios do sistema *Windows* e *system32*. A tarefa tem como objetivo detectar vírus ativos rapidamente no sistema sem verificar todo o computador.

Meu Computador

Verifica vírus no computador por meio de uma inspeção completa de todas as unidades de disco, memória e arquivos.

Objetos de inicialização

Verifica vírus em todos os programas carregados na inicialização do sistema operacional.

As configurações padrão dessas tarefas são as recomendadas. É possível editar essas configurações (consulte 11.4.4 na p. 142) ou criar uma programação (consulte 6.5 na p. 75) para a execução das tarefas.

Você também pode criar suas próprias tarefas (consulte 11.4.3 na p. 142) e criar uma programação para elas. Por exemplo, é possível programar uma tarefa de verificação semanal dos bancos de dados de e-mail ou uma tarefa de verificação de vírus na pasta **Meus Documentos**.

Além disso, você pode verificar qualquer objeto quanto à presença de vírus (por exemplo, um disco rígido portátil usado para a transferência de arquivos entre o escritório e sua casa) sem criar uma tarefa de verificação específica. É possível selecionar um objeto para ser verificado na interface do Kaspersky Anti-Virus ou com as ferramentas padrão do sistema operacional Windows (por exemplo, na janela do programa **Explorer** ou na **Área de Trabalho**).

Você pode exibir uma lista completa das tarefas de verificação de vírus no computador clicando em **Verificação** no painel esquerdo da janela principal do programa.

11.1. Gerenciando tarefas de verificação de vírus

Você pode executar uma tarefa de verificação de vírus manual ou automaticamente por meio de uma programação (consulte 6.5 na p. 75).

Para iniciar uma tarefa de verificação de vírus manualmente:

Marque a caixa ao lado do nome da tarefa na seção **Verificação** da janela principal do programa e clique no botão na barra de status.

As tarefas em execução são exibidas no menu de contexto clicando com o botão direito do mouse no ícone da bandeja do sistema.

Para pausar uma tarefa:

Clique no botão na barra de status. O status da tarefa mudará para *em pausa*. A verificação será pausada até ser iniciada manualmente ou ela iniciará automaticamente de acordo com a programação.

Para interromper uma tarefa:

Clique no botão na barra de status. O status da tarefa mudará para *interrompida*. A verificação será interrompida até ser iniciada manualmente ou ela iniciará automaticamente de acordo com a programação. Na próxima vez que você executar a tarefa, o programa perguntará se deseja continuar a tarefa do ponto em que foi interrompida ou iniciá-la novamente.

11.2. Criando uma lista de objetos para verificação

Para exibir uma lista dos objetos que devem ser verificados por uma determinada tarefa, selecione o nome da tarefa (por exemplo, **Meu Computador**) na seção **Verificação** da janela principal do programa. A lista de objetos será exibida à direita da janela, abaixo da barra de status (veja a fig. 41).

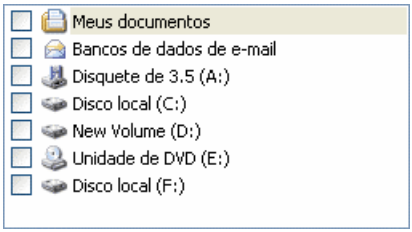


Figura 41. Lista de objetos para verificação

As tarefas padrão já possuem listas de objetos para verificação criadas na instalação do programa. Você pode criar uma lista de objetos ao criar suas próprias tarefas ou selecionar um objeto para uma tarefa de verificação de vírus.

É possível adicionar ou editar uma lista de objetos para verificação usando os botões à direita da lista. Para adicionar um novo objeto para verificação à lista, clique no botão **Adicionar** e, na janela que é aberta, selecione o objeto a ser verificado.

Para sua conveniência, é possível adicionar categorias a uma área de verificação, como bancos de dados de e-mail, RAM, objetos de inicialização, backup do sistema operacional e arquivos da pasta de Quarentena do Kaspersky Anti-Virus.

Além disso, ao adicionar uma pasta que contém objetos incorporados a uma área de verificação, você pode editar a recursão. Para fazê-lo, use o item correspondente no menu de contexto.

Para excluir um objeto, selecione-o na lista (ao fazê-lo, o nome do objeto será realçado em cinza) e clique no botão **Excluir**. É possível desabilitar temporariamente a verificação de objetos individuais para qualquer tarefa sem excluí-los da lista. Para fazê-lo, desmarque a caixa ao lado do objeto que não deseja verificar.

Para iniciar uma tarefa de verificação, clique no botão **Verificação**, selecione **Iniciar** no menu que é aberto ao clicar no botão **Ações**.

Além disso, você pode selecionar um objeto para ser verificado usando as ferramentas padrão do sistema operacional Windows (por exemplo, na janela do programa Explorer ou na Área de Trabalho, etc.) (veja a fig. 42). Para fazê-lo, selecione o objeto, abra o menu de contexto do Windows clicando com o botão direito do mouse e selecione **Verificar vírus**.

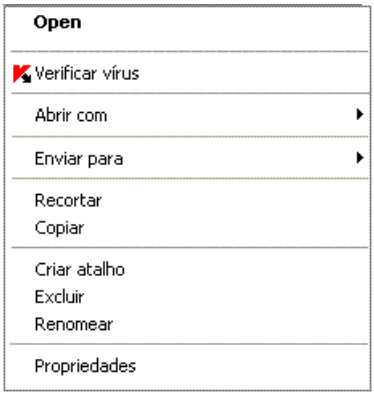


Figura 42. Verificando objetos a partir do menu de contexto do Windows

11.3. Criando tarefas de verificação de vírus

Para verificar objetos no computador quanto à presença de vírus, você pode usar as tarefas de verificação internas incluídas no programa e criar suas próprias tarefas. As novas tarefas de verificação são criadas usando tarefas existentes como modelo.

Para criar uma nova tarefa de verificação de vírus:

1. Selecione a tarefa com as configurações mais próximas do necessário na seção **Verificação** da janela principal do programa.
2. Abra o menu de contexto clicando com o botão direito do mouse no nome da tarefa ou clique no botão **Ações** à direita da lista de objetos para verificação e selecione **Salvar como...**.
3. Insira o nome da nova tarefa na janela que é aberta e clique em **OK**. Uma tarefa com esse nome aparecerá na lista de tarefas na seção **Verificação** da janela principal do programa.

Aviso!

O número de tarefas que podem ser criadas pelo usuário é limitado. O máximo são quatro tarefas.

A nova tarefa é uma cópia daquela na qual foi baseada. É necessário continuar sua configuração por meio da criação de uma lista de objetos para verificação (consulte 11.4.2 na página 139), da configuração de propriedades que controlarão a tarefa (consulte 11.4.4 na página 142) e, se necessário, da

configuração de uma programação (consulte 6.5 na página 75) para executar a tarefa automaticamente.

Para renomear uma tarefa:

Selecione a tarefa na seção **Verificação** da janela principal do programa. Clique com o botão direito do mouse no nome da tarefa para abrir o menu de contexto ou clique no botão **Ações** à direita da lista de objetos para verificação e selecione **Renomear**.

Insira o novo nome da tarefa na janela que é aberta e clique em **OK**. O nome da tarefa também será mudado na seção **Verificação**.

Para excluir uma tarefa:

Selecione a tarefa na seção **Verificação** da janela principal do programa. Clique com o botão direito do mouse no nome da tarefa para abrir o menu de contexto ou clique no botão **Ações** à direita da lista de objetos para verificação e selecione **Excluir**.

Você deverá confirmar que deseja excluir a tarefa. A tarefa será então excluída da lista de tarefas na seção **Verificação**.

Aviso!

É possível renomear e excluir somente as tarefas criadas por você.

11.4. Configurando tarefas de verificação de vírus

Os métodos utilizados para verificar objetos no computador são determinados pelas propriedades atribuídas a cada tarefa.

Para configurar tarefas:

Selecione o nome da tarefa na seção **Verificação** da janela principal. Clique com o botão direito do mouse no nome da tarefa para abrir o menu de contexto ou clique no botão **Ações** à direita da lista de objetos para verificação e selecione **Configurações**.

Você pode usar a janela de configurações de cada tarefa para:

- Selecionar o nível de segurança que será usado pela tarefa (consulte 11.4.1 na p. 138)
- Editar configurações avançadas:
    - definir os tipos de arquivos que devem ser verificados quanto à presença de vírus (consulte 11.4.2 na p. 139)

- configurar o início da tarefa usando um perfil de usuário diferente (consulte 6.4 na p. 74)
- definir as configurações avançadas de verificação (consulte 11.4.5 na p. 144)

- restaurar as configurações padrão de verificação (consulte 11.4.3 na p. 142)
- selecionar uma ação que o programa aplicará ao detectar um objeto infectado ou suspeito (consulte 11.4.4 na p. 142)
- criar uma programação (consulte 6.5 na p. 75) para executar tarefas automaticamente.

Além disso, você pode definir configurações globais (consulte 11.4.6 na p. 146) para executar todas as tarefas.

As seções a seguir examinam detalhadamente as configurações de tarefas listadas acima.

11.4.1. Selecionando um nível de segurança

É possível atribuir um nível de segurança a cada tarefa de verificação de vírus (veja a fig. 43):

Alto – a verificação mais completa de todo o computador ou de discos, pastas ou arquivos individuais. É recomendável usar este nível no caso de suspeita de que um vírus infectou o computador.

Recomendado – os especialistas da Kaspersky Lab recomendam este nível. Serão verificados os mesmos arquivos que na configuração **Alto**, exceto pelos bancos de dados de e-mails.

Baixo – o nível com configurações que permitem usar tranqüilamente aplicativos que consomem muitos recursos, pois o escopo dos arquivos verificados é menor.

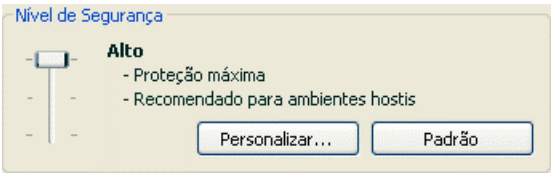


Figura 43. Selecionando um nível de segurança de verificação de vírus

Por padrão, o nível de segurança do Antivírus de Arquivos é definido como **Recomendado**.

Você pode aumentar ou diminuir o nível de segurança da verificação selecionando o nível desejado ou alterando as configurações do nível atual.

Para editar o nível de segurança:

Ajuste os controles deslizantes. Ao ajustar o nível de segurança, você define a taxa da velocidade de verificação com relação ao número total de arquivos verificados: quanto menos arquivos verificados quanto à presença de vírus, maior a velocidade de verificação.

Se nenhum dos níveis de segurança de arquivos atender às suas necessidades, você poderá personalizar as configurações de proteção. Para fazê-lo, selecione o nível mais próximo do necessário como ponto inicial e edite suas configurações. Se o fizer, o nível será renomeado para **Personalizado**.

Para modificar as configurações de um nível de segurança:

clique no botão **Configurações** na janela de configurações de tarefas. Edite as configurações de verificação na janela que é aberta e clique em **OK**.

Como resultado, será criado um quarto nível de segurança, **Personalizado**, que contém as configurações de proteção configuradas.

11.4.2. Especificando os tipos de objetos para verificação

Ao especificar os tipos de objetos que devem ser verificados, você estabelece os formatos, tamanhos e unidades de arquivos nos quais serão verificados vírus quando essa tarefa for executada.

Os tipos de arquivos verificados são definidos na seção **Tipos de arquivos** (veja a fig. 44). Selecione uma das três opções:

- **Verificar todos os arquivos**. Com esta opção, todos os objetos serão verificados, sem exceção.
- **Verificar programas e documentos (por conteúdo)**. Se você selecionar este grupo de programas, apenas os arquivos possivelmente infectados serão verificados; aqueles nos quais um vírus poderia ter se infiltrado.

Observação:
Existem arquivos nos quais os vírus não podem se inserir, pois em seu conteúdo não há nada onde o vírus possa se prender. Um exemplo são os arquivos .txt.

Por outro lado, há formatos de arquivos que contêm ou podem conter código executável. Por exemplo, os formatos .exe, .dll ou .doc. O risco de inserção e ativação de código mal-intencionado nesses arquivos é bastante alto.

Antes de pesquisar um objeto quanto à presença de vírus, seu cabeçalho interno é analisado com relação ao formato do arquivo (txt, doc, exe, etc.).

- **Verificar programas e documentos (por extensão)**. Nesse caso, o programa verificará apenas os arquivos possivelmente infectados e, ao fazê-lo, o formato do arquivo será determinado pela extensão de seu nome. Usando o link, você pode analisar uma lista de extensões de arquivos verificados com essa opção (consulte A.1 na p. 224).

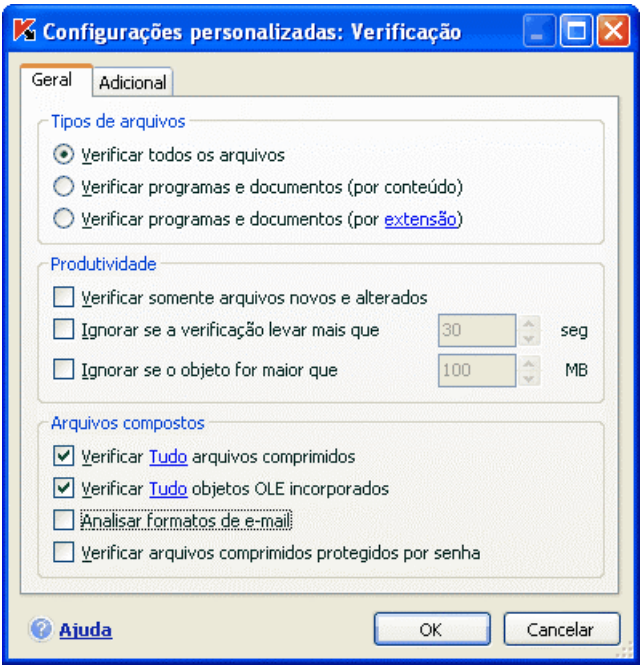


Figura 44. Configurando a verificação

Dica:
Não esqueça que alguém pode enviar para o seu computador um vírus com a extensão .txt que, na verdade, é um arquivo executável renomeado como .txt. Se você selecionar a opção **Programas e documentos (por extensão)**, a verificação ignorará esse arquivo. Se a opção **Verificar programas e documentos (por conteúdo)** for selecionada, o programa analisará os cabeçalhos dos arquivos, descobrindo que o arquivo é um arquivo .exe e o verificando extensivamente quanto à presença de vírus.

Na seção **Produtividade**, você pode especificar que apenas os arquivos novos e modificados desde a verificação anterior serão verificados. Esse modo reduz visivelmente o tempo de verificação e aumenta a velocidade de operação do programa. Para fazê-lo, marque ☑ **Verificar somente arquivos novos e alterados**. Esse modo estende-se a arquivos simples e compostos.

Você também pode definir limites de tempo e de tamanho de arquivo para a verificação na seção **Produtividade**.

☑ **Ignorar se a verificação levar mais que... seg.** Marque esta opção e insira o tempo máximo de verificação de um objeto. Se esse tempo for excedido, o objeto será removido da fila de verificação.

☑ **Ignorar se o objeto for maior que... MB**. Marque esta opção e insira o tamanho máximo de um objeto. Se esse tamanho for excedido, o objeto será removido da fila de verificação.

Na seção **Arquivos compostos**, especifique os arquivos compostos que devem ser analisados quanto à presença de vírus:

☑ **Verificar todos os/somente novos arquivos comprimidos** – verifica arquivos comprimidos .rar, .arj, .zip, .cab, .lha, .jar e .ice.

Aviso!

O Kaspersky Anti-Virus não exclui automaticamente os arquivos comprimidos em formatos aos quais ele não dá suporte (por exemplo, .ha, .uue, .tar), mesmo se você optar pela neutralização ou exclusão automática no caso de não ser possível neutralizar os objetos.

Para excluir esses arquivos comprimidos, clique no link Excluir arquivos comprimidos na notificação de detecção de objetos perigosos. Essa notificação será exibida na tela depois que o programa inicia o processamento dos objetos detectados na verificação. Você também pode excluir os arquivos comprimidos infectados manualmente.

☑ **Verificar todos os/somente novos objetos OLE incorporados** - verifica objetos incorporados em arquivos (por exemplo planilhas do Excel ou uma macro incorporada em um arquivo do Microsoft Word, anexos de e-mail, etc.).

Você pode selecionar e verificar todos os arquivos ou somente os novos de cada tipo de arquivo composto. Para fazê-lo, use o link ao lado do nome do objeto. Ele muda seu valor quando você clica nele. Se a seção **Produtividade** tiver sido configurada para verificar somente arquivos novos e modificados, você não poderá selecionar o tipo de arquivos compostos que serão verificados.

Analisar formatos de e-mail – verifica arquivos e bancos de dados de e-mails. Se esta caixa de seleção estiver marcada, o Kaspersky Anti-Virus separará o arquivo de e-mail e analisará cada componente (corpo, anexos) quanto à presença de vírus. Se a caixa não estiver marcada, o arquivo de e-mail será verificado como um único objeto.

Observe que, ao verificar bancos de dados de e-mail protegidos por senha:

- O Kaspersky Anti-Virus detecta código mal-intencionado em bancos de dados do Microsoft Outlook 2000, mas não os neutraliza;
- O Kaspersky Anti-Virus não dá suporte a verificações de código mal-intencionado em bancos de dados protegidos do Microsoft Outlook 2003.

Verificar arquivos comprimidos protegidos por senha – verifica arquivos comprimidos protegidos por senha. Com este recurso, uma janela solicitará uma senha antes de verificar objetos de arquivos comprimidos. Se a caixa não estiver marcada, os arquivos comprimidos protegidos por senha serão ignorados.

11.4.3. Restaurando configurações de verificação padrão

Ao definir as configurações de tarefas de verificação, é sempre possível retornar para as configurações recomendadas. A Kaspersky Lab as considera ideais e as combinou no nível de segurança **Recomendado**.

Para restaurar as configurações de verificação de arquivos padrão:

1. Selecione o nome da tarefa na seção **Verificação** da janela principal. Clique com o botão direito do mouse no nome da tarefa para abrir o menu de contexto ou clique no botão **Ações** à direita da lista de objetos para verificação e selecione **Configurações**.
2. Clique no botão **Padrão** na seção **Nível de segurança**.

11.4.4. Selecionando ações para objetos

Se, durante uma verificação, for descoberto que um arquivo está infectado ou é suspeito, as próximas etapas do programa dependerão do status do objeto e da ação selecionada.

Um dos seguintes status pode ser atribuído ao objeto após a verificação:

- Status de programa mal-intencionado (por exemplo, *vírus, cavalo de Tróia*).
- *Possivelmente infectado*, quando a verificação não consegue determinar se o objeto está infectado. É provável que o programa tenha detectado uma seqüência de código de um vírus desconhecido ou de um vírus conhecido modificado.

Por padrão, todos os arquivos infectados são desinfectados e, se estiverem possivelmente infectados, serão enviados para a Quarentena.

Para editar uma ação para um objeto:

selecione o nome da tarefa na seção **Verificação** da janela principal do programa e use o link Configurações para abrir a janela de configurações da tarefa. Todas as respostas possíveis são exibidas nas seções apropriadas (veja a fig. 45).

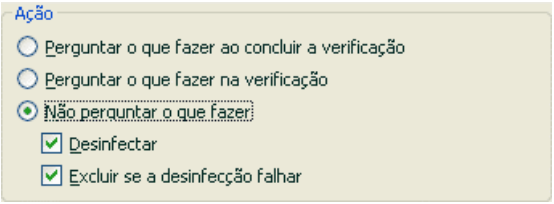


Figura 45. Selecionando ações para objetos perigosos

Se a ação selecionada for	**Ao detectar um objeto infectado ou possivelmente infectado**
Perguntar o que fazer ao concluir a verificação	O programa não processa os objetos até o final da verificação. Quando a verificação for concluída, a janela de estatísticas será aberta com uma lista dos objetos detectados e será perguntado se você deseja processar os objetos.
Perguntar o que fazer na verificação	O programa emitirá uma mensagem de aviso com informações sobre o código mal-intencionado que infectou, ou possivelmente infectou, o arquivo e permite que você escolha uma das ações a seguir.

Não perguntar o que fazer	O programa registra as informações sobre os objetos detectados no relatório, sem processá-los nem notificar o usuário. Não é recomendável usar esta opção, pois os objetos infectados e possivelmente infectados permanecem no computador, sendo praticamente impossível evitar a infecção.
Não perguntar o que fazer **Desinfectar**	O programa tenta neutralizar o objeto detectado sem solicitar a confirmação do usuário. Se a desinfecção falhar, será atribuído o status de *possivelmente infectado* ao arquivo e ele será movido para a Quarentena (consulte 14.1 na p. 167). Essas informações são registradas no relatório (consulte 14.3 na p. 173). Posteriormente, você pode tentar desinfectar esse objeto.
Não perguntar o que fazer **Desinfectar** **Excluir se a desinfecção falhar**	O programa tenta neutralizar o objeto detectado sem solicitar a confirmação do usuário. Se o objeto não puder ser desinfectado, ele será excluído.
Não perguntar o que fazer **Desinfectar** **Excluir**	O programa exclui o objeto automaticamente.

Ao desinfectar ou excluir um objeto, o Kaspersky Anti-Virus cria uma cópia do mesmo e a envia para o Backup (consulte 14.2 na p. 171), caso seja necessário restaurá-lo ou surja uma oportunidade de neutralizá-lo posteriormente.

11.4.5. Opções avançadas de verificação de vírus

Além de definir as configurações básicas de verificação de vírus, você também pode usar configurações adicionais (veja a fig. 46):

Habilitar tecnologia iChecker – usa a tecnologia que pode aumentar a velocidade de verificação por meio da exclusão de determinados objetos.

Um objeto é excluído da verificação usando um algoritmo específico que leva em conta a data de lançamento das assinaturas de ameaças, a data mais recente em que o objeto foi verificado e as modificações das configurações de verificação.

Por exemplo, você tem um arquivo armazenado que o programa verificou e ao qual atribuiu o status de não infectado. Na próxima verificação, o programa ignorará esse arquivo, a menos que ele tenha sido modificado ou que as configurações de verificação tenham sido alteradas. Mas o programa verificará o arquivo comprimido novamente se sua estrutura tiver mudado porque foi adicionado um novo objeto a ele, se as configurações de verificação tiverem sido alteradas ou se as assinaturas de ameaças tiverem sido atualizadas.

A tecnologia iChecker™ tem algumas limitações: ela não funciona com arquivos grandes e se aplica somente a objetos com uma estrutura reconhecida pelo Kaspersky Anti-Virus (por exemplo, .exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar).

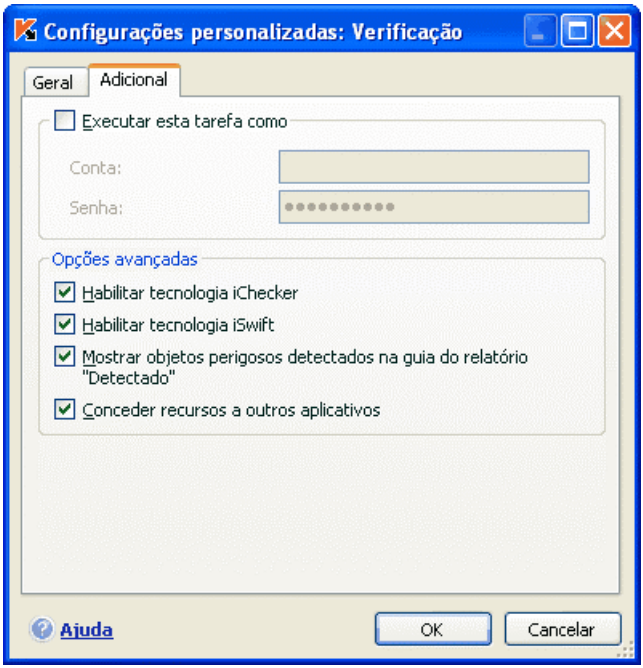


Figura 46. Configurações avançadas de verificação

Habilitar tecnologia iSwift – Esta tecnologia é um desenvolvimento da tecnologia iChecker para computadores que usam o sistema de arquivos NTFS. A tecnologia iSwift tem algumas limitações: ela é ligada a um local

específico para o arquivo do sistema de arquivos e pode ser aplicada somente a objetos em um sistema de arquivos NTFS.

A tecnologia iSwift não está disponível em computadores com o Microsoft Windows 98SE/ME/XP64.

Mostrar objetos perigosos detectados na guia do relatório "Detectado" – exibe uma lista de ameaças detectadas durante a verificação na guia **Detectados** da janela do relatório (consulte 14.3.2 na p. 177). Talvez seja apropriado desabilitar essa função em verificações específicas, por exemplo, de conjuntos de textos, para aumentar a velocidade de verificação.

Conceder recursos a outros aplicativos – pausa a tarefa de verificação de vírus se o processador estiver ocupado com outros aplicativos.

11.4.6. Definindo configurações globais de verificação para todas as tarefas

Cada tarefa de verificação é executada de acordo com suas próprias configurações. Por padrão, as tarefas criadas ao instalar o programa no computador usam as configurações recomendadas pela Kaspersky Lab.

Você pode definir configurações globais de verificação para todas as tarefas. Como ponto de partida, você usará um conjunto de propriedades utilizadas para verificar vírus em um objeto individual.

Para atribuir configurações globais de verificação para todas as tarefas:

1. Selecione a seção **Verificação** à esquerda da janela principal do programa e clique em Configurações.
2. Na janela de configurações que é aberta, defina as configurações de verificação: Selecione o nível de segurança (consulte 11.4.1 na p. 138), defina as configurações de nível avançado e selecione uma ação (consulte 11.4.4 na p. 142) para os objetos.
3. Para aplicar essas novas configurações a todas as tarefas, clique no botão **Aplicar** na seção **Outras configurações de tarefas**. Confirme as configurações globais selecionadas na caixa de diálogo pop-up.

CAPÍTULO 12. TESTANDO OS RECURSOS DO KASPERSKY ANTI-VIRUS

Despois de instalar e configurar o Kaspersky Anti-Virus, é recomendável verificar se as configurações e se a operação do programa estão corretas usando um vírus de teste e suas variações.

12.1. O vírus de teste da EICAR e suas variações

O vírus de teste foi especialmente desenvolvido pela eicar (The European Institute for Computer Antivirus Research) pra testar a funcionalidade dos antivírus.

O vírus de teste NÃO É UM VÍRUS e não contém nenhum código de programa que possa danificar seu computador. Contudo, a maioria dos programas antivírus o identificarão como um vírus.

Nunca use vírus reais para testar a funcionalidade de um antivírus!

Você pode baixar o vírus de teste do site oficial da **EICAR**: http://www.eicar.org/anti_virus_test_file.htm.

O arquivo que é baixado do site da **EICAR** contém o corpo de um vírus de teste padrão. O Kaspersky Anti-Virus o detectará, o rotulará como um **vírus** e executará a ação definida para esse tipo de objeto.

Para testar as reações do Kaspersky Anti-Virus quando diferentes tipos de objetos são detectados, você pode modificar o conteúdo do vírus de teste padrão, adicionando um dos prefixos mostrados na tabela.

Prefixo	Status do vírus de teste	Ação correspondente quando o aplicativo processar o objeto
Sem prefixo, vírus de teste padrão	O arquivo contém um vírus de teste. Não é possível desinfectar o objeto.	O aplicativo identificará o objeto como sendo mal-intencionado e não passível de neutralização, e o excluirá.
CORR-	Corrompido.	O aplicativo poderia acessar o objeto, mas não verificá-lo, pois ele está corrompido (por exemplo, a estrutura do arquivo foi violada ou tem um formato de arquivo inválido).
SUSP- WARN-	O arquivo contém um vírus de teste (modificação). Não é possível desinfectar o objeto.	Esse objeto é uma modificação de um vírus conhecido ou desconhecido. No momento da detecção, os bancos de dados de assinaturas de ameaças não contêm uma descrição do procedimento para neutralizar esse objeto. O aplicativo o colocará na Quarentena para que seja processado posteriormente com assinaturas de ameaças atualizadas.
ERRO-	Erro de processamento.	Ocorreu um erro ao processar o objeto: o aplicativo não pode acessar o objeto que está sendo verificado, pois a integridade do mesmo foi violada (por exemplo, não existe um final em um arquivo comprimido com vários volumes) ou não é possível conectá-lo (se o objeto estiver sendo verificado em uma unidade de rede).

Prefixo	Status do vírus de teste	Ação correspondente quando o aplicativo processar o objeto
CURE–	O arquivo contém um vírus de teste. Ele pode ser neutralizado. O objeto é passível de desinfecação, e o texto do corpo do vírus mudará para CURE.	O objeto contém um vírus que pode ser neutralizado. O aplicativo verificará o objeto quanto à presença de vírus e, em seguida, será totalmente neutralizado.
DELE–	O arquivo contém um vírus de teste. Não é possível desinfectar o objeto.	Esse objeto contém um vírus que não pode ser desinfectado ou que é um cavalo de Tróia. O aplicativo exclui esses objetos.

A primeira coluna da tabela contém os prefixos que precisam ser adicionados ao início da seqüência de caracteres de um vírus de teste padrão. A segunda coluna descreve o status e a reação do Kaspersky Anti-Virus aos vários tipos de vírus de teste. A terceira coluna contém informações sobre objetos com o mesmo status que o aplicativo processou.

Os valores das configurações de verificação de vírus determinam a medida tomada sobre cada um dos objetos.

12.2. Testando o Antivírus de Arquivos

Para testar a funcionalidade do Antivírus de Arquivos;

1. Crie uma pasta em um disco; copie o vírus de teste baixado do site oficial da organização (consulte 12.1 na p. 147) e as modificações do vírus de teste que você criou para essa pasta.
2. Permita que todos os eventos sejam registrados de forma que o arquivo de relatório mantenha os dados de objetos corrompidos e objetos não verificados devido a erros. Para fazê-lo, marque **Registrar eventos não críticos** na janela de configurações do relatório (consulte 14.3.1 na p. 176).
3. Execute o vírus de teste ou uma de suas modificações.

O Antivírus de Arquivos interceptará sua tentativa de acessar o arquivo, o verificará e informará que um objeto perigoso foi detectado:

Figura 47. Objeto perigoso detectado

Selecionando opções diferentes para lidar com os objetos detectados, você pode testar a reação do Antivírus de Arquivos ao detectar vários tipos de objetos.

Você pode ver os detalhes do desempenho do Antivírus de Arquivos no relatório do componente.

12.3. Teste das tarefas de verificação de vírus

Para testar as tarefas de verificação de vírus:

1. Crie uma pasta em um disco; copie o vírus de teste baixado do site oficial da organização (consulte 12.1 na p. 147) e as modificações do vírus de teste que você criou para essa pasta.
2. Crie uma nova tarefa de verificação de vírus (consulte 11.3 na página 136) e selecione a pasta que contém o conjunto de vírus de teste para ser verificada (consulte 11.2 na p. 134).
3. Permita que todos os eventos sejam registrados de forma que o arquivo de relatório mantenha os dados de objetos corrompidos e objetos não verificados devido a erros. Para fazê-lo, marque **Registrar eventos não críticos** na janela de configurações do relatório.

4. Execute a tarefa de verificação de vírus (consulte 11.1 na página 134).

Ao executar uma verificação, conforme os objetos suspeitos ou infectados forem detectados, serão exibidas notificações na tela com informações sobre os objetos, perguntando ao usuário sobre a próxima medida a ser tomada:

Figura 48. Objeto perigoso detectado

Dessa forma, selecionando opções diferentes para as ações, você pode testar as reações do Kaspersky Anti-Virus ao detectar vários tipos de objetos.

Você pode ver os detalhes do desempenho da tarefa de verificação de vírus no relatório do componente.

CAPÍTULO 13. ATUALIZAÇÕES DO PROGRAMA

Manter o software antivírus atualizado é um investimento na segurança do computador. Com o aparecimento diário de novos vírus, cavalos de Tróia e software mal-intencionado, é importante atualizar periodicamente o aplicativo para manter suas informações sempre protegidas. Esta tarefa é gerenciada pelo componente *Atualização*.

A atualização do aplicativo envolve o download e a instalação dos seguintes componentes no computador:

- **Assinaturas de ameaças**

  O aplicativo usa assinaturas de ameaças para proteger as informações contidas no computador. Os componentes de software que oferecem proteção usam o banco de dados de assinaturas de ameaças para pesquisar e desinfectar objetos nocivos no computador. As assinaturas são completadas a cada hora, com registros de novas ameaças e métodos para combatê-las. Assim, é recomendável atualizá-las periodicamente.

  Além das assinaturas de ameaças, os drivers de rece que permitem que os componentes de proteção interceptem o tráfego de rede também são atualizados.

  As versões anteriores dos aplicativos da Kaspersky Lab davam suporte a conjuntos de bancos de dados *padrão* e *estendido*. Cada banco de dados era responsável por proteger o computador de diferentes tipos de objetos perigosos. No Kaspersky Anti-Virus, não é necessário se preocupar com a seleção do conjunto de assinaturas de ameaças apropriado. Agora, nossos produtos usam assinaturas de ameaças que o protegem de objetos mal-intencionados e possivelmente perigosos, e de ataques de hackers.

- **Módulos do aplicativo**

  Além das assinaturas, você pode atualizar os módulos internos do Kaspersky Anti-Virus. Novas atualizações do aplicativo surgem periodicamente.

As principais fontes de atualização do Kaspersky Anti-Virus são os servidores de atualização da Kaspersky Lab. Alguns dos endereços são os seguintes:

http://downloads1.kaspersky-labs.com/updates/

http://downloads2.kaspersky-labs.com/updates/

ftp://downloads1.kaspersky-labs.com/updates/

Para baixar as atualizações disponíveis dos servidores de atualização, é necessário que o computador esteja conectado à Internet.

Se não tiver acesso aos servidores de atualização da Kaspersky Lab (por exemplo, se o computador não estiver conectado à Internet), você poderá ligar para o escritório central da Kaspersky Lab, no número +7 (495) 797-87-00, e solicitar informações de contato dos parceiros da empresa que podem fornecer atualizações em disquetes ou CDs.

É possível baixar as atualizações de um dos seguintes modos:

- *Automático*. O Kaspersky Anti-Virus verifica os pacotes de atualização na fonte em intervalos definidos. É possível definir as verificações de forma que sejam mais freqüentes durante os surtos de vírus e menos freqüentes quando eles terminarem. Ao detectar novas atualizações, o programa as baixa e instala no computador. Essa é a configuração padrão.
- *Na programação*. A atualização é programada para iniciar em uma hora especificada.
- *Manual*. Com esta opção, você inicia a Atualização manualmente.

Durante a atualização, o aplicativo compara as assinaturas de ameaças e os módulos do aplicativo no computador com as versões disponíveis no servidor de atualização. Se o computador possuir a versão mais recente das assinaturas e dos módulos do aplicativo, aparecerá uma janela de notificação confirmando que ele está atualizado. Se as assinaturas e os módulos no computador forem diferente daqueles no servidor de atualização, somente as partes ausentes das atualizações serão baixadas. A Atualização não baixa assinaturas de ameaças e módulos que você já possui, o que aumenta significativamente a velocidade de download e economiza tráfego da Internet.

Antes de atualizar as assinaturas de ameaças, o Kaspersky Anti-Virus cria cópias delas, que podem ser usadas se for necessário executar uma reversão (consulte 13.2 na página 154). Se, por exemplo, o processo de atualização corromper as assinaturas de ameaças e inutilizá-las, você poderá facilmente reverter para a versão anterior e tentar atualizar as assinaturas mais tarde.

Você pode distribuir as atualizações recuperadas em uma fonte local enquanto atualiza o aplicativo (consulte 13.4.4 na p.163). Esse recurso permite atualizar os bancos de dados e os módulos usados por duplicações do 6.0 em computadores em rede para economizar largura de banda.

13.1. Iniciando a Atualização

É possível iniciar o processo de atualização a qualquer momento. Ele será executado a partir da fonte de atualização selecionada (consulte 13.4.1 na p. 156).

Você pode iniciar a Atualização:

- do menu de contexto (consulte 4.2 na p. 42).
- da janela principal do programa (consulte 4.3 na p. 43)

Para iniciar a Atualização no menu de atalho:

1. Clique com o botão direito do mouse no ícone do aplicativo na bandeja do sistema para abrir o menu de atalho.
2. Selecione **Atualização**.

Para iniciar a Atualização na janela principal do programa:

1. Selecione **Atualização** na seção **Serviço**.
2. Clique no botão **Atualizar agora** no painel direito da janela principal ou use o botão na barra de status.

O andamento da atualização será exibido em uma janela específica, que pode ser ocultada clicando em **Fechar**. A atualização continuará com a janela oculta.

Observe que as atualizações são distribuídas para a fonte local durante o processo de atualização, desde que esse serviço esteja habilitado (consulte 13.4.4 na p. 163).

13.2. Revertendo para a atualização anterior

Sempre que você iniciar a Atualização, o Kaspersky Anti-Virus criará uma cópia de backup das assinaturas de ameaças atuais antes de começar o download das atualizações. Dessa forma, você poderá voltar a usar a versão anterior das assinaturas, se a atualização falhar.

A opção de reversão pode ser útil se, por exemplo, o processo de atualização falhar devido a um erro de conexão. Você pode reverter para as assinaturas de ameaças anteriores e tentar atualizá-las novamente depois.

Para reverter para a versão anterior das assinaturas de ameaças:

1. Selecione o componente **Atualização** na seção **Serviço** da janela principal do programa.
2. Clique no botão **Reverter** no painel direito da janela principal do programa.

13.3. Criando tarefas de atualização

O Kaspersky Anti-Virus possui uma tarefa de atualização interna para atualizar módulos do programa e assinaturas de ameaças. Você também pode criar suas próprias tarefas de atualização com várias configurações e programações de início.

Por exemplo, você instalou o Kaspersky Anti-Virus em um laptop que usa em casa e no escritório. Em casa, você atualiza o programa dos servidores de atualização da Kaspersky Lab e, no escritório, de uma pasta local que armazena as atualizações necessárias. Use duas tarefas diferentes para não precisar alterar as configurações de atualização a cada vez que mudar de local.

Para criar uma tarefa de atualização avançada:

1. Selecione **Atualização** na seção **Serviço** da janela principal do programa, abra o menu de contexto clicando com o botão direito do mouse e selecione **Salvar como**.
2. Insira o nome da tarefa na janela que é aberta e clique em **OK**. Uma tarefa com esse nome aparecerá então na seção **Serviço** da janela principal do programa.

Aviso!

O número de tarefas de atualização que podem ser criadas pelo usuário é limitado. Número máximo: duas tarefas.

A nova tarefa herda todas as propriedades da tarefa na qual foi baseada, exceto as configurações de programação. A configuração padrão dessa verificação automática é desabilitada.

Depois de criar uma tarefa, defina as configurações adicionais: especifique a fonte de atualização (consulte 13.4.1 na página 156), as configurações de rede (consulte 13.4.3 na página 161) e, se necessário, habilite as tarefas com privilégios (consulte 6.4 na página 144) e configure a programação (consulte 6.5 na p. 75).

Para renomear uma tarefa:

Selecione a tarefa na seção **Serviço** da janela principal do programa, abra o menu de contexto clicando com o botão direito do mouse e selecione **Renomear**.

Insira o novo nome da tarefa na janela que é aberta e clique em **OK**. O nome da tarefa será mudado então na seção **Serviço**.

Para excluir uma tarefa:

Selecione a tarefa na seção **Serviço** da janela principal do programa, abra o menu de contexto clicando com o botão direito do mouse e selecione **Excluir**.

Confirme se você deseja excluir a tarefa na janela de confirmação. A tarefa será então excluída da lista de tarefas na seção **Serviço**.

Aviso!

Somente as tarefas personalizadas poderão ser renomeadas e excluídas.

13.4. Configurando a atualização

As configurações da Atualização especificam os seguintes parâmetros:

- A fonte para o download e a instalação das atualizações (consulte 13.4.1 na p. 156)
- O modo de execução do procedimento de atualização (consulte 13.4.2 na p. 159)
- Quais objetos são atualizados
- As ações que devem ser executadas após a conclusão da atualização (consulte 13.4.4 na p. 163)

As seções a seguir examinam estes aspectos detalhadamente.

13.4.1. Selecionando uma fonte de atualização

A *fonte de atualização* é o local de onde você baixa as atualizações das assinaturas das ameaças e dos módulos internos do Kaspersky Anti-Virus.

A principal fonte de atualização são os *servidores de atualização da Kaspersky Lab*. São sites específicos que contêm as atualizações disponíveis das assinaturas de ameaças e dos módulos internos de todos os produtos da Kaspersky Lab.

Se não for possível acessar os servidores de atualização da Kaspersky Lab (por exemplo, se não houver uma conexão com a Internet), você poderá ligar para o escritório central da Kaspersky Lab, no número +7 (495) 797-87-00, e solicitar informações de contato dos parceiros da empresa que podem fornecer atualizações compactadas em disquetes ou CDs.

Aviso!

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

Você pode copiar as atualizações de um disco e carregá-las em um site FTP ou HTTP, ou salvá-las em uma pasta local ou de rede.

Selecione a fonte de atualização na guia **Fonte de atualização** (veja a fig. 49).

A opção padrão faz o download das atualizações dos servidores de atualização da Kaspersky Lab. A lista de endereços representados por este item não pode ser editada. Na atualização, o Kaspersky Anti-Virus chama essa lista, seleciona o endereço do primeiro servidor e tentar baixar os arquivos desse servidor. Se não for possível baixar as atualizações do primeiro servidor, o aplicativo tentará se conectar a cada servidor, até ser bem-sucedido. O endereço do servidor do qual as atualizações são baixadas com êxito é automaticamente colocado no início da lista, de forma que da próxima vez, o aplicativo tentará conectar esse servidor primeiro.

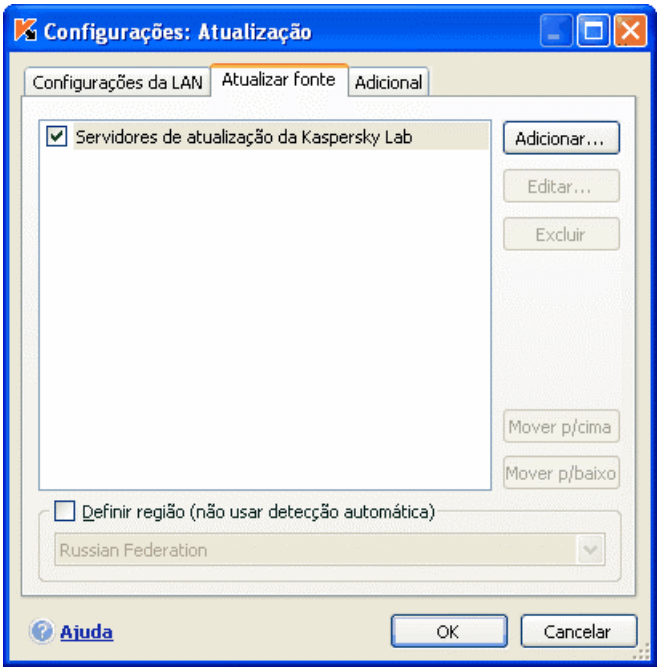


Figura 49. Selecionando uma fonte de atualização

Para baixar atualizações de outro site FTP ou HTTP:

1. Clique em **Adicionar**.
2. Na caixa de diálogo **Selecionar fonte de atualização**, selecione o site FTP ou HTTP de destino ou especifique o endereço IP, o nome do caractere ou endereço da URL desse site no campo **Fonte**.

Aviso!

Se um recurso localizado fora da rede local for selecionado como fonte de atualização, é necessário ter uma conexão com a Internet para a atualização.

Para atualizar de uma pasta local:

1. Clique em **Adicionar**.
2. Na caixa de diálogo **Selecionar fonte de atualização**, selecione uma pasta ou especifique o caminho completo da pasta no campo **Fonte**.

O Kaspersky Anti-Virus adiciona novas fontes de atualização ao início da lista e habilita a fonte automaticamente, marcando a caixa ao lado de seu nome.

Se vários recursos forem selecionados como fontes de atualização, o aplicativo tentará se conectar a cada um deles, começando pelo primeiro na lista, e recuperará as atualizações da primeira fonte disponível. Você pode alterar a ordem das fontes na lista, usando os botões **Mover para cima** e **Mover para baixo**.

Para editar a lista, use os botões **Adicionar**, **Editar** e **Remover**. A única fonte que não pode ser editada ou excluída é aquela rotulada como servidores de atualização da Kaspersky Lab.

Se você usar os servidores de atualização da Kaspersky Lab como fonte de atualização, poderá selecionar o local de servidor ideal para o download das atualizações. A Kaspersky Lab possui servidores em vários países. A escolha do servidor de atualização da Kaspersky Lab mais próximo economizará tempo e o download das atualizações será mais rápido.

Para escolher o servidor mais próximo, marque **Definir região (não usar detecção automática)** e selecione o país mais próximo do seu local atual na lista suspensa. Se você marcar essa caixa de seleção, as atualização serão executadas levando em conta a região selecionada na lista. Por padrão, essa caixa de seleção está desmarcada, sendo usadas as informações sobre a região atual do Registro do sistema operacional.

13.4.2. Selecionando um método de atualização e o que atualizar

Ao definir as configurações de atualização, é importante especificar o que será atualizado e qual método de atualização será usado.

Objetos de atualização (veja a fig. 50) são os componentes que serão atualizados:

- Assinaturas de ameaças
- Módulos do aplicativo
- Drivers de rede que permitem que os componentes de proteção interceptem o tráfego de rede.

As assinaturas de ameaças são atualizadas sempre, enquanto os módulos do aplicativo e drivers de rede são atualizados dependendo da configuração.

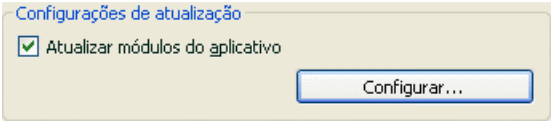


Figura 50. Selecionando objetos de atualização

Se desejar baixar e instalar atualizações dos módulos do programa:

Marque ☑ **Atualizar módulos do programa** na caixa de diálogo **Configurações** do componente **Atualização**.

Se houver atualizações de módulos do programa na fonte de atualização, o programa baixará as atualizações necessárias e as aplicará quando o computador for reiniciado. As atualizações de módulos não serão instaladas até que o computador seja reiniciado.

Se a próxima atualização do programa ocorrer antes que o computador seja reiniciado e que as atualizações dos módulos do programa anteriores sejam instaladas, somente as assinaturas de ameaças serão atualizadas.

Se desejar baixar e instalar o banco de dados de drivers de rede:

Marque ☑ **Atualizar drivers de rede** na janela de configurações do componente **Atualização**.

O Modo de execução (veja a fig. 51) define como a Atualização será iniciada. Você pode selecionar um dos seguintes métodos:

◉ **Automaticamente**. O Kaspersky Anti-Virus verifica a fonte de atualizações dos pacotes de atualização em intervalos definidos (consulte 0 na página 156). Ao detectar novas atualizações, o programa as baixa e instala no computador. Este é o modo utilizado por padrão.

Se você tiver uma conexão discada com a Internet e um recurso de rede for especificado como fonte de atualização, o Kaspersky Anti-Virus tentará iniciar a Atualização sempre que o computador se conectar àquele recurso ou depois que um determinado intervalo, como especificado no pacote de atualização anterior.

Se uma pasta local for selecionada como fonte de atualização, o aplicativo tentará baixar as atualizações a partir da pasta local com a mesma freqüência especificada no pacote de atualização baixado na atualização anterior. Esta opção permite que a Kaspersky Lab regule a freqüência com que o programa será atualizado no caso de surtos de vírus e outras situações possivelmente perigosas. Seu aplicativo receberá as atualizações mais recentes de assinaturas de ameaças, ataques de rede e módulos de software oportunamente, evitando assim a invasão do computador por software mal-intencionado.

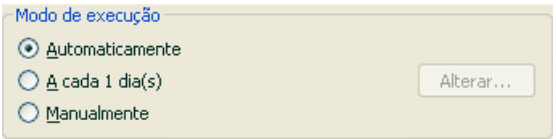


Figura 51. Selecionando um modo de execução da atualização

Cada 1 dia(s) A Atualização é programada para iniciar em uma hora especificada. O programação padrão executa a Atualização diariamente. Para editar a programação padrão, clique no botão **Alterar…** na caixa **Modo de execução** e faça as alterações necessárias na janela que é aberta (para obter mais detalhes, consulte 6.5 na p. 75).

Manualmente. Com esta opção, você inicia a Atualização manualmente. O Kaspersky Anti-Virus o notifica quando é necessário que seja atualizado:

- Uma mensagem pop-up informando que a atualização é necessária aparece acima do ícone do aplicativo na bandeja do sistema (se as notificações estiverem habilitadas; consulte 14.11.1 na p. 195)
- O segundo indicador na janela principal do programa informa que seu computador está desatualizado (consulte 5.1.1 na p. 49)
- Uma recomendação de que é necessário atualizar o aplicativo aparece na seção de mensagens na janela principal do programa (consulte 4.3 na p. 43)

13.4.3. Configurando a conexão

Se você configurar o programa para recuperar atualizações dos servidores de atualização da Kaspersky Lab ou de outros sites FTP ou HTTP, é recomendável verificar primeiro suas configurações de conexão.

Por padrão, para estabelecer uma conexão com a Internet, o aplicativo usa as configurações do Microsoft Internet Explorer. Para alterar as configurações de conexão, é necessário saber se um servidor proxy está sendo usado e se você está atrás de um firewall. Se você não souber essas informações, entre em contato com o administrador do sistema ou com o provedor de Internet.

Todas as configurações estão agrupadas em uma guia específica – **Configurações da LAN** (veja a fig. 52).

Marque **Se possível, usar modo de FTP passivo** se você baixar as atualizações de um servidor FTP no modo passivo (por exemplo, através de um firewall). Se estiver trabalhando no modo FTP ativo, desmarque essa caixa de seleção.

No campo **Tempo limite da conexão… (seg)**, atribua o tempo alocado para a conexão com o servidor de atualização. Se a conexão falhar e esse período tiver acabado, o programa tentará conectar-se ao próximo servidor de atualização. Isso continuará até que uma conexão seja bem-sucedida ou até que se tenha tentado todos os servidores de atualização disponíveis.

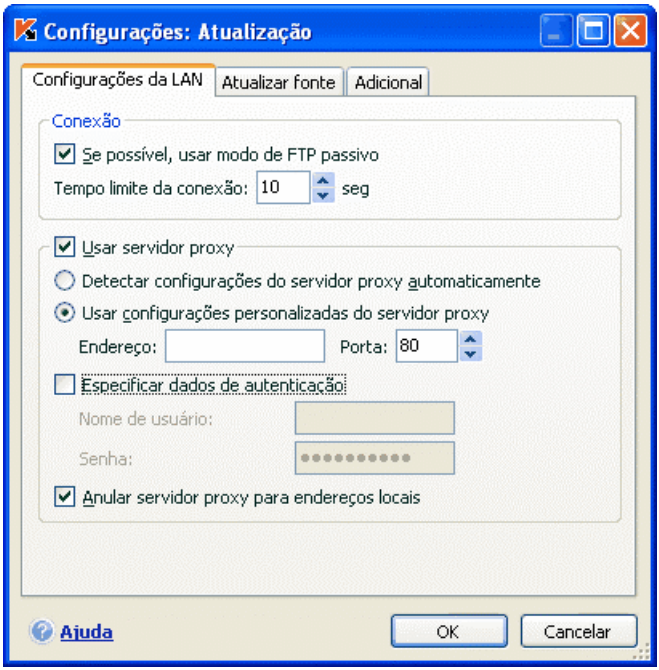


Figura 52. Definindo as configurações de atualização de rede

Marque **Usar servidor proxy** se estiver usando um servidor proxy para acessar a Internet e, se necessário, selecione as configurações a seguir:

- Selecione as configurações do servidor proxy que serão usadas durante a atualização:

  Detectar configurações do servidor proxy automaticamente. Se você selecionar esta opção, as configurações de proxy serão detectadas automaticamente usando o WPAD (Web Proxy Auto-Discovery Protocol). Se esse protocolo não conseguir detectar o endereço, o Kaspersky Anti-Virus usará as configurações de servidor proxy especificadas no Microsoft Internet Explorer.

  Usar configurações de proxy personalizadas - Usa um proxy diferente daquele especificado nas configurações de conexão do navegador. No campo **Endereço**, insira o endereço IP ou o nome simbólico do servidor proxy e especifique o número da porta proxy usada para atualizar o aplicativo no campo Porta.

- Especifique se o servidor proxy requer autenticação. *Autenticação* é o processo de verificação dos dados de registro do usuário para fins de controle de acesso.

Se a autenticação for necessária para conectar-se ao servidor proxy, marque ☑ O proxy exige autenticação e especifique o nome de usuário e a senha nos campos seguintes. Nesse caso, serão tentadas primeiro a autenticação NTLM e depois a autenticação BASIC. Se esta caixa de seleção não estiver marcada ou se os dados não forem inseridos, será tentada a autenticação NTLM utilizando a conta de usuário que foi usada para iniciar a atualização (consulte 0 na p. 144).

Se o servidor proxy exigir autenticação e você não inseriu o nome de usuário e a senha ou se, por algum motivo, os dados especificados não foram aceitos pelo servidor proxy, uma janela pop-up será exibida ao iniciar as atualizações, solicitando um nome de usuário e uma senha para autenticação. Se a autenticação for bem-sucedida, o nome de usuário e a senha serão usados da próxma vez em que o programa for atualizado. Caso contrário, as configurações de autenticação serão solicitadas novamente.

Para evitar o uso de um proxy quando a fonte de atualização for uma pasta local, selecione ☑ **Anular servidor proxy para endereços locais**.

Este recurso não está disponível no Microsoft Windows 9X/NT 4.0. Entretanto, por padrão, o servidor proxy não é usado para endereços locais.

13.4.4. Distribuição de atualizações

Caso seus computadores domésticos estejam conectados em uma rede doméstica, não será necessário baixar e instalar as atualizações em cada um deles separadamente, pois isso consumiria mais largura de banda da rede. Você pode usar o recurso de distribuição de atualizações, que ajuda a reduzir o tráfego por meio da recuperação de atualizações da seguinte maneira:

1. Um dos computadores na rede recupera um pacote de atualização do aplicativo e da assinatura de ameaças nos servidores da Kaspersky Lab ou de outros recursos da Web que hospedem um conjunto de atualizações. As atualizações recuperadas são colocadas em uma pasta de acesso público.

2. Os outros computadores da rede acessam essa pasta para recuperar as atualizações do aplicativo.

Para habilitar a distribuição de atualizações, marque a caixa de seleção ☑ **Pasta de distribuição de atualizações** na guia **Adicional** (veja a Figura 53) e, no campo a seguir, especifique a pasta compartilhada na qual serão colocadas as atualizações recuperadas. Você pode inserir o caminho manualmente ou selecioná-lo na janela que é aberta ao clicar em **Procurar**. Se a caixa de

seleção estiver marcada, as atualizações serão copiadas automaticamente para essa pasta quando forem recuperadas.

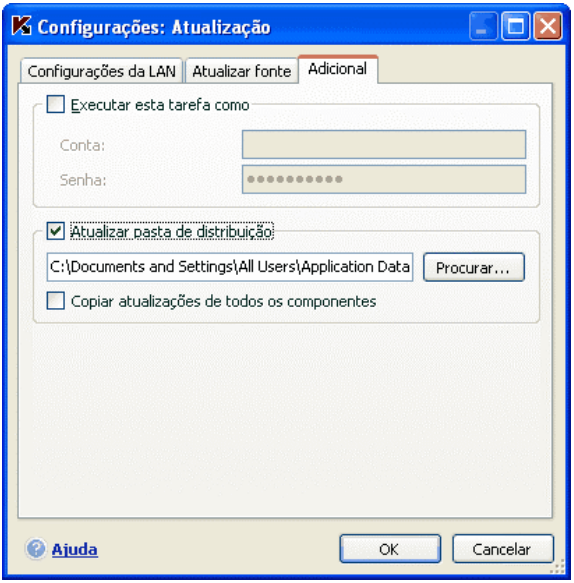


Figura 53. Configurações da ferramenta de distribuição de atualizações

Você também pode especificar o método de distribuição de atualizações:

- *completo*, copia as atualizações de assinaturas de ameaças e de componentes de todos os aplicativos da versão 6.0 da Kaspersky Lab. Para selecionar as atualizações completas, marque a caixa de seleção **Copiar atualizações de todos os componentes**.
- *personalizado*, copia apenas as assinaturas de ameaças e atualizações dos componentes do Kaspersky Anti-Virus 6.0 que estão instalados. Se desejar selecionar este método de atualização, desmarque a caixa de seleção **Copiar atualizações de todos os componentes**.

Se desejar que outros computadores na rede sejam atualizados da pasta que contém atualizações copiadas da Internet, execute as seguintes etapas:

1. Conceda acesso público a esta pasta.
2. Especifique a pasta compartilhada como fonte de atualização nos computadores da rede, nas configurações da Atualização.

13.4.5. Ações após a atualização do programa

Cada atualização de assinaturas de ameaças contém novos registros que protegem seu computador das ameaças mais recentes.

A Kaspersky Lab recomenda verificar os *objetos em quarentena* e os *objetos de inicialização* sempre que o banco de dados for atualizado.

Por que esses objetos devem ser verificados?

A área de quarentena contém objetos que foram sinalizados pelo programa como suspeitos ou possivelmente infectados (consulte 14.1 na p. 167). Usando a versão mais recente das assinaturas de ameaças, talvez o Kaspersky Anti-Virus possa identificar a ameaça e eliminá-la.

Por padrão, o aplicativo verifica os objetos em quarentena depois de cada atualização das assinaturas de ameaças. Também é recomendável verificar periodicamente os objetos em quarentena porque o status dos mesmos pode mudar após várias verificações. Alguns objetos podem ser então restaurados para os locais anteriores e você poderá continuar trabalhando com eles.

Para desabilitar as verificações de objetos em quarentena, desmarque **Verificarquarentena novamente** na seção **Ação após a atualização**.

Os objetos de inicialização são críticos para a segurança do computador. Se algum deles estiver infectado com um aplicativo mal-intencionado, isso pode provocar uma falha na inicialização do sistema operacional. O Kaspersky Anti-Virus possui uma tarefa interna de verificação de objetos de inicialização (consulte Capítulo 11 na p. 133). É recomendável configurar uma programação para essa tarefa de forma que ela seja iniciada automaticamente depois de cada atualização das assinaturas de ameaças (consulte 6.5 na p. 75).

CAPÍTULO 14. OPÇÕES AVANÇADAS

O Kaspersky Anti-Virus possui outros recursos que expandem sua funcionalidade.

O programa coloca alguns objetos em áreas de armazenamento específicas para garantir a proteção máxima dos dados, com o mínimo de perdas.

- O Backup contém cópias de objetos que o Kaspersky Anti-Virus alterou ou excluiu (consulte 14.2 na p. 171). Se não foi possível recuperar integralmente um objeto que continha informações importantes para você durante o processamento do antivírus, sempre é possível restaurá-lo a partir de sua cópia de backup.

- A Quarentena contém objetos possivelmente infectados que não puderam ser processados usando as assinaturas de ameaças atuais (consulte 14.1 na p. 167).

É recomendável examinar periodicamente a lista de objetos armazenados. Alguns deles já podem estar desatualizados e alguns podem ter sido restaurados.

As opções avançadas incluem diversos recursos úteis. Por exemplo:

- O Suporte Técnico fornece assistência abrangente ao Kaspersky Anti-Virus (consulte 14.5 na p. 183) A Kaspersky fornece vários canais de suporte, incluindo o suporte on-line e um fórum de perguntas e comentários para usuários dos programas.

- O recurso de Notificações configura as notificações do usuário sobre eventos-chave do Kaspersky Anti-Virus (consulte 14.11.1 na p. 195). Podem ser eventos de natureza informativa ou sobre erros críticos que devem ser eliminados imediatamente.

- A Autodefesa protege os arquivos do próprio programa contra modificações ou danos provocados por hackers, bloqueia o uso dos recursos do programa por administração remota e restringe a execução de determinadas ações no Kaspersky Anti-Virus por outros usuários (consulte 0 na p. 199). Por exemplo, alterar o nível de proteção pode influir significativamente sobre a segurança das informações no computador.

- O Gerenciador de Chaves de Licença pode obter informações detalhadas sobre a licença usada, ativar sua cópia do programa e gerenciar os arquivos de chaves de licença (consulte 14.5 na p. 183).

O programa também fornece uma seção de Ajuda (consulte 14.4 na p. 182) e relatórios detalhados (consulte 14.3 na p. 173) sobre a operação de todos os componentes de proteção e tarefas de verificação de vírus.

As portas monitoradas podem controlar quais módulos do Kaspersky Anti-Virus controlam os dados transferidos nas portas selecionadas (consulte 14.7 na p. 186).

O Disco de Recuperação pode ajudar a restaurar a funcionalidade do computador após uma infecção (consulte 14.10 na p. 191). Isso é particularmente útil quando não é possível iniciar o sistema operacional do computador depois que um código mal-intencionado danificou arquivos do sistema.

Você também pode alterar a aparência do Kaspersky Anti-Virus e personalizar a interface do programa (consulte 14.8 na p. 188).

As seções a seguir abordam estes recursos mais detalhadamente.

14.1. Quarentena de objetos possivelmente infectados

A **Quarentena** é uma área de armazenamento específica que mantém os objetos possivelmente infectados.

Os **objetos possivelmente infectados** são aqueles que se suspeita estarem infectados com vírus ou modificações deles.

Por que *possivelmente infectados*? Por vários motivos, nem sempre é possível determinar se um objeto está infectado:

- *O código do objeto verificado se parece com uma ameaça conhecida, mas está parcialmente modificado.*

  As assinaturas de ameaças contêm ameaças que já foram estudadas pela Kaspersky Lab. Se um programa mal-intencionado for modificado por um hacker mas essas alterações ainda não tiverem sido inseridas nas assinaturas, o Kaspersky Anti-Virus classificará o objeto infectado com esse programa mal-intencionado como possivelmente infectado e indicará a ameaça com a qual a infecção se parece.

- *O código do objeto detectado se parece, estruturalmente, com um programa mal-intencionado; contudo, não há nada semelhante registrado nas assinaturas de ameaças.*

  É bastante provável que se trate de um novo tipo de ameaça, então o Kaspersky Anti-Virus classifica esse objeto como possivelmente infectado.

O analisador de *código heurístico* detecta possíveis vírus, identificando até 92% de novos vírus. Esse mecanismo é bastante eficiente e raramente produz falsos positivos.

Um objeto possivelmente infectado pode ser detectado e colocado na quarentena pelo Antivírus de Arquivos, pelo Antivírus de E-Mail, pela Defesa Proativa ou durante uma verificação de vírus.

Você pode colocar um objeto em quarentena clicando em **Quarentena**, na notificação pop-up que é exibida quando um objeto possivelmente infectado é detectado.

Quando você coloca um objeto na Quarentena, ele é movido, não copiado. O objeto é excluído do disco ou do e-mail e salvo na pasta Quarentena. Os arquivos em Quarentena são salvos em um formato específico e não são perigosos.

14.1.1. Ações sobre objetos em quarentena

O número total de objetos em Quarentena é exibido selecionando o item **Arquivos de dados** na área **Serviço** da janela principal do aplicativo. À direita da tela, a seção *Quarentena* exibe:

- o número de objetos possivelmente infectados detectados com o Kaspersky Anti-Virus;
- o tamanho atual da Quarentena.

Você pode excluir todos os objetos da quarentena com o botão **Limpar**. Observe que, ao fazê-lo, os arquivos de Backup e de relatório também serão excluídos.

Para acessar os objetos na Quarentena:

Clique em qualquer local da caixa *Quarentena* para abrir a janela Proteção, que resume a proteção fornecida pelo aplicativo.

As seguintes ações podem ser executadas na guia Quarentena (veja a fig. 54):

- Mover para a Quarentena um arquivo que você suspeita estar infectado, mas que o programa não detectou. Para fazê-lo, clique em **Adicionar** e selecione o arquivo na janela de seleção padrão. Ele será adicionado à lista com o status *adicionado pelo usuário*.
- Verificar e desinfectar todos os objetos possivelmente infectados na Quarentena usando as assinaturas de ameaças atuais, clicando em **Verificar tudo**.

  Depois de verificar e desinfectar qualquer objeto em quarentena, seu status pode mudar para *infectado, possivelmente infectado, falso positivo, OK,* etc.

O status *infectado* significa que o objeto foi identificado como infectado, mas não pôde ser neutralizado. É recomendável excluí-lo.

Todos os objetos marcados como *falso positivo* podem ser restaurados, pois seu status *possivelmente infectado* anterior não foi confirmado pelo programa após nova verificação.

- Restaurar os arquivos para uma pasta selecionada pelo usuário ou para sua pasta original antes da Quarentena (padrão). Para restaurar um objeto, selecione-o na lista e clique em **Restaurar**. Ao restaurar objetos de arquivos comprimidos, bancos de dados de e-mails e arquivos em formato de e-mail da Quarentena, selecione também o diretório no qual serão restaurados.

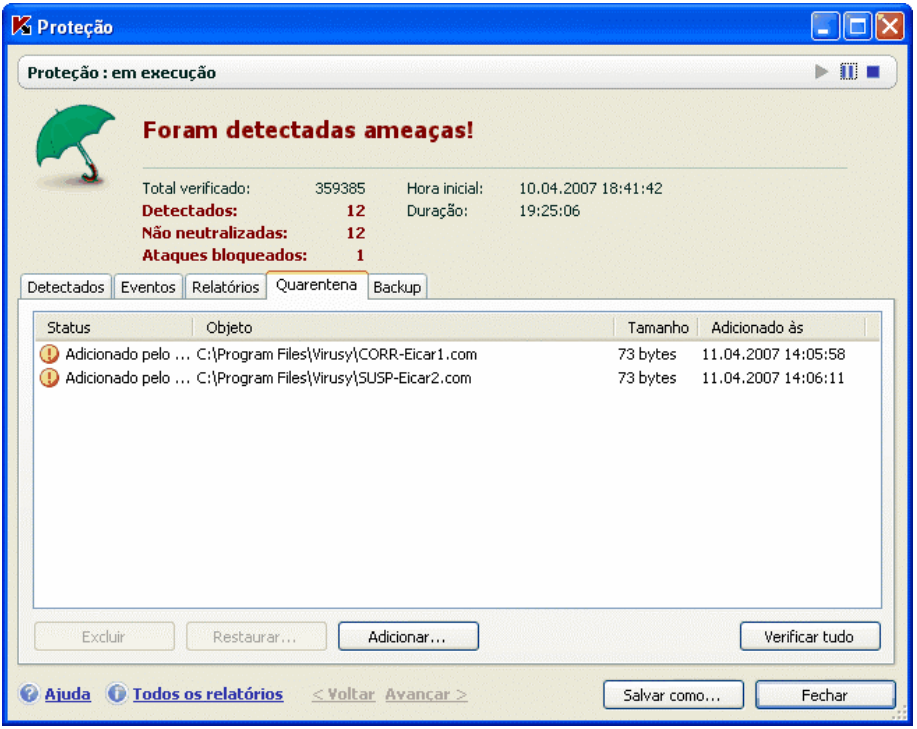


Figura 54. Lista de objetos em quarentena

Dica:
É recomendável restaurar apenas objetos com status *falso positivo, OK* e *desinfectado*, pois a restauração de outros objetos pode levar à infecção do computador.

- Excluir todos os objetos ou grupos de objetos selecionados em quarentena. Exclua os objetos apenas se não puderem ser desinfectados. Para excluir os objetos, selecione-os na lista e clique em **Excluir**.

14.1.2. Configurando a Quarentena

Você pode configurar o layout e o funcionamento da Quarentena, mais especificamente:

- Configurar verificações automáticas de objetos em Quarentena após cada atualização das assinaturas de ameaças (para obter mais detalhes, consulte 13.4.4 na p. 163).

  Aviso!

  O programa não poderá verificar objetos em quarentena imediatamente após a atualização das assinaturas de ameaças, se você estiver acessando a área de Quarentena.

- Definir o tempo máximo de armazenamento na Quarentena.

  O tempo de armazenamento padrão é de 30 dias e, ao término dele, os objetos são excluídos. Você pode alterar o tempo de armazenamento da Quarentena ou desabilitar totalmente esta restrição.

Para fazê-lo:

1. Abra a janela de configurações do Kaspersky Anti-Virus clicando em Configurações na janela principal do programa.
2. Selecione **Arquivos de dados** na árvore de configurações.
3. Na seção **Quarentena e Backup** (veja a fig. 55), insira o período depois do qual os objetos na Quarantine serão excluídos automaticamente. Alternativamente, desmarque a caixa de seleção para desabilitar a exclusão automática.

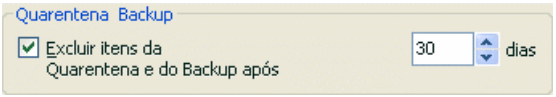


Figura 55. Configurando o período de armazenamento na Quarentena

14.2. Cópias de backup de objetos perigosos

Às vezes, quando os objetos são desinfectados, sua integridade é perdida. Se um arquivo desinfectado contiver informações importantes que foram parcial ou totalmente corrompidas, você pode tentar restaurar o objeto original a partir de uma cópia de backup.

Uma **cópia de backup** é uma cópia do objeto perigoso original criada antes de o objeto ser desinfectado ou excluído. Ela é salva no Backup.

O **Backup** é uma área de armazenamento específica que mantém cópias de backup dos objetos perigosos. Os arquivos no Backup são salvos em um formato específico e não são perigosos.

14.2.1. Ações sobre cópias de backup

O número total de cópias de objetos no Backup é exibido em **Arquivos de dados**, na seção **Serviço** da janela principal do aplicativo. À direita da tela, a seção *Backup* exibe:

- o número de cópias de backup de objetos criados pelo Kaspersky Anti-Virus
- o tamanho atual do Backup.

Aqui, você pode excluir todas as cópias do Backup com o botão **Esvaziar**. Observe que, ao fazê-lo, os objetos na Quarentena e arquivos de relatório também serão excluídos.

Para acessar as cópias de objetos perigosos:

Clique em qualquer local da caixa *Backup* para abrir a janela **Proteção**, que resume a proteção fornecida pelo aplicativo.

Uma lista de cópias de backup será exibida na guia Backup (veja a fig. 56). As seguintes informações são exibidas para cada cópia: o nome e o caminho completo do objeto, o status do objeto atribuído pela verificação e seu tamanho.

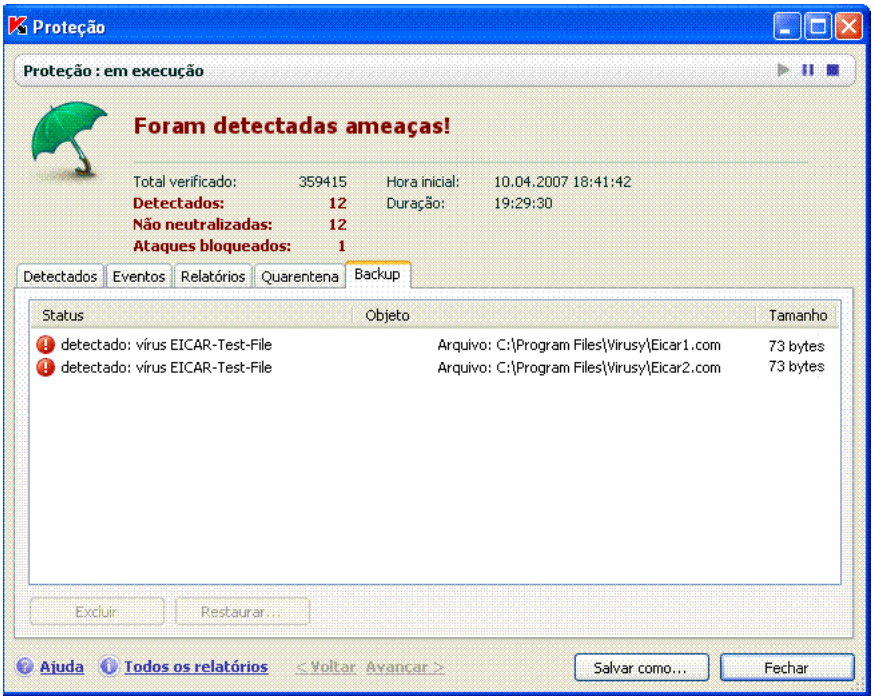


Figura 56. Cópias de backup de objetos excluídos ou desinfectados

Você pode restaurar cópias selecionadas usando o botão **Restaurar**. O objeto é restaurado do Backup com o mesmo nome que tinha antes da desinfecção.

Se houver um objeto com esse nome no local original (isto é possível se foi feita uma cópia do objeto que está sendo restaurado antes da desinfecção), será exibido um aviso. Você pode alterar o local do objeto restaurado ou renomeá-lo.

É recomendável verificar os objetos de backup quanto à presença de vírus imediatamente após sua restauração. É possível que, com as assinaturas atualizadas, você consiga desinfectá-lo sem perder a integridade do arquivo.

É recomendável **não** restaurar cópias de backup de objetos, exceto quando absolutamente necessário. Isto pode levar à infecção do computador.

É recomendável examinar a área de Backup e esvaziá-la usando o botão **Excluir** periodicamente. Você também pode configurar o programa de modo a excluir automaticamente as cópias mais antigas de Backup (consulte 14.2.2 na p. 173).

14.2.2. Configurando o Backup

Você pode definir o tempo máximo que as cópias permanecem na área de Backup.

O tempo de armazenamento padrão do Backup é 30 dias e, ao término dele, as cópias são excluídas. Você pode alterar o tempo de armazenamento ou remover totalmente esta restrição. Para fazê-lo:

1. Abra a janela de configurações do Kaspersky Anti-Virus clicando em Configurações na janela principal do programa.
2. Selecione **Arquivos de dados** na árvore de configurações.
3. Defina a duração do armazenamento de cópias de backup no repositório na seção **Quarentena e Backup** (veja a fig. 55) à direita da tela. Alternativamente, desmarque a caixa de seleção para desabilitar a exclusão automática.

14.3. Relatórios

As ações de componentes do Kaspersky Anti-Virus, as tarefas de verificação de vírus e as atualizações são registradas em relatórios.

O número total de relatórios criados pelo programa e seu tamanho total são exibidos clicando em **Arquivos de dados**, na seção **Serviço** da janela principal do programa. As informações são exibidas na caixa *Relatórios*.

Para exibir relatórios:

Clique em qualquer local da caixa *Relatórios* para abrir a janela Proteção, que resume a proteção fornecida pelo aplicativo. Será aberta uma janela na guia **Relatórios** (veja a fig. 57).

A guia Relatórios lista os relatórios mais recentes de todos os componentes e tarefas de verificação de vírus executados nesta sessão do Kaspersky Anti-Virus. O status é mostrado ao lado de cada componente ou tarefa, por exemplo, *interrompido* ou *concluído*. Se desejar exibir o histórico completo da criação do relatório da sessão atual do programa, marque ☑ **Mostrar histórico de relatórios**.

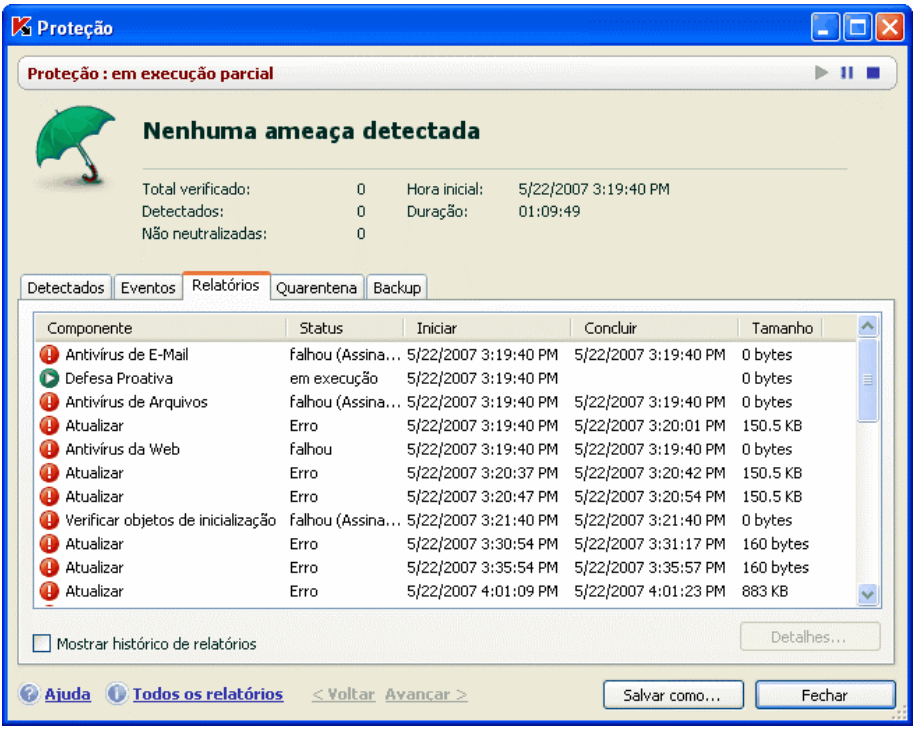


Figura 57. Relatórios de funcionamento do componente

Para analisar todos os eventos registrados para um componente ou tarefa:

Selecione o nome do componente ou tarefa na guia **Relatórios** e clique no botão **Detalhes**.

Uma janela será aberta, contendo informações detalhadas sobre o desempenho do componente da ou tarefa selecionada. As estatísticas de desempenho resultantes são exibidas na parte superior da janela e informações detalhadas são fornecidas nas guias. Dependendo do componente ou tarefa, as guias podem variar:

- A guia **Detectados** contém uma lista de objetos perigosos detectados por um componente ou uma tarefa de verificação de vírus.
- A guia **Eventos** exibe os eventos de componentes ou tarefas.
- A guia **Estatísticas** contém estatísticas detalhadas de todos os objetos verificados.

- A guia **Configurações** exibe as configurações usadas pelos componentes de proteção, verificações de vírus ou atualizações de assinaturas de ameaças.
- As guias **Macros** e **Registro** aparecem apenas no relatório da Defesa Proativa e contêm informações sobre todas as macros que tentaram executar no computador e todas as tentativas de modificar o Registro do sistema operacional.

Você pode exportar todo o relatório como um arquivo de texto. Este recurso é útil quando ocorre um erro que você não consegue eliminar sozinho e você precisa de assistência do Suporte Técnico. Se isso acontecer, o relatório deve ser enviado como um arquivo .txt para o Suporte Técnico, para que nossos especialistas possam estudar o problema detalhadamente e solucioná-lo assim que possível.

Para exportar um relatório como arquivo de texto:

Clique em **Salvar como** e especifique o local onde deseja salvar o arquivo do relatório.

Depois de terminar o trabalho com o relatório, clique em **Fechar**.

Existe um botão Ações em todas as guias (exceto em **Configurações** e **Estatísticas**) que você pode usar para definir respostas aos objetos na lista. Ao clicar nele, um menu de contexto é aberto, com uma seleção dos seguintes itens de menu (i menu é diferente dependendo do componente; todas as opções possíveis estão relacionadas a seguir):

Desinfectar – tenta desinfectar um objeto perigoso. Se o objeto não for desinfectado com êxito, você pode deixá-lo nesta lista para que seja verificado posteriormente com assinaturas de ameaças atualizadas ou excluí-lo. Você pode aplicar esta ação a um único objeto na lista ou a vários objetos selecionados.

Descartar – exclui do relatório o registro sobre a detecção do objeto.

Adicionar à zona confiável – exclui o objeto da proteção. Será aberta uma janela com uma regra de exclusão para o objeto.

Ir para o arquivo – abre a pasta na qual o objeto está localizado no Windows Explorer.

Neutralizar tudo – neutraliza todos os objetos da lista. O Kaspersky Anti-Virus tentará processar os objetos usando as assinaturas de ameaças.

Descartar tudo – limpa o relatório sobre objetos detectados. Ao usar esta função, todos os objetos perigosos detectados permanecem no computador.

Exibir em www.viruslist.com – vai para uma descrição do objeto na Enciclopédia de Vírus (em inglês) no site da Kaspersky Lab.

Pesquisar www.google.com – localiza informações sobre o objeto usando este mecanismo de pesquisa.

Pesquisar – insere termos de pesquisa para objetos da lista, por nome ou status.

Além disso, você pode classificar as informações exibidas na janela em ordem crescente e decrescente, para cada coluna, clicando no cabeçalho da coluna.

14.3.1. Configurando relatórios

Para configurar a criação e a forma como os relatórios são salvos:

1. Abra a janela de configurações do Kaspersky Anti-Virus clicando em Configurações na janela principal do programa.
2. Selecione **Arquivos de dados** na árvore de configurações.
3. Edite as configurações na caixa **Relatórios** (veja a fig. 58) da seguinte maneira:
   - Permita ou desabilite o registro de eventos informativos. Geralmente, estes eventos não são importantes para a segurança. Para registrar os eventos, marque **Registrar eventos não críticos**;
   - Escolha relatar apenas os eventos que ocorreram desde a última vez que a tarefa foi executada. Isto economiza espaço em disco por reduzir o tamanho do relatório. Se **Manter apenas eventos recentes** estiver marcado, o relatório será iniciado do zero sempre que você reiniciar a tarefa. Entretanto, apenas as informações não críticas serão substituídas.
   - Defina o tempo de armazenamento dos relatórios. Por padrão, o tempo de armazenamento de relatórios é de 30 dias e, ao término dele, os relatórios são excluídos. Você pode alterar o tempo máximo de armazenamento ou remover totalmente esta restrição.

Figura 58. Configurando relatórios

14.3.2. A guia *Detectados*

Esta guia (veja a fig. 59) contém uma lista de objetos perigosos detectados pelo Kaspersky Anti-Virus. O caminho e o nome completo de cada objeto são mostrados, com o status atribuído a ele pelo programa na sua verificação ou processamento.

Se desejar que a lista contenha os objetos perigosos e os objetos neutralizados com êxito, marque **Mostrar objetos neutralizados**.

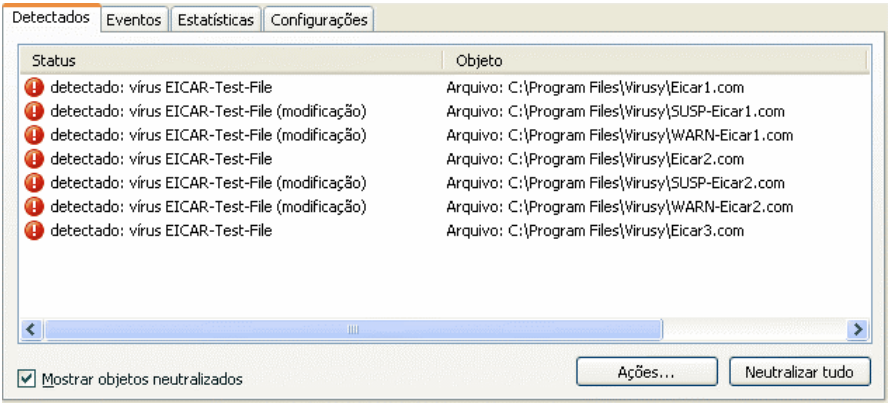


Figura 59. Lista de objetos perigosos detectados

Os objetos perigosos detectados pelo Kaspersky Anti-Virus são processados usando o botão **Neutralizar** (para um objeto ou grupo de objetos selecionados) ou **Neutralizar tudo** (para processar todos os objetos da lista). Ao processar cada objeto, será exibida uma notificação na tela, na qual você decide as ações que serão tomadas a seguir.

Se você marcar **Aplicar a todos** na janela de notificação, a ação selecionada será aplicada a todos os objetos com o status selecionado na lista, antes de iniciar o processamento.

14.3.3. A guia *Eventos*

Esta guia (veja a fig. 60) fornece uma lista completa de todos os eventos importantes no funcionamento do componente, nas verificações de vírus e nas atualizações de assinaturas de ameaças que não foram substituídos por uma regra de controle de atividade (consulte 10.1.1 na p. 118).

Estes eventos podem ser:

Eventos críticos são aqueles de importância crítica que indicam problemas na operação do programa ou vulnerabilidades do seu computador. Por exemplo, *vírus detectado*, *erro de funcionamento*.

Eventos importantes são aqueles que devem ser investigados, pois refletem situações importantes no funcionamento do programa. Por exemplo, *interrompido*.

Mensagens informativas são do tipo de referência, que geralmente não contêm informações importantes. Por exemplo, *OK, não processado*. Esse eventos serão exibidos no log de eventos somente se **Mostrar todos os eventos** estiver marcado.

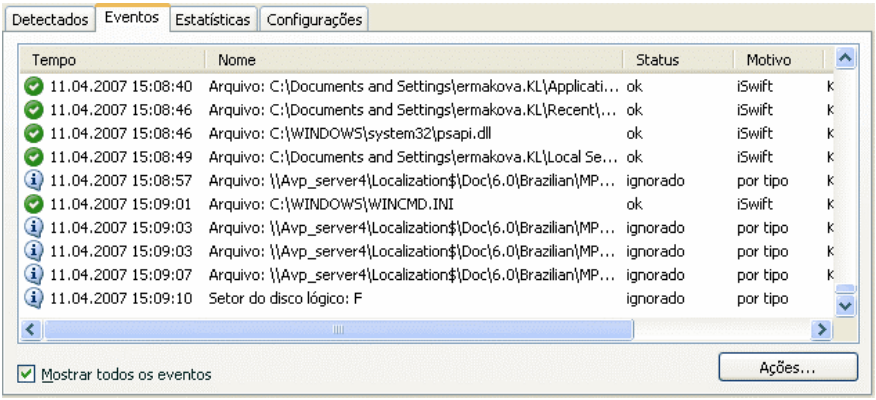


Figura 60. Eventos que ocorrem no funcionamento do componente

O formato para exibição de eventos no log de eventos pode variar de acordo com o componente ou tarefa. Para tarefas de atualização, são fornecidas as seguintes informações:

- Nome do evento
- Nome do objeto envolvido no evento
- Hora em que o evento ocorreu
- Tamanho do arquivo carregado

Para tarefas de verificação de vírus, o log de eventos contém o nome do objeto verificado e o status atribuído a ele pela verificação/processamento.

14.3.4. A guia Estatísticas

Esta guia (veja a fig. 61) fornece estatísticas detalhadas sobre os componentes e tarefas de verificação de vírus. Aqui, você pode descobrir:

- Quantos objetos foram verificados quanto a indícios perigosos nesta sessão de um componente ou após a conclusão de uma tarefa. É exibido o número de arquivos comprimidos, arquivos compactados e arquivos protegidos por senha verificados, e de objetos corrompidos.
- Quantos objetos perigosos foram detectados, não desinfectados, excluídos e colocados em Quarentena.

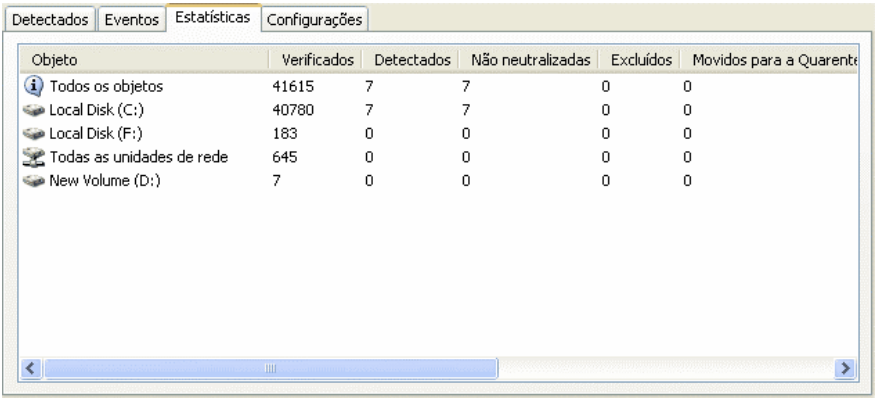


Figura 61. Estatísticas do componente

14.3.5. A guia Configurações

A guia **Configurações** (veja a fig. 62) exibe uma visão geral completa das configurações de componentes, verificações de vírus e atualizações do programa. Você pode descobrir o nível de segurança atual de um componente ou verificação de vírus, quais ações são executadas com relação a objetos perigosos ou quais configurações são usadas para as atualizações do programa. Use o link Alterar configurações para configurar o componente.

Você pode definir configurações avançadas para verificações de vírus:

- Estabeleça a prioridade das tarefas de verificação usadas, se o processador estiver sobrecarregado. A configuração padrão de ☑ **Conceder recursos a outros aplicativos** é desmarcada. Com este recurso, o programa controla a carga nos subsistemas do processador e do disco, de acordo com a atividade de outros aplicativos. Se a carga do processador aumentar de forma significativa e impedir a operação normal dos aplicativos do usuário, o programa reduzirá a atividade de verificação. Isto aumenta o tempo de verificação e libera os recursos para os aplicativos do usuário.

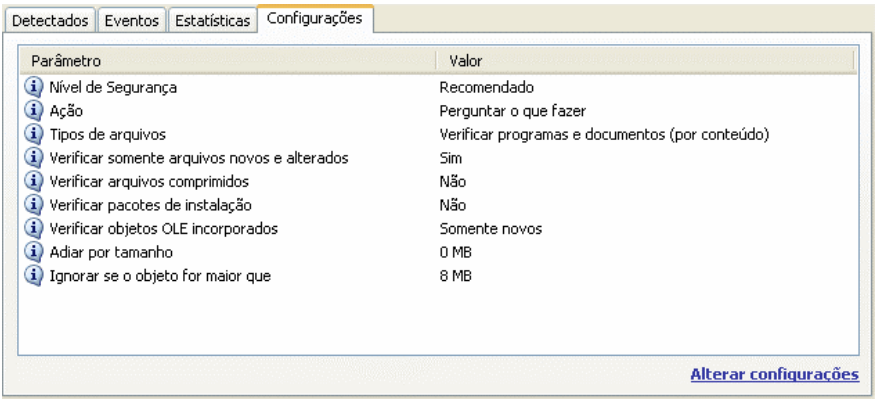


Figura 62. Configurações do componente

- Defina o modo de operação do computador após a conclusão de uma verificação de vírus. Você pode configurar o computador para desligar, reiniciar ou entrar em modo em espera ou em suspensão. Para selecionar uma opção, clique no link até a opção desejada ser exibida.

  Você pode precisar deste recurso se, por exemplo, iniciar uma verificação de vírus no fim do dia de trabalho e não quiser esperar que ela termine.

  Entretanto, para usar este recurso, é necessário tomar as seguintes medidas adicionais: antes de iniciar a verificação, desabilite as solicitações de senha para os objetos que estão sendo verificados, se estiverem habilitadas, e habilite o processamento automático de objetos perigosos, para desabilitar os recursos interativos do programa.

14.3.6. A guia *Macros*

Todas as macros que tentaram ser executadas durante a sessão atual do Kaspersky Anti-Virus são listadas na guia **Macros** (veja a Figura 63). Aqui, você encontrará o nome completo de cada macro, a hora em que foi executada e seu status após o processamento.

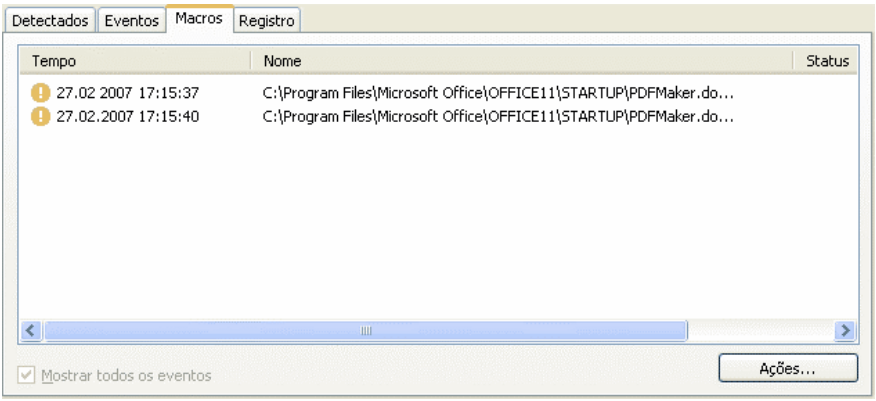


Figura 63. Macros perigosas detectadas

Você pode escolher o modo de exibição desta guia. Se não desejar ver eventos informativos, desmarque ☑ **Mostrar todos os eventos**.

14.3.7. A guia *Registro*

O programa registra as operações com chaves do registro que foram tentadas desde que o programa foi iniciado na guia **Registro** (veja a fig. 64), a menos que proibido por uma regra (consulte 0 na p. 131).

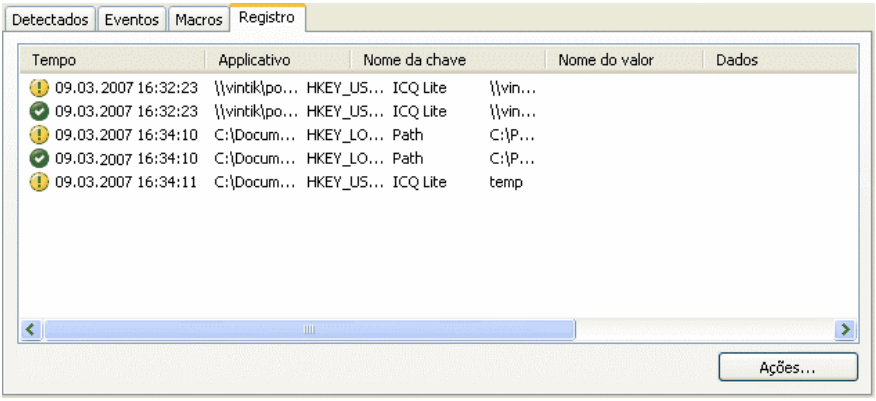


Figura 64. . Ler e modificar eventos do registro do sistema

A guia lista o nome completo da chave, seu valor, o tipo de dados e as informações sobre a operação que foi realizada: qual ação se tentou executar, a que horas e se foi permitida.

14.4. Informações gerais sobre o programa

Você pode exibir informações gerais sobre o programa na seção **Serviço** da janela principal (veja a fig. 65).

Figura 65. Informações sobre o programa, a licença e o sistema em que está instalado

Todas as informações estão divididas em três seções:

- A versão do programa, a data da última atualização e o número de ameaças conhecidas até o momento são exibidos na caixa **Informações do produto**.
- As informações básicas sobre o sistema operacional instalado no computador são mostradas na caixa **Informações do sistema**.
- Informações básicas sobre a licença do Kaspersky Anti-Virus que você comprou estão na caixa **Informações da licença**.

Você precisará de todas essas informações quando entrar em contato com o Suporte Técnico da Kaspersky Lab (consulte 14.5 na p. 183).

14.5. Gerenciando licenças

O Kaspersky Anti-Virus precisa de uma *chave de licença* para funcionar. Você recebe uma chave ao adquirir o programa. Ela lhe concede o direito de usar o programa a partir do dia em quem instala a chave.

Sem uma chave de licença, a menos que uma versão de teste do aplicativo tenha sido ativada, o Kaspersky Anti-Virus será executado no modo de uma atualização. O programa não baixará novas atualizações.

Se uma versão de teste do programa tiver sido ativada (válida por 30 dias), depois de expirado esse período, o Kaspersky Anti-Virus não será executado.

Quando a chave de licença comercial expirar, o programa continuará funcionando, exceto pelo fato de você não poder atualizar as assinaturas de ameaças. Como antes, você poderá verificar seu computador quanto à presença de vírus e usar os componentes de proteção, mas apenas com as assinaturas de ameaças que você tinha antes de a licença expirar. Não podemos garantir que você estará protegido contra os vírus que surgirem depois que a licença do programa expirar.

Para evitar infectar o computador com novos vírus, é recomendável estender a licença do Kaspersky Anti-Virus. O programa o notificará duas semanas antes da expiração da licença e, durante essas semanas, essa mensagem será exibida sempre que for aberto.

Para prorrogar sua licença, compre e instale uma nova chave de licença do Kaspersky Anti-Virus ou insira um código de ativação do programa. Para fazê-lo:

Entre em contato com o fornecedor de quem comprou o produto e adquira um novo código de ativação.

ou:

Adquira uma chave de licença ou um código de ativação diretamente da Kaspersky Lab, clicando no link Comprar licença na janela da chave de licença. Preencha o formulário no site. Depois que o pagamento for feito, enviaremos um link para o endereço de e-mail que você inseriu no formulário de pedido. Com esse link, você poderá baixar uma chave de licença ou receber um código de ativação do programa.

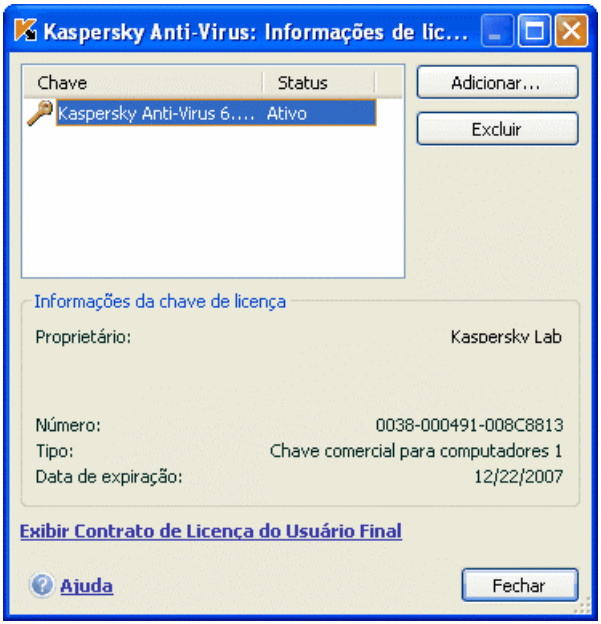


Figura 66. Informações de licença

Periodicamente, a Kaspersky Lab lança ofertas de extensões de licença de nossos produtos. Verifique as ofertas no site da Kaspersky Lab, em **Products → Sales and special offers**.

Informações sobre a chave de licença usada estão disponíveis na caixa **Informações da licença** na seção **Serviço** na janela principal do programa. Para abrir a janela do gerenciador de licenças, clique em qualquer local da caixa. Na janela que é aberta (veja a Figura 66), você pode ver informações sobre a chave atual, adicionar ou excluir uma chave.

Ao selecionar uma chave na lista da caixa **Informações da licença**, serão exibidas informações sobre o número, o tipo e a data de expiração da licença. Para adicionar uma nova chave de licença, clique em **Adicionar** e ative o aplicativo com o assistente de ativação (consulte 3.2.2 na p. 34). Para excluir uma chave da lista, use o botão **Excluir**.

Para examinar os termos do EULA, clique em Exibir Contrato de Licença do Usuário Final. Para obter uma licença através da loja eletrônica no site da Kaspersky Lab, clique no link Comprar licença.

14.6. Suporte Técnico

O Kaspersky Anti-Virus fornece uma grande variedade de opções para dúvidas e problemas relacionados com o funcionamento do programa. Elas estão localizadas em **Suporte** (veja a fig. 67), na seção **Serviço**.

Figura 67. Informações sobre o suporte técnico

Dependendo do problema, fornecemos vários serviços de suporte técnico:

Fórum de usuários. Este recurso é uma seção dedicada do site da Kaspersky Lab com perguntas, comentários e sugestões de usuários do programa. Você pode examinar os tópicos básicos do fórum e deixar um comentário. Talvez também encontre a resposta para sua pergunta.

Para acessar este recurso, use o link Fórum de usuários.

Base de dados de conhecimento. Este recurso também é uma seção dedicada do site da Kaspersky Lab e contém recomendações de Suporte Técnico para o uso do software da Kaspersky Lab e respostas para perguntas freqüentes. Tente encontrar uma resposta para sua pergunta ou uma solução para seu problema com este recurso.

Para obter suporte técnico on-line, clique no link Base de dados de conhecimento.

Comentários sobre a operação do programa. Este serviço foi criado para postar comentários sobre o funcionamento do programa ou descrever um problema que apareceu durante sua operação. É necessário preencher um formulário específico no site da empresa, descrevendo a situação detalhadamente. Para lidar com o problema da melhor forma, a Kaspersky Lab precisará de algumas informações sobre o seu sistema. Você pode descrever a configuração do sistema sozinho ou usar o coletor de informações automático no seu computador.

Para ir para o formulário de comentários, use o link Informar sobre este erro ou enviar um comentário.

Suporte técnico. Se precisar de ajuda ao usar o Kaspersky Anti-Virus, clique no link localizado na caixa **Serviço de Suporte Local**. O site da Kaspersky Lab será aberto com informações sobre como contatar nossos especialistas.

14.7. Criando uma lista de portas monitoradas

Os componentes como o Antivírus de E-Mail e o Antivírus da Web monitoram fluxos de dados transmitidos usando determinados protocolos e que passam por determinadas portas abertas no computador. Assim, por exemplo, o Antivírus de E-Mail analisa informações transferidas usando o protocolo SMTP e o Antivírus da Web analisa informações transferidas usando HTTP.

A lista de portas padrão que geralmente são usadas para transmitir tráfego de e-mail e HTTP é fornecida com o pacote do programa. Você pode adicionar uma nova porta ou desabilitar a monitoração de uma determinada porta, desabilitando assim a detecção de objetos perigosos para o tráfego que passa por essa porta.

Para editar a lista de portas monitoradas, execute as seguintes etapas:

1. Abra a janela de configurações do Kaspersky Anti-Virus clicando no link Configurações na janela principal do programa.
2. Selecione **Configurações de rede** na seção **Serviço** da árvore de configurações do programa.
3. Clique em **Configurações de porta** à direita da janela de configurações.

4. Edite a lista de portas monitoradas na janela que é aberta (veja a fig. 68).

Esta janela fornece uma lista de portas monitoradas pelo Kaspersky Anti-Virus. Para verificar os fluxos de dados de todas as portas de rede abertas, selecione a opção **Monitorar todas as portas**. Para editar a lista de portas monitoradas manualmente, selecione **Monitorar somente portas selecionadas**.

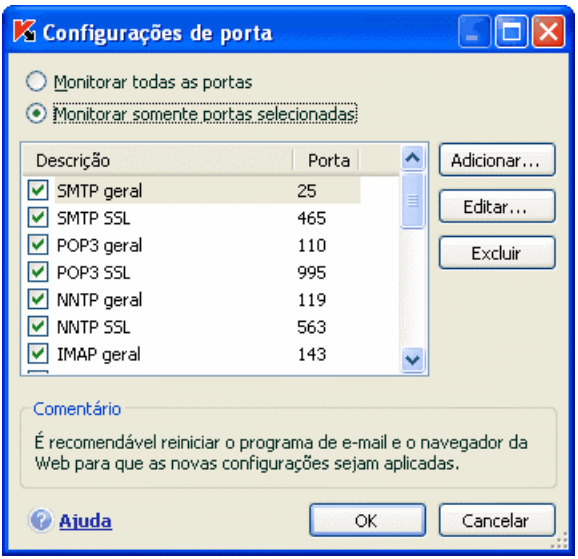


Figura 68. Lista de portas monitoradas

Para adicionar uma nova porta à lista de portas monitoradas:

1. Clique no botão **Adicionar** na janela **Configurações de porta**.
2. Insira o número e uma descrição da porta nos campos apropriados na janela **Nova porta**.

Por exemplo, pode haver uma porta não-padrão no computador, através da qual são trocados dados com um computador remoto usando o protocolo HTTP, que é monitorado pelo Antivírus da Web. Para analisar esse tráfego quanto à presença de código mal-intencionado, adicione essa porta a uma lista de portas controladas.

Quando algum de seus componentes é iniciado, o Kaspersky Anti-Virus abre a porta 1110 como ouvinte para todas as conexões de entrada. Se ela estiver ocupada no momento, as portas 1111, 1112, etc. serão selecionadas como ouvintes.

Se você usar o Kaspersky Anti-Virus e o firewall de outra empresa simultaneamente, configure o firewall para permitir que o processo *avp.exe* (processo interno do Kaspersky Anti-Virus) acesse todas as portas relacionadas acima.

Por exemplo, se o firewall contém uma regra para *iexplorer.exe*, que permite que esse processo estabeleça conexões na porta 80.

Entretanto, quando o Kaspersky Anti-Virus intercepta a consulta de conexão iniciada por *iexplorer.exe* na porta 80, ele a transfere para *avp.exe* que, por sua vez, tenta estabelecer uma conexão com a página da Web de forma independente. Se não houver uma regra de permissão para *avp.exe*, o firewall bloqueará essa consulta. Então, o usuário não poderá acessar a página da Web.

14.8. Verificando a conexão SSL

Conectar-se usando o protocolo SSL protege a troca de dados pela Internet. O protocolo SSL identifica as partes que trocam dados usando certificados eletrônicos, codifica os dados que são transferidos e assegura sua integridade durante a transferência.

Esses recursos do protocolo são usados por hackers para disseminar programas mal-intencionados, pois a maioria dos programas antivírus não verifica o tráfego SSL.

O Kaspersky Anti-Virus 6.0 possui a opção de verificar vírus no tráfego SSL. Quando for feita uma tentativa de conexão segura a um recurso da Web, uma notificação aparecerá na tela (veja a Figura 69) perguntando o que fazer.

A notificação contém informações sobre o programa que iniciou a conexão segura, junto com o endereço remoto e a porta. O programa solicita que você decida se a conexão deve ser verificada quanto à presença de vírus:

- **Processar** – verifica o tráfego quanto à presença de vírus ao conectar-se ao site de maneira segura.

  É recomendável sempre verificar o tráfego SSL se você estiver usando um site suspeito ou se uma transferência de dados SSL começar quando você passa para outra página. É bastante provável que isso seja um sinal de transferência de um programa mal-intencionado em um protocolo seguro.

- **Ignorar** – continua a conexão segura com o site, sem verificar o tráfego quanto à presença de vírus.

Para aplicar a ação selecionada a todas as tentativas de estabelecer conexões SSL, marque **Aplicar a todos**.

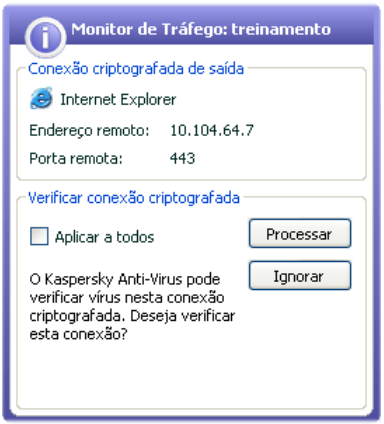


Figura 69. Notificação de detecção de conexão SSL

Para verificar conexões criptografadas, o Kaspersky Anti-Virus substitui o certificado de segurança solicitado por um certificado assinado por ele mesmo. Em alguns casos, os programas que estão estabelecendo conexões não aceitarão esse certificado e nenhuma conexão será estabelecida. É recomendável desabilitar a verificação de tráfego SSL nos seguintes casos:

- Ao conectar-se a um recurso da Web confiável, como a página do seu banco, na qual você gerencia sua conta pessoal. Nesse caso, é importante receber a confirmação da autenticidade do certificado do banco.
- Se o programa que está estabelecendo a conexão verificar o certificado do site acessado. Por exemplo, o MSN Messenger verifica a autenticidade da assinatura digital da Microsoft Corporation ao estabelecer uma conexão com o servidor.

Você pode configurar a verificação de SSL na guia **Configurações de rede** da janela de configurações do programa:

Verificar todas as conexões criptografadas – verifica vírus em todo o tráfego de entrada no protocolo SSL.

Perguntar ao usuário quando uma nova conexão criptografada for detectada – exibe uma mensagem que pergunta o que fazer sempre que uma conexão SSL é estabelecida.

Não verificar conexões criptografadas – não verifica vírus no tráfego de entrada do protocolo SSL.

14.9. Configurando a interface do Kaspersky Anti-Virus

O Kaspersky Anti-Virus lhe dá a opção de alterar a aparência do programa, criando e usando capas. Você também pode configurar o uso dos elementos de interface ativos, como o ícone da bandeja do sistema e as mensagens pop-up.

Para configurar a interface do programa, execute as seguintes etapas:

1. Abra a janela de configurações do Kaspersky Anti-Virus clicando no link Configurações na janela principal do programa.
2. Selecione **Aparência** na seção **Serviço** da árvore de configurações do programa (veja a fig. 70).

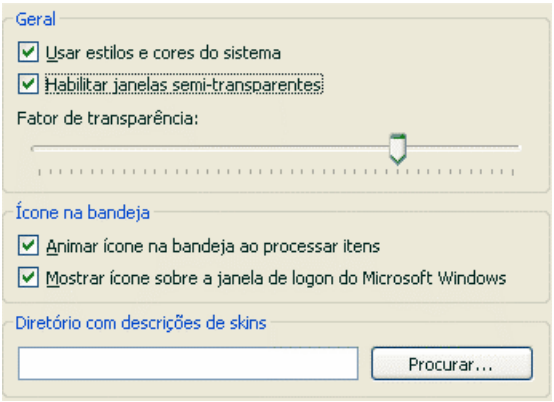


Figura 70. Configurando a aparência do programa

À direita da janela de configurações, você pode determinar:

- Se o indicador de proteção do Kaspersky Anti-Virus será exibido quando o sistema operacional for iniciado.

  Por padrão, esse indicador aparece no canto superior direito da tela quando o programa é carregado. Ele informa se o computador está protegido de todos os tipos de ameaça. Se não desejar usar o indicador de proteção, desmarque ☑ **Mostrar ícone sobre a janela de logon do Microsoft Windows**.

- Se a animação será usada no ícone da bandeja do sistema.

  Dependendo da operação do programa realizada, o ícone da bandeja do sistema muda. Por exemplo, se um script estiver sendo verificado, uma

pequena ilustração de um script aparecerá no plano de fundo do ícone e, se um e-mail estiver sendo verificado, um envelope. Por padrão, a animação do ícone está ativada. Se desejar desativar a animação, desmarque **Animar ícone na bandeja ao processar itens**. Em seguida, o ícone indicará apenas o status de proteção do computador. Se a proteção estiver habilitada, o ícone ficará colorido e, se a proteção for pausada ou desabilitada, o ícone ficará cinza.

- Grau de transparência das mensagens pop-up.

  Todas as operações do Kaspersky Anti-Virus que devem ser informadas a você imediatamente ou que exigem que você tome uma decisão são apresentadas como mensagens pop-up acima do ícone da bandeja do sistema. As janelas de mensagem são transparentes, de modo a não interferir no seu trabalho. Se você mover o cursor sobre a mensagem, a transparência desaparecerá. Você pode alterar o grau de transparência dessas mensagens. Para fazê-lo, ajuste a escala do **Fator de transparência** para a posição desejada. Para remover a transparência da mensagem, desmarque **Habilitar janelas semi-transparentes**.

Esta opção não estará disponível se você estiver executando o aplicativo no Microsoft Windows 98/NT 4.0/ME.

- Use suas próprias capas para a interface do programa.

  Todas as cores, fontes, ícones e textos usados na interface do Kaspersky Anti-Virus podem ser alterados. Você pode criar seus próprios elementos gráficos para o programa ou localizá-los em outro idioma. Para usar uma capa, especifique o diretório com suas configurações no campo **Diretório com descrições de capas**. Use o botão **Procurar** para selecionar o diretório.

  Por padrão, as cores e estilos do sistema são usados na capa do programa. Você pode removê-los, desmarcando **Usar estilos e cores do sistema**. Então, os estilos especificados nas configurações do tema da tela serão usados.

Observe que as alterações das configurações da interface do Kaspersky Anti-Virus não serão salvas se você restaurar as configurações de operação padrão ou desinstalar o programa.

14.10. Disco de Recuperação

O Kaspersky Anti-Virus possui uma ferramenta para a criação de um disco de recuperação.

O disco de recuperação foi criado para restaurar a funcionalidade do sistema após um ataque de vírus danificar arquivos do sistema e tornar impossível iniciar o sistema operacional. Este disco inclui:

- Arquivos do sistema Microsoft Windows XP Service Pack 2
- Um conjunto de utilitários de diagnóstico do sistema operacional
- Arquivos de programa do Kaspersky Anti-Virus
- Arquivos contendo assinaturas de ameaças

Para criar um disco de recuperação:

1. Abra a janela principal do programa e selecione **Disco de recuperação** na seção **Serviço**.
2. Clique no botão **Iniciar Assistente** para iniciar o processo de criação do disco de recuperação.

Um Disco de Recuperação se destina ao computador no qual foi criado. O uso do disco em outros computadores poderia ter conseqüências imprevisíveis, pois ele contém informações sobre os parâmetros de um determinado computador (informações sobre os setores de inicialização, por exemplo).

Você pode criar um disco de recuperação somente no Windows XP ou no Microsoft Windows Vista. O recurso do disco de recuperação não está disponível em outros sistemas operacionais com suporte, incluindo o Microsoft Windows XP Professional x64 Edition e o Microsoft Windows Vista x64.

14.10.1. Criando um disco de recuperação

Aviso! O disco de instalação do Microsoft Windows XP Service Pack 2 é necessário para criar um disco de emergência.

Você precisa do programa **PE Builder** para criar o Disco de Recuperação.

Instale o PE Builder no computador antes de criar um disco de emergência com ele.

Um Assistente específico o orientará no processo de criação de um disco de recuperação. Ele consiste em uma série de janelas/etapas nas quais você pode navegar usando os botões **Avançar** e **Voltar**. Você pode concluir o Assistente clicando em **Concluído**. O botão **Cancelar** interromperá o Assistente a qualquer momento.

Etapa 1. Preparando-se para gravar o disco

Para criar um disco de recuperação, especifique o caminho para as seguintes pastas:

- Pasta do programa PE Builder
- Pasta na qual os arquivos do disco de recuperação serão salvos antes de gravar o CD

  Se esta não for a primeira vez que você cria um disco de emergência, essa pasta já conterá um conjunto de arquivos criados da última vez. Para usar os arquivos salvos anteriormente, marque a caixa correspondente.

  > Observe que uma versão anterior dos arquivos do disco de recuperação conterá assinaturas de ameaças desatualizadas. Para analisar o computador quanto à presença de vírus e restaurar o sistema de forma ideal, é recomendável atualizar as assinaturas de ameaças e criar uma nova versão do disco de recuperação.

- CD de instalação do Microsoft Windows XP Service Pack 2

Depois de inserir os caminhos para as pastas necessárias, clique em **Avançar**. O PE Builder será iniciado e o processo de criação do disco de recuperação começará. Aguarde até o processo ser concluído. Isto pode levar vários minutos.

Etapa 2. Criando um arquivo .iso

Depois que o PE Builder tiver concluído a criação dos arquivos do disco de recuperação, uma janela **Criar arquivo ISO** será aberta.

O arquivo .iso é uma imagem em CD do disco de recuperação, salva como um arquivo. A maioria dos programas para gravação de CDs reconhece corretamente os arquivos .iso (o Nero, por exemplo).

Se esta não for a primeira vez que você cria um disco de recuperação, você poderá selecionar o arquivo .iso no disco anterior. Para fazê-lo, selecione **Arquivo ISO existente**.

Etapa 3. Gravando o disco

Esta janela do Assistente solicitará que você decida gravar os arquivos do disco de recuperação no CD agora ou depois.

Se você optar por gravar o disco imediatamente, especifique se deseja formatar o CD antes de gravá-lo. Para fazê-lo, marque a caixa correspondente. Esta opção estará disponível somente se você estiver usando um CD-RW.

O CD começará a ser gravado quando você clicar no botão **Avançar**. Aguarde até o processo ser concluído. Isto pode levar vários minutos.

Etapa 4. Concluindo a criação de um disco de recuperação

Esta janela do Assistente informa que você criou um disco de recuperação com êxito.

14.10.2. Usando o disco de recuperação

Observe que o Kaspersky Anti-Virus funcionará no modo de recuperação do sistema somente se a janela principal estiver aberta. Ao fechar a janela principal, o programa será fechado.

O Bart PE, o programa padrão, não dá suporte a arquivos .chm, nem a navegadores da Internet; portanto, você não poderá exibir a Ajuda do Kaspersky Anti-Virus, nem os links na interface do programa no Modo de Recuperação.

Se um ataque de vírus impossibilitar o carregamento do sistema operacional, execute as seguintes etapas:

1. Crie um disco de inicialização de emergência usando o Kaspersky Anti-Virus em um computador não infectado.
2. Insira o disco de emergência na unidade de disco do computador infectado e o reinicie. O Microsoft Windows XP SP2 será iniciado com a inteface do Bart PE.
   O Bart PE possui suporte a rede interno para usar sua LAN. Quando o programa é iniciado, ele pergunta se você deseja habilitá-lo. Habilite o suporte à rede se planeja atualizar as assinaturas de ameaças na rede local antes de verificar o computador. Se a atualização não for necessária, cancele o suporte à rede.
3. Para abrir o Kaspersky Anti-Virus, clique em **Iniciar** → **Programas** → **Kaspersky Anti-Virus 6.0** → **Iniciar**.

   A janela principal do Kaspersky Anti-Virus será aberta. No modo de recuperação do sistema, você pode acessar apenas as verificações de vírus e as atualizações de assinaturas de ameaças na rede local (se você tiver habilitado o suporte à rede no Bart PE).
4. Inicie a verificação de vírus.

Observe que, por padrão, são usadas as assinaturas de ameaças da data em que o disco de recuperação é criado. Por isso, é recomendável atualizar as assinaturas de ameaças antes de iniciar a verificação.

Observe também que o aplicativo usará apenas as assinaturas de ameaças atualizadas somente durante a sessão atual com o disco de recuperação, antes de reiniciar o computador.

Aviso! Se foram detectados objetos infectados ou possivelmente infectados ao verificar o computador, e eles foram processados e movidos para a Quarentena ou o Backup, é recomendável concluir o processamento desses objetos durante a sessão atual com um disco de recuperação.

Caso contrário, eles serão perdidos ao reiniciar o computador.

14.11. Usando opções avançadas

O Kaspersky Anti-Virus fornece os seguintes recursos avançados:

- Notificações sobre determinados eventos que ocorrem no programa.
- Autodefesa do Kaspersky Anti-Virus contra a desabilitação, exclusão ou edição de módulos, além da proteção do programa por senha.
- Resolução de conflitos com o Kaspersky Anti-Virus (consulte 14.11.3 na p. 202) ao usar outros aplicativos.

Para configurar estes recursos:

1. Abra a janela de configuração do programa com o link Configurações na janela principal.
2. Selecione **Serviço** na árvore de configurações.

À direita da tela, você pode definir se vai ou não usar os recursos adicionais na operação do programa.

14.11.1. Notificações de eventos do Kaspersky Anti-Virus

Diferentes tipos de eventos ocorrem no Kaspersky Anti-Virus. Eles podem ser de natureza informativa ou conter informações importantes. Por exemplo, um evento pode informá-lo de que o programa foi atualizado com êxito ou registrar um erro em um componente que deve ser eliminado imediatamente.

Para receber atualizações sobre o funcionamento do Kaspersky Anti-Virus, você pode usar o recurso de notificação.

Os avisos podem ser entregues de várias formas:

- Mensagens pop-up acima do ícone de programa, na bandeja do sistema
- Mensagens sonoras
- E-mails
- Registro de eventos em log

Para usar este recurso:

1. Marque **Habilitar notificações** na caixa **Interação com o usuário** (veja a fig. 71).

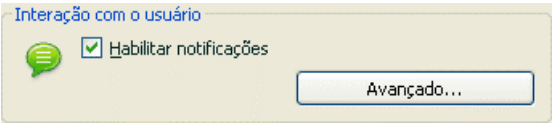


Figura 71. Habilitando notificações

2. Clique no botão **Configurações** para abrir a janela **Configurações de notificação**.
3. Na guia **Eventos**, defina os tipos de eventos do Kaspersky Anti-Virus sobre os quais você deseja ser notificado e o método de entrega das notificações (consulte 0 na p. 196).
4. Clique em **Configurações de E-mail** para abrir a janela **Configurações de notificação** e configurar a entrega de notificações por e-mail, se esse for o método de notificação em uso (consulte 0 na p. 198).

Tipos de eventos e métodos de entrega de notificações

Durante o funcionamento do Kaspersky Anti-Virus, ocorrem os seguintes tipos de eventos:

Notificações críticas envolvem eventos de importância crítica. As notificações são altamente recomendadas, pois indicam problemas no funcionamento do programa ou vulnerabilidades do computador. Por exemplo, *assinaturas de ameaças corrompidas* ou *licença expirada*.

Falha funcional – eventos que levam ao não funcionamento do aplicativo. Por exemplo, quando não existe uma licença ou assinaturas de ameaças.

Notificações importantes são eventos que devem ser investigados, pois refletem situações importantes no funcionamento do programa. Por

exemplo, *proteção desabilitada* ou *não é feita uma verificação de vírus no computador há muito tempo*.

Notificações secundárias são do tipo de referência, que geralmente não contêm informações importantes. Por exemplo, *todos os objetos perigosos foram desinfectados*.

Para especificar quais eventos o programa deve notificar e de que forma:

1. Clique no link Configurações na janela principal do programa.
2. Na janela de configurações do programa, selecione **Serviço**, marque **Habilitar notificações** e edite as configurações detalhadas, clicando no botão **Avançado**.

Você pode configurar os seguintes métodos de notificação dos eventos listados acima, na janela **Configurações de notificação**que é aberta (veja a fig. 72):

- *Mensagens pop-up* acima do ícone de programa, na bandeja do sistema, que contêm uma mensagem informativa sobre o evento que ocorreu.

  Para usar esse tipo de notificação, marque na seção **Balão** para o evento sobre o qual você deseja ser informado.

- *Notificação sonora*

  Se desejar que este aviso seja acompanhado de um som, marque **Som** para o evento.

- *Notificação por e-mail*

  Para usar este tipo de aviso, marque a coluna **E-mail** para o evento sobre o qual você deseja ser informado e defina as configurações para o envio de avisos (consulte 0 na p. 198).

- *Registro de eventos em log*

  Para registrar no log informações sobre os eventos ocorridos, marque na coluna **Log** e configure o log de eventos (consulte 0 na página 199).

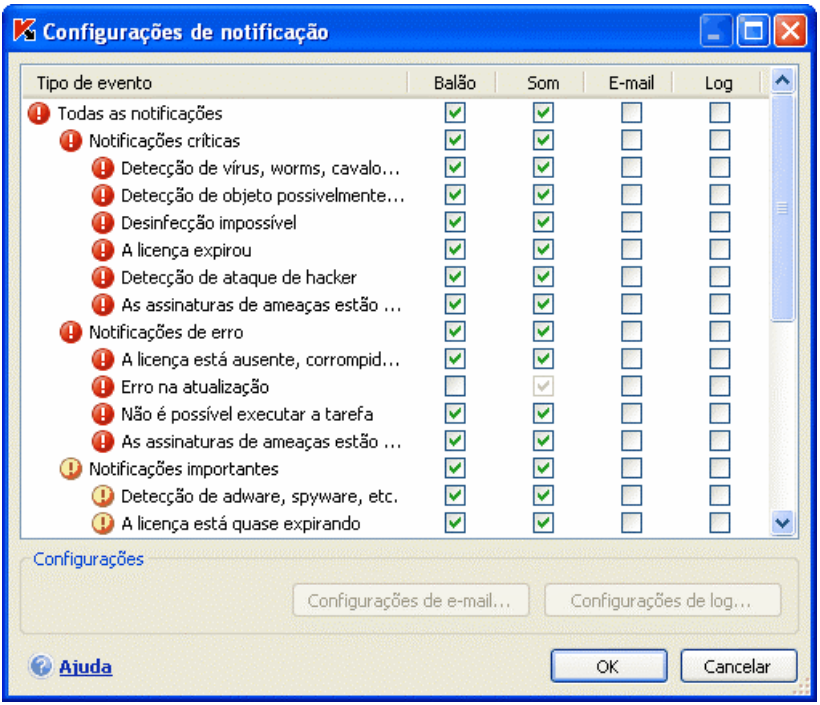


Figura 72. Eventos do programa e métodos de notificação de eventos

Configurando a notificação por e-mail

Depois de selecionar os eventos (consulte 0 na p. 196) sobre os quais você deseja receber notificações por e-mail, configure a entrega de notificações. Para fazê-lo:

1. Abra a janela de configuração do programa com o link Configurações na janela principal.
2. Selecione **Serviço** na árvore de configurações.
3. Clique em **Avançado** na seção **Interação com o usuário**, à direita da tela.
4. Na guia **Configurações de notificação**, marque a caixa de seleção ☑ no gráfico de **E-mail** para os eventos que devem acionar uma mensagem de e-mail.
5. Na janela que é aberta (veja a fig. 73) ao clicar em **Configurações de e-mail**, configure o seguinte para o envio de notificações por e-mail:

- Atribua a configuração de notificação de envio para **De: endereço de e-mail**.
- Especifique o endereço de e-mail para o qual os avisos serão enviados em **Para: endereço de e-mail**.
- Atribua um método de entrega de notificações por e-mail em **Modo de envio**. Se desejar que o programa envie um e-mail assim que o evento ocorrer, selecione **Imediatamente na ocorrência do evento**. Para notificações sobre eventos após de um determinado período, preencha a programação de envio de e-mails informativos clicando em **Editar**. Notificações diárias são o padrão.

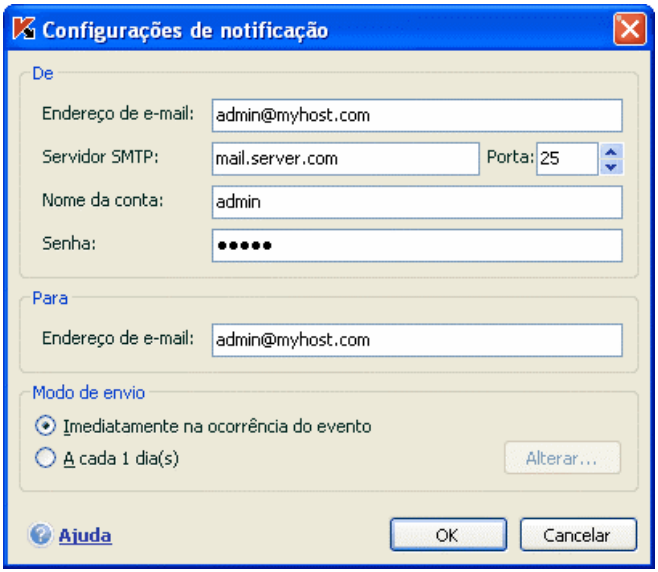


Figura 73. Configurando a notificação por e-mail

Configurando o log de eventos

Para configurar o log de eventos:

1. Abra a janela de configuração do aplicativo com o link Configurações na janela principal.
2. Selecione **Serviço** na árvore de configurações.
3. Clique em **Avançado** na seção **Interação com o usuário**, à direita da tela.

Na janela **Configurações de notificação**, selecione a opção de registrar informações de um evento e clique no botão **Configurações do log**.

O Kaspersky Anti-Virus permite registrar informações sobre eventos ocorridos durante a execução do programa, no log de eventos geral do Microsoft Windows (**Aplicativo**) ou em um log de eventos dedicado do Kaspersky Anti-Virus (**Log de Eventos Kaspersky**).

Os logs podem ser exibidos em **Visualizar Eventos** do Microsoft Windows, que pode ser aberto em **Iniciar/Configurações/Painel de Controle/Ferramentas Administrativas/Visualizar eventos**.

Não é possível registrar eventos em log no Microsoft Windows 98/ME, e você não pode registrar no **Log de Eventos Kaspersky** no Microsoft Windows NT 4.0.

Essas limitações se devem às peculiaridades desses sistemas operacionais.

14.11.2. Autodefesa e restrição de acesso

O Kaspersky Anti-Virus garante a segurança do computador contra programas mal-intencionados e, por isso, ele próprio pode ser alvo de programas mal-intencionados que tentam bloqueá-lo ou excluí-lo do computador.

Além disso, várias pessoas, com níveis diferentes de experiência em informática, podem usar um computador. Permitir o acesso ao programa e suas configurações pode diminuir bastante a segurança do computador como um todo.

Para assegurar a estabilidade do sistema de segurança do computador, os mecanismos de Autodefesa, defesa contra acesso remoto e proteção por senha foram adicionados ao programa.

A autodefesa do aplicativo não estará disponível se o Kaspersky Anti-Virus estiver instlado no Microsoft Windows 98/ME/XP Professional x64 Edition.

Nos computadores que executam sistemas operacionais de 64 bits e o Microsoft Windows Vista, a autodefesa estará disponível apenas para evitar que os arquivos do próprio programas em unidades locais e o Registro do sistema sejam modificados ou excluídos.

Para habilitar a Autodefesa:

1. Abra a janela de configuração do programa com o link Configurações na janela principal.
2. Selecione **Serviço** na árvore de configurações.
3. Defina as seguintes configurações na caixa **Autodefesa** (veja a fig. 74):

Habilitar Autodefesa. Se esta caixa estiver marcada, o programa protegerá seus próprios arquivos, processos na memória e entradas no registro do sistema contra exclusão e modificação.

Desabilitar controle de serviço externo. Se esta caixa estiver marcada, qualquer programa de administração remota que tentar usar o programa será bloqueado.

Se houver alguma tentativa de executar as ações relacionadas, aparecerá uma mensagem sobre o ícone do programa na bandeja do sistema (se o serviço de notificação não tiver sido desabilitado pelo usuário).

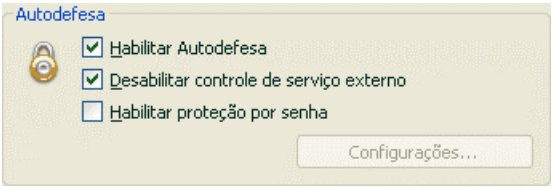


Figura 74. Configuração da defesa do programa

Para proteger o programa por senha, marque **Habilitar proteção por senha**. Clique no botão **Configurações** para abrir a janela **Proteção por senha** e insira a senha e a área a ser coberta pela restrição de acesso (veja a fig. 75). Você pode bloquear todas as operações do programa, exceto notificações de detecção de objetos perigosos, ou evitar que qualquer das seguintes ações sejam executadas:

- Alterar as configurações de desempenho do programa
- Fechar o Kaspersky Anti-Virus.
- Desabilitar ou pausar a proteção do computador

Cada uma dessas ações diminui o nível de proteção do computador; assim, tente estabelecer quais usuários do computador são confiáveis para executá-las.

Agora, sempre que um usuário do computador tentar executar as ações selecionadas, o programa solicitará uma senha.

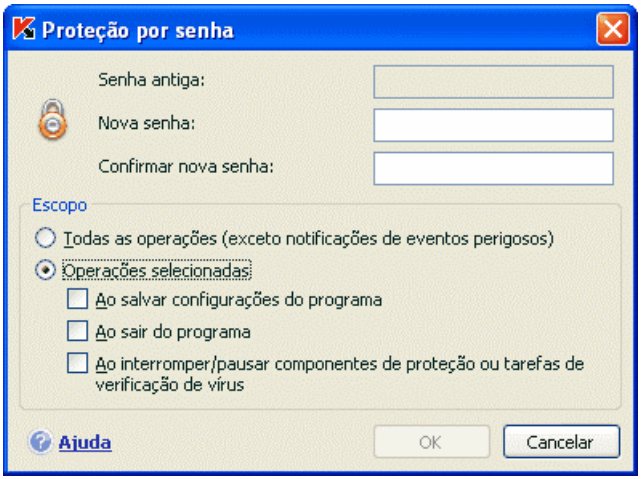


Figura 75. Configurações de proteção do programa por senha

14.11.3. Resolvendo conflitos com outros aplicativos

Em alguns casos, o Kaspersky Anti-Virus pode causar conflitos com outros aplicativos instalados em um computador. Isso ocorre porque esses programas possuem mecanismos de autodefesa internos que são ativados quando o Kaspersky Anti-Virus tenta inspecioná-los. Esses aplicativos incluem o plug-in do Authentica para Acrobat Reader, que verifica o acesso a arquivos .pdf, o Oxygen Phone Manager II e alguns jogos que possuem ferramentas de gerenciamento de direitos digitais.

Para corrigir este problema, marque ☑ **Modo de compatibilidade para programas que usam métodos de autoproteção** na seção **Serviço** da janela de configurações do aplicativo. Reinicie o sistema operacional para que esta alteração tenha efeito.

Contudo, observe que, se você marcar a caixa de seleção, a Proteção do Microsoft Office não funcionará. Se você habilitar a Proteção do Microsoft Office, a compatibilidade com a autodefesa do aplicativo será desabilitada automaticamente. Uma vez habilitada, as verificações de vírus terão início assim que você reiniciar o sistema operacional.

14.12. Importando e exportando configurações do Kaspersky Anti-Virus

O Kaspersky Anti-Virus permite que você importe e exporte suas configurações.

Esse recurso é útil quando, por exemplo, o programa é instalado no seu computador doméstico e no seu escritório. Você pode configurar o programa da maneira desejada em casa, salvar as configurações em um disco e, usando o recurso de importação, carregá-las no computador do trabalho. As configurações são salvas em um arquivo de configuração específico.

Para exportar as configurações atuais do programa:

1. Abra a janela principal do Kaspersky Anti-Virus.
2. Selecione a seção **Serviço** e clique em Configurações.
3. Clique no botão **Salvar** na seção **Gerenciador de configurações**.
4. Insira um nome para o arquivo de configuração e selecione um destino para salvá-lo.

Para importar configurações de um arquivo de configuração:

1. Abra a janela principal do Kaspersky Anti-Virus.
2. Selecione a seção **Serviço** e clique em Configurações.
3. Clique no botão **Carregar** e selecione o arquivo do qual deseja importar configurações do Kaspersky Anti-Virus.

14.13. Redefinindo as configurações padrão

Sempre é possível retornar às configurações padrão do programa, que são consideradas ideais e recomendadas pela Kaspersky Lab. Isso pode ser feito usando o Assistente para Instalação.

Para redefinir as configurações de proteção:

1. Selecione a seção **Serviço** e clique em Configurações para ir para a janela de configurações do programa.

2. Clique no botão **Redefinir** na seção **Gerenciador de configurações**.

A janela que é aberta solicita que você defina as configurações que devem ser restauradas para seus valores padrão.

A janela lista os componentes do programa cujas configurações foram alteradas pelo usuário. Se tiverem sido criadas configurações específicas para algum componente, elas também serão mostradas na lista.

Seguem alguns exemplos de configurações específicas: listas de endereços confiáveis usadas pelo Antivírus da Web; regras de exclusão criadas para os componentes do programa e regras de aplicativos da Defesa Proativa.

Essas listas são preenchidas gradualmente conforme o programa é usado, com base em requisitos de segurança e tarefas individuais. Freqüentemente, este processo leva algum tempo. Portanto, é recomendável salvá-lo ao redefinir as configurações do programa.

Por padrão, o programa salva todas as configurações personalizadas na lista (elas estão desmarcadas). Se você não precisar salvar uma das configurações, marque a caixa correspondente.

Depois de concluir a configuração, clique no botão **Avançar**. O Assistente para Instalação será aberto. Siga suas instruções.

Depois de concluir o Assistente para Instalação, o nível de segurança **Recomendado** será definido para todos os componentes, exceto pelas configurações que você decidiu manter. Além disso, as configurações feitas no Assistente para Instalação também serão aplicadas.

CAPÍTULO 15. TRABALHANDO COM O PROGRAMA NO PROMPT DE COMANDO

Você pode usar o Kaspersky Anti-Virus a partir do prompt de comando. É possível executar as seguintes operações:

- Iniciar, interromper, pausar e reiniciar a atividade dos componentes do aplicativo
- Iniciar, interromper, pausar e reiniciar as verificações de vírus
- Obter informações sobre o status atual dos componentes, das tarefas e das estatísticas
- Verificar objetos selecionados
- Atualizar assinaturas de ameaças e módulos do programa
- Acessar a Ajuda sobre a sintaxe do prompt de comando
- Acessar Ajuda sobre a sintaxe de comandos

A sintaxe do prompt de comando é a seguinte:

```
avp.com <comando> [configurações]
```

As seguintes instruções podem ser usadas como **<comando>**:

ACTIVATE	Ativa o aplicativo pela Internet usando um código de ativação
ADDKEY	Ativa o aplicativo usando um arquivo de chave de licença
START	Inicia um componente ou uma tarefa
PAUSE	Pausa um componente ou uma tarefa
RESUME	Reinicia um componente ou uma tarefa
STOP	Interrompe um componente ou uma tarefa

STATUS	Exibe o status atual do componente ou da tarefa na tela
STATISTICS	Exibe estatísticas do componente ou da tarefa na tela
HELP	Ajuda da sintaxe de comandos e da lista de comandos
SCAN	Verifica objetos quanto à presença de vírus
UPDATE	Inicia a atualização do programa
ROLLBACK	Reverte para a atualização mais recente do programa
EXIT	Fecha o programa (este comando só pode ser executado com a senha atribuída na interface do programa)
IMPORT	Importa configurações do aplicativo
EXPORT	Exporta configurações do aplicativo

Cada comando usa suas próprias configurações específicas daquele componente do Kaspersky Anti-Virus.

15.1. Ativando o aplicativo

Você pode ativar o programa de duas formas:

- pela Internet, usando um código de ativação (comando ACTIVATE)
- usando um arquivo de chave de licença (comando ADDKEY)

Sintaxe do comando:

```
ACTIVATE <código_de_ativação>
ADDKEY <nome_arquivo>
```

Descrição dos parâmetros:

<código_de_ativação>	Código de ativação do programa fornecido ao adquiri-lo.
<nome_arquivo>	Nome do arquivo da chave de licença com a extensão *.key.

Exemplo:

```
avp.com ACTIVATE 00000000-0000-0000-0000-000000000000
avp.com ADDKEY 00000000.key
```

15.2. Gerenciando tarefas e componentes do programa

Você pode gerenciar os componentes e as tarefas do Kaspersky Anti-Virus a partir do prompt de comando, com os seguintes comandos:

- START
- PAUSE
- RESUME
- STOP
- STATUS
- STATISTICS

A tarefa ou o componente ao qual o comando se aplica é determinado por seu parâmetro.

STOP e PAUSE podem ser executados somente com uma senha do Kaspersky Anti-Virus atribuída na interface do programa.

Sintaxe do comando:

```
avp.com <comando> <perfil|id tarefa>
avp.com STOP
PAUSE <perfil|id tarefa> /password=<senha>
```

Um dos valores a seguir é atribuído a **<perfil|id tarefa>**:

RTP	Todos os componentes de proteção

FM	Antivírus de Arquivos
EM	Antivírus de E-Mail
WM	Antivírus da Web
BM	Defesa Proativa
UPDATER	Atualização
SCAN_OBJECTS	Tarefa de verificação de vírus
SCAN_MY_COMPUTER	Tarefa Meu Computador
SCAN_CRITICAL_AREAS	Tarefa Áreas críticas
SCAN_STARTUP	Tarefa Objetos de inicialização
<nome tarefa>	Tarefa definida pelo usuário

Os componentes e tarefas iniciados no prompt de comando são executados de acordo com as configurações definidas na interface do programa.

Exemplos:

Para habilitar o Antivírus de Arquivos, digite no prompt de comando:

```
avp.com START FM
```

Para exibir o status atual da Defesa Proativa no computador, digite o seguinte texto no prompt de comando:

```
avp.com STATUS BM
```

Para interromper uma tarefa de verificação de Meu Computador, digite no prompt de comando:

```
avp.com STOP SCAN_MY_COMPUTER /password=<sua senha>
```

15.3. Verificações antivírus

Em geral, a sintaxe para iniciar a verificação de vírus em uma determinada área e processar objetos mal-intencionados a partir do prompt de comando tem a seguinte aparência:

```
avp.com SCAN [<objeto verificado>] [<ação>]
[<consulta ação>] [<tipos de arquivos>] [<exclusões>]
[<arquivo_configurações>] [<configurações relatório>]
```

Para verificar objetos, você também pode iniciar uma das tarefas criadas no Kaspersky Anti-Virus do prompt de comando (consulte 15.1 na p. 206). A tarefa será executada de acordo com as configurações definidas na interface do programa.

Descrição dos parâmetros.

<objeto verificado> - este parâmetro fornece a lista de objetos que serão verificados quanto à presença de código mal-intencionado. Pode incluir vários valores da seguinte lista, separados por espaços.	
<arquivos>	Lista dos caminhos dos arquivos e/ou pastas a serem verificados. Você pode inserir caminhos absolutos ou relativos. Os itens da lista são separados por um espaço. Observações: • Se o nome do objeto contiver um espaço, será necessário colocá-lo entre aspas • Se você selecionar uma pasta específica, todos os arquivos contidos nela serão verificados.
/MEMORY	Objetos da memória do sistema
/STARTUP	Objetos de inicialização
/MAIL	Bancos de dados de e-mail
/REMDRIVES	Todas as unidades de mídia removíveis
/FIXDRIVES	Todas as unidades internas
/NETDRIVES	Todas as unidades de rede
/QUARANTINE	Objetos em quarentena
/ALL	Verificação completa

/@:<filelist.lst>	Caminho para o arquivo que contém uma lista de objetos e pastas a serem incluídos na verificação. O arquivo deve estar no formato de texto e cada objeto da verificação deve iniciar uma nova linha. Você pode inserir um caminho absoluto ou relativo para o arquivo. Se contiver espaços, o caminho deverá estar entre aspas.
<ação> - este parâmetro define as respostas para objetos mal-intencionados detectados durante a verificação. Se este parâmetro não for definido, o valor padrão será **/i2**.	
/i0	Não é tomada nenhuma ação com relação ao objeto; suas informações são registradas no relatório.
/i1	Neutraliza os objetos infectados e, se falhar, os ignora.
/i2	Neutraliza objetos infectados e, se falhar, os exclui. Exceções: não exclui objetos infectados de objetos compostos; exclui objetos compostos com cabeçalhos executáveis, ou seja, arquivos comprimidos sfx (padrão).
/i3	Neutraliza objetos infectados e, se falhar, os exclui. Também exclui todos os objetos compostos completamente, se não for possível excluir o conteúdo infectado.
/i4	Neutraliza objetos infectados e, se falhar, os exclui. Também exclui todos os objetos compostos completamente, se não for possível excluir o conteúdo infectado.
<consulta ação> - este parâmetro define as ações que solicitarão uma resposta do usuário durante a verificação. Se o parâmetro não for definido, o valor padrão será /a2.	
/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 passarão pela verificação antivírus. Se este parâmetro não for definido, o valor padrão será /fi.	
/fe	Verifica somente os arquivos possivelmente infectados, por extensão.
/fi	Verifica somente os arquivos possivelmente infectados, por conteúdo (padrão).
/fa	Verifica todos os arquivos
<exclusões> - este parâmetro define os objetos que serão excluídos da verificação. Pode incluir vários valores da lista fornecida, separados por espaços.	
/e:a	Não verifica arquivos comprimidos
/e:b	Não verifica bancos de dados de e-mail
/e:m	Não verifica e-mails em texto sem formatação
/e:<máscara>	Não verifica objetos por máscara
/e:<segundos>	Ignora objetos cujo tempo de verificação ultrapassa o tempo especificado pelo parâmetro **<segundos>**.
/es:<tamanho>	Ignora arquivos maiores (em MB) que o valor atribuído por **<tamanho>**.
<arquivo de configuração> - define o caminho do arquivo de configuração que contém as configurações de verificação do programa. Você pode inserir um caminho absoluto ou relativo para o arquivo. Se este parâmetro não for definido, serão usados os valores especificados na interface do Kaspersky Anti-Virus.	
/C:<arquivo_configurações>	Usa os valores de configuração atribuídos no arquivo **<arquivo_configurações>**

<configurações do relatório> - este parâmetro determina o formato do relatório sobre os resultados da verificação. Você pode usar um caminho absoluto ou relativo para o arquivo. Se o parâmetro não for definido, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.	
/R:<arquivo_relatório>	Registra somente os eventos importantes nesse arquivo
/RA:<arquivo_relatório>	Registra todos os eventos nesse arquivo

Exemplos:

*Iniciar a verificação da RAM, dos programas de inicialização, dos bancos de dados de e-mail, dos diretórios **Meus Documentos** e **Arquivos de Programas** e do arquivo **test.exe**:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and
Settings\Todos os Usuários\Meus Documentos"
"C:\Arquivos de Programas" "C:\Downloads\test.exe"
```

Pausar a verificação de objetos selecionados e iniciar uma verificação completa do computador; continuar a verificação de vírus nos objetos selecionados:

```
avp.com PAUSE SCAN_OBJECTS /password=<sua_senha>
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

*Verificar a RAM e os objetos relacionados no arquivo **object2scan.txt**: Use o arquivo de configuração **scan_setting.txt**. Após a verificação, gerar um relatório que registre todos os eventos:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt
/C:scan_settings.txt /RA:scan.log
```

15.4. Atualizações do programa

A sintaxe para atualizar os módulos do programa e as assinaturas de ameaças do Kaspersky Anti-Virus a partir do prompt de comando é a seguinte:

```
avp.com UPDATE [<caminho/URL>]
[/R[A]:<arquivo_relatório>]
[/C:<arquivo_configurações>] [/APP]
```

Descrição dos parâmetros:

[<caminho/URL>]	Servidor HTTP ou FTP ou pasta de rede para baixar as atualizações. Se não for selecionado um caminho, a fonte da atualização será obtida nas configurações da Atualização.
/R[A]:<arquivo_relatório>	**/R:<arquivo_relatório>** – registra somente os eventos importantes no relatório. **/R[A]:<arquivo_relatório>** – registra todos os eventos no relatório. Você pode usar um caminho absoluto ou relativo para o arquivo. Se o parâmetro não for definido, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.
/C:<arquivo_configurações>	Caminho do arquivo de configuração com as definições para atualizações do programa. Você pode inserir um caminho absoluto ou relativo para o arquivo. Se este parâmetro não for definido, serão usados os valores especificados na interface do Kaspersky Anti-Virus.
/APP	Atualizar módulos do programa

Exemplos:

Atualizar as assinaturas de ameaças e registrar todos os eventos no relatório:

```
avp.com UPDATE /RA:avbases_upd.txt
```

*Atualizar os módulos do programa Kaspersky Anti-Virus usando as definições do arquivo de configuração **updateapp.ini**:*

```
avp.com UPDATE /APP /C:updateapp.ini
```

15.5. Configurações de reversão

Sintaxe do comando:

```
ROLLBACK [/R[A]:<arquivo_relatório>]
```

/R[A]:<arquivo_relatório>	**/R:<arquivo_relatório>** – registra somente os eventos importantes no relatório. **/R[A]:<arquivo_relatório>** – registra todos os eventos no relatório. Você pode usar um caminho absoluto ou relativo para o arquivo. Se o parâmetro não for definido, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.

Exemplo:

```
avp.com ROLLBACK /RA:rollback.txt
```

15.6. Exportando configurações

Sintaxe do comando:

```
avp.com EXPORT <perfil|id tarefa> <nome_arquivo>
```

Descrição dos parâmetros:

<perfil>	Componente ou tarefa com as configurações exportadas. Um dos seguintes valores pode ser usado: **RTP** – todos os componentes de proteção **FM** – Antivírus de Arquivos **EM** – Antivírus de E-Mail **WM** – Antivírus da Web **BM** - Defesa Proativa

<nome_arquivo>	Caminho do arquivo para o qual as configurações do Kaspersky Anti-Virus serão exportadas. Você pode usar um caminho absoluto ou relativo. O arquivo de configuração é salvo no formato binário (*.dat*) e poderá ser usado posteriormente para importar as configurações do aplicativo em outros computadores. O arquivo de configuração pode ser salvo como um arquivo de texto. Para fazê-lo, especifique a extensão *.txt* no nome do arquivo.

Exemplo:

```
avp.com EXPORT c:\settings.dat
```

15.7. Importando configurações

Sintaxe do comando:

```
avp.com IMPORT <nome_arquivo> [/password=<senha>]
```

<nome_arquivo>	Caminho do arquivo do qual as configurações do Kaspersky Anti-Virus serão importadas. Você pode usar um caminho absoluto ou relativo.
<senha>	Senha do Kaspersky Anti-Virus atribuída na interface do programa.

Observe que este comando não poderá ser executado sem a senha.

Exemplo:

```
avp.com IMPORT c:\ settings.dat /password=<sua_senha>
```

15.8. Iniciando o programa

Sintaxe do comando:

```
avp.com
```

15.9. Interrompendo o programa

Sintaxe do comando:

```
EXIT /password=<senha>
```

<senha>	Senha do Kaspersky Anti-Virus atribuída na interface do programa.

Observe que não será possível executar este comando sem informar a senha.

15.10. Exibindo a Ajuda

Este comando está disponível para exibir a Ajuda sobre a sintaxe do prompt de comando:

```
avp.com [ /? | HELP ]
```

Para obter ajuda sobre a sintaxe de um comando específico, use um dos comandos a seguir:

```
avp.com <comando> /?
avp.com HELP <comando>
```

15.11. Códigos de retorno da interface da linha de comando

Esta seção contém uma lista de códigos de retorno da linha de comando. 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 na conclusão da tarefa
4	Tarefa cancelada
Códigos de retorno da tarefa de verificação de vírus	
101	Todos os objetos perigosos foram processados
102	Objetos perigosos detectados

CAPÍTULO 16. MODIFICANDO, REPARANDO E REMOVENDO O PROGRAMA

O aplicativo pode ser desinstalado das maneiras a seguir:

- Usando o Assistente para Instalação (consulte 16.1 na p. 218)
- Do prompt de comando (consulte 16.2 na p. 220)

16.1. Modificando, reparando e removendo o programa usando o Assistente para Instalação

Talvez seja necessário reparar o programa, se você detectar erros no funcionamento depois de uma configuração incorreta ou da corrupção de arquivos.

A modificação do programa pode resultar na instalação de componentes ausentes do Kaspersky Anti-Virus e na exclusão de componentes indesejados.

Para reparar ou modificar componentes ausentes do Kaspersky Anti-Virus ou excluir o programa:

2. Saia do programa. Para fazê-lo, clique no ícone do programa na bandeja do sistema e selecione **Sair** no menu de contexto.
3. Insira o CD de instalação utilizado para instalar o programa na unidade de CD-ROM. Se você instalou o Kaspersky Anti-Virus a partir de outra fonte (pasta de acesso público, pasta do disco rígido, etc.), verifique se o pacote de instalação se encontra na pasta e se você tem acesso a ela.
4. Selecione **Iniciar** → **Programas** → **Kaspersky Anti-Virus 6.0 for Windows Workstations** → **Modificar, reparar ou remover**.

Um assistente para instalação do programa será aberto. Vamos examinar mais detalhadamente as etapas necessárias para reparar, modificar ou excluir o programa.

Etapa 1. Janela de boas-vindas da instalação

Se você executar todas as etapas descritas acima, necessárias para reparar ou modificar o programa, a janela de boas-vindas da instalação do Kaspersky Anti-Virus será exibida. Para continuar, clique no botão **Avançar**.

Etapa 2. Selecionando uma operação

Neste estágio, selecione a operação que deseja executar. Você pode modificar os componentes do programa, reparar os componentes instalados ou remover componentes ou o programa todo. Para executar a operação desejada, clique no botão apropriado. A resposta do programa dependerá da operação selecionada.

A modificação do programa se assemelha à instalação personalizada do mesmo, e você pode especificar os componentes que deseja instalar ou excluir.

O reparo do programa depende dos componentes instalados. Serão reparados os arquivos de todos os componentes instalados e o nível de segurança Recomendado será definido para cada um deles.

Se remover o programa, você poderá selecionar os dados criados e usados pelo programa que deseja salvar no computador. Para excluir todos os dados do Kaspersky Anti-Virus, selecione **Desinstalação concluída**. Para salvar os dados, selecione **Salvar objetos do aplicativo** e especifique os objetos que não deverão ser excluídos da lista:

- *Dados de ativação* – chave de licença ou código de ativação do programa.
- *Assinaturas de ameaças* – conjunto completo de assinaturas de programas perigosos, vírus e outras ameaças da atualização mais recente.
- *Arquivos de backup* – cópias de backup dos objetos excluídos ou desinfectados. É recomendável salvar esses arquivos, caso possam ser restaurados posteriormente.
- *Arquivos da Quarentena* – arquivos possivelmente infectados por vírus ou suas modificações. Esses arquivos contêm códigos semelhantes ao código de um vírus conhecido, mas é difícil determinar se eles são mal-intencionados. É recomendável salvá-los, pois eles podem não estar infectados ou talvez possam ser desinfectados após a atualização das assinaturas de ameaças.
- *Configurações do aplicativo* – configurações de todos os componentes do programa.

- *Dados do iSwift* – banco de dados com informações sobre os objetos verificados nos sistemas de arquivos NTFS, que podem aumentar a velocidade de verificação. Ao usar esse banco de dados, o Kaspersky Anti-Virus verifica somente os arquivos modificados desde a última verificação.

> Aviso!
>
> Se passar muito tempo entre a desinstalação de uma versão do Kaspersky Anti-Virus e a instalação de outra, não é recomendável usar o banco de dados do *iSwift* de uma instalação anterior. Um programa perigoso poderia invadir o computador durante este período e seus efeitos não seriam detectados pelo banco de dados, o que poderia resultar em uma infecção.

Para iniciar a operação selecionada, clique no botão **Avançar**. O programa começará a copiar os arquivos necessários para o computador ou a excluir os componentes e dados selecionados.

Etapa 3. Concluindo a modificação, o reparo ou a remoção do programa

O processo de modificação, reparo ou remoção será exibido na tela, sendo informado a seguir sobre sua conclusão.

Em geral, a remoção do programa exige a reinicialização do computador, pois é necessário informar essas modificações ao sistema. O programa perguntará se deseja reiniciar o computador. Clique em **Sim** para reiniciar imediatamente. Para reiniciar mais tarde, clique em **Não**.

16.2. Desinstalando o programa do prompt de comando

Para desinstalar o Kaspersky Anti-Virus 6.0 do prompt de comando, insira:

```
msiexec /i <nome_do_pacote>
```

O Assistente para Instalação será aberto. Você pode usá-lo para desinstalar o aplicativo (consulte Capítulo 16 na p. 218).

Você também pode usar os comandos fornecidos a seguir.

Para desinstalar o aplicativo em segundo plano, sem reiniciar o computador (o computador deve ser reiniciado manualmente após a desinstalação), digite:

```
msiexec /i <nome_do_pacote> /qn
```

Para desinstalar o aplicativo em segundo plano e reiniciar o computador, digite:

```
msiexec /x <nome_do_pacote> ALLOWREBOOT=1 /qn
```

CAPÍTULO 17. PERGUNTAS FREQÜENTES

Este capítulo é dedicado às perguntas mais freqüentes dos usuários com relação à instalação, configuração e ao funcionamento do Kaspersky Anti-Virus; aqui, tentaremos respondê-las detalhadamente.

Pergunta: É possível usar o Kaspersky Anti-Virus 6.0 com produtos antivírus de outros fornecedores?

Não. É recomendável desinstalar os produtos antivírus de outros fornecedores antes de instalar o Kaspersky Anti-Virus para evitar conflitos de software.

Pergunta: O Kaspersky Anti-Virus não verifica novamente os arquivos que já foram verificados. Por quê?

É verdade. O Kaspersky Anti-Virus não verifica novamente os arquivos que não foram alterados desde a última verificação.

Isso é possível devido às novas tecnologias iChecker e iStream. A tecnologia é implementada no programa usando um banco de dados e um armazenamento de somas de verificação de arquivos em fluxos NTFS alternados.

Pergunta: Por que é necessário um arquivo de chave de licença? O Kaspersky Anti-Virus funcionará sem ele?

O Kaspersky Anti-Virus será executado sem uma chave de licença, mas você não poderá acessar a Atualização e o Suporte Técnico.

Se ainda não tiver decidido adquirir o Kaspersky Anti-Virus, podemos lhe fornecer uma licença de teste que funcionará por duas semanas ou um mês. Ao final desse período, a chave expirará.

Pergunta: Depois da instalação do Kaspersky Anti-Virus, o sistema operacional começou a se comportar de maneira estranha ("tela azul", reinicialização freqüente, etc.). O que devo fazer?

Apesar de ser raro, é possível que o Kaspersky Anti-Virus e outros softwares instalados no computador entrem em conflito.

Para restaurar a funcionalidade do sistema operacional, faça o seguinte:

1. Pressione a tecla **F8** repetidamente no período entre o início do carregamento do computador e a exibição do menu de inicialização.
2. Selecione **Modo de Segurança** e carregue o sistema operacional.
3. Abra o Kaspersky Anti-Virus.
4. Use o link Configurações na janela principal e selecione a seção **Proteção** na janela de configurações do programa.
5. Desmarque **Executar o aplicativo na inicialização do sistema** e clique em **OK**.
6. Reinicie o sistema operacional no modo normal.

Depois disso, entre em contato com o Serviço de Suporte Técnico através do site corporativo da Kaspersky Lab (**Serviços → Suporte Técnico**). Descreva o problema detalhadamente e as situações nas quais ele ocorre.

Verifique se você anexou um arquivo com um arquivo de despejo completo do sistema operacional Microsoft Windows à pergunta. Para criar este arquivo, faça o seguinte:

1. Clique com o botão direito do mouse em **Meu Computador** e selecione o item **Propriedades** no menu de atalho que será aberto.
2. Selecione a guia **Avançado** na janela **Propriedades do sistema** e pressione o botão **Configurações** na seção **Inicialização e recuperação**.
3. Selecione a opção **Despejo de memória completo** na lista suspensa da seção **Gravando informações de depuração**, na janela **Inicialização e recuperação**.

   Por padrão, o arquivo de despejo será salvo na pasta do sistema, como *memory.dmp*. Você pode alterar a pasta de armazenamento do despejo editando o nome da pasta no campo correspondente.
4. Reproduza o problema relacionado com o funcionamento do Kaspersky Anti-Virus.
5. Verifique se o arquivo de despejo de memória completo foi salvo com êxito.

APÊNDICE A. INFORMAÇÕES DE REFERÊNCIA

Este apêndice contém material de referência sobre os formatos de arquivos e máscaras de extensão usados nas configurações do Kaspersky Anti-Virus.

A.1. Lista de arquivos verificados por extensão

Se você selecionar **Verificar programas e documentos (por extensão)**, o Antivírus de Arquivos verificará detalhadamente os arquivos com as extensões a seguir quanto à presença de vírus. O Antivírus de E-Mail também verificará esses arquivos, se você habilitar a filtragem de anexos.

com – arquivo executável de um programa

exe – arquivo executável ou arquivo comprimido de extração automática

sys – driver do sistema

prg – texto de programa do dBase, Clipper ou Microsoft Visual FoxPro, ou de um programa de criação de arquivos WAV

bin - arquivo binário

bat – arquivo em lotes

cmd – arquivo de comando do Microsoft Windows NT (semelhante a um arquivo .bat do DOS), OS/2

dpl – biblioteca compactada do Borland Delphi

dll – biblioteca de carga dinâmica

scr – tela de abertura do Microsoft Windows

cpl – módulo do painel de controle do Microsoft Windows

ocx – objeto OLE (Object Linking and Embedding) da Microsoft

tsp – programa executado em modo split-time

drv – driver de dispositivo

vxd – driver virtual de dispositivo do Microsoft Windows

pif – arquivo de informações do programa

lnk – arquivo de link do Microsoft Windows

reg – arquivo de chave do Registro do sistema do Microsoft Windows

ini – arquivo de inicialização

cla – classe Java

vbs – script do Visual Basic

vbe – extensão de vídeo do BIOS

js, *jse* – texto de origem JavaScript

htm – documento de hipertexto

htt – cabeçalho de hipertexto do Microsoft Windows

hta – programa de hipertexto do Microsoft Internet Explorer

asp – script de Active Server Pages

chm – arquivo HTML compilado

pht – HTML com scripts PHP incorporados

php – script incorporado em arquivos HTML

wsh – arquivo Microsoft Windows Script Host

wsf – script do Microsoft Windows

the – papel de parede da área de trabalho do Microsoft Windows 95

hlp – arquivo da Ajuda do Win

eml – arquivo de e-mail do Microsoft Outlook Express

nws – arquivo de e-mail de notícias do Microsoft Outlook Express

msg – arquivo de e-mail do Microsoft Mail

plg – e-mail

mbx – extensão de e-mails salvos do Microsoft Office Outlook

doc – documento do Microsoft Office Word

dot – modelo de documento do Microsoft Office Word

fpm – programa de banco de dados, arquivo inicial do Microsoft Visual FoxPro

rtf – documento RTF

shs – fragmento do Shell Scrap Object Handler

dwg – banco de dados de blueprints do AutoCAD

msi – pacote do Microsoft Windows Installer

otm – projeto VBA do Microsoft Office Outlook

pdf – documento do Adobe Acrobat

swf – arquivo flash do Shockwave

jpg, jpeg – formato de imagem gráfica compactada

emf – Meta arquivos do sistema operacional Microsoft Windows da próxima geração em formato Enhanced Metafile. Os arquivos EMF não têm suporte no Microsoft Windows de 16 bits.

ico – arquivo de ícone

ov? – arquivos executáveis do Microsoft DOC

*xl** - documentos e arquivos do Microsoft Office Excel, como: *xla* – extensão do Microsoft Office Excel, *xlc* - diagrama, *xlt* - modelos de documento, etc.

*pp** – documentos e arquivos do Microsoft Office PowerPoint, como: *pps* – slide do Microsoft Office PowerPoint, *ppt* - apresentação, etc.

*md** – documentos e arquivos do Microsoft Office Access, como: *mda* – grupo de trabalho do Microsoft Office Access, mdb - banco de dados, etc.

Lembre-se de que o formato real de um arquivo pode não corresponder ao formato indicado por sua extensão.

A.2. Possíveis máscaras de exclusão de arquivos

Vamos examinar alguns exemplos de máscaras que podem ser usadas na criação de listas de exclusão de arquivos:

1. Máscaras sem caminhos de arquivos:
   - ***.exe** - todos os arquivos com extensão *.exe*
   - ***.ex?** – todos os arquivos com extensão *.ex?*, onde ? representa qualquer caractere
   - **teste** - todos os arquivos com o nome *teste*
2. Máscaras com caminhos de arquivos absolutos:
   - **C:\dir*.***, **C:\dir*** ou **C:\dir** - todos os arquivos na pasta *C:\dir*
   - **C:\dir*.exe** – todos os arquivos da *pasta C:\dir* com extensão *.exe*
   - **C:\dir*.ex?**– todos os arquivos com extensão *.ex?* da pasta *C:\dir*, onde ? representa qualquer caractere
   - **C:\dir\teste** - somente o arquivo *C:\dir\teste*

   Se não desejar que o programa verifique os arquivos nas subpastas dessa pasta, desmarque ☑ **Incluir subpastas** ao criar a máscara.
3. Máscaras com caminhos de arquivos relativos:
   - **dir*.***, **dir*** ou **dir** - todos os arquivos em todas as pastas de *dir*

- **dir\teste** - todos os arquivos *teste* nas pastas *dir*
- **dir*.exe** - todos os arquivos com a extensão *.exe* em todas as pastas *dir*
- **dir*.ex?** – todos os arquivos com a extensão *.ex?* em todas as pastas de *C:\dir*, onde ? representa qualquer caractere

Se não desejar que o programa verifique os arquivos nas subpastas dessa pasta, desmarque **Incluir subpastas** ao criar a máscara.

Dica:
As máscaras de exclusão *.* e * poderão ser usadas somente se você atribuir uma classificação de ameaça excluída da Enciclopédia de Vírus. Caso contrário, a ameaça especificada não será detectada em nenhum objeto. O uso dessas máscaras sem a seleção de uma classificação basicamente desabilita o monitoramento.
Também não é recomendável selecionar uma unidade virtual criada com base em um diretório do sistema de arquivos que use o comando *subst* como exclusão. Não há motivo para fazer isso, pois durante a verificação o programa trata essa unidade virtual como uma pasta e a verifica.

A.3. Classificações de exclusão de possíveis ameaças da Enciclopédia de Vírus

Ao adicionar ameaças com uma determinada classificação da Enciclopédia de Vírus como exclusões, você pode especificar:

- o nome completo da ameaça, como aparece na Enciclopédia de Vírus (em inglês), em www.viruslist.com (por exemplo, **not-a-virus:RiskWare.RemoteAdmin.RA.311** ou **Flooder.Win32.Fuxx);**
- o nome da ameaça por máscara. Por exemplo:
  - **not-a-virus*** – exclui programas possivelmente perigosos da verificação, além de programas de piadas.
  - ***Riskware.*** - exclui riskware da verificação.
  - ***RemoteAdmin.*** - exclui todos os programas de administração remota da verificação.

Para alguns vereditos, você pode atribuir condições avançadas para a aplicação de regras no campo **Configurações avançadas**. Na maioria dos casos, o

programa preenche esse campo automaticamente quando você adiciona uma regra de exclusão em um aviso da Defesa Proativa.

Você pode adicionar configurações avançadas aos seguintes vereditos, entre outros:

- *Internet*. Para esse veredito, você pode fornecer um nome, máscara ou caminho completo do objeto incorporado (por exemplo, um arquivo .dll) como uma condição de exclusão adicional.

Iniciando navegador da Internet. Para esse veredito, você pode listar configurações de abertura do navegador como configurações de exclusão adicionais.
Por exemplo, você bloqueou a abertura de navegadores com determinadas configurações na análise de atividade de aplicativos da Defesa Proativa. Contudo, deseja que o navegador possa ser aberto no domínio *www.kaspersky.com* com um link do Microsoft Office Outlook como uma regra de exclusão. Para fazê-lo, selecione o Outlook como **Objeto** da exclusão e Iniciando navegador da Internet como **Veredito**, e insira uma máscara de domínio permitida no campo **Configurações avançadas**.

APÊNDICE B. KASPERSKY LAB

Fundada em 1997, a Kaspersky Lab é conhecida como líder no segmento de tecnologias de segurança da informação. A empresa produz uma grande variedade de softwares de segurança de dados, fornecendo soluções abrangentes e de alto desempenho para a proteção de computadores e redes contra todos os tipos de programas mal-intencionados, mensagens de e-mail não solicitadas e indesejadas, e ataques de hackers.

A Kaspersky Lab é uma empresa internacional. Sediada na Federação Russa, a empresa possui representações oficiais no Reino Unido, França, Alemanha, Japão, EUA (CA), Países Baixos, China, Polônia e Romênia. Um novo departamento da empresa foi aberto recentemente na França, o Centro Europeu de Pesquisa Antivírus. A rede de parceiros da Kaspersky Lab incorpora mais de 500 empresas no mundo inteiro.

Atualmente, a Kaspersky Lab emprega mais de 450 especialistas, todos peritos em tecnologias de antivírus, sendo que dez deles são graduados com MBAs, 16 com PhDs e vários especialistas sêniores, membros da Organização de Pesquisadores de Antivírus de Computador (Computer Anti-Virus Researchers Organization - CARO).

A Kaspersky Lab oferece as melhores soluções de segurança do mercado, com base em sua experiência única e nos conhecimentos obtidos em mais de 14 anos na batalha contra os vírus de computador. Uma análise completa das atividades de vírus de computador habilita a empresa a fornecer proteção abrangente contra ameaças atuais e futuras. A resistência a ataques futuros é a diretivo básica implementada em todos os produtos da Kaspersky Lab. Os produtos da empresa estão sempre pelo menos um passo à frente de vários outros fornecedores na oferta de cobertura abrangente de antivírus, tanto para usuários domésticos quanto para clientes corporativos.

Anos de muito trabalho fizeram da empresa um dos principais fabricantes de softwares de segurança. A Kaspersky Lab foi uma das primeiras empresas do segmento a desenvolver os mais altos padrões para a defesa antivírus. O principal produto da empresa, o Kaspersky Anti-Virus, fornece proteção integral para todos os níveis de uma rede, incluindo estações de trabalho, servidores de arquivos, sistemas de e-mail, firewalls, gateways da Internet e computadores portáteis. Suas ferramentas de gerenciamento convenientes e fáceis de usar asseguram a automação avançada para uma proteção rápida em toda a empresa. Vários fabricantes conhecidos usam o kernel do Kaspersky Anti-Virus, incluindo Nokia ICG (EUA), F-Secure (Finlândia), Aladdin (Israel), Sybari (EUA), G Data (Alemanha), Deerfield (EUA), Alt-N (EUA), Microworld (Índia) e BorderWare (Canadá).

Os clientes da Kaspersky Lab tiram proveito de uma vários serviços adicionais que asseguram o funcionamento estável dos produtos da empresa e a

conformidade com requisitos comerciais específicos. O banco de dados de antivírus da Kaspersky Lab é atualizado a cada hora. A empresa fornece a seus clientes serviço de suporte técnico 24 horas, disponível em vários idiomas para atender a seus clientes internacionais.

B.1. Outros produtos da Kaspersky Lab

Kaspersky® Internet Security 6.0

O Kaspersky® Internet Security 6.0 é uma solução integrada para a proteção de PCs contra as principais ameaças relacionadas a informações, como vírus, hackers, spams e spyware. Uma interface de usuário comum permite a configuração e o gerenciamento de todos os componentes da solução.

O recurso de proteção antivírus inclui:

- **Verificação antivírus do tráfego de e-mail** no nível do protocolo de transmissão de dados (POP3, IMAP e NNTP para e-mails recebidos e SMTP para mensagens enviadas), independentemente do programa de e-mail usado. O programa inclui plug-ins para os programas de e-mail conhecidos (Microsoft Office Outlook, Microsoft Outlook Express e The Bat!) e dá suporte à desinfecção de seus bancos de dados de e-mail.
- **Verificação antivírus em tempo real do tráfego da Internet** transferido via HTTP.
- **Proteção do sistema de arquivos**: verificação antivírus de arquivos, diretórios ou unidades individuais. Além disso, o aplicativo pode executar a análise de antivírus exclusivamente em áreas críticas do sistema operacional e em objetos de inicialização do Microsoft Windows.
- **Proteção proativa**: o programa executa um monitoramento constante da atividade de aplicativos e dos processos em execução na memória RAM, evitando alterações perigosas ao sistema de arquivos e ao Registro, e restaura o sistemas após influências mal-intencionadas.

A **proteção contra fraudes da Internet** é assegurada pela capacidade de reconhecer ataques de phishing, o que ajuda a evitar vazamentos de dados confidenciais (primeiramente, os números de suas senhas, contas bancárias e de cartões de crédito) e bloquear a execução de scripts perigosos em páginas da Web, janelas pop-up e banners de anúncios. O recurso de **bloquear chamadas telefônicas cobradas** ajuda a identificar softwares que tentam usar o modem para conexões não autorizadas ocultas com serviços telefônicos pagos e evita que isso aconteça.

O Kaspersky® Internet Security 6.0 **registra tentativas de verificar as portas do computador**, o que freqüentemente antecede ataques de rede, e faz uma defesa bem-sucedida contra os ataques de hackers típicos. O programa usa **regras definidas como base** para o controle de todas as transações de rede, rastreando todos os **pacotes de dados enviados e recebidos**. O **modo invisível** (devido à tecnologia SmartStealth™) **impede a detecção externa do computador**. Quando você alterna para esse modo, o sistema bloqueia toda a atividade de rede, exceto algumas transações permitidas nas regras definidas pelo usuário.

O programa utiliza uma abordagem complexa para a filtragem de spam das mensagens de e-mail recebidas:

- Verificação com relação às listas negra e branca de destinatários (incluindo endereços de sites de phishing).
- Inspeção de frases no corpo da mensagem.
- Análise do texto da mensagem usando um algoritmo de auto-aprendizagem.
- Reconhecimento de spam enviado em arquivos de imagens.

Kaspersky Lab News Agent

O News Agent destina-se ao envio oportuno de notícias publicadas pela Kaspersky Lab, de notificações sobre o estado atual das atividades de vírus e notícias recentes. O programa lê a lista de canais de notícias disponíveis e seu conteúdo no servidor de notícias da Kaspersky Lab com a freqüência especificada.

O produto executa as seguintes funções:

- Um ícone da bandeja do sistema indica o status atual da atividade de vírus.
- O produto permite aos usuários fazerem e cancelarem a assinatura de canais de notícias.
- Ele recupera notícias de todos os canais assinados com a freqüência especificada e notifica o usuário sobre notícias recentes.
- Ele permite examinar as notícias nos canais assinados.
- Permite editar a lista de canais e seus status.
- Permite abrir páginas com detalhes das notícias no seu navegador.

O News Agent é um aplicativo autônomo do Microsoft Windows que pode ser usado independentemente ou agregado a várias soluções integradas oferecidas pela Kaspersky Lab Ltd.

Kaspersky® OnLine Scanner

O programa é um serviço gratuito oferecido aos visitantes do site corporativo da Kaspersky Lab. Ele permite uma verificação antivírus on-line eficiente de seu computador. O Kaspersky OnLine Scanner é executado diretamente no navegador da Web. Assim, os usuários podem testar rapidamente seus computadores, se suspeitarem de infecção mal-intencionada. Usando o serviço, os visitantes podem:

- Excluir arquivos comprimidos e bancos de dados de e-mail da verificação.
- Selecionar bancos de dados de antivírus padrão/estendido para a verificação.
- Salvar um relatório sobre os resultados da verificação nos formatos txt ou html.

Kaspersky® OnLine Scanner Pro

O programa é um serviço de assinatura oferecido aos visitantes do site corporativo da Kaspersky Lab. Ele permite uma verificação antivírus on-line eficiente de seu computador e a desinfecção de arquivos perigosos. O Kaspersky OnLine Scanner Pro é executado diretamente no navegador da Web. Usando o serviço, os visitantes podem:

- Excluir arquivos comprimidos e bancos de dados de e-mail da verificação.
- Selecionar bancos de dados de antivírus padrão/estendido para a verificação.
- Salvar um relatório sobre os resultados da verificação nos formatos txt ou html.

Kaspersky® Security for PDA

O Kaspersky® Security for PDA fornece uma proteção antivírus confiável para dados armazenados em vários tipos de computadores portáteis e smartphones. O programa inclui um conjunto ideal de ferramentas de defesa antivírus:

- **verificação antivírus** que verifica as informações (salvas na memória interna do PDA e de smartphones ou em cartões de memória de qualquer tipo) por solicitação do usuário;
- **monitor antivírus** para interceptar vírus em arquivos copiados de outros portáteis ou transferidos com a tecnologia HotSync™.

O Kaspersky® Security for PDA protege seu computador portátil (PDA) da invasão não autorizada, criptografando o acesso ao dispositivo e os dados armazenados em cartões de memória.

Kaspersky Anti-Virus Mobile

O Kaspersky® Anti-Virus Mobile oferece proteção antivírus para dispositivos móveis que executam os sistemas operacionais Symbian e Microsoft Windows Mobile. O programa fornece proteção antivírus abrangente:

- **Verificação por demanda** da memória do dispositivo móveis, de cartões de memória, pastas individuais ou arquivos específicos. Se um arquivo infectado for detectado, ele será movido para a pasta Quarentena ou será excluído;
- **Proteção em tempo real**: verifica automaticamente todos os objetos e arquivos recebidos ou modificados quando forem feitas tentativas de acessá-los;
- **Verificações programadas** de dados armazenados na memória dos dispositivos móveis;
- **Proteção contra spams por SMS e MMS**.

Kaspersky Anti-Virus® Business Optimal

Este pacote fornece uma solução de segurança configurável única para redes corporativas de pequeno e médio porte.

O Kaspersky Anti-Virus® Business Optimal assegura uma proteção antivírus completa[3] para:

- *Estações de trabalho* que executam o Microsoft Windows 98/ME, o Microsoft Windows NT/2000/XP Workstation e o Linux.
- *Servidores de arquivos* que executam o Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Microsoft Windows 2003 Server, Novell Netware, FreeBSD e Linux, e sistemas de armazenamento de arquivos Samba.
- *Sistemas de e-mail*, incluindo o Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail e Qmail.
- *Gateways da Internet*: CheckPoint Firewall –1; Microsoft ISA Server 2004 Standard Edition.

O kit de distribuição do Kaspersky Anti-Virus® Business Optimal inclui o Kaspersky® Administration Kit, uma ferramenta exclusiva para implementação e administração automatizadas.

Você pode escolher qualquer desses aplicativos antivírus, de acordo com os sistemas operacionais e os outros aplicativos usados.

[3] Dependendo do tipo de kit de distribuição.

Kaspersky® Corporate Suite

Este pacote fornece às redes corporativas de qualquer tamanho e complexidade uma proteção antivírus escalonável e abrangente. Os componentes do pacote foram desenvolvidos para proteger todos os níveis de uma rede corporativa, mesmo em ambientes de computação mistos. O Kaspersky® Corporate Suite dá suporte à maioria dos sistemas operacionais e aplicativos instalados em toda a empresa. Todos os componentes do pacote são gerenciados em um console e possuem uma interface de usuário unificada. O Kaspersky® Corporate Suite fornece um sistema de proteção confiável e de alto desempenho, totalmente compatível com as necessidades específicas da configuração de sua rede.

O Kaspersky® Corporate Suite fornece uma proteção antivírus abrangente para:

- *Estações de trabalho* que executam o Microsoft Windows 98/ME, o Microsoft Windows NT/2000/XP Workstation e o Linux;
- *Servidores de arquivos* que executam o Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD e Linux, e sistemas de armazenamento de arquivos Samba;
- *Sistemas de e-mail*, incluindo o Microsoft Exchange Server 2000/2003, o Lotus Notes/Domino, o Sendmail, o Postfix, o Exim e o Qmail;
- *Gateways da Internet*: CheckPoint Firewall –1; Microsoft ISA Server 2000 Enterprise Edition;
- *Computadores portáteis* (PDAs) que executam os sistemas operacionais Symbian, Microsoft Windows CE e Palm, além de smartphones que executam o Microsoft Windows Mobile 2003 for Smartphone e o Microsoft Smartphone 2002.

O kit de distribuição do Kaspersky® Corporate Suite inclui o Kaspersky® Administration Kit, uma *ferramenta exclusiva para implementação e administração automatizadas*.

Você pode escolher qualquer desses aplicativos antivírus, de acordo com os sistemas operacionais e os outros aplicativos usados.

Kaspersky® Anti-Spam

O Kaspersky® Anti-Spam é um conjunto inovador de softwares projetado para ajudar as organizações com redes de pequeno e médio porte na batalha contra os ataques de e-mail indesejados (spam). O produto combina a revolucionária tecnologia de análise lingüística com métodos modernos de filtragem de e-mail, incluindo listas negras de DNS e recursos de cartas formais. Sua exclusiva combinação de serviços permite aos usuários identificar e eliminar até 95% do tráfego indesejado.

O Kaspersky® Anti-Spam, instalado na entrada de uma rede, monitora spams no tráfego de e-mail recebido, atuando como uma barreira aos e-mails não solicitados. O produto é compatível com qualquer sistema de e-mail e pode ser instalado em servidores de e-mail existentes ou dedicados.

O alto desempenho do Kaspersky® Anti-Spam é assegurado por atualizações diárias do banco de dados de filtragem de conteúdo, adicionando amostras fornecidas pelos especialistas do laboratório de lingüística da empresa. Os bancos de dados são atualizados a cada 20 minutos.

Kaspersky® SMTP Gateway

O Kaspersky® SMTP-Gateway para Linux/Unix é uma solução projetada para o processamento de antivírus em e-mails transmitidos via SMTP. O aplicativo contém várias ferramentas adicionais para a filtragem do tráfego de e-mail por nome e tipo MIME de anexos, além de várias ferramentas que reduzem a carga do sistema de e-mail e evitam ataques de hackers. O suporte a listas negras DNS oferece proteção contra e-mails provenientes de servidores inclusos nessas listas como fontes de distribuição de e-mails indesejados (spam).

Kaspersky Security® for Microsoft Exchange 2003

O Kaspersky Security for Microsoft Exchange executa o processamento antivírus de mensagens de e-mail enviadas e recebidas, mensagens armazenadas no servidor e cartas e pastas públicas.

Ele filtra a correspondência não solicitada usando técnicas "inteligentes" de reconhecimento de spam em combinação com as tecnologias da Microsoft. O aplicativo verifica todas as mensagens que chegam ao Exchange Server via protocolo SMTP, verificando-as quanto à presença de vírus através das tecnologias antivírus da Kaspersky Lab e quanto à presença de atributos de SPAM. Os spams são filtrados com base em atributos formais (endereços de e-mail, endereços IP, tamanho da carta, cabeçalhos) e analisa o conteúdo das mensagens e seus anexos usando tecnologias “inteligentes”, incluindo assinaturas gráficas exclusivas para a identificação de SPAM gráfico. O aplicativo verifica o corpo da mensagem e os arquivos anexos.

Kaspersky® Mail Gateway

O Kaspersky Mail Gateway é uma solução abrangente que fornece proteção completa a usuários de sistemas de e-mail. Este aplicativo, instalado entre a rede corporativa e a Internet, verifica todos os componentes dos e-mails quanto à presença de vírus e outros malwares (Spyware, Adware, etc.), e filtra os spams dos e-mails centralmente. Esta solução também inclui alguns recursos adicionais para a filtragem do tráfego de e-mail (por nome e tipo MIME de anexos), além de vários recursos que ajudam a reduzir a carga do servidor de e-mail e evitar ataques de hackers.

Kaspersky Anti-Virus® for Proxy Servers

O Kaspersky Anti-Virus® for Proxy Servers é uma solução antivírus para a proteção do tráfego da Web roteado por meio de servidores proxy via protocolo HTTP. O aplicativo verifica o tráfego da Web quanto à presença de vírus em tempo real, protege contra a penetração de malwares no sistema enquanto você navega na Web e verifica os arquivos baixados da Internet.

Kaspersky Anti-Virus® for MIMESweeper for SMTP

O Kaspersky Anti-Virus® for MIMESweeper for SMTP fornece verificação em alta velocidade do tráfego SMTP em servidores que usam o Clearswift MIMESweeper.

O programa é um plug-in para o Clearswift MIMESweeper for SMTP e verifica vírus e prcessa o tráfego de e-mail enviado e recebido em tempo real.

B.2. Entre em contato conosco

Se tiver dúvidas, comentários ou sugestões, envie-os para um de nossos distribuidores ou diretamente para a Kaspersky Lab. Será um prazer ajudá-lo em qualquer assunto relacionado ao nosso produto, por telefone ou e-mail. Esteja certo de que todas as recomendações e sugestões serão analisadas e consideradas.

Suporte técnico	Consulte as informações de suporte técnico em http://www.kaspersky.com/supportinter.html Helpdesk: www.kaspersky.com/helpdesk.html
Informações gerais	WWW: http://www.kaspersky.com http://www.viruslist.com E-mail: info@kaspersky.com

APÊNDICE C. CONTRATO DE LICENÇA

Contrato de Licença do Usuário Final Padrão

AVISO A TODOS OS USUÁRIOS: LEIA CUIDADOSAMENTE O SEGUINTE CONTRATO LEGAL ("CONTRATO") RELATIVO À LICENÇA DO KASPERSKY ANTI-VIRUS (“SOFTWARE”), PRODUZIDO PELA KASPERSKY LAB ("KASPERSKY LAB").

SE VOCÊ ADQUIRIU ESTE SOFTWARE PELA INTERNET, CLICANDO NO BOTÃO ACEITAR, VOCÊ (SEJA UM INDIVÍDUO OU UMA ENTIDADE ÚNICA) CONCORDA EM LIMITAR-SE E TORNAR-SE PARTE NESTE CONTRATO. SE NÃO CONCORDAR COM TODOS OS TERMOS DO PRESENTE CONTRATO, CLIQUE NO BOTÃO QUE INDICA QUE NÃO ACEITA OS TERMOS DO CONTRATO E NÃO INSTALE O SOFTWARE.

SE VOCÊ ADQUIRIU ESTE SOFTWARE EM UMA MÍDIA FÍSICA, AO QUEBRAR O LACRE DO CD, VOCÊ (SEJA UM INDIVÍDUO OU UMA ENTIDADE ÚNICA) CONCORDA EM LIMITAR-SE E TORNAR-SE PARTE NESTE CONTRATO. SE NÃO CONCORDA COM TODOS OS TERMOS DESTE CONTRATO, NÃO QUEBRE O LACRE DO CD, NÃO FAÇA DOWNLOAD, INSTALE OU USE ESTE SOFTWARE.

DE ACORDO COM A LEGISLAÇÃO RELATIVA AO SOFTWARE DA KASPERSKY DESTINADO A CONSUMIDORES INDIVIDUAIS E COMPRADOS NO SITE DA KASPERSKY LAB OU DE SEUS PARCEIROS, O CLIENTE DEVERÁ TER UM PERÍODO DO CATORZE (14) DIAS ÚTEIS A PARTIR DA ENTREGA DO PRODUTO PARA DEVOLVÊ-LO AO COMERCIANTE PARA TROCA OU REEMBOLSO, DESDE QUE O SOFTWARE ESTEJA SELADO.

COM RELAÇÃO AO SOFTWARE DA KASPERSKY DESTINADO A CONSUMIDORES INDIVIDUAIS NÃO ADQUIRIDO ON-LINE, PELA INTERNET, ESSE SOFTWARE NÃO PODERÁ SER DEVOLVIDO OU TROCADO, EXCETO POR PROVISÕES CONTRÁRIAS DO PARCEIRO QUE COMERCIALIZA O PRODUTO. NESTE CASO, A KASPERSKY LAB NÃO ESTARÁ SUJEITA ÀS CLÁUSULAS DO PARCEIRO.

O DIREITO DE DEVOLUÇÃO E REEMBOLSO SE ESTENDE APENAS AO COMPRADOR ORIGINAL.

Todas as referências na presente a “Software” devem ser consideradas como incluindo o código de ativação do software, que será fornecido pela Kaspersky Lab como parte do Kaspersky Anti-Virus 6.0.

1. *Concessão de Licença*. Sujeito ao pagamento das taxas de licença aplicáveis e sujeito aos termos e condições deste Contrato, a Kaspersky Lab concede a você, por meio da presente, o direito não exclusivo e intransferível de usar uma cópia da versão especificada do Software e a documentação que o acompanha (a "Documentação") durante a vigência deste Contrato, unicamente para seus próprios fins comerciais internos. Você pode instalar uma cópia do Software em um computador.

1.1 *Uso*. O Software é licenciado com o um único produto; não pode ser usado em mais de um computador ou por mais de um usuário por vez, exceto conforme determinado nesta Seção.

1.1.1 O Software está "em uso" em um computador quando está carregado na memória temporária (ou seja, a memória RAM) ou instalado na memória permanente (por exemplo, no disco rígido, no CD-ROM ou em outro dispositivo de armazenamento) desse computador. Esta licença o autoriza a fazer quantas cópias de backup do Software forem necessárias para sua utilização dentro dos termos da lei e unicamente para fins de backup, desde que todas essas cópias contenham todos os avisos sobre propriedade do Software. Você deverá manter registros do número e do local de todas as cópias do Software e da Documentação, e deverá adotar todas as precauções necessárias para proteger o Software de uso ou cópia não autorizados.

1.1.2 O Software protege o computador contra vírus cujas assinaturas estão contidas nos bancos de dados de assinaturas de ameaças disponíveis nos servidores de atualização da Kaspersky Lab.

1.1.3 Se você vender o computador no qual o Software está instalado, deverá verificar se todas as cópias do Software foram excluídas anteriormente.

1.1.4 Você não deverá descompilar, aplicar engenharia reversa, desmontar ou reduzir de qualquer outra forma qualquer parte deste Software a um formato legível, nem permitir que qualquer terceiro o faça. As informações de interface necessárias para obter a interoperabilidade do Software com programas de computador criados independentemente serão fornecidas pela Kaspersky Lab quando solicitado, mediante pagamento dos custos plausíveis e das despesas relativas à busca e ao fornecimento dessas informações. No caso de a Kaspersky Lab o notificar de que não pretende disponibilizar essas informações por qualquer motivo, incluindo custos (sem limitações), deverá ser permitido que você tome as medidas necessárias para conseguir a interoperabilidade, desde que seja feita a engenharia reversa ou descompilação do Software apenas até os limites permitidos pela lei.

1.1.5 Você não poderá fazer correções de erros ou de alguma outra forma modificar, adaptar ou converter o Software, nem criar trabalhos derivados do mesmo, nem permitir que terceiros o copiem (a menos que expressamente permitido pelo presente).

1.1.6 Você não poderá alugar, locar ou emprestar o Software a terceiros, nem transferir ou sublicenciar seus direitos de licença a qualquer outra pessoa.

1.1.7 A Kaspersky Lab pode solicitar que o Usuário instale a versão mais recente do Software (a versão e o pacote de manutenção mais recentes).

1.1.8 Você não deverá usar este Software em ferramentas automáticas, semi-automáticas ou manuais projetadas para criar assinaturas de vírus, rotinas de detecção de vírus, qualquer outro código ou dados para detecção de código ou dados mal-intencionados.

2. *Suporte*.

(i) A Kaspersky fornecerá serviços de suporte ("Serviços de Suporte") conforme definido a seguir, por um período especificado no arquivo da chave de licença e indicado na janela "Serviço", a partir do momento da ativação, desde:

(a) o pagamento dos então atuais encargos relativos ao suporte e:

(b) o preenchimento bem-sucedido do Formulário de Assinatura de Serviços de Suporte, como fornecido com este Contrato ou como disponível no site da Kaspersky Lab, que exigirá que você insira o código de ativação fornecido pela Kaspersky Lab com este Contrato. À sua total discrição, a Kaspersky Lab decidirá se você satisfez ou não esta condição para a provisão dos Serviços de Suporte.

Os Serviços de Suporte estarão disponíveis depois da ativação do Software. O serviço de suporte técnico da Kaspersky Lab também é liberado para solicitações a partir do registro adicional do Usuário Final para concessão de identificador para o fornecimento de Serviços de Suporte.

Até a ativação do Software e/ou a obtenção do identificador do Usuário Final (Identificação do Cliente), o serviço de suporte técnico oferece assistência apenas na ativação do Software e no registro do Usuário Final.

(ii) Ao preencher o Formulário de Assinatura de Serviços de Suporte, você concorda com os termos da Diretiva de Privacidade da Kaspersky Lab, localizada em www.kaspersky.com/privacy, e concorda explicitamente com a transferência de dados para outros países, diferentes do seu, conforme definido na Diretiva de Privacidade.

(iii) Os Serviços de Suporte serão encerrados, a menos que sejam renovados anualmente, com o pagamento dos então atuais encargos de suporte anuais e o novo preenchimento bem-sucedido do Formulário de Assinatura de Serviços de Suporte.

(iv) Por “Serviços de Suporte” entendem-se:

(a) Atualizações a cada hora do banco de dados de antivírus;

(b) Atualizações gratuitas de software, incluindo as atualizações de versão;

(c) Suporte técnico pela Internet e pela linha direta de suporte fornecida pelo Fornecedor e/ou Revendedor;

(d) Atualizações de detecção e desinfecção de vírus 24 horas por dia

(v) Os Serviços de Suporte serão fornecidos somente se e quando você tiver a versão mais recente do Software (incluindo os pacotes de manutenção), disponível no site oficial da Kaspersky Lab (www.kaspersky.com), instalado no seu computador.

3. *Direitos de Propriedade*. O Software é protegido por leis de direitos autorais. A Kaspersky Lab e seus fornecedores possuem e detêm todos os direitos, títulos de interesses no e para o Software, incluindo todos os direitos autorais, patentes, marcas comerciais e outros direitos de propriedade intelectual relacionados. A posse, instalação ou uso do Software por você não lhe transfere qualquer título à propriedade intelectual do Software, e você não adquirirá quaisquer direitos ao Software, exceto aqueles expressamente definidos no presente Contrato.

4 *Confidencialidade*. Você concorda que o Software e a Documentação, incluindo o projeto e a estrutura específicos de programas individuais, constituem informações proprietárias confidenciais da Kaspersky Lab. Você não deverá divulgar, fornecer ou disponibilizar de qualquer outra maneira essas informações confidenciais, em qualquer forma, para terceiros, sem o consentimento prévio por escrito da Kaspersky Lab. Você deverá implementar medidas de segurança aceitáveis para proteger essas informações confidenciais mas, sem limitação a isso, deverá usar os melhores meios para manter a segurança do código de ativação.

5. *Garantia Limitada*.

(i) A Kaspersky Lab garante que, por seis (6) meses a partir do primeiro download ou da instalação, o Software adquirido em mídia física terá um desempenho significativamente de acordo com a funcionalidade descrita na Documentação, quando operado corretamente e da forma especificada na Documentação.

(ii) Você assume toda a responsabilidade pela seleção deste Software para preencher seus requisitos. A Kaspersky Lab não garante que o Software e/ou a Documentação serão adequados para suas necessidades, nem que sua utilização será ininterrupta ou isenta de erros.

(iii) A Kaspersky Lab não garante que este Software identifique todos os vírus conhecidos, nem que ocasionalmente o Software não possa relatar erroneamente um vírus em um título não infectado por esse vírus.

(iv) A única solução e toda a responsabilidade da Kaspersky Lab por violações da garantia descrita no parágrafo (i) será, como opção da Kaspersky Lab, que ela repare, substitua ou reembolse o Software, se tal fato for relatado à Kaspersky Lab ou seu representante durante o período da garantia. Você deverá fornecer todas as informações necessárias satisfatórias para auxiliar o Fornecedor na resolução do item com defeito.

(v) A garantia (i) não se aplicará se você (a) fizer ou causar alterações neste Software sem o consentimento da Kaspersky Lab, (b) usar o Software de uma forma para a qual ele não se destina ou (c) usar o Software de forma diferente daquela permitida por este Contrato.

(vi) As garantias e condições declaradas neste Contrato substituem todas as outras condições, garantias ou outros termos relativos ao fornecimento ou suposto fornecimento de, à falha ou atraso no fornecimento do Software ou da Documentação que podem, exceto por este parágrafo (vi), ter valor entre a Kaspersky Lab e você, ou que de outra forma poderiam estar implícitas ou incorporadas neste Contrato ou em qualquer contrato paralelo, seja por estatuto, pela lei comum ou outra, todos excluídos pela presente (incluindo, sem limitações, as condições, garantias ou outros termos implícitos, como os relativos à qualidade satisfatória, adequação às finalidades ou ao uso de habilidades e cuidados satisfatórios).

6. *Limitação de Responsabilidade*.

(i) Nenhuma parte deste Contrato excluirá ou limitará a responsabilidade da Kaspersky Lab por (a) delitos de fraude, (b) morte ou danos pessoais causados por violações de “duty of care” da lei comum ou de qualquer violação por negligência de um termo deste Contrato ou (c) qualquer outra responsabilidade que não possa ser excluída pela lei.

(ii) Sujeita ao parágrafo (i) acima, a Kaspersky Lab não se responsabilizará (seja por contrato, agravo, restituição ou outros) por nenhuma das seguintes perdas e danos (quer essas perdas e danos tenham sido previstos, previsíveis, conhecidos ou de outra forma):

(a) Perda de rendimentos;

(b) Perda de lucros reais ou previstos (incluindo a perda de lucros em contratos);

(c) Perda do uso de dinheiro;

(d) Perda de economias previstas;

(e) Perda de negócios;

(f) Perda de oportunidades;

(g) Perda de boa-fé;

(h) Perda de reputação;

(i) Perda de, danos a ou corrupção de dados ou:

(j) Qualquer perda ou dano indireto ou conseqüente causado de alguma forma (incluindo, para evitar dúvidas, os casos em que essas perdas e danos sejam dos tipos especificados nos parágrafos (ii), (a) a (ii), (i).

(iii) Sujeita ao parágrafo (i), a responsabilidade da Kaspersky Lab (seja por contrato, agravo, restituição ou outros) decorrente de ou em correlação com o fornecimento do Software em nenhuma circunstância excederá o valor igual ao igualmente pago por você pelo Software.

7. Neste Contrato está contido o entendimento integral entre as partes com relação ao assunto do mesmo, tendo prevalência sobre todos e quaisquer entendimentos, compromissos e promessas anteriores entre você e a Kaspersky Lab, sejam eles orais ou por escrito, que tenham sido definidos ou que possam estar implícitos em qualquer elemento escrito ou declarado nas negociações entre nós ou nossos representantes antes deste Contrato e todos os contratos anteriores entre as partes, relacionados aos assuntos mencionados previamente terão sua validade suspensa a partir da Data de Efetivação.

O uso do software de demonstração, não lhe concedo o direito ao Suporte Técnico especificado na Cláusula 2 deste EULA, nem o direito de vender essa cópia a terceiros.

Você tem o direito de usar o software para fins de demonstração, durante o período especificado no arquivo da chave de licença, a partir do momento da ativação (esse período pode ser exibido na janela Serviço da interface do usuário do software).