KASPERSKY LAB

Kaspersky Anti-Virus 7.0

MANUAL DO USUÁRIO

KASPERSKY ANTI-VIRUS 7.0

Manual do Usuário

http://www.kaspersky.com

Data de revisão: março, 2008

Índice

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 permitem o acesso completo ao 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, como 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 de modernas ferramentas de comunicação e de tecnologias de computação amplia 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 carregar determinadas páginas da Web podem executar ações perigosas no seu computador,

modificando o Registro do sistema, recuperando dados pessoais sem o seu consentimento e instalando softwares mal-intencionados.

Usando tecnologias de rede, os hackers conseguem atacar servidores corporativos e PCs remotos. Esses ataques podem causar a desativação de um recurso ou sua utilização como parte de uma rede de zumbis e a obtenção de acesso total a um recurso e às informações contidas nele.

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. Portanto, se algum host da rede for infectado, existe um risco significativo de infecção dos outros hosts. 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 host infectado envia involuntariamente mensagens infectadas para outros destinatários que, por sua vez, enviam novas mensagens infectadas, etc. 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

Os aplicativos possivelmente perigosos incluem 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 vulnerabilidades, 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

São softwares que danificam o host diretamente, mas exibem mensagens informando que já houve ou haverá danos 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.

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

- *Reativo:* é um método criado para pesquisar objetos mal-intencionados usando bancos de dados de aplicativos atualizados continuamente. Nesse método, é necessário que haja pelo menos uma ocorrência de infecção para adicionar a assinatura da ameaça ao banco de dados e distribuir uma atualização do mesmo.
- *Proativo* – diferentemente da proteção reativa, esse método não se baseia na análise de código do objeto, mas na análise de seu comportamento no 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.

Aviso!

Desse ponto em diante, usaremos o termo "vírus" para nos referirmos a programas perigosos e mal-intencionados. O tipo do programa mal-intencionado será enfatizado somente quando necessário.

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 da baixa probabilidade de

esses sintomas indicarem uma infecção, é recomendável executar uma verificação completa do computador (consulte a seção 5.3 na p. 54) caso eles se manifestem.

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.
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 Microsoft Windows, criado na instalação do sistema operacional.
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.
6. Atualize os bancos de dados e os módulos do aplicativo (consulte a seção 5.6 na p. 56). Se possível, baixe as atualizações da 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 a seção 5.3 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 a gravidade dos possíveis danos.

Um dos métodos básicos de combate a vírus, exatamente como na medicina, é a *prevenção* oportuna. Nos computadores, a profilaxia compreende algumas regras que, se forem seguidas, podem reduzir significativamente a probabilidade de infecção por vírus e a perda de dados.

Segue uma lista de regras básicas de segurança que, se seguidas, ajudarão a reduzir o risco de ataques de vírus.

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

- Instale o Kaspersky Anti-Virus assim que possível.
- Atualize regularmente (consulte a seção 5.6 na p. 56) as assinaturas de ameaças do programa. No caso de surtos de vírus, as atualizações devem ocorrer várias vezes por dia, e os bancos de dados do aplicativo nos servidores da Kaspersky Lab são atualizados imediatamente.
- 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. Se não tiver instalado o Firewall, é recomendável fazê-lo para proteger seu computador ao usar a Internet.

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

- Verifique todas as unidades de armazenamento removíveis, por exemplo, disquetes, CDs/DVDs e unidades flash, quanto à presença de vírus antes de usá-las (consulte a seção 5.5 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 correspondente de infecção ainda é baixa, e você poderá se proteger da nova infecção baixando os bancos de dados de aplicativos atualizados.

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

Regra nº 5:*Use o Microsoft Windows Update* e instale as atualizações do sistema operacional Microsoft 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/DVDs, unidades flash e outras mídias de armazenamento de distribuição com software e informações importantes em um local seguro.
- Crie um Disco de Recuperação (consulte a seção 15.4 na p. 186) que possa ser usado para inicializar o sistema usando um sistema operacional limpo.

Regra nº 9: *Examine periodicamente a lista de softwares instalados no computador*. Isso pode ser feito usando **Instalar ou Remover Programas** no **Painel de Controle** ou simplesmente exibindo o conteúdo da pasta **Arquivos de Programas**. Você pode 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, programas como esses são perigosos.

CAPÍTULO 2. KASPERSKY ANTI-VIRUS 7.0

O Kaspersky Anti-Virus 7.0 representa uma nova geração de produtos de segurança de dados.

O que realmente diferencia o Kaspersky Anti-Virus 7.0 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 7.0

O Kaspersky Anti-Virus 7.0 (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 os recursos existentes em todos os produtos da empresa em uma única solução de segurança. O programa oferece proteção contra vírus. Os novos módulos protegem contra ameaças desconhecidas.

Não é mais necessário instalar vários produtos no computador para obter segurança total. Basta simplesmente instalar o Kaspersky Anti-Virus 7.0.

Sua proteção abrangente protege todos os canais de dados de entrada e de saída. Uma configuração flexível de todos os componentes do aplicativo permite a personalização total do Kaspersky Anti-Virus 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 a seção Capítulo 10 na p. 120) é a principal vantagem do programa. Ela analisa o comportamento dos aplicativos instalados no computador, monitorando as alterações do Registro do sistema 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 para diminuir a carga no processador central e nos subsistemas e para aumentar a velocidade das verificações de arquivos usando as tecnologias iChecker e iSwift. Dessa maneira, o programa evita que os arquivos sejam verificados duas vezes.
- 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.
- São fornecidas tarefas individuais para verificar as áreas críticas do computador e os objetos de inicialização que, se infectados, poderiam gerar problemas sérios e para a detecção de rootkits usados para ocultar malware no sistema. Você pode configurar essas tarefas para serem executadas sempre que o sistema é iniciado.
- A proteção de e-mail contra programas mal-intencionados foi aprimorada significativamente. 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 (incluindo MAPI e 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 Microsoft Office Outlook, o Microsoft Outlook Express (Windows Mail) e o The Bat!, que permitem a configuração da proteção de e-mail contra vírus diretamente no programa de e-mail.
- A função de notificação do usuário (consulte a seção 15.9.1 na p. 199) foi ampliada para determinados eventos que acontecem durante o funcionamento do programa. Você mesmo pode selecionar o método de notificação para cada tipo de evento: e-mails, notificações por som, mensagens pop-up.
- Agora, o programa consegue verificar o tráfego enviado pelo protocolo SSL.
- Novos recursos incluíram a tecnologia de autodefesa ao aplicativo, a proteção contra acesso remoto não autorizado de serviços do Kaspersky Anti-Virus 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.
- Foi adicionado o News Agent. É um módulo criado para a entrega de conteúdo de notícias da Kaspersky Lab em tempo real.

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 e inclui uma seção de Ajuda completa. Um assistente de segurança incorporado no aplicativo fornece um instantâneo completo do status de proteção do host e permite executar a resolução do problema diretamente.

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 dez vezes.
- 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.
- Um recurso de reversão foi implementado para recuperar uma versão anterior do banco de dados de aplicativos, no caso de corrupção do arquivo ou erros de 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. Essa configuração torna o sistema flexível, com opções de configuração fáceis para todos os componentes, que podem se ajustar à necessidade de um usuário específico ou da empresa como um todo.

O Kaspersky Anti-Virus inclui:

- Componentes de proteção (consulte a seção 2.2.1 na p. 22), que oferecem proteção em tempo real de todas as transferências de dados e caminhos de entrada do computador.
- Tarefas de verificação de vírus (consulte a seção 2.2.2 na p. 23), usadas para verificar arquivos, pastas, unidades ou áreas individuais quanto à presença de vírus ou para executar uma verificação completa do computador.
- Atualizações (consulte a seção 2.2.3 na p. 24) para garantir que os bancos de dados e módulos internos do aplicativo usados para verificar malware estejam atualizados.

2.2.1. Componentes de proteção em tempo real

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 do computador 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 abertos, executados ou salvos no computador e nas unidades conectadas. O programa intercepta todas as tentativas de acessar um arquivo e verifica o arquivo com relação a vírus conhecidos, disponibilizando-o para uso somente se não estiver

infectado ou se for desinfectado com êxito pelo Antivírus de Arquivos. Se, por algum motivo, não for possível desinfectar um arquivo, ele será excluído e uma cópia do mesmo será salva no Backup (consulte 15.2 na p. 176) ou ele será movido para a Quarentena (consulte 15.1 na p. 172).

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

A abertura de vários sites coloca o computador sob o risco de infecção por vírus que serão instalados usando scripts contidos nessas páginas, além do download de objetos perigosos.

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

O número de programas mal-intencionados cresce a cada dia. Esses programas estão se tornando mais complexos, combinando vários tipos de ameaças e modificando as formas de disseminação. Assim, torna-se cada vez mais difícil detectá-los.

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 parar a disseminação de programas mal-intencionados que não foram detectados pelos componentes de

proteção em tempo real devido ao baixo nível de proteção selecionado ou por outros motivos.

As seguintes tarefas são fornecidas pelo Kaspersky Anti-Virus para a verificação de vírus:

Áreas críticas

Verifica todas as áreas críticas do computador quanto à presença de vírus. Estão incluídos: a memória do sistema, objetos de inicialização do sistema, registros mestre de inicialização, pastas do sistema do *Microsoft Windows*. Seu objetivo é detectar rapidamente vírus ativos no sistema sem executar uma verificação completa do 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.

Verificação de rootkits

Verifica no computador rootkits que ocultam programas mal-intencionados no sistema operacional. Esses utilitários injetados no sistema ocultam sua presença e a presença de processos, pastas e chaves do Registro dos programas mal-intencionados descritos na configuração do rootkit.

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 das caixas de correio ou uma tarefa de verificação de vírus na pasta **Meus Documentos**.

2.2.3. Atualização

Para estar sempre pronto para excluir um vírus ou qualquer outro programa perigoso, o Kaspersky Anti-Virus precisa de suporte em tempo real. A *Atualização* foi criada para fazer exatamente isso. Ela é responsável por atualizar os bancos de dados e módulos do aplicativo utilizados pelo Kaspersky Anti-Virus.

O recurso de distribuição de atualizações permite salvar os bancos de dados e módulos do programa baixadas dos servidores da Kaspersky Lab em uma pasta local e, assim, outros computadores na rede podem acessá-los de forma a reduzir o tráfego na Internet.

2.2.4. 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.

Arquivos de dados e relatórios

No tempo de execução, o aplicativo gera um relatório sobre cada componente de proteção em tempo real, tarefa de verificação de vírus e atualização do aplicativo. Ele contém informações as operações realizadas e seus resultados. Os detalhes de todos os componentes do Kaspersky Anti-Virus estão disponíveis por meio do recurso *Relatórios*. No caso de ocorrerem problemas, esses relatórios podem ser encaminhados para a Kaspersky Lab, para que nossos especialistas examinem a situação mais detalhadamente e possam fornecer assistência o mais rápido possível.

O Kaspersky Anti-Virus coloca todos os objetos suspeitos em uma área específica conhecida como *Quarentena*, onde são armazenados em formato criptografado, de forma a evitar a infecção do computador. Esses objetos podem ser verificados quanto à presença de vírus, restaurados no local original ou excluídos. Os objetos podem ser colocados na quarentena manualmente. Todos os objetos que a verificação considerar não infectados são restaurados automaticamente em seu local original.

O Armazenamento de Backup mantém cópias dos objetos desinfectados ou excluídos pelo aplicativo. Essas cópias são criadas caso seja necessário restaurar os objetos ou recriar o caminho da infecção. Os backups também são armazenados em formato criptografado para proteger o computador de infecções. Um objeto do backup pode ser restaurado no local original ou excluído.

Ativação

Ao adquirir o Kaspersky Anti-Virus, você estabelece um contrato de licença com a Kaspersky Lab que regula o uso do aplicativo, além do acesso às atualizações do banco de dados do aplicativo e ao Suporte Técnico por um período determinado. Os termos de uso e outras informações necessárias para a funcionalidade integral do programa são fornecidos em um arquivo de chave.

Com o recurso Ativação, você pode encontrar informações detalhadas sobre a chave que está usando ou adquirir uma nova chave.

Suporte

Todos os usuários registrados do Kaspersky Anti-Virus podem tirar proveito de nosso serviço de suporte técnico. Para saber onde você pode obter suporte técnico, use o recurso *Suporte*.

Seguindo esses links, você pode participar do fórum de usuários da Kaspersky Lab ou enviar um comentário ou um relatório de erro ao Suporte Técnico, preenchendo um formulário on-line específico.

Também é possível acessar o Suporte Técnico on-line e seu Gabinete Pessoal, e 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 7.0 seja executado corretamente, seu computador deve atender a estes requisitos mínimos:

Requisitos gerais:

- 50 MB de espaço livre no disco rígido
- Unidade de CD/DVD-ROM (para instalar o Kaspersky Anti-Virus 7.0 a partir de um CD/DVD de instalação)
- Microsoft Internet Explorer 5.5 ou superior (para atualizar os bancos de dados e módulos do programa pela Internet)
- Microsoft Windows Installer 2.0

Microsoft Windows 2000 Professional (Service Pack 2 ou superior), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 2 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 versão 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 com um CD de instalação contendo os arquivos do programa e a documentação em formato PDF
- Um Manual do Usuário impresso (quando o item tiver sido incluído no pedido) ou um Manual do Produto
- 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 durante a validade da chave:

- Atualizações dos bancos de dados do aplicativo e novas versões do programa a cada hora, gratuitamente

- Consultoria sobre questões relativas à instalação, configuração e funcionamento do programa, por telefone e por e-mail
- Notificações sobre os lançamentos de novos produtos da Kaspersky Lab e novos vírus (este serviço é fornecidos para os usuários que assinarem as mensagens de notícias da Kaspersky Lab no site do Serviço de Suporte Técnico http://support.kaspersky.com/subscribe/)

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 7.0

Há diversas formas de instalar o Kaspersky Anti-Virus 7.0 em um host:

- interativamente, usando o Assistente de Configuração do aplicativo (consulte a seção 3.1 na p. 29); esse modo exige a participação do usuário para a continuidade da instalação;
- de maneira não interativa; esse tipo de instalação é executada a partir da linha de comando e não exige a participação do usuário para a continuidade da instalação (consulte a seção 3.3 na p. 41).

Cuidado!

É recomendável fechar todos os aplicativos em execução para instalar o Kaspersky Anti-Virus.

3.1. Procedimento de instalação usando o Assistente de Configuração

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.

Para instalar o Kaspersky Anti-Virus no computador, execute o arquivo setup que se encontra no CD do produto.

Assim, será feita a tentativa de localizar o pacote de instalação do aplicativo (um arquivo com a *extensão *.msi*) e, se o pacote for localizado, será solicitado que você verifique as atualizações do Kaspersky Anti-Virus nos servidores da Kaspersky Lab. Se o pacote de instalação não for localizado, será solicitado que você faça o download do mesmo. Após o download, a instalação do aplicativo será iniciada. No caso de o usuário optar por não fazer o download, a instalação continuará normalmente.

Um assistente de configuração 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.

Step 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.

Step 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**. Para cancelar a instalação, clique em **Cancelar**.

Step 3. Exibindo o Contrato de Licença do Usuário Final

A janela a seguir contém o Contrato de Licença do Usuário Final estabelecido 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. Para cancelar a instalação, clique em **Cancelar**.

Step 4. Selecionando o tipo de instalação

Nesta etapa, você deve selecionar o tipo de instalação:

Instalação expressa. Se esta opção for selecionada, o Kaspersky Anti-Virus será instalado com as configurações padrão recomendadas pelos especialistas da Kaspersky Lab. No final da instalação, será aberto um assistente de ativação (consulte a seção 3.2.2 na p. 34).

Instalação personalizada. Com essa opção, você deverá selecionar os componentes do aplicativo que serão instalados e a pasta de instalação, além de ativar e configurar a instalação usando um assistente específico (consulte a seção 3.2 na p. 34).

Com a primeira opção, a instalação será executada no modo não interativo, ou seja, as etapas seguintes descritas nesta seção serão ignoradas. No segundo caso, será necessário inserir ou confirmar determinados dados.

Step 5. 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:

- Para sistemas de 32 bits: **<Unidade>\Arquivos de Programas\Kaspersky Lab\Kaspersky Anti-Virus 7.0**
- Para sistemas de 64 bits: **<Unidade> → Arquivos de Programas (x86) → Kaspersky Lab → Kaspersky Anti-Virus 7.0**.

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.

Cuidado!

Se você especificar um caminho de diretório completo manualmente, observe que ele não pode exceder 200 caracteres, nem conter caracteres especiais.

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

Step 6. Selecionando os componentes do programa a serem instalados

Observação

Esta etapa não será executada, a menos que a instalação **Personalizada** seja selecionada.

Se você selecionou a instalação Personalizada, poderá escolher os componentes do Kaspersky Anti-Virus que deseja instalar. Por padrão, a proteção em tempo real e a verificação de vírus são selecionadas.

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. 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 **O recurso não estará disponível** 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**.

Step 7. Usando as configurações de instalação salvas anteriormente

Nesta etapa, é solicitado que você especifique se deseja usar as configurações de segurança ou os bancos de dados do aplicativo salvos anteriormente, caso eles tenham sido realmente salvos ao remover uma instalação anterior do Kaspersky Anti-Virus do computador.

Vamos examinar mais detalhadamente as formas de acessar a funcionalidade acima.

Se uma versão (build) anterior do Kaspersky Anti-Virus foi instalada no computador e os bancos de dados do aplicativo foram salvos, eles podem ser importados para a versão que está sendo instalada. Marque ☑ **Bancos de dados do aplicativo**. Os bancos de dados fornecidos com o aplicativo não serão copiados para o computador.

Para usar as configurações de proteção definidas para uma versão anterior e salvas no computador, marque ☑ **Configurações de tempo de execução do aplicativo**.

Step 8. 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® 6.0, no caso de uma instalação manual, é recomendável salvar o arquivo da chave usado antes de excluí-lo, de forma que você possa usar essa chave para o Kaspersky Anti-Virus 7.0. 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.

No caso de o Kaspersky Anti-Virus 6.0 ser desinstalado automaticamente, suas informações de ativação serão salvas pelo software e serão recuperadas na instalação da Versão 7.0.

Cuidado!

O Kaspersky Anti-Virus 7.0 dá suporte aos arquivos de chave da Versão 6.0 e da Versão 7.0. Não há suporte para as chaves usadas nos aplicativos da Versão 5.0.

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

Step 9. Concluindo a instalação do programa

Neste estágio, o programa solicitará que você conclua sua instalação no computador.

É recomendável não desmarcar ☑ **Habilitar Autodefesa antes da instalação** ao instalar o Kaspersky Anti-Virus 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 essa caixa de seleção.

Se o aplicativo for instalado remotamente por meio da **Área de Trabalho Remota do Windows**, é recomendável desmarcar ☑ **Habilitar Autodefesa antes da instalação**. Caso contrário, talvez o procedimento de instalação não seja concluído ou completado corretamente.

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

Cuidado!

As conexões de rede atuais são interrompidas durante a instalação de componentes do Kaspersky Anti-Virus que interceptam tráfego de rede. A maioria dessas conexões é restabelecida após um período.

Step 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 de Configuração 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 de Configuração.

3.2. Assistente de Configuração

O Assistente de Configuração do Kaspersky Anti-Virus 7.0 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 de Configuração foi criada como um Assistente do Microsoft 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 a seção 15.9.4 na p. 206).

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 7.0. Podem estar incluídos os arquivos da quarentena ou do backup, ou as configurações de proteção.

Para usar esses dados na Versão 7.0, marque as caixas desejadas.

3.2.2. Ativando o programa

Antes de ativar o programa, verifique se as configurações de data do sistema do computador correspondem à data e hora atuais.

O procedimento de ativação consiste na instalação de uma chave, que é usada pelo Kaspersky Anti-Virus para verificar a licença a ser usada pelo aplicativo e sua data de validade.

A chave 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 validade da chave.

3.2.2.1. Selecionando um método de ativação do programa

Existem várias opções de ativação do programa, dependendo de você ter uma chave 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 de ativação, você poderá obter um arquivo de chave que dá acesso à funcionalidade integral do aplicativo durante a vigência do contrato de 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 gratuita com um período de teste limitado, conforme definido pelo contrato de licença pertinente.
- **Aplicar chave existente**. Ativa o aplicativo usando o arquivo da chave do Kaspersky Anti-Virus 7.0.
- **Ativar mais tarde**. Se você escolher esta opção, o estágio de ativação será ignorado. O Kaspersky Anti-Virus 7.0 será instalado no seu computador e você terá acesso a todos os recursos do programa, exceto as atualizações (é possível atualizar o aplicativo somente após a instalação).

Cuidado!

Uma conexão com a Internet é necessária para as duas primeiras opções de ativação. Se, no momento da instalação, não houver uma conexão com a Internet disponível, você poderá executar a ativação mais tarde (consulte a seção Capítulo 14 na p. 169), através da interface do aplicativo ou conectando-se à Internet de um outro computador e conseguindo uma chave com um código de ativação obtido por meio do registro no site de Suporte Técnico da Kaspersky Lab.

3.2.2.2. Inserindo o código de ativação

Para ativar o programa, insira o código de ativação. Quando o aplicativo é comprado pela Internet, o código de ativação é enviado por e-mail. No caso de compra do aplicativo em mídia física, o código de ativação está impresso no disco de instalação.

O código de ativação é uma seqüência de números e letras separados por hífens em quatro grupos de cinco símbolos, sem espaços. Por exemplo, 11AA1-11AAA-1AA11-1A111. Observe que o código de ativação deve ser inserido em caracteres latinos.

Se você já tiver se registrado junto à Kaspersky Lab, no site do Serviço de Suporte Técnico, e tiver um número do cliente e uma senha, marque a caixa de seleção **Eu já tenho uma ID do cliente** e insira essas informações na parte inferior da janela.

Caso ainda não tenha se registrado, pressione o botão **Avançar**, deixando a caixa desmarcada. Insira o número do cliente e a senha na parte inferior da janela, se você já executou o procedimento de registro do cliente da Kaspersky Lab e possui essas informações. Se ainda não tiver efetuado seu registro, deixe os campos em branco. Dessa forma, o assistente de ativação solicitará suas informações de contato e fará o registro na etapa seguinte. No final do registro, serão atribuídos um número do cliente e uma senha, necessários para obter suporte técnico. Ao usar o assistente de ativação para registrar-se, o número do cliente pode ser exibido na seção **Suporte** da janela principal do aplicativo (consulte a seção 15.10 na p. 207).

3.2.2.3. Registro do usuário

Esta etapa do assistente de ativação exige que você forneça suas informações de contato: endereço de e-mail, cidade e país de residência. Essas informações são necessárias para que o Suporte Técnico da Kaspersky Lab o identifique como um usuário registrado.

Depois de inserir as informações, elas serão enviadas pelo assistente de ativação para um servidor de ativação, e será atribuída uma identificação do cliente e uma senha para o Gabinete Pessoal no site do Suporte Técnico. As informações sobre a identificação do cliente estão disponíveis em **Suporte** na janela principal do aplicativo.

3.2.2.4. Obtendo um arquivo de chave

O Assistente de Configuração 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 um arquivo de chave. Se você instalar a versão de demonstração do programa, o Assistente de Configuração receberá o arquivo da chave de teste sem um código de ativação.

O arquivo obtido será instalado automaticamente no aplicativo e você verá uma janela de conclusão da ativação com informações detalhadas sobre a chave em uso.

Observação

Quando este método de ativação for selecionado, o aplicativo não baixará um arquivo físico com a extensão **.key* de um servidor, mas obterá determinados dados que estão gravados no Registro do sistema operacional e no sistema de arquivos.

O registro do usuário no site da Kaspersky Lab é necessário para obter uma chave de ativação atualizada.

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.

3.2.2.5. Selecionando um arquivo de chave

Se você possuir um arquivo de chave do Kaspersky Anti-Virus 7.0, o Assistente perguntará se deseja instalá-lo. Se desejar, use o botão **Procurar** e selecione o caminho do arquivo com a extensão *.key* na janela de seleção de arquivos.

Após a instalação bem-sucedida da chave, as informações da chave atual serão exibidas na parte inferior da janela: nome do proprietário, código da chave, tipo de chave (comercial, teste beta, teste, etc.) e data de validade.

3.2.2.6. Concluindo a ativação do programa

O Assistente de Configuração o informará que a ativação do programa foi bem-sucedida. Também serão exibidas informações sobre a chave de licença instalada: nome do proprietário, código da chave, tipo de chave (comercial, teste beta, teste, etc.) e data de validade.

3.2.3. Selecionando um modo de segurança

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

Proteção básica. Esta é a configuração padrão, criada para usuários que não têm muita experiência com computadores ou com software antivírus. Ela define os componentes do aplicativo com seus níveis de segurança recomendados e informa o usuário apenas sobre eventos perigosos (como a detecção de código mal-intencionado ou atividades perigosas).

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

atividades não autorizadas na rede. Todas essas atividades 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 o monitoramento do Registro do sistema** – 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 dos bancos de dados e módulos do programa. Nesta janela, o Assistente de Configuração 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.

Os bancos de dados e módulos do programa fornecidos com o software podem estar desatualizados no momento da instalação do 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.

Para configurar as atualizações (selecionar a fonte de atualizações, executar as atualizações com um logon específico ou ativar o download de atualizações de uma fonte local), clique no botão **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 Assistente de Configuração 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 Microsoft 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 modificar as configurações do programa** - solicita a senha quando um usuário tenta salvar alterações das configurações do programa.
  - **Saindo do programa** – solicita a senha se um usuário tentar fechar o programa.
  - **Ao interromper/pausar componentes de proteção ou tarefas de verificação** – solicita uma senha quando o usuário tenta pausar ou desligar completamente um componente de proteção ou uma tarefa de verificação de vírus em tempo real.

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 de Configuração

A última janela do Assistente perguntará se você deseja reiniciar o computador para concluir a instalação do programa. É necessário reiniciar para que os drivers do Kaspersky Anti-Virus sejam registrados.

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

3.3. Instalando o programa do prompt de comando

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

```
msiexec /i <nome_do_pacote>
```

O Assistente de Configuração será iniciado (consulte a seção 3.1 na p. 29). Depois que o programa for instalado, reinicie o computador.

Para instalar o aplicativo de maneira não interativa (sem executar o Assistente de Configuração), digite:

```
msiexec /i <nome_do_pacote> /qn
```

CAPÍTULO 4. INTERFACE DO PROGRAMA

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

- Ícone na área de notificação da barra de tarefas (consulte a seção 4.1 na p. 42)
- Menu de contexto (consulte a seção 4.2 na p. 43)
- Janela principal (consulte a seção 4.3 na p. 45)
- Janela de configurações do programa (consulte a seção 4.4 na p. 49)

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

- Microsoft Office Outlook (consulte a seção 8.2.2 na p. 101)
- The Bat! (consulte a seção 8.2.3 na p. 102)
- Microsoft Internet Explorer (consulte Capítulo 9 na p. 109)
- Microsoft Windows Explorer (consulte a seção 11.2 na p. 139)

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

4.1. Ícone na área de notificação da barra de tarefas

Logo após a instalação do Kaspersky Anti-Virus, o ícone do programa será exibido na área de notificação da barra de tarefas.

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), a proteção completa ou alguns de seus componentes estarão em execução. Se o ícone estiver inativo (preto e branco), toda a proteção estará desabilitada (consulte a seção 2.2.1 na p. 22) ou em pausa.

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.

 Os bancos de dados e módulos do Kaspersky Anti-Virus estão sendo atualizados.

 O computador deve ser reinicializado para aplicar as atualizações.

 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 a seção 4.2 na p. 43) e a janela principal (consulte a seção 4.3 na p. 45).

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.

Se houver notícias da Kaspersky Lab disponíveis, o ícone  aparecerá na área de notificação da barra de tarefas. Clique duas vezes no ícone para exibir as notícias em uma nova janela.

4.2. O menu de contexto

Você pode executar tarefas de proteção básicas do menu de contexto (veja a Figura 1).

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 uma verificação de vírus. A lista padrão contém vários arquivos, como a pasta **Meus Documentos**, a pasta Inicialização, caixas de correio, todas as

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

Atualização - inicia as atualizações do banco de dados e dos módulos do Kaspersky Anti-Virus no computador.

Ativar – ativa o programa. É necessário ativar sua versão do Kaspersky Anti-Virus para obter o status de usuário registrado, que permite o acesso à funcionalidade integral do aplicativo e ao Suporte Técnico. 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 45).

Pausar a proteção / Habilitar proteção – desabilita temporariamente ou habilita os componentes de proteção em tempo real (consulte a seção 2.2.1 na p. 22). Este item do menu não afeta tarefas de atualização do programa ou de verificação de vírus.

Sobre o programa - abre uma janela com informações sobre o Kaspersky Anti-Virus.

Sair – fecha o Kaspersky Anti-Virus (ao selecionar esta opção, o aplicativo será descarregado da RAM do computador).

Figura 1. O menu de contexto

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 Figura 2) pode ser dividido em três partes:

- a parte superior da janela indica o status de proteção atual do computador.

  Três estados de proteção são possíveis (consulte a seção 5.1 na p. 51), representadas por códigos de cores semelhantes às da sinalização de trânsito. O verde indica que o computador está protegido adequadamente, enquanto o amarelo e o vermelho indicam problemas diversos na configuração ou operação do Kaspersky Anti-Virus.

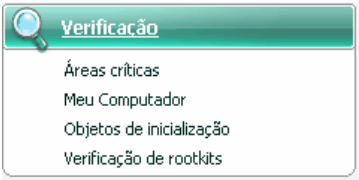
  Para obter informações detalhadas sobre a solução de problemas e sua resolução rápida, use o Assistente de Segurança que é aberto ao clicar no link da notificação de ameaça de segurança.

Figura 2. Janela principal do Kaspersky Anti-Virus

- *Painel de navegação (à esquerda da janela):* dá acesso rápido e fácil a qualquer componente, tarefa de verificação de vírus, atualizações, funcionalidade de suporte do aplicativo;
- à direita da janela, o *painel informativo* contém informações sobre o componente de proteção selecionado à esquerda e exibe suas configurações, fornecendo ferramentas para executar verificações de vírus, trabalhar com arquivos em quarentena e cópias de backup, gerenciar chaves de licença, etc.

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

Agora, vamos examinar mais detalhadamente os elementos do painel de navegação da janela principal.

Seção da **janela principal**	**Finalidade**
	A principal função da seção **Proteção** é fornecer acesso aos componentes básicos de proteção em tempo real do seu computador. Para exibir o status de um componente de proteção ou de seus módulos, configurá-los ou abrir um relatório pertinente, selecione o componente na lista sob **Proteção**. Esta seção também contém links para acessar as tarefas mais comuns: a verificação de vírus e as atualizações do banco de dados do aplicativo. Você pode exibir informações sobre o status dessas tarefas, configurá-las ou executá-las.
	A seção **Verificação** dá acesso às tarefas de verificação de vírus em objetos. Ela mostra as tarefas criadas pelos especialistas da Kaspersky Lab (verificação de vírus em áreas críticas, em objetos de inicialização, verificação completa do computador, verificação de rootkits), além das tarefas do usuário. Quando uma tarefa é selecionada no painel direito, são fornecidas informações pertinentes à tarefa, é possível configurar a tarefa, é gerada uma lista de objetos a serem verificados ou a tarefa é executada. Para verificar um único objeto (arquivo, pasta ou unidade), selecione **Verificação**, use o painel direito para adicionar o objeto à lista a ser verificada e execute a tarefa. Além disso, esta seção pode ser usada para criar um disco de recuperação (consulte a seção 15.4 na p. 186).

	A seção **Atualização** contém informações sobre as atualizações do aplicativo: a data de publicação do banco de dados e a contagem de registros de assinaturas de vírus. É possível utilizar links para iniciar uma atualização, exibir um relatório detalhado, configurar atualizações e reverter uma atualização para uma versão anterior.
	A seção **Arquivos de dados e relatórios** pode ser usada para exibir um relatório detalhado de qualquer componente do aplicativo, uma tarefa de verificação de vírus ou de atualização (consulte a seção 15.3 na p. 178) e para trabalhar com os objetos colocados na quarentena (consulte a seção 15.1 na p. 172) ou no backup (consulte a seção 15.2 na p. 176).
	A seção **Ativação** é usada para manipular as chaves necessárias para o funcionamento integral dos aplicativos (consulte a seção Capítulo 14 na p. 169). Se não houver uma chave instalada, é recomendável adquiri-la imediatamente para poder ativar o aplicativo (consulte a seção 3.2.2 na p. 34). Se houver uma chave instalada, esta seção mostrará informações sobre o tipo de chave usada e sua data de validade. Quando uma chave expira, ela pode ser renovada no site da Kaspersky Lab.
	A seção **Suporte** fornece informações sobre o Suporte Técnico disponível para usuários registrados do Kaspersky Anti-Virus.

Cada elemento do painel de navegação é acompanhado por um menu de contexto específico. O menu contém itens para os componentes de proteção que ajudam a configurá-los rapidamente, gerenciá-los e exibir relatórios. Existe

um item de menu adicional para tarefas de verificação de vírus 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.

Na parte inferior esquerda da janela há dois botões: **Ajuda**, que dá acesso ao sistema de ajuda do Kaspersky Anti-Virus, e **Configurações**, que abre a janela de configurações do aplicativo.

4.4. Janela de configurações do programa

Você pode abrir a janela de configurações do Kaspersky Anti-Virus da janela principal (consulte a seção 4.3 na p. 45) ou do menu de contexto do aplicativo (consulte a seção 4.2 na p. 43). Clique em **Configurações** na seção inferior da janela principal ou selecione a opção apropriada no menu de contexto do aplicativo.

A janela de configurações (veja a Figura 3) tem um layout semelhante ao da janela principal:

- à esquerda da janela, você tem acesso rápido e fácil às configurações de cada componente do aplicativo, da atualização, das tarefas de pesquisa de vírus e do aplicativo;
- 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 configurações avançadas, você pode abrir janelas de configurações de segundo e terceiro níveis. Uma descrição detalhada das configurações do programa encontra-se nas seções do Manual do Usuário.

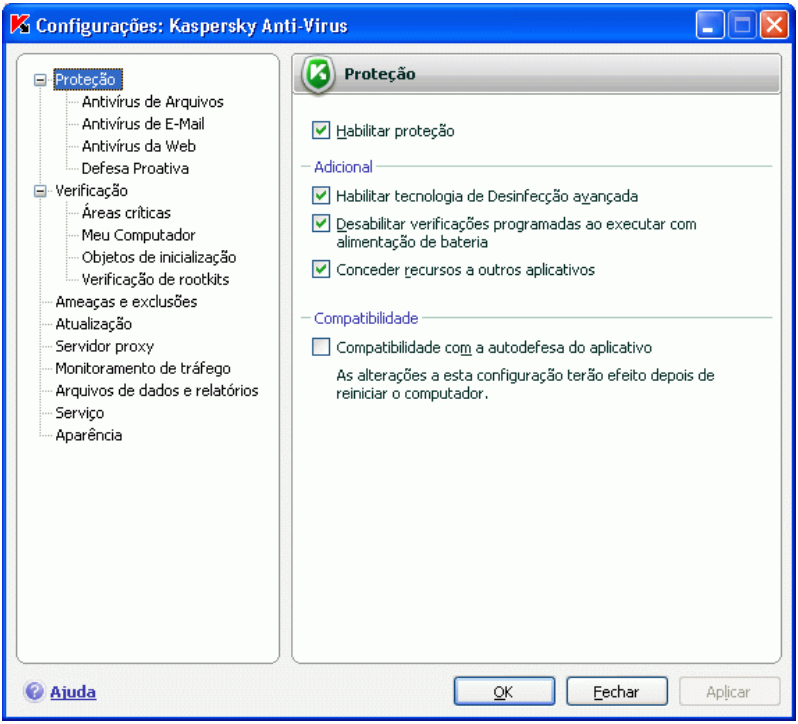


Figura 3. Janela de configurações do Kaspersky Anti-Virus

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 de Configuração (consulte a seção 3.2 na p. 34) 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 51) para certificar-se de que o Kaspersky Anti-Virus está sendo executado no nível apropriado.
- Atualize o programa (consulte a seção 5.6 na p. 56) se o Assistente de Configuração não o fizer automaticamente depois de instalar o programa.
- Verifique o computador (consulte a seção 5.3 na p. 54) quanto à presença de vírus.

5.1. Qual é o status de proteção do computador?

O status de proteção do computador representa graficamente se existem ameaças à segurança geral do sistema em algum momento. Para os fins deste documento, as ameaças incluem malware e bancos de dados do aplicativo desatualizados, desativação de alguns componentes de proteção, uso de configurações mínimas do aplicativo, etc.

O status de proteção é exibido na parte superior da janela principal do aplicativo e utiliza o código de cores da sinalização de trânsito. Dependendo da situação,

a cor da seção superior da janela mudará e, no caso de ameaças de segurança, as cores serão complementadas com mensagens informativas implementadas como links para o Assistente de Segurança.

Os seguintes códigos de cores são usados para indicar o status da proteção:

- A janela principal do aplicativo está *verde*. Esse status indica uma proteção adequada do computador.

  Isso significa que os bancos de dados foram atualizados oportunamente, todos os componentes de proteção estão ativados, o aplicativo está sendo executado com as configurações recomendadas pelos especialistas da Kaspersky Lab, nenhum objeto mal-intencionado foi detectado na verificação completa do computador ou esses objetos mal-intencionados foram desabilitados.

- A janela principal do aplicativo está *amarela*. O nível de proteção do computador é inferior ao anterior. Esse status de proteção indica determinados problemas com o aplicativo ou com suas configurações.

  Por exemplo, existem determinados desvios com relação ao modo de operação recomendado, os bancos de dados do aplicativo não foram atualizados por vários dias.

- A janela principal do aplicativo está *vermelha*. Este status indica problemas que poderiam levar à infecção do computador e à perda de dados. Por exemplo, houve falha em um ou mais componentes de proteção, o produto não foi atualizado por muito tempo ou objetos mal-intencionados foram detectados e precisam ser desabilitados urgentemente ou o produto não foi ativado.

Se houver problemas no sistema de proteção, é recomendável corrigi-los imediatamente. Use o Assistente de Segurança que pode ser acessado clicando na notificação sobre as ameaças de segurança. O assistente de segurança o ajudará a examinar todas as ameaças atuais e o levará para o local apropriado para removê-las. O nível de perigo da ameaça é representado pela cor do indicador:

 - *o indicador indica ameaças não-críticas* que podem, contudo, diminuir o nível de proteção geral do computador. Preste atenção às recomendações dos especialistas da Kaspersky Lab.

 - *o indicador mostra que há ameaças sérias* à segurança do computador. Siga as recomendações a seguir cuidadosamente. Seu objetivo é a melhor proteção de seu computador. São fornecidos links para as ações recomendadas.

Para percorrer a lista de ameaças existentes, clique no botão Avançar. É fornecida uma descrição detalhada de cada ameaça, e as seguintes ações estão disponíveis:

- *Eliminar a ameaça imediatamente*. Usando os links correspondentes, você pode eliminar a ameaça diretamente. Para obter informações detalhadas sobre os eventos relacionados a esta ameaça, consulte o arquivo de relatório. A ação recomendada é eliminar a ameaça imediatamente.
- *Adiar a eliminação da ameaça*. Se, por algum motivo, não for possível eliminar a ameaça imediatamente, é possível adiar essa ação e voltar a ela posteriormente. Para fazê-lo, use o link Adiar.

  Esta opção não está disponível para ameaças graves. Essas ameaças incluem, por exemplo, objetos mal-intencionados que não podem ser desinfectados, pane dos componentes ou arquivos do banco de dados do programa danificados.

Se ainda houver ameaças depois de concluir o Assistente de Segurança, aparecerá um lembrete na parte superior da janela principal, informando que é necessário eliminá-las. Se você abrir o Assistente de Segurança novamente, as ameaças adiadas não estarão na lista de ameaças ativas. Contudo, ainda é possível voltar para exibir e eliminar as ameaças adiadas clicando no link Exibir ameaças adiadas na última janela do assistente.

5.2. Verificando o status de cada componente de proteção individual

Para exibir o status atual de um componente de proteção em tempo real, abra a janela principal do aplicativo e selecione o componente desejado em **Proteção**. Informações resumidas sobre o componente selecionado serão apresentadas à direita.

O status do componente é o indicador mais importante:

- *<nome do componente>: em execução* – a proteção fornecida pelo componente está no nível desejado.
- *<nome do componente>: em pausa* – o componente está desabilitado por um determinado período. O componente será reiniciado automaticamente após um determinado período ou após reiniciar o aplicativo. O componente pode ser ativado manualmente. Clique em Continuar operação.

- *<nome do componente>: interrompido* – o componente foi interrompido pelo usuário. A proteção pode ser reabilitada clicando em Habilitar.
- *<nome do componente>: não executando* – por algum motivo, a proteção fornecida pelo componente não está disponível.
- *<nome do componente>: desabilitado (erro)* – o componente encontrou um erro.

  Se um componente encontrar um erro, tente reiniciá-lo. Se houver o erro ao reiniciar, examine o relatório do componente, que deve conter o motivo da falha. Se não conseguir solucionar o problema, salve o relatório do componente em um arquivo usando **Ação → Salvar como** e entre em contato com o Suporte Técnico da Kaspersky Lab.

Após o status do componente, pode haver informações sobre as configurações usadas por ele (como o nível de segurança e a ação a ser executada com relação a objetos perigosos). Se um componente tiver mais de um módulo, o status do módulo será exibido como habilitado ou desabilitado. Para editar as configurações atuais do componente, clique em Configurar.

Além disso, são exibidas algumas estatísticas de tempo de execução do componente. Para exibir um relatório detalhado, clique em Abrir relatório.

Se, por algum motivo, em algum momento o componente for pausado ou interrompido, os resultados no momento da desativação poderão ser exibidos clicando em Abrir relatório da última execução.

5.3. 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.

A seleção da tarefa **Meu Computador** exibirá as configurações nível de segurança atual e ação a ser tomada com relação aos objetos mal-intencionados. Um relatório sobre a última verificação também está disponível.

Para verificar programas mal-intencionados no computador,

1. Selecione a tarefa **Meu Computador** em **Verificação** na janela principal do aplicativo.

2. Clique no link Iniciar verificação.

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 ficará oculta, mas a verificação não será interrompida.

5.4. 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**.

A seleção de **Áreas críticas** exibirá as configurações da tarefa: nível de segurança atual e ação a ser tomada com relação aos objetos mal-intencionados. 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,

1. Selecione a tarefa **Áreas críticas** em **Verificação** na janela principal do aplicativo.
2. Clique no link Iniciar verificação.

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.

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

Em algumas situações, é necessário verificar vírus em objetos individuais e não em todo o computador. Por exemplo, um dos discos rígidos onde estão localizados seus programas e jogos, bancos de dados de e-mail trazidos do trabalho para casa, arquivos comprimidos provenientes de e-mails etc. Você

pode selecionar um objeto para verificá-lo com as ferramentas padrão do sistema operacional Microsoft Windows (por exemplo, na janela do programa **Explorer** ou na **Área de Trabalho**, entre outros.).

Para verificar um objeto,

Coloque o cursor sobre o nome do objeto selecionado, abra o menu de contexto do Microsoft Windows clicando com o botão direito do mouse e selecione **Verificar vírus** (veja a Figura 4).

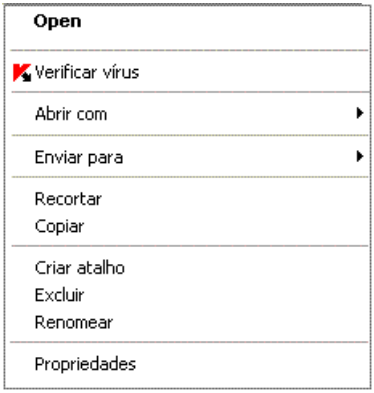


Figura 4. Verificando um objeto selecionado usando um menu de contexto padrão do Microsoft Windows

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.

5.6. Como atualizar o programa

A Kaspersky Lab atualiza os bancos de dados e módulos do Kaspersky Anti-Virus usando servidores de atualização exclusivos.

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,

1. Selecione a seção **Atualização** na janela principal do aplicativo.
2. Clique em Atualizar bancos de dados.

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

5.7. 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 *executando (mal funcionamento do subsistema)*, tente reiniciar o programa.

Se o problema não for resolvido depois de reiniciar o programa, é recomendável corrigir possíveis erros usando o recurso de restauração do aplicativo (consulte a seção Capítulo 17 na p. 226).

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 em arquivo e enviá-lo para o Suporte Técnico para investigação.

Para salvar o relatório do componente em um arquivo:

1. Selecione o componente em **Proteção** na janela principal do aplicativo e clique em Abrir relatório (componente em execução no momento) ou em Abrir relatório da última execução (componente desabilitado).
2. Na janela do relatório, clique em **Ações → Salvar como** e, na janela que é aberta, especifique o nome do arquivo no qual o relatório será salvo.

CAPÍTULO 6. SISTEMA DE GERENCIAMENTO DA PROTEÇÃO

Esta seção fornece informações sobre a definição das configurações comuns do aplicativo usadas por todas as tarefas e componentes de proteção em tempo real, além de informações sobre a criação de escopos de proteção e listas de ameaças a serem tratadas pelo aplicativo, e uma lista de objetos confiáveis que devem ser ignorados pela proteção:

- Gerenciamento da proteção em tempo real (consulte a seção 6.1 na p. 58);
- Utilização da Tecnologia de desinfecção avançada (consulte a seção 6.2 na p. 62);
- Execução de tarefas em um computador portátil (consulte a seção 6.3 na p. 63);
- Cooperação do Kaspersky Anti-Virus com outros aplicativos (consulte a seção 6.4 na p. 63);
- Compatibilidade do Kaspersky Anti-Virus com recursos de autodefesa de outros aplicativos (consulte a seção 6.5 na p. 64);
- Lista de ameaças (consulte a seção 6.2 na p. 62) contra as quais o aplicativo oferecerá proteção;
- Lista de objetos confiáveis (consulte a seção 6.9 na p. 69) que serão ignorados pela proteção.

6.1. Interrompendo e reiniciando a proteção do computador em tempo real

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 7.0* no canto superior direito da tela indicam que a proteção está ativa.

Todos os componentes de proteção em tempo real (consulte a seção 2.2.1 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 em tempo real**, 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 em tempo real significa desabilitar temporariamente todos os componentes de proteção que monitoram os arquivos no computador, os e-mails enviados e recebidos, os scripts executáveis e o comportamento dos aplicativos.

Para pausar a proteção em tempo real do computador:

1. Selecione **Pausar proteção** no menu de contexto do programa (consulte a seção 4.2 na p. 43).
2. Na janela **Pausar proteção** que é aberta (veja a Figura 5), 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 continuará se você abrir o programa no menu **Iniciar** ou após reiniciar o computador, desde que o programa esteja definido para iniciar automaticamente na inicialização (consulte a seção 15.11 na p. 209).
   - 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.

Se você pausar a proteção, todos os componentes de proteção em tempo real serão pausados. Isso é indicado por:

- Nomes inativos (cinza) dos componentes desabilitados na seção **Proteção** da janela principal.

- Ícone inativo (cinza) na área de notificação da barra de tarefas.

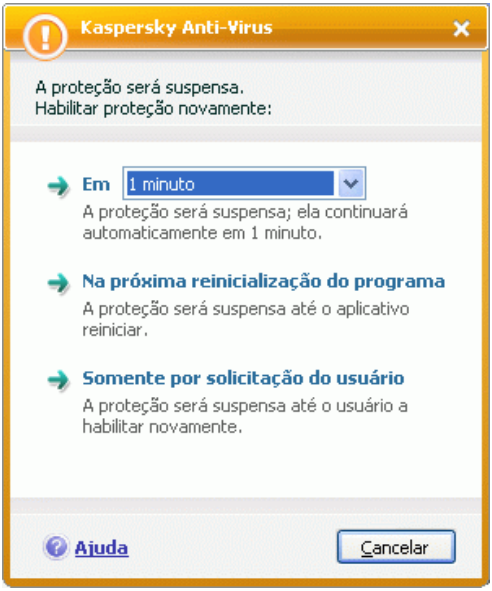


Figura 5. Janela Pausar proteção

6.1.2. Interrompendo a proteção

Interromper a proteção significa desabilitar totalmente os componentes de proteção em tempo real. 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 6.9 na página 69).

Para interromper a proteção em tempo real:

1. Abra a janela de configurações do aplicativo e selecione **Proteção**.
2. Desmarque ☑ **Habilitar proteção**.

Quando a proteção for desabilitada, 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 área de notificação da barra de tarefas.

6.1.3. Pausando / interrompendo a componentes de proteção individuais

Existem várias maneiras de interromper um componente de proteção. 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 a seção 6.9 na p. 69).

Para pausar um componente de proteção individual:

Abra a janela principal do aplicativo, selecione o componente em **Proteção** e clique em Pausar.

O status do componente mudará para *em pausa*. O componente ficará em pausa até o aplicativo ser reiniciado ou até o componente ser reativado clicando em Continuar operação.

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

Para interromper um componente de proteção individual:

Abra a janela principal do aplicativo, selecione o componente em **Proteção** e clique em Parar.

O status do componente mudará para *desabilitado* e seu nome em **Proteção** ficará inativo (cinza). A proteção oferecida pelo componente será desabilitada até ser reativada clicando em Habilitar.

Todos os componentes de proteção também podem ser desligado na janela de configurações do aplicativo. Abra a janela de configurações, selecione o componente em **Proteção** e desmarque ☑ **Habilitar o <nome do componente>**.

Ao desabilitar um componente de proteção, todas as estatísticas do trabalho anterior serão limpas e, quando o componente for iniciado, serão substituídas.

Os componentes de proteção individuais também serão desabilitados se a proteção em tempo real do computador forem interrompidas (consulte a seção 6.1.2 na p. 60).

6.1.4. Restaurando a proteção no computador

Se, em algum momento, você pausou ou interrompeu a proteção em tempo real do 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*.

  Selecione a seção **Proteção** à esquerda da janela principal e clique em Habilitar proteção.

O status de proteção muda imediatamente para *em execução*. O ícone do programa na área de notificação da barra de tarefas se torna ativo (colorido).

6.2. Tecnologia de Desinfecção Avançada

Malwares avançados podem invadir os níveis mais baixos do sistema operacional, o que torna praticamente impossível removê-los. Quando uma ameaça ativa é descoberta no sistema, o Kaspersky Anti-Virus 7.0 sugere um procedimento de desinfecção estendida específico, que desabilitará e removerá a ameaça do computador.

Quando o procedimento for concluído, será necessário reiniciar o computador. É recomendável executar uma verificação completa de vírus depois de reiniciar o computador. Para aplicar o procedimento de Desinfecção avançada, abra a janela de configurações do aplicativo, selecione **Proteção** e marque ☑ **Habilitar tecnologia de Desinfecção avançada** (veja a Figura 6).

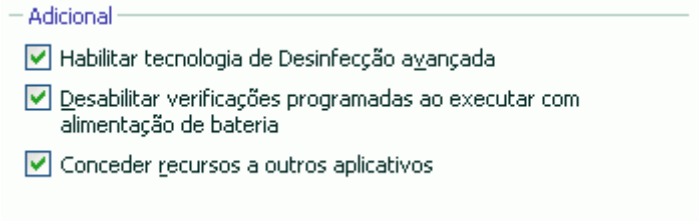


Figura 6. Definindo as configurações comuns

6.3. Executando o aplicativo em um computador portátil

Para economizar energia em um computador portátil, as tarefas de verificação de vírus podem ser adiadas.

Como a verificação de vírus e a atualização do programa geralmente exige recursos e tempo significativos, é recomendável reprogramar essas tarefas. Isso ajudará a economizar bateria. Você poderá atualizar o aplicativo (consulte a seção 5.6 na p. 56) ou executar uma verificação de vírus (consulte a seção 5.3 na p. 54) manualmente, conforme necessário. Para economizar a bateria, abra a janela de configurações do aplicativo, selecione **Proteção** e marque **Desabilitar verificações programadas ao executar com alimentação de bateria** em **Adicional** (veja a Figura 6).

6.4. Desempenho do computador em tempo de execução

As tarefas de verificação de vírus podem ser adiadas para limitar a carga do subsistema de armazenamento e da CPU.

A verificação de vírus sobrecarrega o subsistema de armazenamento e a CPU, tornando outros programas mais lentos. Se isso ocorrer, por padrão, o aplicativo suspenderá a verificação de vírus e disponibilizará recursos para os aplicativos do usuário.

Entretanto, há vários programas que são executados conforme os recursos de CPU são disponibilizados, sendo executados em segundo plano. Para que as verificações de vírus sejam executadas independentemente desses programas, abra a janela de configurações do aplicativo, selecione **Proteção** e marque **Conceder recursos a outros aplicativos** em **Adicional** (veja a Figura 6).

Observe que esta configuração pode ser definida individualmente para cada tarefa de verificação de vírus. A configuração da tarefa individual terá uma prioridade maior.

6.5. Solucionando problemas de compatibilidade do Kaspersky Anti-Virus com outros aplicativos

Às vezes, a execução do Kaspersky Anti-Virus pode gerar conflitos com outros aplicativos instalados. Isso ocorre porque esses aplicativos possuem mecanismos de autodefesa internos que são ativados quando o Kaspersky Anti-Virus tenta se integrar a eles. Esses aplicativos incluem o plug-in do Authentica para Acrobat Reader, que verifica o acesso a documentos pdf, o Oxygen Phone Manager II para gerenciamento de celulares e alguns jogos bloqueados.

Para resolver este problema, abra a janela de configurações do aplicativo, selecione **Proteção** e marque ☑ **Compatibilidade com a autodefesa do aplicativo** em **Compatibilidade** (veja a Figura 7). É necessário reiniciar o sistema operacional para que essas alterações tenham efeito.

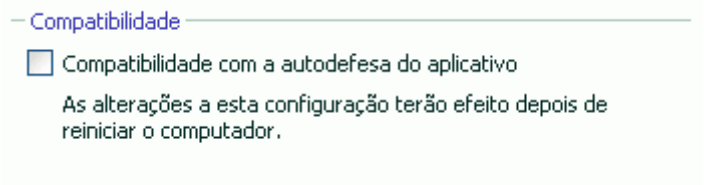


Figura 7. Configurando a compatibilidade

Cuidado!

Caso o aplicativo esteja instalado em um computador com o Microsoft Windows Vista ou o Microsoft Windows Vista x64, não há suporte a resolução da compatibilidade emitida para mecanismos internos de bloqueio de outros aplicativos.

6.6. Executando verificações de vírus e atualizações como outro usuário

O Kaspersky Anti-Virus 7.0 possui um recurso para iniciar tarefas de verificação no perfil de outro usuário (personificação). Por padrão, este recurso está desabilitado e as tarefas são executadas com o usuário atual.

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 em outro perfil que possua esses direitos.

Para configurar que uma tarefa de verificação seja executada com outro usuário:

1. Abra a janela de configurações do aplicativo e selecione a tarefa em **Verificação**.
2. Clique em **Personalizar** em **Nível de Segurança** e, na caixa de diálogo que é aberta, abra a guia **Adicional**.

Para configurar que uma tarefa de atualização seja executada com outro usuário

1. Abra a janela de configurações do aplicativo e selecione **Atualização**.
2. Clique em **Configurar** em **Configurações da atualização** e, na caixa de diálogo que é aberta, abra a guia **Adicional** (veja a Figura 8).

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

A menos que o recurso Executar como seja usado, as atualizações programadas serão executadas com o usuário atual. No caso de nenhum usuário ter feito logon no sistema e de o recurso Executar como não estar configurado, a atualização programada será executada com SYSTEM.

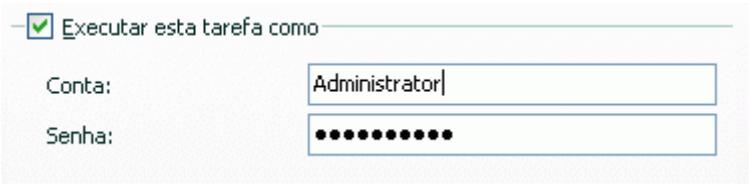


Figura 8. Configurando uma tarefa de atualização em outro perfil

6.7. Configurando notificações e tarefas programadas

A configuração da programação é a mesma para tarefas de verificação de vírus, atualizações do aplicativo e mensagens de tempo de execução do Kaspersky Anti-Virus.

Por padrão, as tarefas de verificação de vírus criadas na instalação do aplicativo estão desabilitadas. A única exceção e a verificação dos objetos de inicialização que são executadas sempre que o Kaspersky Anti-Virus é iniciado. Por padrão, as atualizações são configuradas para serem executadas automaticamente conforme são disponibilizadas nos servidores de atualização da Kaspersky Lab.

Se desejar, você poderá reconfigurar a programação.

O valor principal a ser definido é a freqüência de um evento (notificação ou execução da tarefa). Selecione a opção desejada em **Freqüência** (veja a Figura 9). Em seguida, especifique as configurações da atualização da opção selecionada em **Configurações da atualização**. As seguintes opções estão disponíveis:

- **Em uma hora especificada**. Executa uma tarefa ou envia uma notificação na data e hora especificadas.
- **Ao iniciar o aplicativo**. Executa uma tarefa ou envia uma notificação sempre que o Kaspersky Anti-Virus é iniciado. Também é possível especificar um período após o início do aplicativo para a execução da tarefa.
- **Após cada atualização**. A tarefa é executada após cada atualização do banco de dados do aplicativo (esta opção se aplica somente a tarefas de verificação de vírus).
- **Em minutos**. O intervalo entre as notificações ou execuções da tarefa será de alguns minutos. Defina o intervalo em minutos, nas configurações da programação. Ele não deve exceder 59 minutos.
- **Horas**. O intervalo entre as notificações e execuções da tarefa será de algumas horas. Se esta opção estiver selecionada, especifique o intervalo

nas configurações da programação: **A cada n horas** e defina o valor de *n*. Para execuções a cada hora, por exemplo, especifique **A cada 1 horas.**

Figura 9. Criando a programação de execução de tarefas

Dias. As tarefas serão iniciadas ou as notificações enviadas a cada alguns dias. Especifique o intervalo nas configurações da programação:

- Selecione **A cada N dias** e especifique o valor de *N*, se desejar um intervalo de um determinado número de dias.
- Selecione **Todos os dias da semana**, se desejar executar as tarefas diariamente, de segunda a sexta-feira.
- Selecione **Todos os finais de semana** para executar as tarefas somente aos sábados e domingos.

  No campo **Hora**, especifique o horário em que a tarefa de verificação será executada.

Semanas. As tarefas serão executadas ou as notificações enviadas em determinados dias da semana. Se esta freqüência for selecionada, marque os dias da semana em que as tarefas serão executadas nas configurações da programação. Use o campo **Hora** para definir o horário.

Mensal. A tarefa será iniciada ou as notificações enviadas uma vez por mês, na hora especificada.

Se, por algum motivo, a tarefa não puder ser executada (por exemplo, se o programa de e-mail não estiver instalado ou o computador estiver desligado),

você poderá configurar a tarefa para ser executada automaticamente assim que possível. Marque **Executar tarefa se ignorado** na janela da programação.

6.8. Tipos de malware monitorados

O Kaspersky Anti-Virus o protege de vários tipos de programas mal-intencionados. Independentemente das suas configurações, o programa sempre protege o computador dos tipos de malware mais perigosos, como 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-intencionados dos quais o Kaspersky Anti-Virus o protegerá, abra a janela de configurações do aplicativo e selecione **Ameaças e Exclusões** (veja a Figura 10).

A caixa **Categorias de malware** contém os tipos de ameaças (consulte a 1.3 na p. 12):

- **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. Isso não inclui programas possivelmente perigosos e outros que poderiam estar instalados no seu computador e que poderiam danificar seus arquivos, roubar seu dinheiro ou ocupar seu tempo.

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 perigoso, é recomendável criar uma exclusão para ele (consulte 6.9 na p. 69).

Para selecionar os tipos de malware a serem monitorados,

Abra a janela de configurações do aplicativo e selecione **Ameaças e exclusões**. A configuração será feita em **Categorias de malware** (veja a Figura 10).

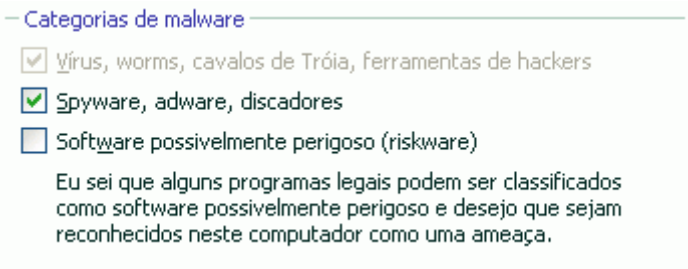


Figura 10. Selecionando as ameaças monitoradas

6.9. 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 confiável com base nas propriedades dos arquivos usados e dos 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 de tipos de ameaças da Enciclopédia de Vírus (o status que o programa atribui aos objetos durante uma verificação).

Observação

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 aplicativo e selecione **Ameaças e exclusões** (veja a Figura 10).

2. Clique no botão **Zona confiável** em **Exclusões**.
3. Configure as regras de exclusão para objetos e crie uma lista de aplicativos confiáveis na janela que é aberta (veja a Figura 11).

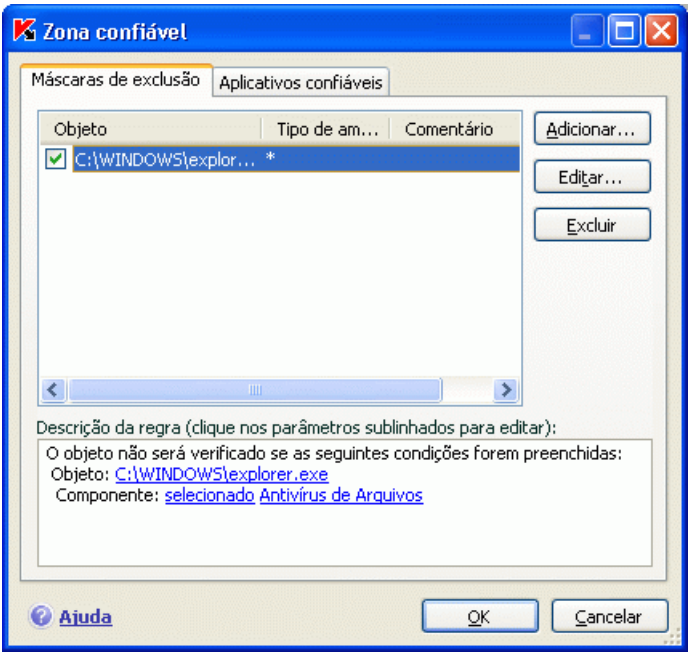


Figura 11. Criando uma zona confiável

6.9.1. 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.

O *Tipo de ameaça* é o status que o Kaspersky Anti-Virus atribui a um objeto durante a verificação. Um veredito se baseia 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 ou ocultar processos, 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 da ameaça 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 tipo de ameaça.

Ao adicionar uma exclusão, será criada uma regra que vários componentes do programa (Antivírus de Arquivos, Antivírus de E-Mail, Defesa Proativa, Antivírus da Web) 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 **Máscaras de exclusão**:*

1. Clique no botão **Adicionar** na janela **Máscaras de exclusão** (veja a Figura 11).
2. Na janela que é aberta (veja a Figura 12), 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.

   ☑ **Tipo de ameaça** - exclusão de um objeto das verificações com base em seu status na classificação da Enciclopédia de Vírus.

   Se você marcar as duas caixas de uma vez, será criada uma regra para aquele objeto com um determinado status de acordo com a classificação de tipos de ameaça 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 **Tipo de ameaça**, o arquivo especificado será excluído 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 a máscara do veredito) como **Tipo de ameaça**, os objetos com esse status serão excluídos da verificação somente quando essa área ou pasta forem verificadas.

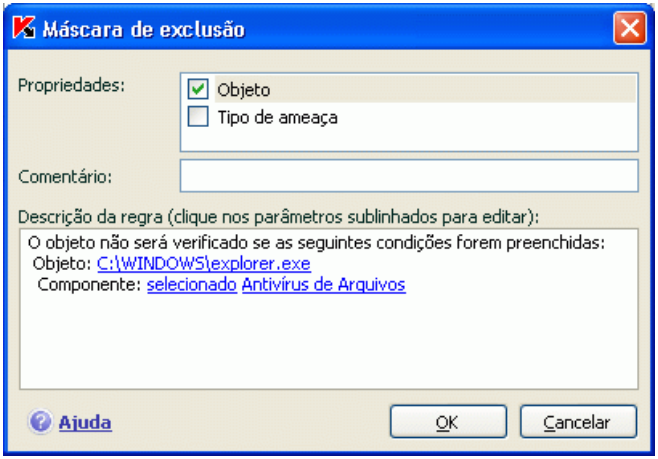


Figura 12. Criando uma regra de exclusão

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, uma pasta específica ou uma máscara de arquivos (consulte a seção A.2 na p. 235). 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 (consulte a seção A.3 na p. 235) para o **Tipo de ameaça**.

Para alguns tipos de ameaça, 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 uma notificação da Defesa Proativa.

Você pode adicionar configurações avançadas às seguintes ameaças, entre outras:

- Invasor (se insere nos processos do programa). Para essa ameaça, 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.
- Iniciando navegador da Internet. Para essa ameaça, 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 Microsoft Office Outlook como **Objeto** e *Iniciando navegador da Internet* como **Tipo de ameaça**, e insira uma máscara de domínios permitidos 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.

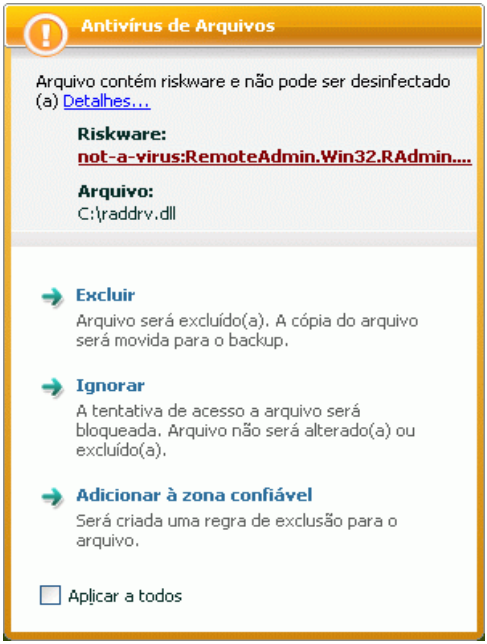


Figura 13. Notificação de detecção de objeto perigoso

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 Figura 13).
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 Figura 14).
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**.

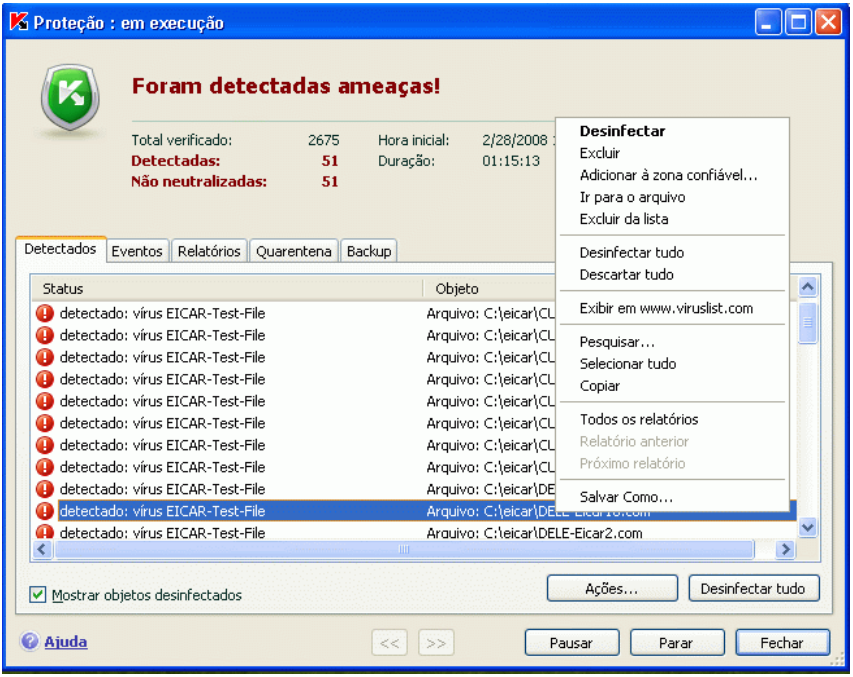


Figura 14. Criando uma regra de exclusão em um relatório

6.9.2. Aplicativos confiáveis

O Kaspersky Anti-Virus pode criar uma lista de aplicativos confiáveis, cuja atividade, suspeita ou não, arquivos, rede e acesso ao Registro do sistema, não são monitorados.

Por exemplo, você acha que os objetos e processos usados pelo **Bloco de Notas** do Microsoft 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 a seção 6.9.1 na p. 70).

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 específica **Aplicativos confiáveis** (veja a Figura 15). A lista padrão criada na instalação contém aplicativos confiáveis cuja atividade não é verificada, conforme recomendações da Kaspersky Lab. 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.

Para adicionar um programa à lista de aplicativos confiáveis:

1. Clique no botão **Adicionar** à direita da guia **Aplicativos confiáveis**.
2. Na janela **Aplicativos Confiáveis** (veja a Figura 16) 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.

   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.

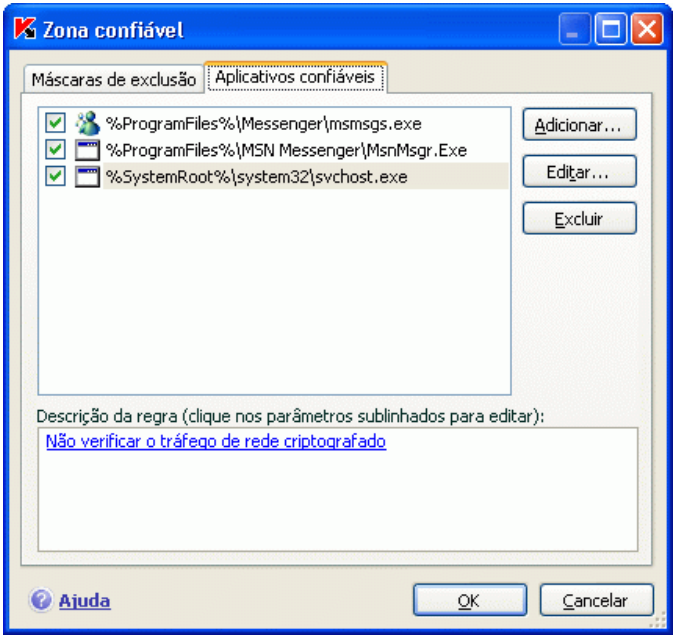


Figura 15. Lista de aplicativos confiáveis

Figura 16. Adicionando um aplicativo à lista de aplicativos confiáveis

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 de rede** – exclui das verificações de vírus 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.

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 área de notificação da barra de tarefas, 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. O componente intercepta as tentativas de acessar qualquer arquivo feitas por usuários ou programas.
2. O Antivírus de Arquivos verifica as informações do arquivo interceptado nos bancos de dados do iChecker™ e do iSwift™. 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 os bancos de dados do aplicativo, que contêm descrições de todos os programas mal-intencionados e ameaças 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 em um arquivo, o Antivírus de Arquivos o bloqueará e tentará desinfectá-lo. Após a desinfecção bem-sucedida, o arquivo ficará acessível para operação. Se a desinfecção falhar, o aplicativo o excluirá. Quando um arquivo é desinfectado ou excluído, o Antivírus coloca uma cópia do mesmo no *Backup*.
    b. Se o Antivírus detectar em um arquivo algum código desconhecido com aparência de malware, mas não tiver certeza disso, esse arquivo será colocado em um armazenamento específico, na *Quarentena*. Posteriormente,

você poderá tentar desinfectá-lo com bancos de dados atualizados.

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 Figura 17):

- **Proteção máxima** – 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
- **Alta velocidade** – o nível com configurações que permitem usar tranqüilamente aplicativos que exigem recursos significativos do sistema, pois o escopo dos arquivos verificados é menor.

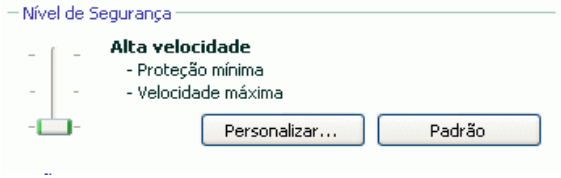


Figura 17. Nível de segurança do Antivírus de Arquivos

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. Isso mudará o nome do nível de segurança para **Personalizado**. Vamos examinar um exemplo em que pode ser necessário modificar o nível de segurança pré-configurado.

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:

1. Abra a janela de configurações do aplicativo e selecione **Antivírus de Arquivos** em **Proteção**.
2. Clique em **Personalizar** em **Nível de Segurança** (veja a Figura 17).
3. Edite os parâmetros de proteção na janela que é aberta e clique em **OK**.

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 a seção 7.2.1 na p. 82) que deverão ser verificados quanto à presença de vírus
- Configurações que definem o escopo da proteção (consulte a seção 7.2.2 na p. 85)
- Configurações que definem como o programa responderá a objetos perigosos (consulte a seção 7.2.6 na p. 92)
- Configurações que definem o uso de métodos heurísticos (consulte a seção 7.2.4 na p. 90)
- Configurações adicionais do Antivírus de Arquivos (consulte a seção 7.2.3 na p. 87)

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 ter se infiltrado.

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. Exemplos incluem os formatos .exe, .dll ou .doc. O risco de infiltração e ativação de código mal-intencionado nesses arquivos é bastante alto.

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 seção A.1 na p. 231) que são verificados com essa opção.

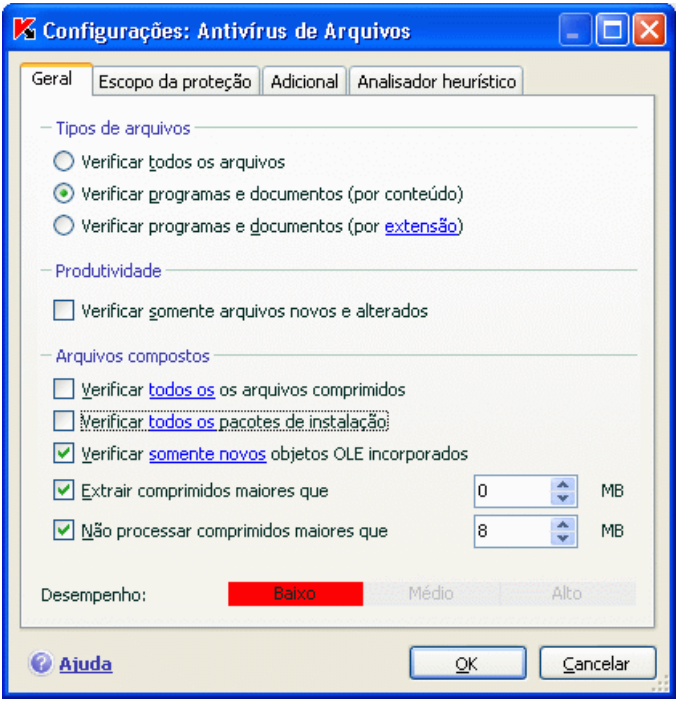


Figura 18. Selecionando os tipos de arquivos verificados quanto à presença de vírus

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 desde a verificação anterior. Esse modo reduz sensivelmente o tempo de verificação e aumenta a velocidade de operação do programa. Para selecionar este modo, marque **Verificar somente arquivos novos e alterados**. 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 Microsoft Office Excel ou macros incorporadas em um arquivo do Microsoft Office 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. Abra a janela de configurações do aplicativo e selecione **Antivírus de Arquivos** em **Proteção**.
2. Clique no botão **Personalizar** na área **Nível de Segurança** (veja a Figura 17).
3. Selecione a guia **Escopo de proteção** na caixa de diálogo que é aberta (veja a Figura 19).

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:

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

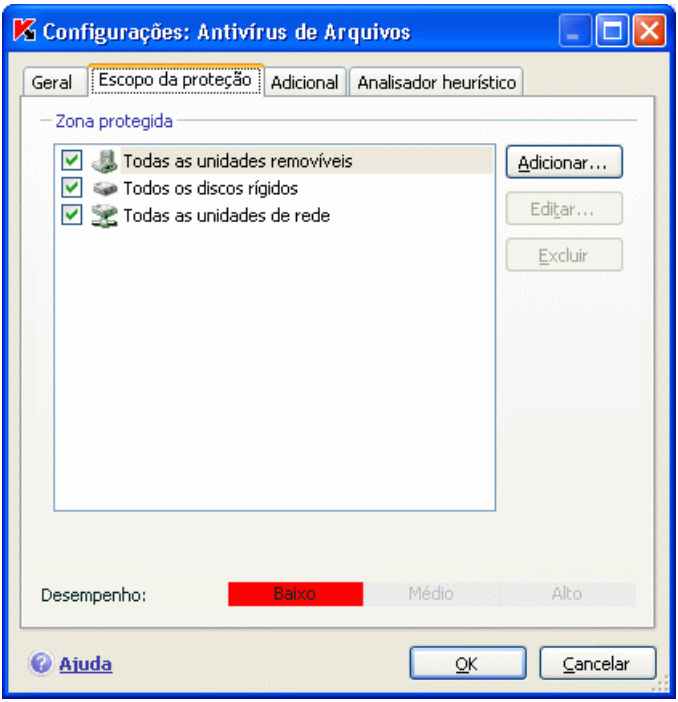


Figura 19. Criando uma zona de proteção

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

- **C:\dir*.*** ou **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. Abra a janela de configurações do aplicativo e selecione **Antivírus de Arquivos** em **Proteção**.
2. Clique no botão **Personalizar** na área **Nível de Segurança** (veja a Figura 17).
3. Selecione a guia **Adicional** na caixa de diálogo que é aberta (veja a Figura 20).

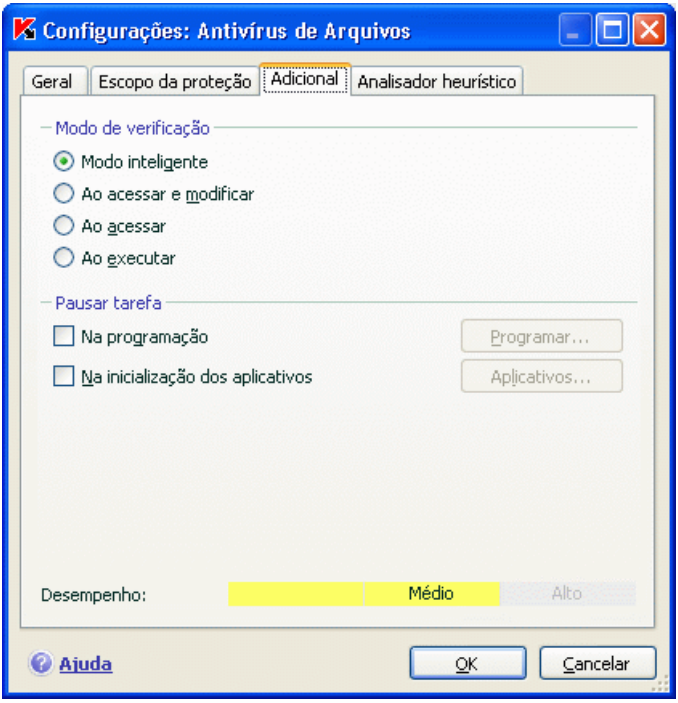


Figura 20. Definindo as configurações adicionais do Antivírus de Arquivos

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 20), 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.

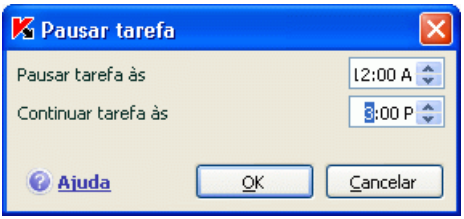


Figura 21. Pausando o componente

Para desabilitar o componente ao trabalhar com programas que exigem muitos recursos, marque **Na inicialização dos aplicativos** e edite a lista de programas na janela que é aberta (veja a Figura 22) clicando em **Lista**.

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.

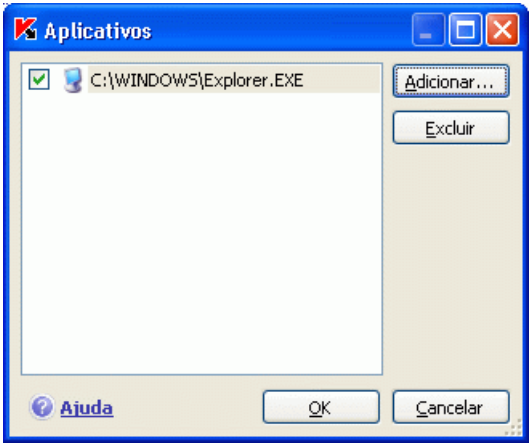


Figura 22. Criando uma lista de aplicativos

7.2.4. Usando a análise heurística

Os métodos heurísticos são utilizados por vários componentes de proteção em tempo real, como o Antivírus de Arquivos, de E-Mail e da Web, além das tarefas de verificação de vírus.

Claro, a verificação usando o método de assinatura com um banco de dados criado anteriormente contendo uma descrição das ameaças conhecidas e os métodos para neutralizá-las oferece uma resposta definitiva sobre se um objeto verificado é mal-intencionado e a que classe de programas perigosos ele pertence. O método heurístico, diferentemente do método de assinatura, é direcionado à detecção de comportamento típico de operações, em vez de assinaturas de códigos mal-intencionados, o que permite ao programa elaborar uma conclusão sobre determinado arquivo com uma certa probabilidade. A vantagem do método heurístico é que seu funcionamento não exige bancos de dados preenchidos anteriormente. Por isso, as novas ameaças são detectadas antes de serem encontradas pelos analistas de vírus.

O analisador heurístico emula a execução de objetos no ambiente virtual seguro do Kaspersky Anti-Virus. Se um objeto não exibir um comportamento suspeito, sua execução no ambiente operacional será permitida. Se for descoberta alguma atividade suspeita na execução do objeto, ele será considerado como mal-intencionado e sua execução não será permitida no host, ou será exibida uma mensagem solicitando instruções do usuário:

- Quarentena - a nova ameaça será verificada e processada posteriormente usando bancos de dados atualizados

- Excluir o objeto
- Ignorar (se tiver certeza de que o objeto não é mal-intencionado).

Para usar o método heurístico, selecione **Usar analisador heurístico**. Você pode selecionar ainda o nível de detalhamento da verificação. Para fazê-lo, mova o controle deslizante para uma destas posições: **Superficial**, **Médio** ou **Detalhado**. A resolução da verificação permite equilibrar a profundidade e, assim, a qualidade da verificação de novas ameaças com relação à carga no sistema operacional e a duração da verificação. Quando mais alto o nível heurístico definido, mais recursos do sistema serão exigidos pela verificação e mais tempo ela levará.

Aviso:

As novas ameaças detectadas usando a análise heurística são analisadas rapidamente pela Kaspersky Lab e os métodos para desinfectá-las são adicionados às atualizações do banco de dados a cada hora.

Portanto, se os bancos de dados do aplicativo forem atualizados periodicamente e os níveis de proteção do computador forem otimizados, não haverá a necessidade de utilizar a análise heurística continuamente.

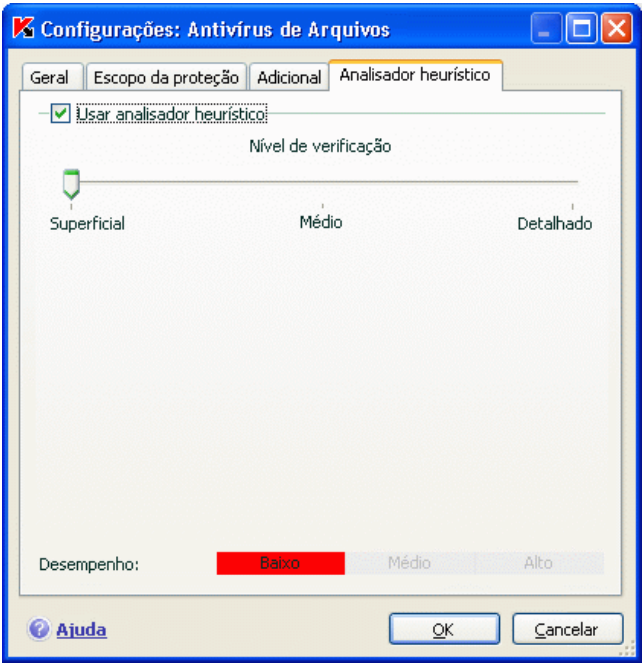


Figura 23. Usando a análise heurística

A guia **Analisador heurístico** (veja a Figura 23) pode ser usada para desabilitar/habilitar a análise heurística de ameaças desconhecidas do Antivírus de Arquivos. Para fazê-lo, execute as seguintes etapas:

1. Abra a janela de configurações do aplicativo e selecione **Antivírus de Arquivos** em **Proteção**.
2. Clique no botão **Personalizar** na área **Nível de Segurança** (veja a Figura 17).
3. Selecione a guia **Analisador heurístico** na caixa de diálogo que é aberta.

7.2.5. 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. Abra a janela de configurações do aplicativo e selecione **Antivírus de Arquivos** em **Proteção**.
2. Clique no botão **Padrão** na área **Nível de Segurança** (veja a Figura 17).

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 **Escopo de proteção** na janela **Restaurar configurações** que é aberta.

7.2.6. 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*) (consulte a 1.3 na p. 12).
- *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:

Abra a janela de configurações do aplicativo e selecione **Antivírus de Arquivos** em **Proteção**. Todas as ações possíveis são exibidas nas seções apropriadas (veja a Figura 24).

Figura 24. 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 a seção 15.3 na p. 178). 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 for bem-sucedida, ele será restaurado para uso normal. Se a desinfecção falhar, será atribuído o status de *possivelmente infectado* ao arquivo e ele será movido para a Quarentena (consulte a seção 15.1 na p. 172). Essas informações são registradas no relatório. Posteriormente, você pode tentar desinfectar esse objeto.

Se a ação selecionada for	Ao detectar um objeto perigoso
Bloquear o acesso **Desinfectar** **Excluir se a desinfecção falhar**	O Antivírus de Arquivos 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 desinfectado, ele será excluído. Uma cópia do objeto será armazenada no Backup (consulte a seção 15.2 na p. 176).
Bloquear o acesso **Excluir**	O Antivírus de Arquivos bloqueará o acesso ao objeto e o excluirá.

Antes de desinfectar ou excluir o objeto, o Kaspersky Anti-Virus cria uma cópia de backup, caso seja necessário restaurá-lo 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** em **Proteção** na janela principal do aplicativo e clique em Abrir relatório.
2. Selecione os objetos que o interessam na guia **Detectados** e clique no botão **Ações** ⟶ **Desinfectar 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 das conexões seguras (SSL) usando POP3 e IMAP.

A atividade do componente é indicada pelo ícone do Kaspersky Anti-Virus na área de notificação da barra de tarefas, 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 os *bancos de dados* fornecidos com o programa e utilizando o algoritmo heurístico. Os bancos de dados 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 foram inseridos nos bancos de dados.
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,

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

informando que o mesmo foi processado pelo Kaspersky Anti-Virus.

- 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 a seção 8.2.2 na p. 101) para o Microsoft Office 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. 102) 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 Microsoft Outlook Express (Windows Mail), Mozilla Thunderbird, Eudora, Incredimail), o Antivírus de E-Mail verifica as mensagens nos protocolos SMTP, POP3, IMAP, MAPI e NNTP.

Os e-mails transmitidos por IMAP não serão verificadas no Thunderbird se você usar filtros que as movam para fora da **Caixa de Entrada**.

8.1. Selecionando um nível de segurança de e-mail

O Kaspersky Anti-Virus protege seus e-mails em um dos seguintes níveis (veja a fig. Figura 25):

Proteção máxima – 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 Lab recomendam este nível. São verificados os mesmos objetos que no nível **Proteção máxima**, com exceção dos anexos ou dos e-mails que levarem mais de três minutos para serem verificados.

Alta velocidade – 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.

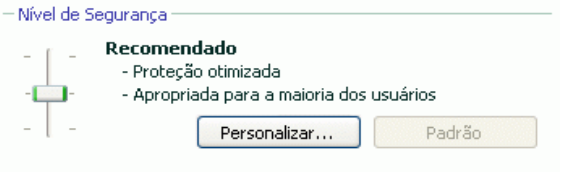


Figura 25. Selecionando um nível de segurança de e-mail

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, suas configurações poderão ser personalizadas. É recomendável selecionar o nível mais próximo de suas necessidades como base e editar seus parâmetros. Isso mudará o nome do nível de segurança para **Personalizado**. Vamos examinar um exemplo em que pode ser necessário modificar o nível de segurança pré-configurado.

Exemplo:

O computador está fora da rede local e usa uma conexão discada com a Internet. Você usa o Microsoft 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 **Proteção máxima**, 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 o nível de segurança atual:

1. Abra a janela de configurações do aplicativo e selecione **Antivírus de E-Mail** em **Proteção**.
2. Clique em **Personalizar** em **Nível de Segurança** (veja a Figura 25).
3. Edite os parâmetros 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 a seção 8.2.1 na p. 98)
- Configurações que definem o uso de métodos heurísticos (consulte a seção 8.2.4 na p. 104)
- Configurações de verificação de e-mail do Microsoft Office Outlook (consulte a seção 8.2.2 na p. 101) e do The Bat! (consulte a seção 8.2.3 na p. 102)
- configurações que definem ações para objetos de e-mail perigosos (consulte a seção 8.2.4 na p. 104)

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. Abra a janela de configurações do aplicativo e selecione **Antivírus de E-Mail** em **Proteção**.
2. Clique no botão **Personalizar** na área **Nível de Segurança** (veja a Figura 25).
3. Na janela que é aberta (veja a Figura 26), selecione **Somente e-mails recebidos** na seção **Escopo**.

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.

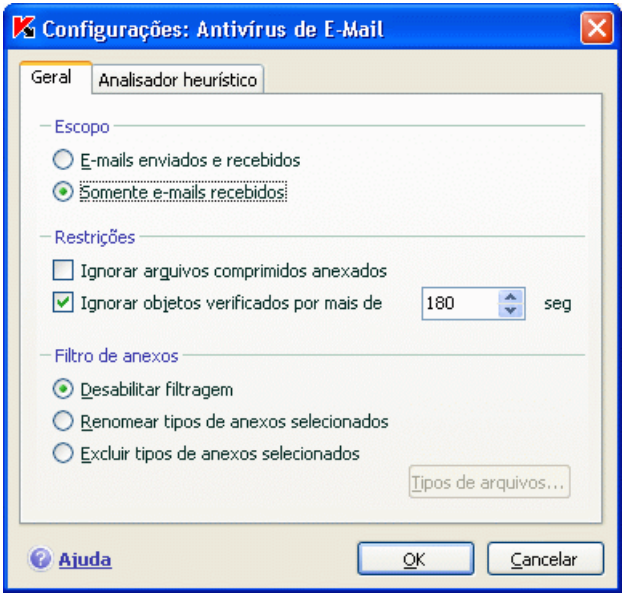


Figura 26. Configurações do Antivírus de E-Mail

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. 231.

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 Microsoft Office Outlook como programa de e-mail, poderá definir configurações personalizadas para as verificações de vírus.

Um plug-in específico é instalado no Microsoft Office 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.

O plug-in é fornecido na forma de uma guia **Antivírus de E-Mail** específica, localizada em **Serviço** → **Opções** (veja a Figura 27).

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 Microsoft Office 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**.

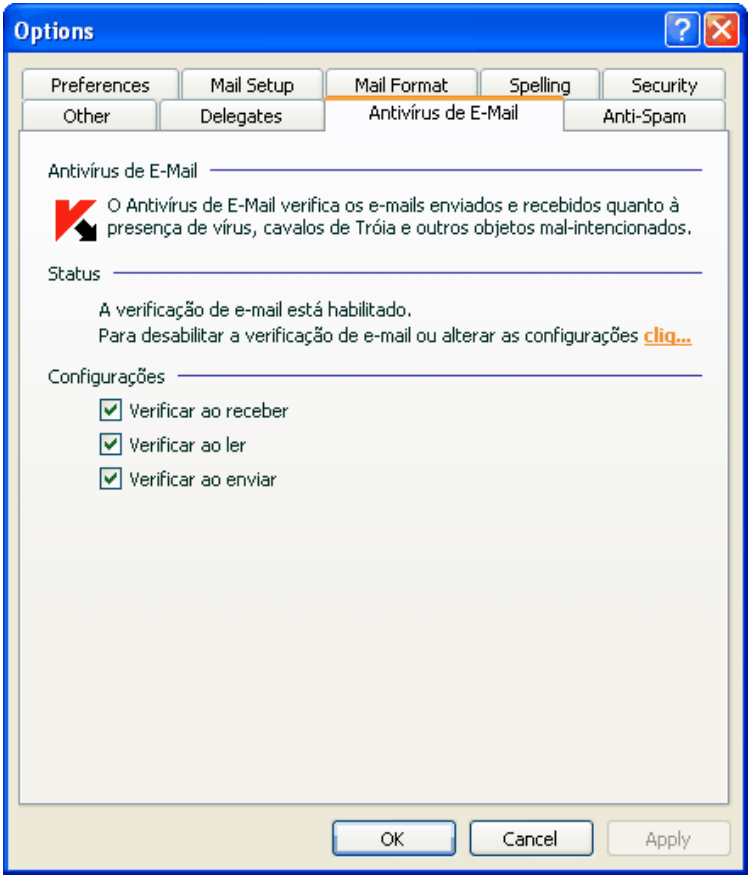


Figura 27. Configurando o Antivírus de E-Mail no Microsoft Office Outlook

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 a seção 8.2.1 na p. 98).

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 Figura 28) estendem-se a todos os módulos antivírus instalados no computador que dá suporte ao The Bat!

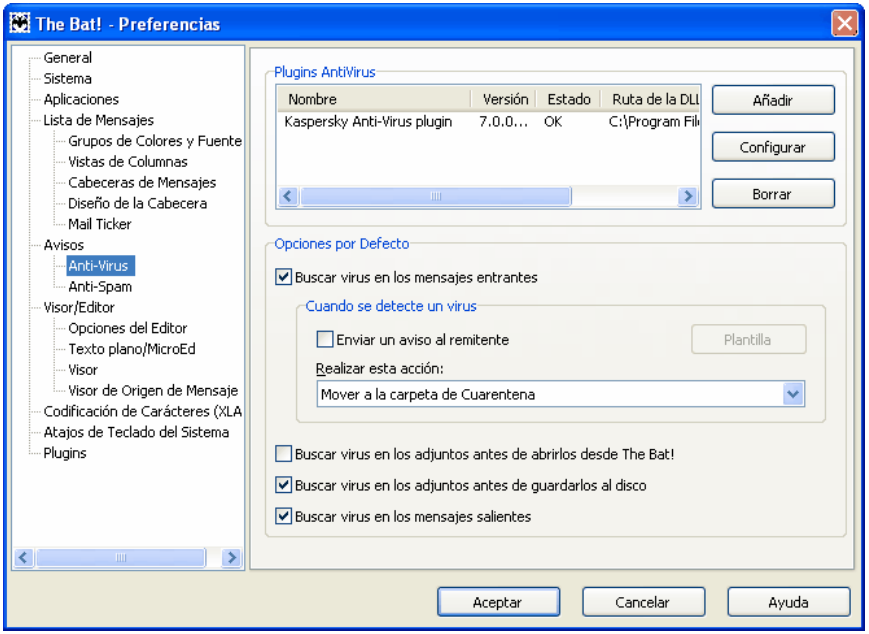


Figura 28. Configurando a verificação de e-mail no The Bat!

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.

Aviso!

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

8.2.4. Usando a análise heurística

Os métodos heurísticos são utilizados por vários componentes de proteção em tempo real e tarefas de verificação de vírus (consulte a seção 7.2.4 na p. 90 para obter mais detalhes).

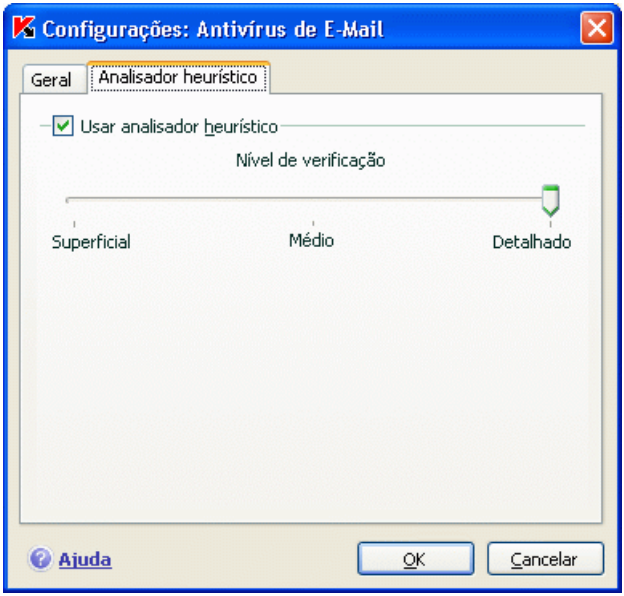


Figura 29. Usando a análise heurística

Os métodos heurísticos de detecção de novas ameaças podem ser habilitados/desabilitados para o componente Antivírus de E-Mail na guia **Analisador heurístico**. Para fazê-lo, execute as seguintes etapas:

1. Abra a janela de configurações do aplicativo e selecione **Antivírus de E-Mail** em **Proteção**.
2. Clique no botão **Personalizar** na área **Nível de Segurança** (veja a Figura 25).
3. Selecione a guia **Analisador heurístico** na caixa de diálogo que é aberta (veja a Figura 29).

Para usar os métodos heurísticos, marque ☑ **Usar analisador heurístico**. Além disso, é possível definir a resolução da verificação, movendo o controle deslizante para uma das seguintes configurações: **Superficial**, **Médio** ou **Detalhado**.

8.2.5. 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. Abra a janela de configurações do aplicativo e selecione **Antivírus de E-Mail** em **Proteção**.
2. Clique no botão **Padrão** em **Nível de Segurança** (veja a Figura 25).

8.2.6. 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 a seção 1.3 na p. 12).
- *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 aplicativo e selecione **Antivírus de E-Mail** em **Proteção**. Todas as ações possíveis para objetos perigosos são relacionadas na caixa **Ação** (veja a Figura 30).

Figura 30. 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 bloqueará o acesso ao objeto. Essas informações são registradas no relatório (consulte a seção 15.3 na p. 178). 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** ☑ **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 o objeto, o Kaspersky Anti-Virus cria uma cópia de backup (consulte a seção 15.2 na p. 176), 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 a seção 15.4 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, é recomendável usar o Antivírus da Web para proteger-se ao usar 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 área de notificação da barra de tarefas, 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 no Microsoft Internet Explorer e também todos os scripts WSH (Java, Visual Basic, etc.) que são carregados enquanto o usuário está no computador.

  Um plug-in específico para o Microsoft Internet Explorer é instalado como parte da instalação do Kaspersky Anti-Virus. O botão  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 os bancos de dados incluídos no Kaspersky Anti-Virus e o algoritmo heurístico. Os bancos de dados 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 foram inseridos nos bancos de dados.
2. Depois da análise, as seguintes medidas a serem tomadas estão disponíveis:
   - Se uma página da Web ou um objeto acessado por um usuário contiver código mal-intencionado, o acesso a ele será bloqueado. Será exibida uma notificação de que o objeto ou página solicitado está infectado.
   - Se um arquivo ou página da Web não contiver código mal-intencionado, ele será disponibilizado imediatamente para o usuário.

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.

Cuidado!

Para que o Antivírus da Web possa interceptar e verificar o tráfego HTTP e os scripts quanto à presença de vírus, ele deve estar em execução antes da conexão com um recurso da Web ser estabelecida. Caso contrário, o tráfego não será verificado.

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 31):

Proteção máxima - 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 todo o conjunto de bancos de dados do aplicativo. Este nível de proteção é recomendado para ambientes agressivos, quando nenhuma outra ferramenta de proteção de HTTP estiver sendo usada.

Recomendado - as configurações deste nível são as recomendadas pelos especialistas da Kaspersky Lab. Neste nível, são verificados os mesmos objetos de **Proteção máxima**, mas o tempo de cache para fragmentos do arquivo é limitado, o que acelera a verificação e retorna os objetos ao usuário mais rapidamente.

Alta velocidade – 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 bancos de dados do aplicativo. É recomendável selecionar este nível de proteção se você tiver outro software de proteção da Web instalado no computador.

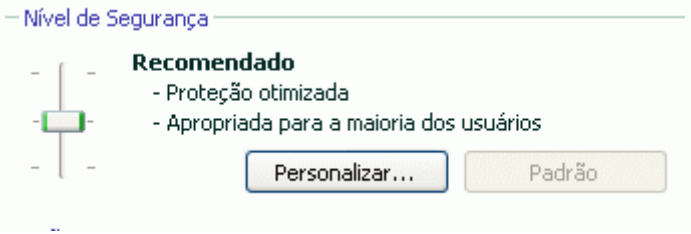


Figura 31. Selecionando um nível de segurança da Web

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 nenhum dos níveis pré-instalados atender às suas necessidades, suas configurações poderão ser personalizadas. É recomendável selecionar o nível mais próximo de suas necessidades como base e editar seus parâmetros. Isso mudará o nome do nível de segurança para **Personalizado**. Vamos examinar um exemplo em que pode ser necessário modificar o nível de segurança pré-configurado.

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 **Proteção máxima** 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:

1. Abra a janela de configurações do aplicativo e selecione **Antivírus da Web** em **Proteção**.
2. Clique em **Personalizar** em **Nível de Segurança** (veja a Figura 31).
3. Edite os parâmetros de proteção da navegação na janela que é aberta e clique em **OK**.

9.2. Configurando o Antivírus da Web

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

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

- Definir as configurações gerais de verificação (consulte a seção 9.2.1 na p. 113)
- Criar uma lista de endereços da Web confiáveis (consulte a seção 9.2.2 na p. 115)
- Habilitar / desabilitar a análise heurística (consulte a seção 9.2.3 na p. 116)

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. Configurações gerais de verificação

Para aumentar sua taxa de sucesso na detecção de código mal-intencionado, o Antivírus da Web armazena em cache fragmentos de objetos baixados da Internet. Com esse método, o Antivírus da Web verifica um objeto somente depois de seu download completo. Em seguida, o objeto é analisado quanto à presença de vírus e, de acordo com os resultados, o programa bloqueia o objeto ou o retorna para o usuário.

Entretanto, o uso do cache aumenta o tempo de processamento do objeto e o tempo até que o programa retorne os objetos ao usuário, podendo causar também problemas ao copiar e processar objetos grandes devido ao tempo limite da conexão com o cliente HTTP.

Sugerimos limitar o tempo de armazenamento em cache dos fragmentos de objetos baixados da Internet para resolver este problema. Quando esse 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.

Por padrão, o tempo de armazenamento de fragmentos de arquivos em cache é limitado a um segundo. Aumentar esse valor ou desmarcar o limite do tempo de armazenamento em cache levará a verificações antivírus mais eficientes, mas a entrega do objeto será mais lenta.

Para limitar o tempo de armazenamento em cache dos fragmentos de arquivos ou para remover o limite:

1. Abra a janela de configurações do aplicativo e selecione **Antivírus da Web** em **Proteção**.
2. Clique no botão **Personalizar** na área **Nível de Segurança** (veja a Figura 31).
3. Na janela que é aberta (veja a Figura 32), selecione a opção desejada na seção **Configurações de verificação**.

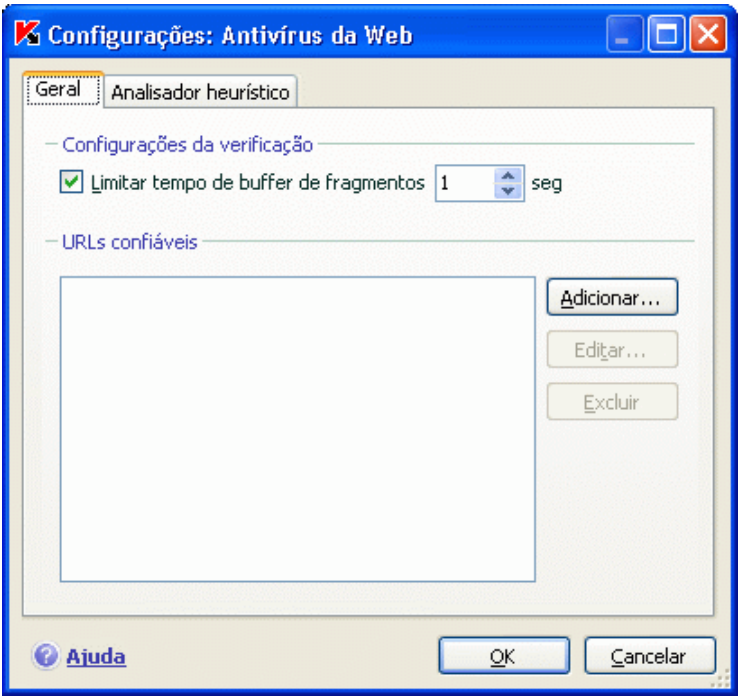


Figura 32. Selecionando o nível de segurança da Web

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. Esta opção pode ser usada quando o Antivírus da Web bloquear repetidamente o download de um determinado arquivo.

Para criar uma lista de endereços confiáveis:

1. Abra a janela de configurações do aplicativo e selecione **Antivírus da Web** em **Proteção**.
2. Clique no botão **Personalizar** em **Nível de Segurança** (veja a Figura 31).
3. Na janela que é aberta (veja a Figura 32), 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 um **?** fizer parte de uma URL real adicionada à lista, ao digitá-la, use uma barra invertida para substituir o ***** ou o **?** 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. Usando a análise heurística

Os métodos heurísticos são utilizados por vários componentes de proteção em tempo real e tarefas de verificação de vírus (consulte a seção 7.2.4 na p. 90 para obter mais detalhes).

Os métodos heurísticos de detecção de novas ameaças podem ser habilitados/desabilitados para o componente Antivírus da Web na guia **Analisador heurístico**. Para fazê-lo, execute as seguintes etapas:

1. Abra a janela de configurações do aplicativo e selecione **Antivírus da Web** em **Proteção**.
2. Clique no botão **Personalizar** na área **Nível de Segurança**.
3. Selecione a guia **Analisador heurístico** na caixa de diálogo que é aberta (veja a Figura 33).

Para usar os métodos heurísticos, marque **Usar analisador heurístico**. Além disso, é possível definir a resolução da verificação, movendo o controle deslizante para uma das seguintes configurações: **Superficial**, **Médio** ou **Detalhado**.

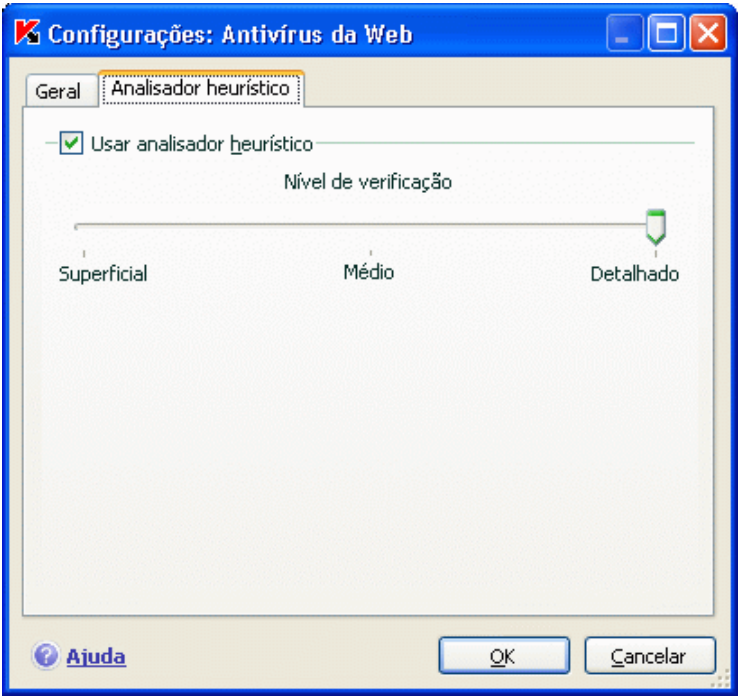


Figura 33. Usando a análise heurística

9.2.4. 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. Abra a janela de configurações do aplicativo e selecione **Antivírus da Web** em **Proteção**.
2. Clique no botão **Padrão** em **Nível de Segurança** (veja a Figura 31).

9.2.5. 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 aplicativo e selecione **Antivírus da Web** em **Proteção**. As possíveis respostas para objetos perigosos estão relacionadas na seção **Ação** (veja a Figura 34).

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.

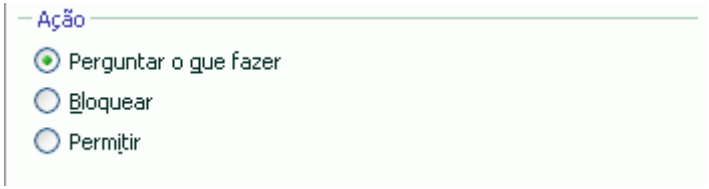


Figura 34. Selecionando ações para scripts perigosos

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 a seção 15.3 na p. 178).
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 um script perigoso, além de desabilitar o módulo de verificação do script.

CAPÍTULO 10. DEFESA PROATIVA

Aviso!

O componente **Controle de integridade do aplicativo** não está disponível nessa versão do aplicativo para computadores que executam o Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista ou Microsoft Windows Vista x64.

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

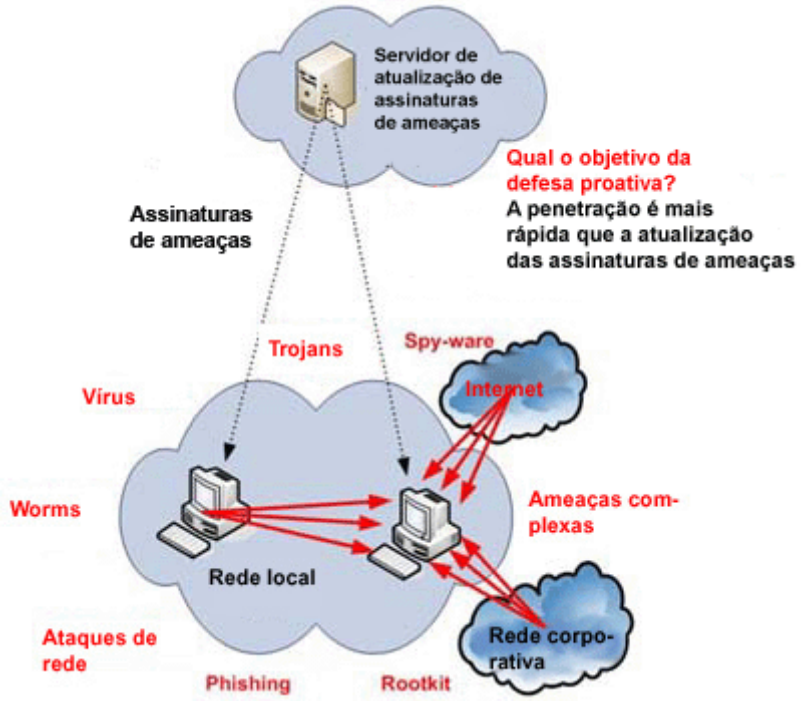
A Defesa Proativa se tornou mais necessária na medida em que os programas começaram a se disseminar mais rápido do que é possível lançar atualizações de antivírus para neutralizá-los. A técnica reativa, na qual se baseia a proteção antivírus, exige que uma nova ameaça infecte pelo menos um computador e precisa de tempo para analisar o código mal-intencionado e adicioná-lo aos bancos de dados do aplicativo, além de 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 do aplicativo, as tecnologias preventivas reconhecem uma nova ameaça no seu computador por meio de uma 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 conjunto total de ações 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 usando o conjunto de regras junto com uma lista de aplicativos excluídos.

A Defesa Proativa usa um conjunto de regras fornecidas com o programa, além de regras criadas pelo usuário ao usá-lo. Uma *regra* é um conjunto de critérios que determina um conjunto de atividades suspeitas e como o Kaspersky Anti-Virus deve reagir a elas.

São fornecidas regras individuais para a atividade de aplicativos e para monitorar alterações ao Registro do sistema e os programas executados no computador. Você mesmo pode editar 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 Kaspersky Anti-Virus, sendo atualizado com os bancos de dados do aplicativo).

   - *Integridade dos módulos dos programas* instalados no computador, o que ajuda a evitar que módulos de aplicativos sejam substituídos por códigos mal-intencionados incorporados neles.

   - *Cada tentativa de editar o Registro do sistema* (excluindo ou adicionando chaves do Registro do sistema, inserindo valores estranhos 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.

     Se o usuário não executar nenhuma ação quando for exibida uma notificação da Defesa Proativa, depois de algum tempo o programa aplicará a ação padrão recomendada para essa ameaça. A ação recomendada pode ser diferente para os vários tipos de ameaças.

As categorias de configurações (veja a Figura 35) 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**. Por padrão, o analisador está habilitado, fornecendo uma análise rigorosa das ações

executadas por todos os programas executados no host. Você pode configurar a ordem de processamento dos aplicativos (consulte 10.1 na p. 124) 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 ☑ **Habilitar Controle de Integridade do Aplicativo**. A integridade é controlada pelo monitoramento da soma de verificação dos módulos do aplicativo e do próprio aplicativo. Você pode criar regras (consulte a seção 10.2 na p. 128) para monitorar a integridade dos módulos de qualquer aplicativo. Para fazê-lo, adicione o aplicativo à lista de aplicativos monitorados.

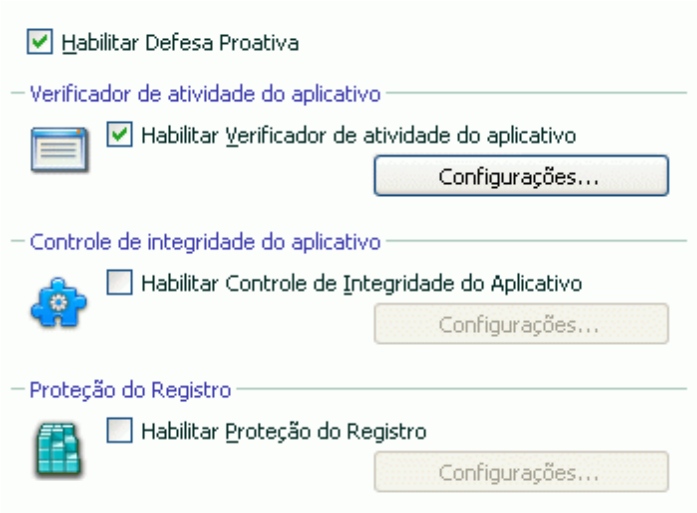


Figura 35. Configurações da Defesa Proativa

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 Microsoft Windows.

Você pode criar suas próprias regras (consulte a seção 10.3.2 na p. 135) para o monitoramento do Registro, dependendo da chave.

É possível configurar exclusões (consulte a seção 6.9.1 na p. 70) para os módulos da Defesa Proativa e criar uma lista de aplicativos confiáveis (consulte a seção 6.9.2 na p. 75).

As seções a seguir examinam estes aspectos mais detalhadamente.

10.1. Regras de monitoramento de atividade

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:

- *Comportamento perigoso*. 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.
- *Iniciando navegador da Internet com parâmetros*. 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 (invasores)* - 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.
- *Detecção de rootkits*. 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.
- *Ganchos de janelas*. 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 configurações do usuário e do sistema que controlam a operação do Microsoft 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 sistema operacional Microsoft Windows e detecta 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.
- *Detecção de uso de teclas*. Esta atividade é usada em tentativas de ler senhas e outras informações confidenciais que você inseriu usando o teclado por programas mal-intencionados.

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 a seção 6.9 na p. 69) relacionando os aplicativos com atividades que você não considera perigosas.

Para configurar o monitoramento de atividades,

1. Abra a janela de configurações do aplicativo e selecione **Defesa Proativa** em **Proteção**.
2. Clique no botão **Configurações** na seção **Verificador de atividade do aplicativo** (veja a Figura 35).

Os tipos de atividade monitorados pela Defesa Proativa estão listados na janela **Configurações: Verificador de atividade do aplicativo** (veja a Figura 36).

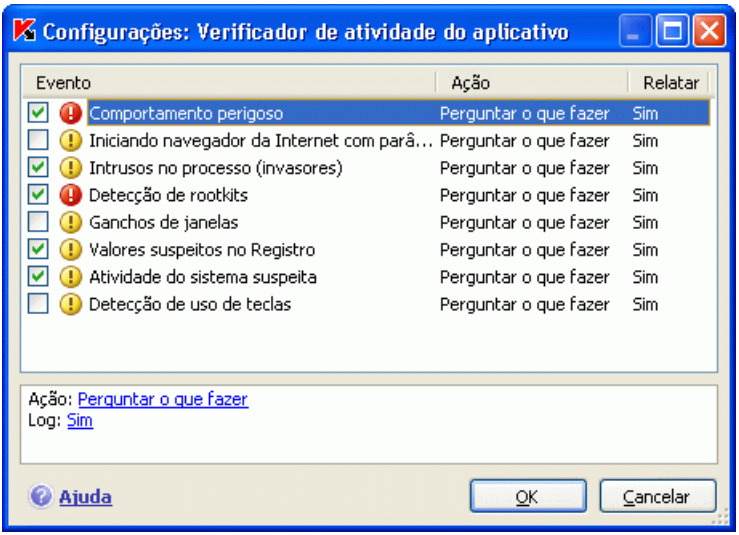


Figura 36. Configurando o controle da atividade de aplicativos

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. A Defesa Proativa não analisará mais esse tipo de atividade.

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 relacionados acima, apenas um tipo de evento do sistema será controlado, o *comportamento perigoso*. O Kaspersky Anti-Virus analisa a atividade dos aplicativos instalados no computador e, com base na lista de regras criadas pelos especialistas da Kaspersky Lab, detecta ações perigosas ou suspeitas.

Se desejar que o Kaspersky Anti-Virus monitore a atividade dos processos do sistema, além dos processos do usuário, marque a caixa de seleção ☑ **Examinar contas de usuário do sistema** (veja a Figura 37). Por padrão, esta opção está desabilitada.

O controle de contas do usuário acessa o sistema e identifica o usuário e seu ambiente de trabalho, o que evita que outros usuários danifiquem o sistema operacional ou os dados. Os processos do sistema são aqueles iniciados por contas do usuário do sistema.

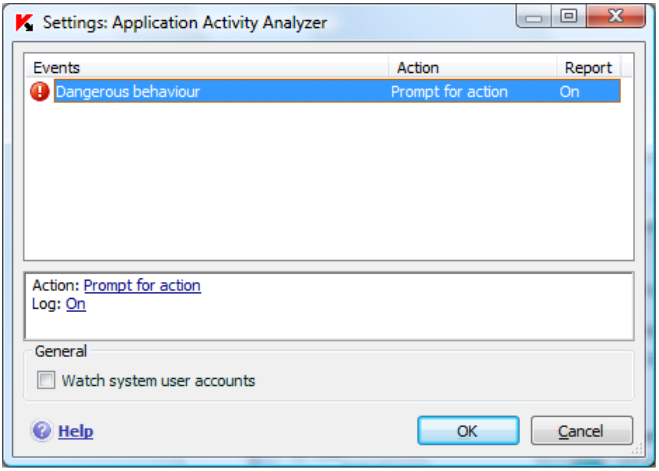


Figura 37. Configurando o controle de atividade de aplicativos no Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista e Microsoft Windows Vista x64

10.2. 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 para se distribuírem, como navegadores, clientes de e-mail, etc. Normalmente, são processos e aplicativos do sistema usados para acessar a Internet, trabalhar com e-mail e outros documentos. Por isso, esses aplicativos são considerados *críticos* no controle de atividades.

A Defesa Proativa monitora os aplicativos críticos e analisa sua atividade, a integridade de seus módulos e observa outros processos iniciados por eles. Uma lista de aplicativos críticos é fornecida com o Kaspersky Anti-Virus, cada qual com sua própria regra de monitoramento para o controle de sua atividade. 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 a atividade de aplicativos que incluem esses módulos seja mal-intencionada, então não é necessário monitorá-los com tanto cuidado. Os especialistas da Kaspersky Lab criaram uma lista desses módulos para diminuir 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 aplicativo e selecione **Defesa Proativa** em **Proteção**.
2. Clique no botão **Configurações** na caixa **Controle de integridade do aplicativo** (veja a Figura 35).

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

10.2.1. 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 deles é criada ao instalar o aplicativo, sendo mostrada na guia **Aplicativos controlados** (veja a Figura 38): cada aplicativo possui sua própria regra de monitoramento. Uma regra de monitoramento é criada para cada um desses aplicativos, para regular 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 controlados**. 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 à parte superior 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.

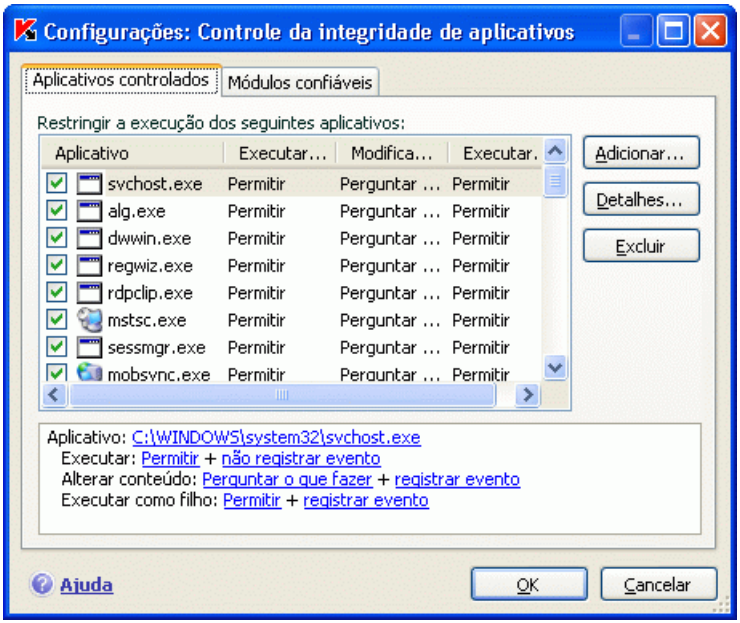


Figura 38. Configurando o Controle de integridade do aplicativo

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 para o aplicativo selecionado. A janela **Configurações: Módulos do aplicativo** contém uma lista dos módulos usados quando um aplicativo monitorado é iniciado. É possível 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.

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 mesmo. 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.

10.2.2. Criando uma lista de componentes comuns

O Kaspersky Anti-Virus fornece uma lista de componentes comuns que podem ser incorporados em todos os aplicativos controlados. Você encontrará essa lista na guia **Módulos confiáveis** (veja a Figura 39). 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 carregar 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.

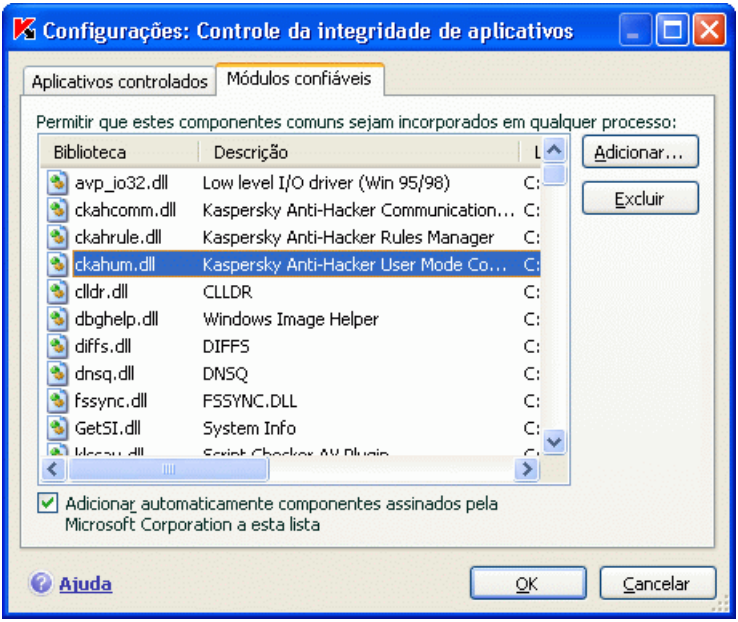


Figura 39. Configurando a lista de módulos confiáveis

10.3. Proteção do Registro

Um dos objetivos de vários programas mal-intencionados é editar o Registro do sistema do Microsoft Windows no computador. Podem ser piadas inofensivas ou malwares mais perigosos 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.

O módulo específico da Defesa Proativa rastreia as modificações dos objetos do Registro do sistema. Esse módulo pode ser ativado ou desativado marcando a caixa **Habilitar Proteção do Registro**.

Para configurar o monitoramento do Registro do sistema:

1. Abra a janela de configurações do aplicativo e selecione **Defesa Proativa** em **Proteção**.
2. Clique no botão **Configurações** na seção **Proteção do Registro** (veja a Figura 35).

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 Figura 40) 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 40. 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 arquivos para monitorar as chaves do Registro do sistema no campo **Nome do grupo**.
2. Selecione a guia **Chaves** e crie uma lista de arquivos do Registro que serão incluídos no grupo monitorado (consulte a seção 10.3.1 na p. 134) 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 a seção 10.3.2 na p. 135) que se aplicará às chaves selecionadas na guia Chaves. Você pode criar várias regras e definir a ordem na qual elas são aplicadas.

10.3.1. 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** fornece uma lista de arquivos para a regra.

Para adicionar um arquivo do Registro do sistema:

1. Clique no botão **Adicionar** na janela **Editar grupo** (veja a Figura 41).
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 objeto ou uma máscara para o grupo de objetos 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.

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.

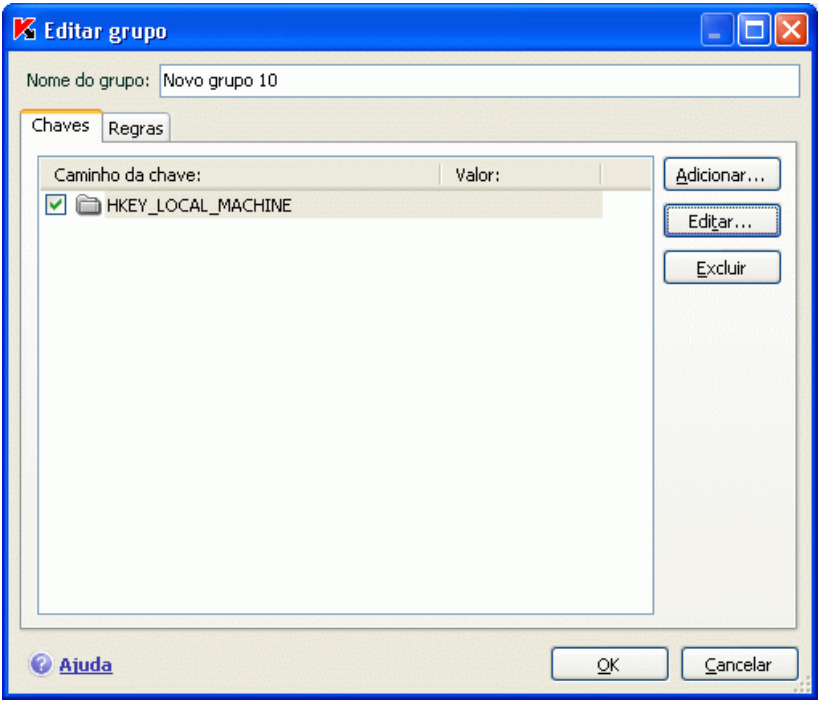


Figura 41. Adicionando chaves do Registro controladas

10.3.2. 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 Figura 42).
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.

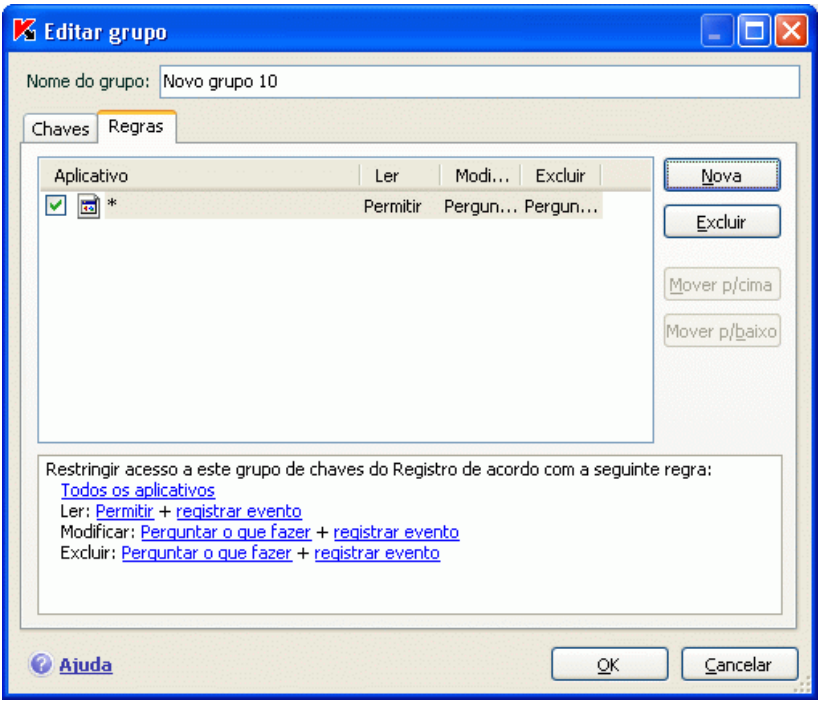


Figura 42. Criando uma regra de monitoramento de chaves do Registro

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 objeto do Registro do sistema na janela de notificação que informa que o programa está tentando executar uma operação com o objeto. Para fazê-lo, clique em Criar regra de permissão na notificação e especifique o objeto do Registro do sistema ao qual regra será aplicada na janela que é aberta.

CAPÍTULO 11. VERIFICANDO VÍRUS NOS COMPUTADORES

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 removíveis, 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 as seguintes 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.

Verificação de rootkits

Verifica no computador rootkits que ocultam programas mal-intencionados no sistema operacional. Esses utilitários injetados no sistema ocultam sua presença e a presença de processos, pastas e chaves do Registro dos programas mal-intencionados descritos na configuração do rootkit.

As configurações padrão dessas tarefas são as recomendadas. É possível editar essas configurações (consulte 11.4 na p. 142) ou criar uma programação (consulte 6.6 na p. 65) para a execução das tarefas.

Você também pode criar suas próprias tarefas (consulte a seção 11.3 na p. 141) e criar uma programação para elas. Por exemplo, é possível programar uma tarefa de verificação semanal das caixas de correio 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, o disco rígido onde estão os programas e jogos, os bancos de dados de e-mails que você trouxe do trabalho para casa, um arquivo anexado a um e-mail, etc.) 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 Microsoft 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.

É possível criar um disco de recuperação (consulte a seção 15.4 na p. 186) para ajudar a recuperar o sistema após um ataque de vírus que cause danos aos arquivos do sistema operacional ou falhas de inicialização. Para fazê-lo, clique em Criar disco de recuperação.

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 6.7 na p. 66).

Para iniciar uma tarefa de verificação de vírus manualmente:

Selecione a tarefa em **Verificação** na janela principal do aplicativo e clique em Iniciar verificação.

As tarefas em execução no momento são exibidas no menu de contexto clicando com o botão direito do mouse no ícone do aplicativo na área de notificação da barra de tarefas.

Para pausar uma tarefa de verificação de vírus:

Selecione **Verificação** na janela principal do aplicativo e clique em Pausar. A verificação será pausada até ser iniciada manualmente ou ela iniciará automaticamente de acordo com a programação. Para iniciar a tarefa manualmente, clique em Continuar.

Para interromper uma tarefa:

Selecione em **Verificação** na janela principal do aplicativo e clique em Interromper. 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 (veja a Figura 43).

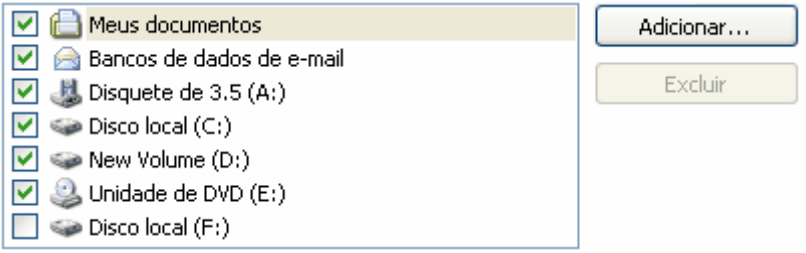


Figura 43. Lista de objetos a serem verificados

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 caixas de correio, RAM, objetos de inicialização, backup do sistema operacional e arquivos da pasta 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, selecione um objeto na lista de objetos a serem verificados, abra o menu de contexto e use a opção **Incluir subpastas**.

Para excluir um objeto, selecione-o na lista e (o nome do objeto será realçado em cinza) clique em **Excluir**. As verificações de determinados objetos podem ser temporariamente desabilitadas para algumas tarefas sem que os próprios objetos sejam excluídos da lista. Basta desmarcar o objeto a ser ignorado.

Para iniciar uma verificação, clique em Iniciar verificação.

Além disso, você pode selecionar um objeto para ser verificado usando as ferramentas padrão do sistema operacional Microsoft Windows (por exemplo, na

janela do programa **Explorer** ou na Área de Trabalho, etc.) (veja a Figura 44). Para fazê-lo, selecione o objeto, abra o menu de contexto do Microsoft Windows clicando com o botão direito do mouse e selecione **Verificar vírus**.

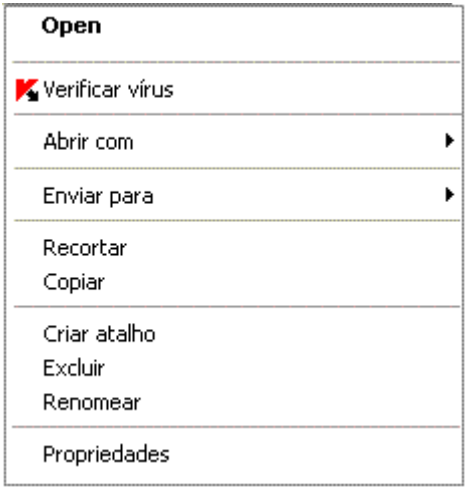


Figura 44. Verificando objetos do menu de contexto do Microsoft Windows

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 cujas configurações sejam mais próximas de suas necessidades em **Verificação** na janela principal do aplicativo.
2. Abra o menu de contexto e selecione **Salvar como** ou clique em Nova tarefa de verificação.
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 11.2 na página 139), da configuração de propriedades que controlarão a tarefa (consulte 11.4 na página 142) e, se necessário, da configuração de uma programação (consulte 6.6 na página 65) para executar a tarefa automaticamente.

Para renomear uma tarefa existente:

selecione a tarefa em **Verificação** na janela principal do aplicativo e clique em Renomear.

Insira o novo nome para a tarefa na janela que é aberta e clique em **OK**. O nome da tarefa também será mudado na seção **Verificação**.

Para excluir uma tarefa existente:

selecione a tarefa em **Verificação** na janela principal do aplicativo e clique em 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:

abra a janela de configurações do aplicativo, selecione o nome da tarefa em **Verificação** e use o link Configurações.

Você pode usar a janela de configurações de cada tarefa para:

- Selecionar o nível de segurança que será usado pela tarefa (consulte a seção 11.4.1 na p. 143)

- Editar configurações avançadas:
- definir os tipos de arquivos que devem ser verificados quanto à presença de vírus (consulte a seção 11.4.2 na p. 144)
- configurar o início da tarefa usando um perfil de usuário diferente (consulte 6.6 na p. 65)
- definir as configurações avançadas de verificação (consulte 11.4.3 na p. 148)
- habilitar as verificações de rootkits (consulte a seção 11.4.4 na p. 149) e o analisador heurístico (consulte a seção 11.4.5 na p. 150);
- restaurar as configurações padrão de verificação (consulte a seção 11.4.6 na p. 151)
- selecionar uma ação que o programa aplicará ao detectar um objeto infectado ou possivelmente infectado (consulte a seção 11.4.7 na p. 151)
- criar uma programação (consulte 6.7 na p. 66) para executar tarefas automaticamente.

Além disso, você pode definir configurações globais (consulte a seção 11.4.8 na p. 153) 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 Figura 45):

Proteção máxima - 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 **Proteção máxima**, exceto pelos bancos de dados de e-mails.

Alta velocidade – o nível com configurações que permitem usar tranqüilamente aplicativos que consomem muitos recursos, pois o escopo dos arquivos verificados é menor.

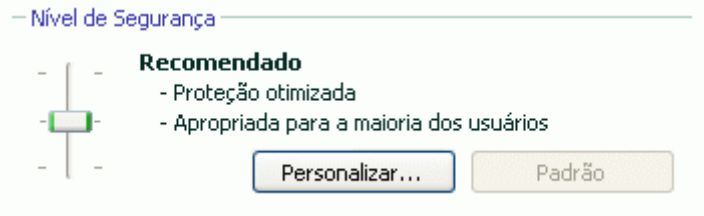


Figura 45. Selecionando um nível de segurança de verificação de vírus

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. É recomendável selecionar o nível mais próximo de suas necessidades como base e editar seus parâmetros. Isso mudará o nome do nível de segurança para **Personalizado**.

Para modificar as configurações de um nível de segurança:

1. Abra a janela de configurações do aplicativo e selecione uma tarefa de verificação em **Verificação**.
2. Clique em **Personalizar** em **Nível de Segurança** (veja a Figura 45).
3. Edite os parâmetros de proteção na janela que é aberta e clique em **OK**.

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 Figura 46). 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. Exemplos incluem os formatos .exe, .dll ou .doc. O risco de infiltração 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 seção A.1 na p. 231).

> **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.

Figura 46. Configurando a verificação

Na seção **Produtividade**, você pode especificar que apenas os arquivos novos e modificados desde a verificação anterior serão verificados. Esse modo reduz sensivelmente 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**.

Parar 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.

Não verificar arquivos comprimidos maiores 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 serão 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. Outras configurações de verificação de vírus

Além de definir as configurações básicas de verificação de vírus, você também pode usar configurações adicionais (veja a Figura 47):

Habilitar tecnologia iChecker – habilita uma 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 dos bancos de dados do aplicativo, a data mais recente em que o objeto foi verificado e as modificações das configurações de verificação.

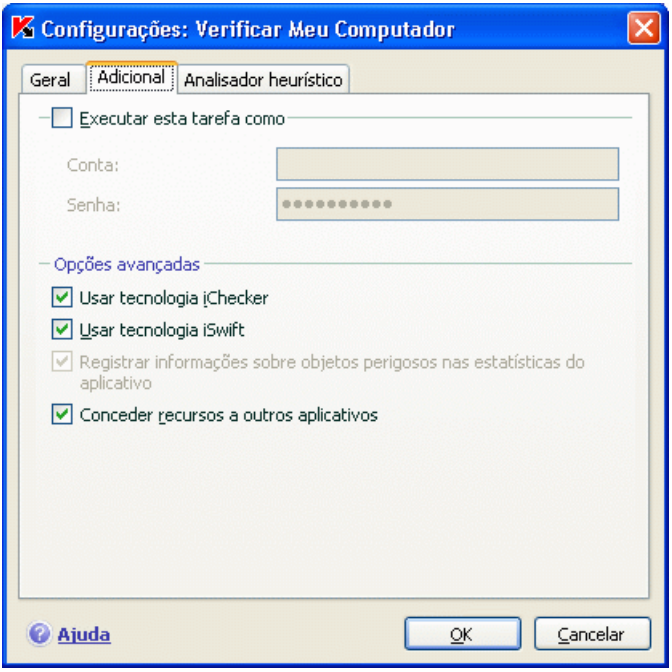


Figura 47. Configurações avançadas de verificação

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 os bancos de dados do aplicativo tiverem sido atualizados.

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*).

- **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.
- **Registrar informações sobre objetos perigosos nas estatísticas do aplicativo** – salva informações sobre objetos perigosos detectados nas estatísticas gerais do aplicativo e exibe uma lista de ameaças na guia Detectados da janela do relatório (consulte a seção 15.3.2 na p. 182). Se esta caixa estiver desmarcada, os dados do objeto perigoso não serão registrados no relatório; assim, será impossível processar esses objetos.
- **Conceder recursos a outros aplicativos** – pausa a tarefa de verificação de vírus se o processador estiver ocupado com outros aplicativos.

11.4.4. Verificando rootkits

O rootkit é um conjunto de utilitários usados para dissimular programas mal-intencionados no sistema operacional. Esses utilitários se inserem no sistema operacional, ocultam sua presença e a presença de processos, pastas e chaves do Registro dos malwares descritos na configuração do rootkit.

As verificação de rootkits pode ser executada por qualquer tarefa de verificação de vírus (desde que esta opção esteja habilitada para a tarefa); contudo, os especialistas da Kaspersky Lab criaram e otimizaram uma outra tarefa de verificação para procurar esse tipo de malware.

Para habilitar a verificação de rootkits, marque **Habilitar detecção de rootkits** em **Verificação de rootkits**. Se a verificação estiver habilitada, um nível de verificação de rootkits rigoroso pode ser solicitado marcando **Habilitar verificação de rootkits estendida**. Se o fizer, a verificação pesquisará cuidadosamente esses programas, analisando um grande número de objetos variados. Por padrão, estas caixas de seleção estão desmarcadas, pois esse modo exige recursos significativos do sistema operacional.

Para configurar verificações de rootkits:

1. Abra a janela de configurações do aplicativo e selecione uma tarefa em **Verificação**.

2. Clique em **Personalizar** em **Nível de Segurança** (veja a Figura 45) e selecione a guia **Analisador heurístico** na janela que é aberta (veja a Figura 48).

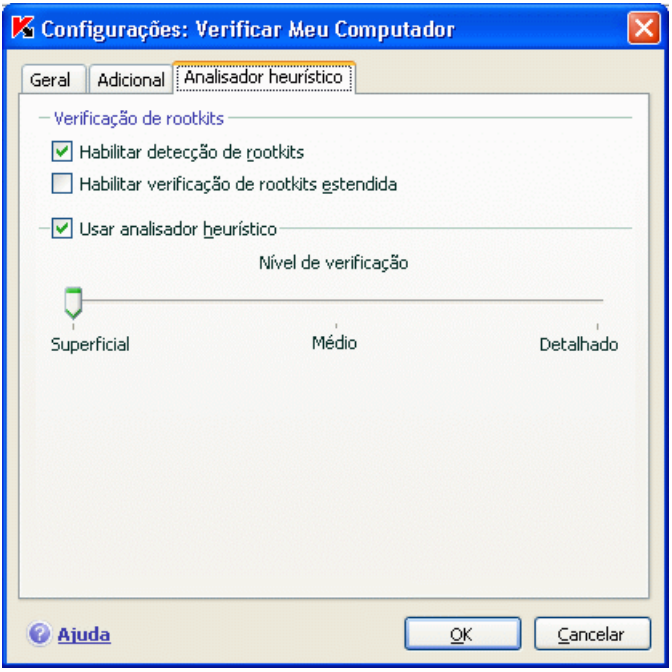


Figura 48. Configurando a verificação de rootkits e os métodos heurísticos

11.4.5. Usando métodos heurísticos

Os métodos heurísticos são utilizados por vários componentes de proteção em tempo real e tarefas de verificação de vírus (consulte a seção 7.2.4 na p. 90 para obter mais detalhes).

A guia **Analisador heurístico** (veja a Figura 48) pode ser usada para desabilitar/habilitar a análise heurística de ameaças desconhecidas na verificação de vírus. Para fazê-lo, execute as seguintes etapas:

1. Abra a janela de configurações do aplicativo e selecione uma tarefa em **Verificação**.

2. Clique em **Personalizar** em **Nível de Segurança** e, na caixa de diálogo que é aberta, abra a guia **Verificação heurística**.

Para usar os métodos heurísticos, marque ☑ **Usar analisador heurístico**. É possível definir um outro nível de profundidade da verificação, movendo o controle deslizante para uma das seguintes configurações: **superficial, médio** ou **detalhado**.

11.4.6. 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 vírus padrão:

1. Abra a janela de configurações do aplicativo e selecione uma tarefa em **Verificação**.
2. Clique no botão **Padrão** em **Nível de Segurança** (veja a Figura 45).

11.4.7. 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:

Abra a janela de configurações do aplicativo e selecione uma tarefa em **Verificação**. Todas as ações possíveis são mostradas na seção pertinente (veja a Figura 49).

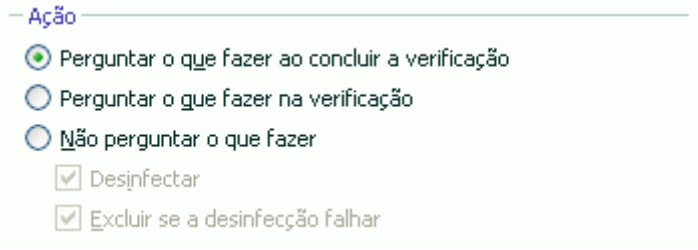


Figura 49. Selecionando ações para objetos perigosos

Se a ação selecionada for	Ao detectar um objeto mal-intencionado 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 a seção 15.1

Se a ação selecionada for	Ao detectar um objeto mal-intencionado ou possivelmente infectado
	na p. 172). Essas informações são registradas no relatório (consulte a seção 15.3 na p. 178). 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 for cria uma cópia do mesmo e a envia para o Backup (consulte 15.2 na p. 176), caso seja necessário restaurá-lo ou surja uma oportunidade de neutralizá-lo posteriormente.

11.4.8. 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. Abra a janela de configurações do programa e selecione a seção **Verificação**.
2. Configure a verificação: Selecione o nível de segurança (consulte 11.4.1 na p. 143), defina as configurações de nível avançado e selecione uma ação (consulte 11.4.7 na p. 151) para os objetos.
3. Para aplicar essas novas configurações a todas as tarefas, clique no botão **Aplicar** na seção **Outras tarefas de verificação**. Confirme as configurações globais selecionadas na caixa de diálogo pop-up.

CAPÍTULO 12. TESTANDO OS RECURSOS DO KASPERSKY ANTI-VIRUS

Depois 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

Prefixo	Status do vírus de teste	Ação correspondente quando o aplicativo processar o objeto
		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 do aplicativo não contêm uma descrição do procedimento para neutralizar esse objeto. O aplicativo o colocará na Quarentena para que seja processado posteriormente com bancos de dados atualizados.
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).
CURE-	O arquivo contém um vírus de teste. Ele pode ser neutralizado. O objeto é passível de desinfecção, 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	Esse objeto contém um vírus que não pode ser desinfectado ou que

Prefixo	Status do vírus de teste	Ação correspondente quando o aplicativo processar o objeto
	desinfectar o objeto.	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. 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** em **Arquivos de dados e relatórios** na janela de configurações do aplicativo (consulte a seção 15.3.1 na p. 181).
2. Crie uma pasta em um disco; copie o vírus de teste baixado do site oficial da organização (consulte a seção 12.1 na p. 154) e as modificações do vírus de teste que você criou para essa pasta.

O Antivírus de Arquivos interceptará sua tentativa de acessar o arquivo, o verificará e informará que um objeto perigoso foi detectado:

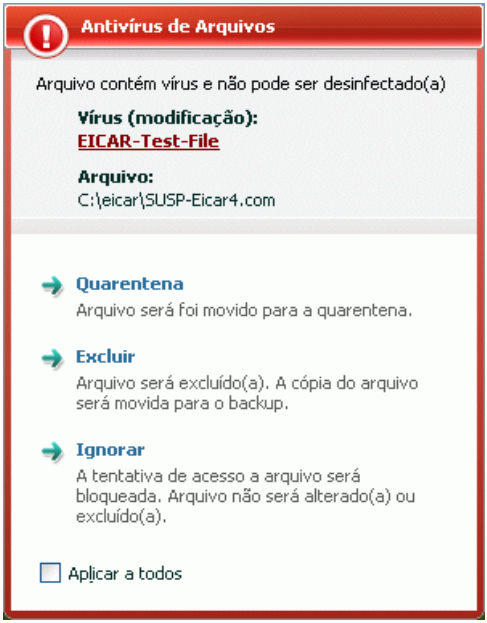


Figura 50. Objeto perigoso detectado

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 a seção 12.1 na p. 154) e as modificações do vírus de teste que você criou para essa pasta.
2. Crie uma nova tarefa de verificação de vírus (consulte a seção 11.3 na p. 140) e selecione a pasta que contém o conjunto de vírus de teste para ser verificada (consulte a seção 12.1 na p. 154).

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** em **Arquivos de dados e relatórios** na janela de configurações do aplicativo (consulte a seção 15.3.1 na p. 181).
4. Execute a tarefa de verificação de vírus (consulte a seção 11.1 na p. 139).

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:

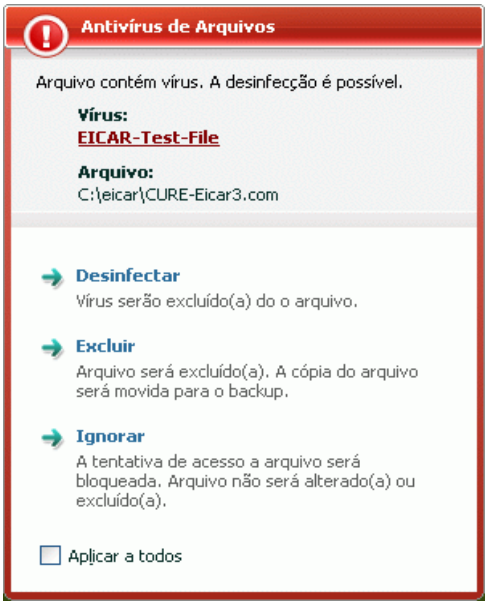


Figura 51. Objeto perigoso detectado

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.

A atualização do aplicativo envolve o download e a instalação dos seguintes componentes no computador:

Bancos de dados de antivírus e drivers de rede

As informações no computador são protegidas usando os bancos de dados do aplicativo. Os componentes de software que oferecem proteção usam o banco de dados de assinaturas de ameaças para pesquisar e desinfectar objetos nocivos no computador. Os bancos de dados são completados 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 rede 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 bancos de dados apropriado. Agora, nossos produtos usam bancos de dados que o protegem de malware e riskware.

Módulos do aplicativo

Além dos bancos de dados do aplicativo, você pode atualizar os módulos do Kaspersky Anti-Virus. Novas atualizações do aplicativo surgem periodicamente.

A principal fonte de atualização do Kaspersky Anti-Virus são os servidores de atualização da Kaspersky Lab. Para baixar as atualizações disponíveis dos servidores de atualização, é necessário que o computador esteja conectado à Internet.

É necessário que o computador esteja conectado à Internet para baixar as atualizações dos servidores de atualização. No caso de a conexão com a Internet utilizar um servidor proxy, será necessário definir as configurações de conexão (consulte a seção 15.7 na p. 194).

Se você não tiver acesso aos servidores de atualização da Kaspersky Lab (por exemplo, se o computador não estiver conectado à Internet), é possível ligar para o escritório central da Kaspersky Lab nos números +7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-00-00 e solicitar informações de contato dos parceiros da Kaspersky Lab que podem fornecer atualizações compactadas em disquetes ou CDs/DVDs.

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 os bancos de dados e os módulos do aplicativo no computador com as versões disponíveis no servidor de atualização. Se o computador possuir a versão mais recente dos bancos de dados e dos módulos do aplicativo, aparecerá uma janela de notificação confirmando que ele está atualizado. Se os bancos de dados e os módulos no computador forem diferentes daqueles no servidor de atualização, somente as partes ausentes das atualizações serão baixadas. A Atualização não baixa os bancos de dados e módulos que você já possui, o que aumenta significativamente a velocidade de download e economiza tráfego da Internet.

Antes de atualizar os bancos de dados, o Kaspersky Anti-Virus cria cópias de backup, que podem ser usadas se for necessário executar uma reversão (consulte 13.2 na página 161). Se, por exemplo, o processo de atualização corromper os bancos de dados e inutilizá-los, você poderá facilmente reverter para a versão anterior e tentar atualizar os bancos de dados mais tarde.

Você pode distribuir as atualizações recuperadas em uma fonte local enquanto atualiza o aplicativo (consulte a seção 13.3.3 na p.166). Esse recurso permite atualizar os bancos de dados e os módulos usados pelos aplicativos 7.0 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 a seção 13.3.1 na p. 162).

Você pode iniciar a Atualização:

- do menu de contexto (consulte a seção 4.2 na p. 43).
- da janela principal do programa (consulte a seção 4.3 na p. 45).

Para iniciar a Atualização no menu de atalho:

1. Clique com o botão direito do mouse no ícone do aplicativo na área de notificação da barra de tarefas para abrir o menu de atalho.
2. Selecione **Atualização**.

Para iniciar a Atualização na janela principal do programa:

1. Abra a janela principal do aplicativo e selecione o componente **Atualização**.
2. Clique no link Atualizar bancos de dados.

As informações sobre a atualização serão exibidas na janela principal. Para obter detalhes sobre o processo de atualização, clique em Detalhes. Um relatório detalhado da tarefa de atualização será exibido. A janela do relatório pode ser fechada. Para fazê-lo, clique em **Fechar**. A atualização continuará.

Observe que as atualizações são distribuídas para a fonte local durante o processo de atualização, desde que esse serviço esteja habilitado (consulte 13.3.3 na p. 166).

13.2. Revertendo para a atualização anterior

Sempre que você iniciar a atualização, o Kaspersky Anti-Virus criará primeiro uma cópia de backup dos bancos de dados e módulos do programa atuais e só então começará o download das atualizações. Dessa forma, você poderá voltar a usar a versão anterior dos bancos de dados, se a atualização falhar.

Para reverter para o banco de dados de ameaças conhecidas anterior:

1. Abra a janela principal do aplicativo e selecione o componente **Atualização**.
2. Clique em Reverter para os bancos de dados anteriores.

13.3. Configurando a atualização

As configurações da Atualização especificam os seguintes parâmetros:

- A fonte para o download e a instalação das atualizações (consulte a seção 13.3.1 na p. 162)
- O modo de execução do procedimento de atualização e os elementos específicos atualizados (consulte a seção 13.3.2 na p. 165)
- A freqüência com que a atualização será executada, se programada (consulte a seção 6.7 na p. 66)
- Com qual usuário a atualização será executada (consulte a seção 6.6 na p. 65)
- Se as atualizações baixadas deverão ser copiadas em um diretório local (consulte a seção 13.3.3 na p. 166)
- As ações que devem ser executadas após a conclusão da atualização (consulte a seção 13.3.3 na p. 166)

As seções a seguir examinam estes aspectos detalhadamente.

13.3.1. Selecionando uma fonte de atualização

A *fonte de atualização* é algum recurso que contém as atualizações dos bancos de dados e dos módulos do aplicativo Kaspersky Anti-Virus. As fontes de atualização podem ser servidores HHTP e FTP, pastas locais ou de rede.

A principal fonte de atualização são os *servidores de atualização da Kaspersky Lab*. Trata-se de sites específicos que contêm as atualizações disponíveis dos bancos de dados e dos módulos 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, nos números +7 (495) 797-87-00, +7 (495) 956-00-00, e solicitar informações de contato dos parceiros da empresa que podem fornecer atualizações compactadas em disquetes ou CDs/DVDs.

Aviso!

Ao solicitar atualizações em mídia removível, especifique se deseja receber também as atualizações dos módulos 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 **Fontes de atualização** (veja a Figura 52).

Por padrão, as atualizações são baixadas 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.

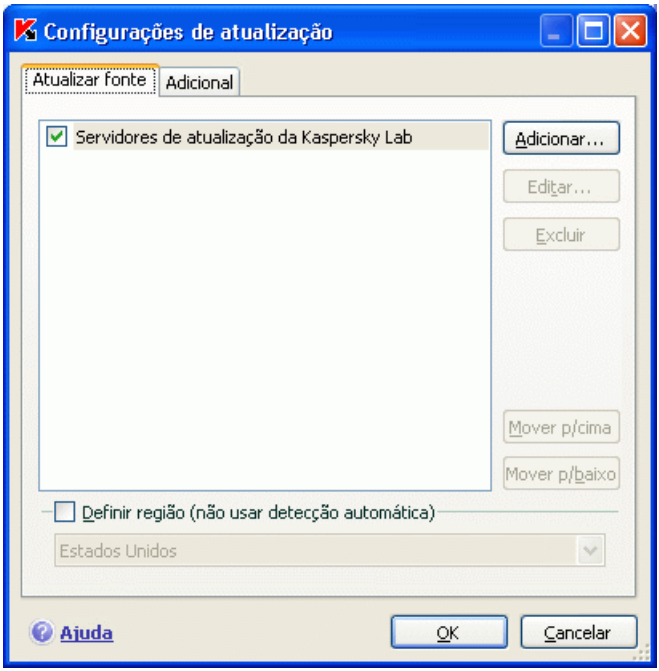


Figura 52. Selecionando uma fonte de atualização

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 característico ou a URL do site no campo **Fonte**. Ao selecionar um site FTP como fonte de atualização, insira as configurações de autenticação na URL do servidor, no formato ftp://usuário:senha@servidor.

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**.**

13.3.2. 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 Figura 53) são os componentes que serão atualizados:

- Bancos de dados do aplicativo
- Drivers de rede que permitem que os componentes de proteção interceptem o tráfego de rede
- Módulos do programa

Os bancos de dados do aplicativo e os drivers de rede são atualizados sempre, enquanto os módulos do aplicativo são atualizados somente se configurado.

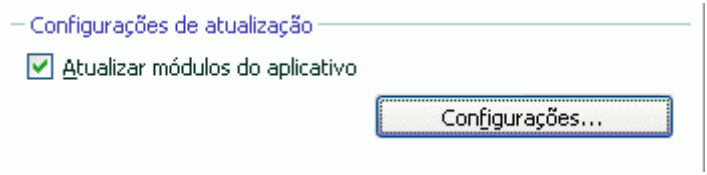


Figura 53. Selecionando objetos de atualização

Se desejar baixar e instalar atualizações dos módulos do programa:

Abra a janela de configurações do aplicativo, selecione **Atualização** e marque **Atualizar módulos do aplicativo**.

Se houver atualizações de módulos do aplicativo na fonte de atualização, o aplicativo baixará as atualizações necessárias e as aplicará quando o computador for reiniciado. As atualizações de módulos baixadas 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 aplicativo anteriores sejam instaladas, somente os bancos de dados do aplicativo serão atualizados.

O método de atualização (veja a Figura 54) define como a Atualização será iniciada. É possível selecionar um dos seguintes modos em **Modo de execução**:

Automaticamente. O Kaspersky Anti-Virus verifica a fonte de atualizações dos pacotes de atualização em intervalos definidos (consulte a 13.3.1 na

p. 162). Ao detectar novas atualizações, o programa as baixa e instala no computador. Este é o modo utilizado por padrão.

Se um recurso de rede for especificado como fonte de atualização, o Kaspersky Anti-Virus tentará executar a atualização depois de algum tempo, conforme especificado no pacote de atualização anterior. Se uma pasta local estiver selecionada como fonte de atualização, o aplicativo tentará baixar as atualizações a partir da pasta local com a freqüência especificada no pacote de atualização baixado na última atualização. Esta opção permite que a Kaspersky Lab regule a freqüência de atualização no caso de surtos de vírus e outras situações possivelmente perigosas. Seu aplicativo receberá as atualizações mais recentes dos bancos de dados e módulos do aplicativo oportunamente, excluindo assim a possibilidade de invasão do computador por software mal-intencionado.

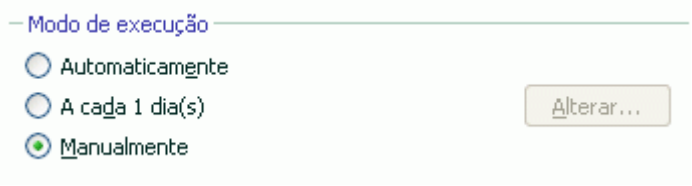


Figura 54. Selecionando um modo de execução da atualização

Na programação. A atualização é programada para iniciar em uma hora especificada. Por padrão, as atualizações programadas ocorrerão diariamente. Para editar a programação padrão, clique no botão **Alterar...** ao lado do título do modo e faça as alterações necessárias na janela que é aberta (para obter mais detalhes, consulte a 6.7 na p. 66).

Manualmente. Com esta opção, você inicia a Atualização manualmente. O Kaspersky Anti-Virus o notifica quando é necessário que seja atualizado:

13.3.3. 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 dos 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 **Atualizar pasta de distribuição** na guia **Adicional** (veja a Figura 55) 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.

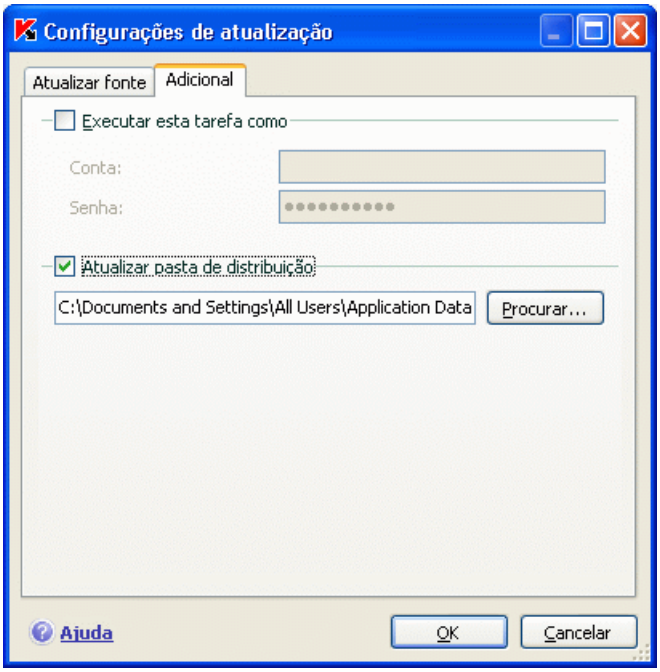


Figura 55. Configurações da ferramenta de cópia de atualizações

Observe que o Kaspersky Anti-Virus 7.0 recupera apenas os pacotes de atualização para aplicativos da versão 7.0 dos servidores de atualização da Kaspersky Lab.

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.

13.3.4. Ações após a atualização do programa

Todas as atualizações dos bancos de dados contêm 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 a seção 15.1 na p. 172). Usando a versão mais recente dos bancos de dados, o Kaspersky Anti-Virus pode identificar a ameaça e eliminá-la.

Por padrão, o aplicativo verifica os objetos em quarentena depois de cada atualização. 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 **Verificar quarentena 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. 138). É recomendável configurar uma programação para essa tarefa de forma que ela seja iniciada automaticamente depois de cada atualização dos bancos de dados (consulte 6.7 na p. 66).

CAPÍTULO 14. GERENCIADO CHAVES

O Kaspersky Anti-Virus precisa de um *arquivo de chave* 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, 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, depois de expirado o período de teste, 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 os bancos de dados do aplicativo. O computador poderá ser verificado usando as tarefas de verificação de vírus e estará protegido pelos componentes de proteção, mas seus bancos de dados estarão atualizados de acordo com a data de expiração da chave. Não podemos garantir que você estará protegido contra os vírus que surgirem depois que a chave do programa expirar.

Para proteger seu computador da infecção por novos vírus, é recomendável renovar a chave do aplicativo. Kaspersky Anti-Virus o notificará antecipadamente sobre a proximidade da data de expiração da chave. Uma mensagem apropriada será exibida sempre que o aplicativo for iniciado.

Informações sobre a chave atual são mostradas em **Ativação** (veja a Figura 56) na janela principal do aplicativo. A seção **Chaves instaladas** mostra a identificação da chave, seu tipo (comercial, de teste, beta), o número de hosts nos quais a chave pode ser instalada, a data de validade da chave e o número de dias até a expiração. Clique em Exibir informações detalhadas das chaves para exibir mais informações.

Para examinar os termos do contrato de licença do aplicativo, clique em Exibir Contrato de Licença do Usuário Final. Para remover uma chave da lista, clique em Excluir chave.

Para adquirir ou renovar uma chave:

1. Compre uma nova chave clicando em Adquirir nova chave (o aplicativo não foi ativado) ou em Estender chave. A página da Web que é aberta contém todas as informações sobre a compra de uma chave na loja on-line ou através dos parceiros corporativos da Kaspersky Lab.

Se você fizer uma compra on-line, um arquivo de chave ou um código de ativação será enviado para o endereço especificado no formulário do pedido assim que o pagamento for efetuado.

2. Instale a chave clicando em Instalar chave em **Ativação** na janela principal do Kaspersky Anti-Virus ou em **Ativação** no menu de contexto do aplicativo. Isso iniciará o assistente de ativação (consulte a seção 3.2.2 na p. 34).

Figura 56. Gerenciamento de chaves

Periodicamente, a Kaspersky Lab lança ofertas de extensões de licença de nossos produtos. Verifique as ofertas no site da Kaspersky Lab, em **Produtos → Vendas e ofertas especiais**.

CAPÍTULO 15. 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 15.2 na p. 176). 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 os bancos de dados do aplicativo atuais (consulte a seção 15.1 na p. 172).

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 15.10 na p. 207). A Kaspersky fornece vários canais de suporte, incluindo o suporte on-line, o fórum de usuários e a Base de dados de conhecimento.

- O recurso de Notificações configura as notificações do usuário sobre eventos-chave do Kaspersky Anti-Virus (consulte 15.9.1 na p. 199). 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 15.9.2 na p. 203). Por exemplo, alterar o nível de proteção pode influir significativamente sobre a segurança das informações no computador.

- O Gerenciamento de Configuração do Aplicativo armazena parâmetros do aplicativo em tempo de execução e facilita a replicação desses

parâmetros em outros computadores (consulte a seção 15.9.3 na p. 205), além da recuperação de configurações padrão (consulte a seção 15.9.4 na p. 206).

O programa também fornece relatórios detalhados (consulte a seção 15.3 na p. 178) sobre o funcionamento de todos os componentes de proteção, tarefas de verificação de vírus e atualizações.

As portas monitoradas podem controlar quais módulos do Kaspersky Anti-Virus controlam os dados transferidos nas portas selecionadas (consulte 15.4 na p. 186). A configuração do servidor proxy (consulte a seção 15.7 na p. 194) permite que o aplicativo acesse a Internet, o que é fundamental para determinados componentes de proteção em tempo real e atualizações.

O Disco de Recuperação pode ajudar a restaurar a funcionalidade do computador após uma infecção (consulte a seção 15.4 na p. 186). 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 15.7 na p. 194).

As seções a seguir abordam estes recursos mais detalhadamente.

15.1. 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 infectado*? 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*.

  Os bancos de dados do aplicativo 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 nos bancos de dados, 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 nos bancos de dados do aplicativo.*

  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. 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.

15.1.1. Ações sobre objetos em quarentena

O número total de objetos em Quarentena é exibido na seção **Arquivos de dados e relatórios** da janela principal. À direita da tela, há uma seção **Quarentena** específica, que 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 usando o link Limpar.

Para acessar os objetos na Quarentena:

Clique em Quarentena.

As seguintes ações podem ser executadas na guia **Quarentena** (veja a Figura 57):

- 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 a versão atual dos bancos de dados do aplicativo, 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.

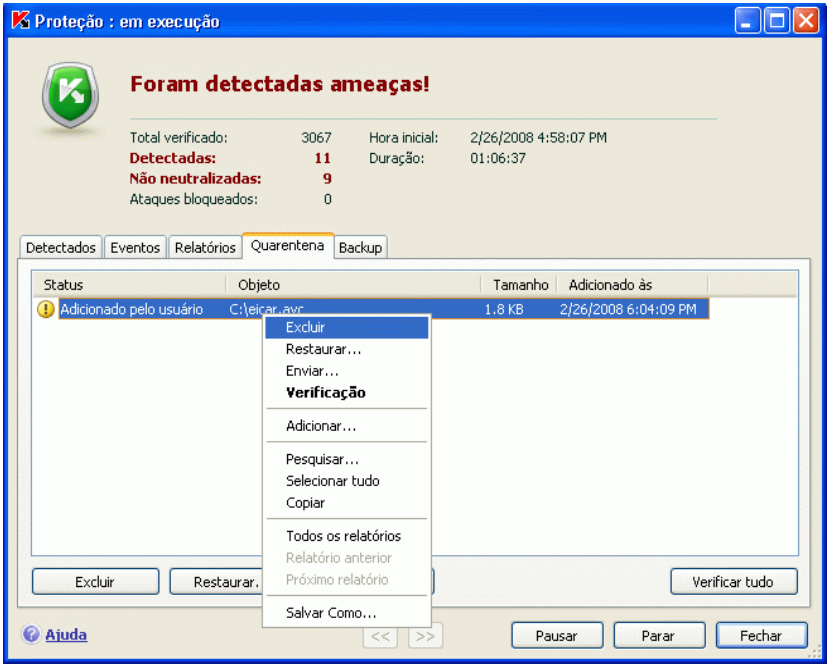


Figura 57. Lista de objetos em quarentena

> **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**.

15.1.2. 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 dos bancos de dados do aplicativo (para obter mais detalhes, consulte 13.3.3 na p. 166).

> **Aviso!**
>
> O programa não poderá verificar objetos em quarentena imediatamente após a atualização dos bancos de dados, 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 aplicativo e selecione a seção **Arquivos de dados e relatórios**.
2. Na seção **Quarentena e Backup** (veja a Figura 58), insira o período depois do qual os objetos na Quarentena serão excluídos automaticamente. Alternativamente, desmarque a caixa de seleção para desabilitar a exclusão automática.

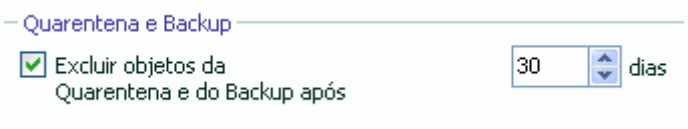


Figura 58. Configurando o período de armazenamento na Quarentena

15.2. 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.

15.2.1. Ações sobre cópias de backup

O número total de cópias de backup de objetos colocados no repositório é exibido na seção **Arquivos de dados e relatórios** da janela principal. À direita da tela, há uma seção **Backup** específica, que exibe:

- o número de cópias de backup de objetos criados pelo Kaspersky Anti-Virus
- o tamanho atual do Backup.

Você pode excluir todas as cópias do backup usando o link Limpar.

Para acessar as cópias de objetos perigosos:

Clique em Backup.

Uma lista de cópias de backup será exibida na guia **Backup** (veja a Figura 59). As seguintes informações são exibidas para cada cópia: o nome e o caminho completo original do objeto, o status do objeto atribuído pela verificação e seu tamanho.

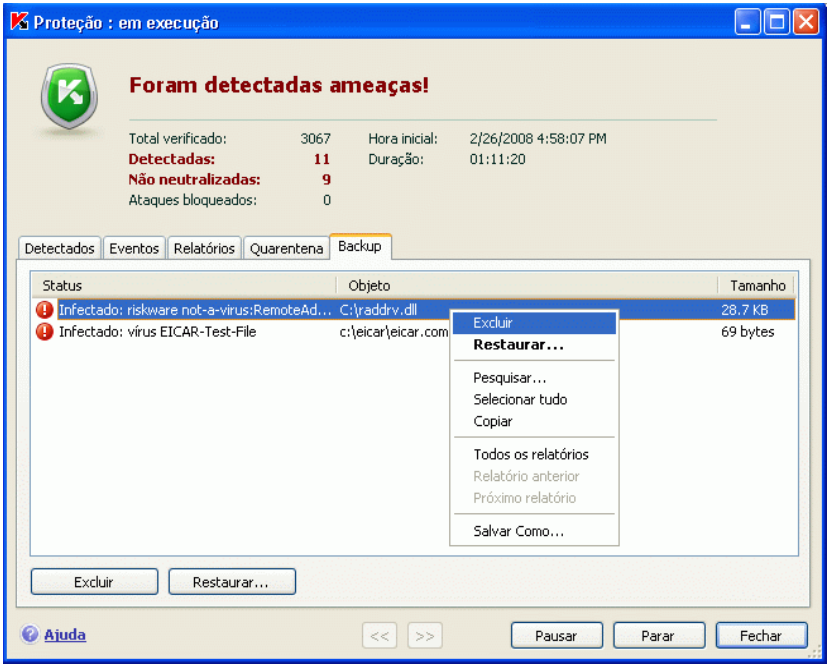


Figura 59. Cópias de backup de objetos excluídos ou desinfectados

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 os bancos de dados do aplicativo atualizados, você consiga desinfectá-lo sem perder a integridade do aplicativo.

Não é recomendável 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 a seção 15.2.2 na p. 178).

15.2.2. 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 aplicativo e selecione a seção **Arquivos de dados e relatórios**.
2. Defina a duração do armazenamento de cópias de backup no repositório na seção **Quarentena e backup** (veja a Figura 58) à direita da tela. Alternativamente, desmarque a caixa de seleção para desabilitar a exclusão automática.

15.3. 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 em um determinado momento e seu tamanho total em bytes são exibidos na seção **Arquivos de dados e relatórios** da janela principal do programa. Essas informações são exibidas na seção **Arquivos de relatórios**.

Para exibir relatórios:

Clique em Relatórios.

A guia **Relatórios** (veja a Figura 60) lista os relatórios mais recentes de todos os componentes e tarefas de atualização e verificação de vírus executados nesta sessão do Kaspersky Anti-Virus. O status é mostrado ao lado de cada componente ou tarefa, por exemplo, *em execução, em pausa* ou *concluído*. Se desejar exibir o histórico completo da criação do relatório da sessão atual do programa, marque ☑ **Mostrar histórico de relatórios**.

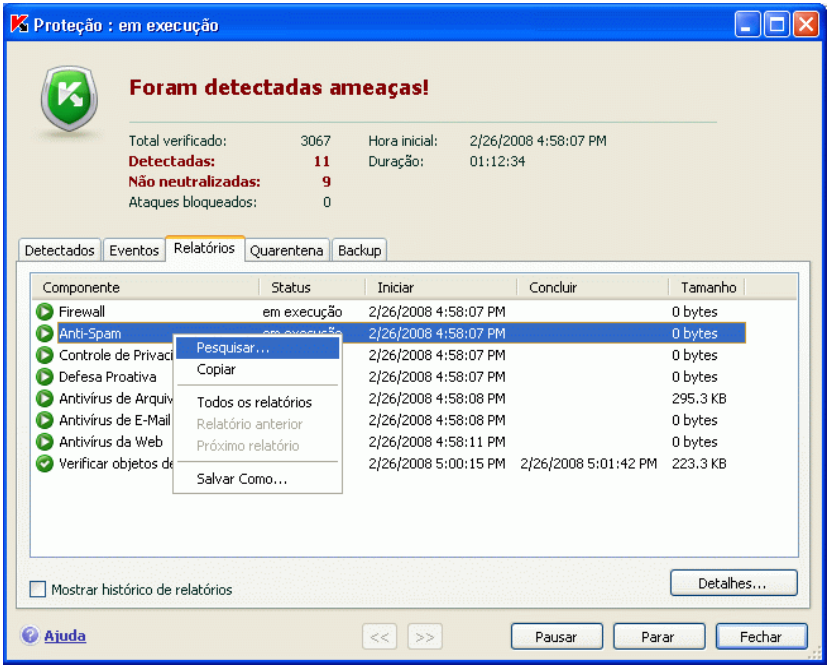


Figura 60. Relatórios de funcionamento do componente

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 executada.
- 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 dos bancos de dados do aplicativo.

- As guias **Registro** aparecem apenas no relatório da Defesa Proativa e contêm informações sobre 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 **Ações → Salvar como** e especifique 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 de acordo com o banco de dados do aplicativo atualizado ou excluí-lo. Você pode aplicar esta ação a um único objeto na lista ou a vários objetos selecionados.

Excluir - exclui o objeto perigoso do computador.

Excluir da lista – remove o registro do objeto detectado do relatório.

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 Microsoft Windows Explorer.

Neutralizar tudo – neutraliza todos os objetos da lista. O Kaspersky Anti-Virus tentará processar os objetos usando os bancos de dados do aplicativo.

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 – insere termos de pesquisa para objetos da lista, por nome ou status.

Salvar como - salva o relatório como arquivo de texto.

Além disso, você pode classificar as informações exibidas na janela em ordem crescente e decrescente, para cada coluna, clicando no cabeçalho da coluna.

Para processar objetos perigosos detectados pelo Kaspersky Anti-Virus, pressione o botão **Desinfectar** (para um objeto ou um grupo de objetos selecionados) ou **Desinfectar tudo** (para processar todos os objetos da lista). Depois que cada objeto for processado, aparecerá uma mensagem na tela. Será necessário decidir então o que fazer com eles.

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.

15.3.1. Configurando relatórios

Para configurar a criação e a forma como os relatórios são salvos:

1. Abra a janela de configurações do aplicativo e selecione a seção **Arquivos de dados e relatórios**.
2. Edite as configurações na caixa **Relatórios** (veja a Figura 61) 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.

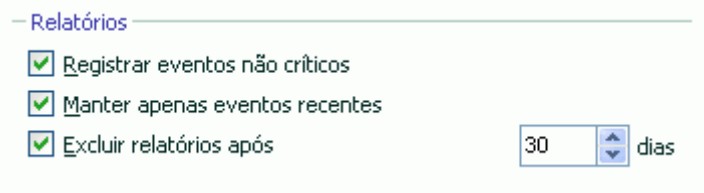


Figura 61. Configurando relatórios

15.3.2. A guia *Detectados*

Esta guia (veja a Figura 62) 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**.

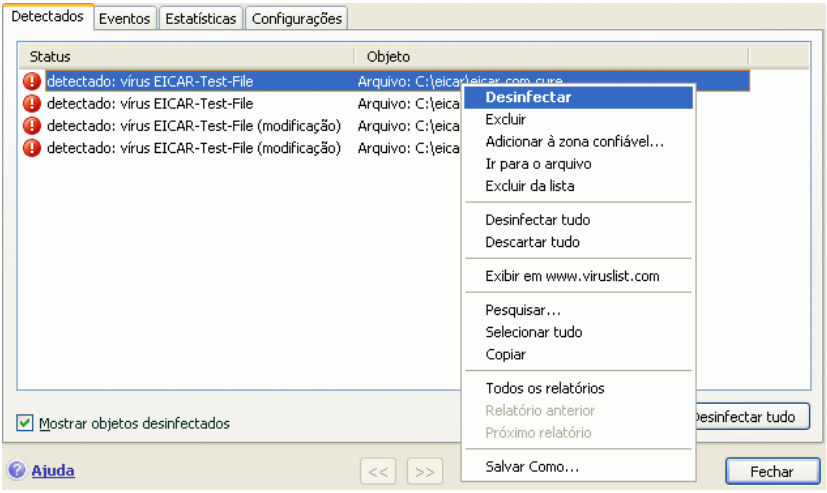


Figura 62. Lista de objetos perigosos detectados

Os objetos perigosos detectados pelo Kaspersky Anti-Virus são processados usando o botão **Desinfectar** (para um objeto ou grupo de objetos selecionados) ou **Desinfectar 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.

15.3.3. A guia *Eventos*

Esta guia (veja a Figura 63) fornece uma lista completa de todos os eventos importantes no funcionamento do componente, nas verificações de vírus e nas atualizações que não foram substituídos por uma regra de controle de atividade (consulte a seção 10.1 na p. 124).

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.

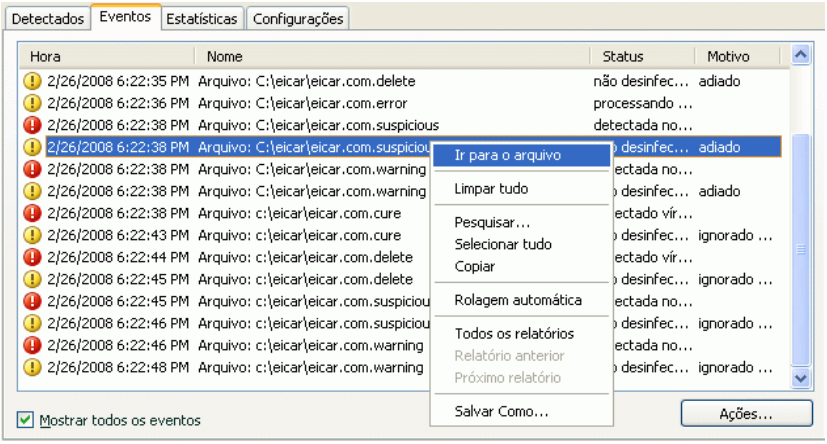


Figura 63. Eventos que ocorrem no funcionamento do componente

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.

15.3.4. A guia Estatísticas

Esta guia (veja a Figura 64) 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 serviço ou depois que uma tarefa foi concluída. 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.

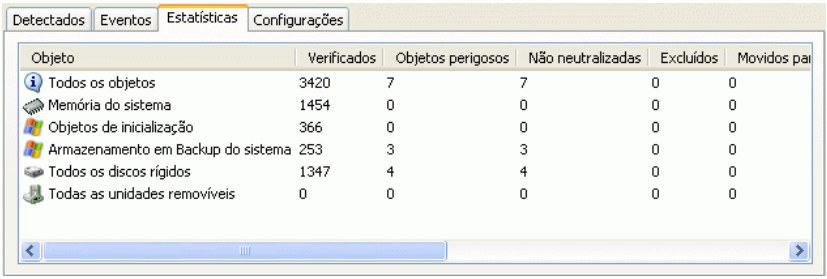


Figura 64. Estatísticas do componente

15.3.5. A guia *Configurações*

A guia **Configurações** (veja a Figura 65) 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. Por padrão, a caixa **Conceder recursos a outros aplicativos** está marcada. 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.

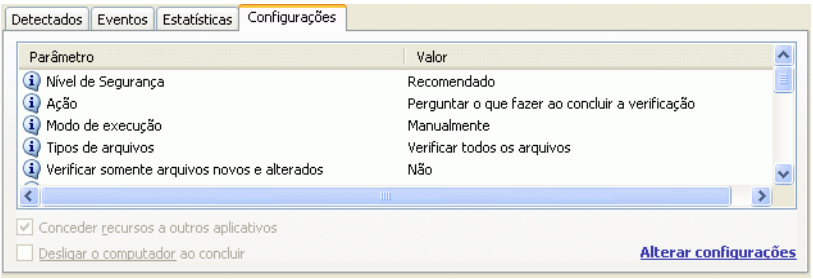


Figura 65. Configurações do componente

- 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.

15.3.6. 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 Figura 66), a menos que proibido por uma regra (consulte a seção 10.3.2 na p. 135).

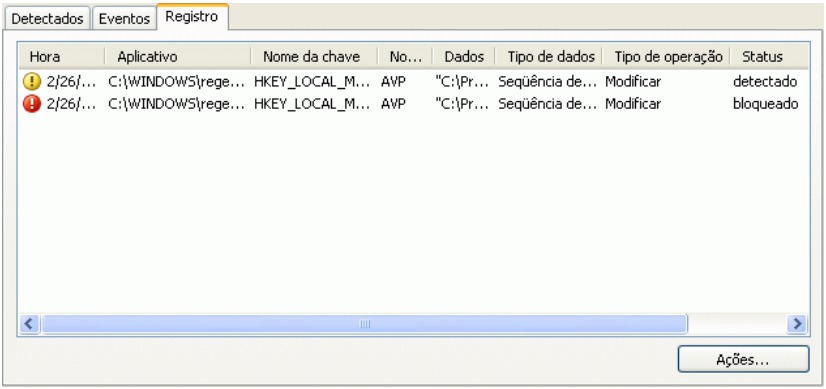


Figura 66. Ler e modificar eventos do registro do sistema

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.

15.4. 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 dos bancos de dados do aplicativo.

Para criar um disco de recuperação:

1. Abra a janela principal do aplicativo e selecione **Verificação**.

2. Clique em Criar disco de recuperação para iniciar o processo de criação do disco.

Um Disco de Recuperação se destina ao computador no qual foi criado. Seu uso em outros computadores poderia ter conseqüências imprevisíveis, pois ele contém informações sobre os parâmetros daquele computador específico (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.

15.4.1. Criando um disco de recuperação

Aviso! O disco de instalação do Microsoft Windows XP Service Pack 2 é necessário para criar um disco de recuperação.

Você precisa do programa **PE Builder** para criar o Disco de Recuperação.

Instale o PE Builder no computador antes de criar um disco 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.

Step 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/DVD
- Se esta não for a primeira vez que você cria um disco, essa pasta já conterá um conjunto de arquivos criados da última vez. Para usar os arquivos salvos anteriormente, marque a caixa correspondente.

Observe que a versão anterior dos arquivos do disco de recuperação contém uma versão antiga dos bancos de dados do aplicativo. Para otimizar as verificações de vírus e a recuperação do sistema, é recomendável que os bancos de dados sejam atualizados e um novo disco de recuperação seja criado.

- 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.

Step 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, 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**.

Step 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.

Step 4. Finalizando o disco de recuperação

Esta janela do Assistente informa que você criou um disco de recuperação com êxito.

15.4.2. 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 recuperação usando o Kaspersky Anti-Virus em um computador não infectado.
2. Insira o disco de recuperação na unidade de disco do computador infectado e o reinicie. O Microsoft Windows XP SP2 será iniciado com a interface do Bart PE.
3. O Bart PE possui um suporte à rede interno para usar sua rede local. Quando o programa é iniciado, ele pergunta se você deseja habilitá-lo. Habilite o suporte à rede se planeja atualizar os bancos de dados do aplicativo na rede local antes de verificar o computador. Se a atualização não for necessária, cancele o suporte à rede.
4. Para abrir o Kaspersky Anti-Virus, clique em Iniciar→Programas→Kaspersky Anti-Virus 7.0→Iniciar.
5. 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 dos bancos de dados do aplicativo na rede local (se você tiver habilitado o suporte à rede no Bart PE).
6. Inicie a verificação de vírus.

Observe que, por padrão, são usados os bancos de dados do aplicativo da data em que o disco de recuperação é criado. Por isso, é recomendável atualizar os bancos de dados antes de iniciar a verificação.

Observe também que o aplicativo usará apenas os bancos de dados do aplicativo atualizados 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.

15.5. 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 aplicativo e selecione **Monitoramento do tráfego**.
2. Clique em Configurações de porta.
3. Atualize a lista de portas monitoradas na caixa de diálogo **Configurações de porta** (veja a Figura 67).

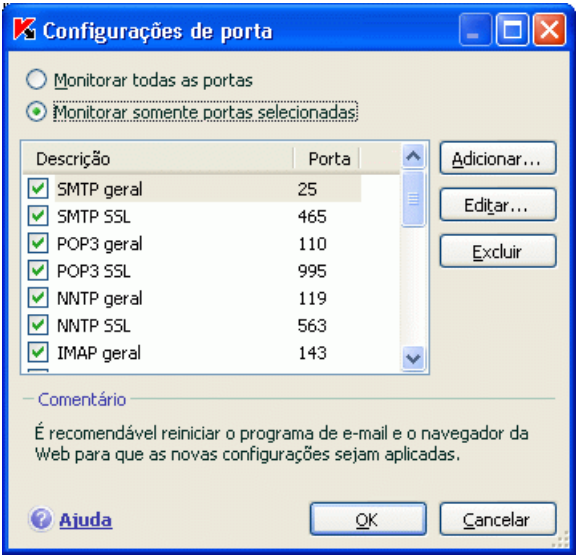


Figura 67. Lista de portas monitoradas

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**.

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.

15.6. Verificando conexões seguras

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, criptografa os dados que são transferidos e assegura sua integridade em trânsito.

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 oferece 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 68) perguntando o que fazer.

A notificação contém informações sobre o programa que iniciou a conexão segura, junto com o endereço remoto e a porta. Selecione uma das opções a seguir para continuar ou interromper a verificação:

- **Processar** – verifica o tráfego quanto à presença de vírus ao conectar-se ao site de maneira segura.
- **Ignorar** – permanece conectado a um recurso da Web sem verificar o tráfego quanto à presença de vírus.

Marque **Aplicar a todos** para aplicar a ação selecionada a todas as tentativas subseqüentes de estabelecer conexões SSL na sessão atual do navegador.

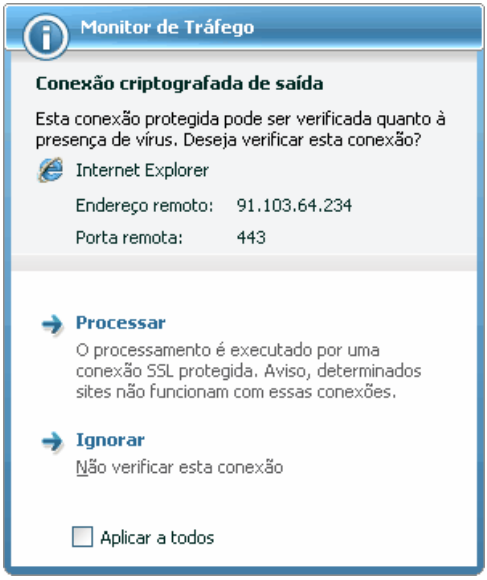


Figura 68. Notificação de detecção de conexão SSL

Para verificar conexões criptografadas, o Kaspersky Anti-Virus substitui o certificado de segurança solicitado por um certificado autoassinado. Em alguns casos, os programas que estão estabelecendo conexões não aceitarão esse certificado e nenhuma conexão será estabelecida. Nessas situações, é recomendável selecionar a opção **Ignorar** no aviso relativo à verificação de uma conexão segura:

- 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 em **Monitoramento do tráfego** na janela de configurações do programa (veja a Figura 69):

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.

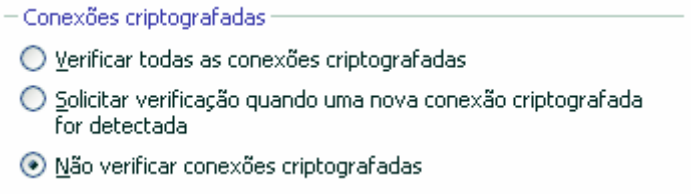


Figura 69. Configurando a verificação de conexões seguras

15.7. Configurando o servidor proxy

A conexão com um servidor proxy deve ser configurada na seção **Servidor proxy** (veja a Figura 70) da janela de configurações do aplicativo (se a conexão com a Internet for via proxy). O Kaspersky Anti-Virus usa essas configurações em vários componentes de proteção em tempo real e para atualizar os bancos de dados e módulos do aplicativo.

Se um servidor proxy for usado para conectar-se à Internet, marque **Usar servidor proxy** e defina as seguintes configurações, conforme necessário:

- Selecione os parâmetros do servidor proxy a serem usados:

  Detectar configurações do servidor proxy automaticamente. Se você selecionar esta opção, as configurações do servidor proxy serão detectadas automaticamente usando o protocolo WPAD (Web Proxy Auto-Discovery Protocol). Se esse protocolo não conseguir determinar o endereço, o Kaspersky Anti-Virus usará as configurações de servidor proxy especificadas no Microsoft Internet Explorer.

  Usar as configurações do servidor proxy especificadas: usa um servidor proxy diferente daquele especificado nas configurações de conexão do navegador. Insira um endereço IP ou um nome de domínio no campo **Endereço** e o número da porta de um servidor proxy no campo **Porta**.

  Para não usar um servidor proxy nas atualizações de diretórios locais ou de rede, marque **Anular servidor proxy para endereços locais**.

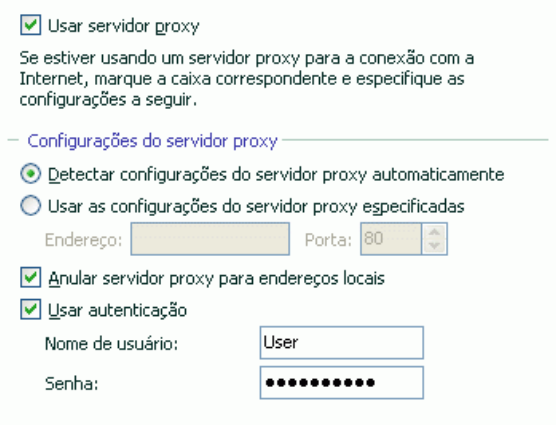


Figura 70. Configurando o servidor proxy

- Especifique se o servidor proxy utiliza autenticação. *Autenticação* é o processo de verificação das informações da conta do usuário para fins de controle de acesso.

  Se a autenticação for necessária para conectar-se ao servidor proxy, marque ☑ **Usar autenticação** e insira o nome de usuário e a senha nos campos apropriados. Assim, será feita uma tentativa de executar uma autorização NTLM, seguida de uma autorização BASIC.

  Se a caixa de seleção estiver desmarcada, a autorização NTLM será tentada com o logon no qual a tarefa (como uma atualização, consulte a seção 6.6 na p. 65) está sendo executada.

  Se o servidor proxy exigiu autenticação, e por algum motivo o nome de usuário e a senha não foram especificados ou foram rejeitados pelo proxy, será exibida uma caixa de diálogo solicitando o nome de usuário e a senha. Se a autorização for bem-sucedida, o nome de usuário e a senha especificados serão lembrados para utilização posterior. Caso contrário, as informações de autorização serão solicitadas novamente.

  Pressionar o botão **Cancelar** na caixa de diálogo de solicitação de autenticação substitui a fonte de atualização atual pela próxima da lista; os parâmetros de autenticação especificados nessa janela ou definidos na interface do programa serão ignorados. Assim, o aplicativo tentará a autenticação NTLM com base na conta usada para iniciar a tarefa.

Se um servidor FTP for usado na atualização, uma conexão passiva será estabelecida por padrão. Se essa conexão retornar um erro, será feita uma tentativa de estabelecer uma conexão ativa.

Por padrão, o tempo limite da conexão com o servidor de atualização é de um minuto. Se a conexão falhar e o tempo limite expirar, será feita uma tentativa de conexão com o próximo servidor de atualização. Essa seqüência continua até que uma conexão seja estabelecida com êxito ou até que se tenha tentado todos os servidores de atualização disponíveis.

15.8. 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 do aplicativo na área de notificação da barra de tarefas e as mensagens pop-up.

Para configurar a interface do Kaspersky Anti-Virus:

Abra a janela de configurações do aplicativo e selecione a seção **Aparência** (veja a Figura 71).

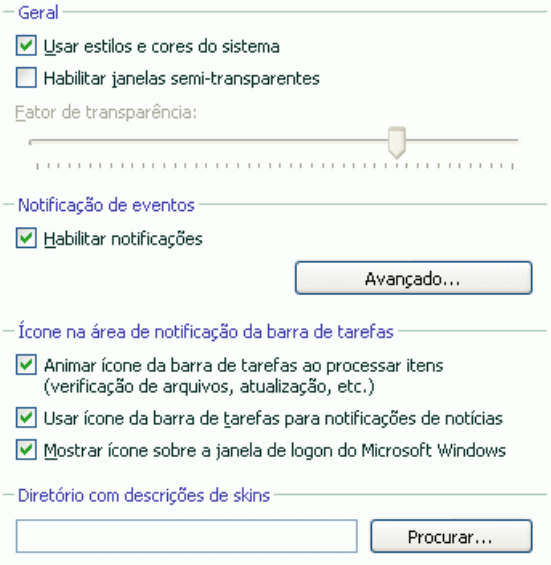


Figura 71. Configurando a interface do aplicativo

À direita da janela de configurações, você pode determinar:

- *Componentes gráficos e esquemas de cores na interface do aplicativo definidos pelo usuário*.

  Por padrão, a interface do usuário utiliza cores e estilos do sistema. Você pode removê-los, desmarcando **Usar e estilos cores do sistema**. Assim, serão habilitados os estilos especificados na configuração dos temas de exibição.

  Todas as cores, fontes, ícones e textos usados na interface do Kaspersky Anti-Virus podem ser configurados. É possível criar capas personalizadas para o aplicativo. O próprio aplicativo pode ser localizado em um outro idioma. Para usar uma capa, especifique o diretório que contém sua descrição em **Diretório com descrições de skins**. Use o botão **Procurar** para selecionar o diretório.

- *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 sobre o ícone do aplicativo na área de notificação da barra de tarefas. 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**.

- *Animação do ícone do aplicativo na área de notificação da barra de tarefas*.

  Dependendo da operação do programa realizada, o ícone 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 da barra de tarefas 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.

- *Notificações de notícias da Kaspersky Lab*

  Por padrão, quando forem recebidas notícias, é exibido um ícone específico na área de notificação da barra de tarefas que, quando clicado, abre uma janela com a notícia. Para desabilitar as notificações, desmarque **Usar ícone da barra de tarefas para notificações de notícias**.

- *Exibir ícone do Kaspersky Anti-Virus na inicialização do sistema operacional*.

  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**.

As modificações das configurações da interface do Kaspersky Anti-Virus não serão salvas se você restaurar as configurações padrão ou desinstalar o aplicativo.

15.9. Usando opções avançadas

O Kaspersky Anti-Virus fornece os seguintes recursos avançados (veja a Figura 72):

- abertura do Kaspersky Anti-Virus na inicialização do sistema operacional (consulte a seção 15.11 na p. 209);
- notificação do usuário sobre determinados eventos do aplicativo (consulte a seção 15.9.1 na p. 199);
- autodefesa do Kaspersky Anti-Virus contra desligamento, remoção ou modificação do módulo, proteção do aplicativo por senha (consulte a seção 15.9.2 na p. 203);
- exportação / importação das configurações de tempo de execução do Kaspersky Anti-Virus (consulte a seção 15.9.3 na p. 205);
- recuperação das configurações padrão (consulte a seção 15.9.4 na p. 206)

Para configurar estes recursos:

Abra a janela de configurações do aplicativo e selecione **Serviço**.

À direita da tela, você pode definir se vai ou não usar os recursos adicionais na operação do programa.

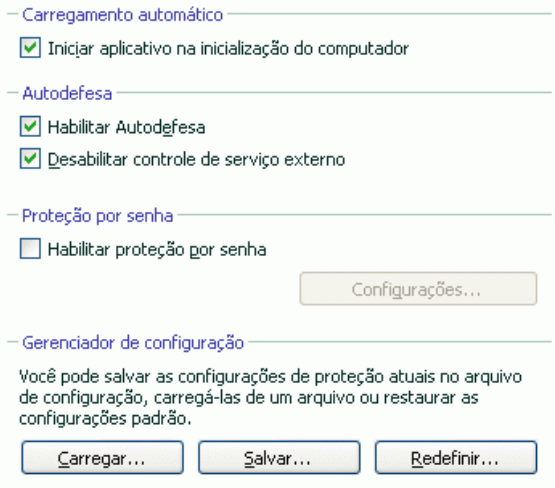


Figura 72. Configurando as opções avançadas

15.9.1. 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 sobre o ícone do aplicativo na área de notificação da barra de tarefas
- Mensagens sonoras
- E-mails
- Registro de eventos em log

Para usar este recurso:

1. Marque ☑ **Habilitar notificações** em **Notificação de eventos** na seção **Aparência** da janela de configurações do aplicativo (veja a Figura 71).

2. Defina os tipos de eventos do Kaspersky Anti-Virus sobre os quais você deseja ser notificado e o método de entrega das notificações (consulte a seção 15.9.1.1 na p. 200).

3. Configure a entrega de notificações por e-mail, se esse for o método de notificação usado (consulte a seção 15.9.1.2 na p. 201).

15.9.1.1. 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, *bancos de dados do aplicativo corrompidos* ou *chave expirada*.

Falhas funcionais são eventos que levam ao não funcionamento do aplicativo. Por exemplo, quando não existe uma chave ou bancos de dados do aplicativo.

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. Abra a janela de configurações do aplicativo e selecione **Aparência** (veja a Figura 71).

2. Marque ☑ **Habilitar notificações** em **Notificações de eventos** e vá para as configurações avançadas clicando em **Avançado**.

É possível configurar os seguintes métodos de notificação sobre os eventos acima na caixa de diálogo **Configurações de notificações de eventos** (veja a Figura 73):

- *Mensagens pop-up* acima do ícone do aplicativo na área de notificação da barra de tarefas, 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 arquivo de 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 a seção 15.9.1.2 na p. 201).

- *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 a seção 15.9.1.3 na p. 203).

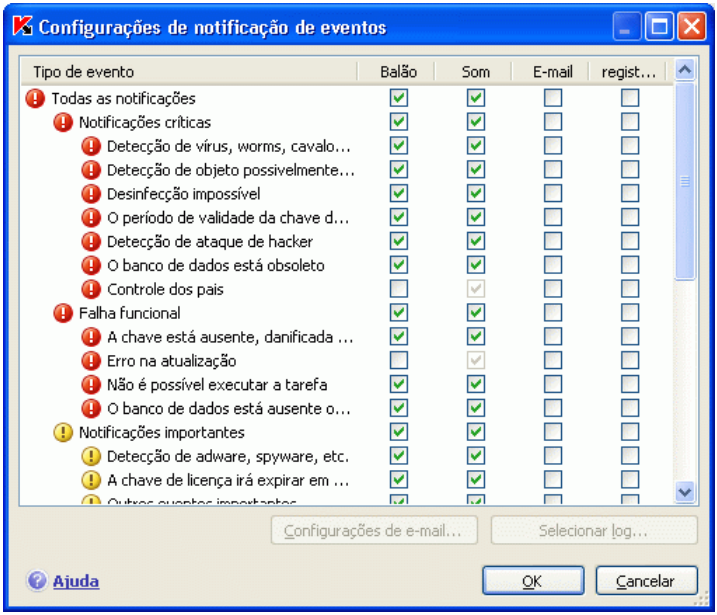


Figura 73. Eventos do programa e métodos de notificação de eventos

15.9.1.2. Configurando a notificação por e-mail

Depois de selecionar os eventos (consulte a seção 15.9.1.1 na p. 200) sobre os quais você deseja receber notificações por e-mail, configure a entrega de notificações. Para fazê-lo:

1. Abra a janela de configurações do aplicativo e selecione **Aparência** (veja a Figura 71).
2. Clique em **Avançado** em **Notificação de eventos**.
3. Na janela **Configurações de notificação de eventos** (veja a Figura 73), marque os eventos que devem disparar uma notificação por e-mail na coluna **E-mail**.
4. Na janela que é aberta (veja a Figura 74) 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 **Alterar**. Notificações diárias são o padrão.

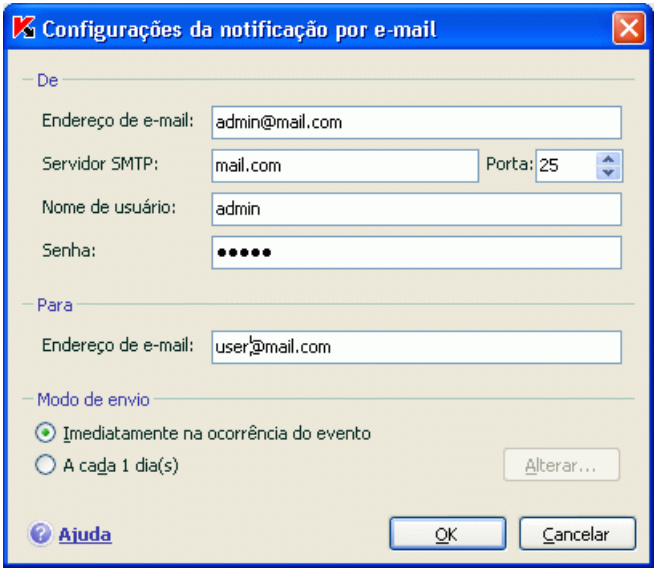


Figura 74. Configurando a notificação por e-mail

15.9.1.3. Configurando o log de eventos

Para configurar o log de eventos:

1. Abra a janela de configurações do aplicativo e selecione **Aparência** (veja a Figura 71).
2. Clique em Avançado em Notificação de eventos.

Use a janela **Configurações de notificação de eventos** para selecionar a opção de registrar informações de um evento e clique no botão **Configurações de 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 exclusivo 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**.

15.9.2. Autodefesa e restrição de acesso

O Kaspersky Anti-Virus é um aplicativo que protege computadores de malware e, portanto, os softwares mal-intencionados têm interesse em tentar desabilitá-lo ou até mesmo removê-lo dos computadores.

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.

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 programa em unidades locais e o Registro do sistema sejam modificados ou excluídos.

Para habilitar a Autodefesa:

1. Abra a janela de configurações do aplicativo e selecione **Serviço** (veja a Figura 72).
2. Defina as seguintes configurações na caixa **Autodefesa**:

☑ **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.

Para que ferramentas de administração remota (como o RemoteAdmin) tenham acesso ao Kaspersky Anti-Virus, elas devem ser adicionadas à lista de aplicativos confiáveis, e a configuração ☑ **Não restringir a atividade de aplicativos** deve estar habilitada (consulte a seção 6.9.2 na p. 75).

Se houver alguma tentativa de executar as ações relacionadas, aparecerá uma mensagem sobre o ícone do aplicativo na área de notificação da barra de tarefas (a menos que o serviço de notificação tenha sido desabilitado pelo usuário).

Para proteger o programa por senha, marque ☑ **Habilitar proteção por senha** na área com o mesmo nome. 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 Figura 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.

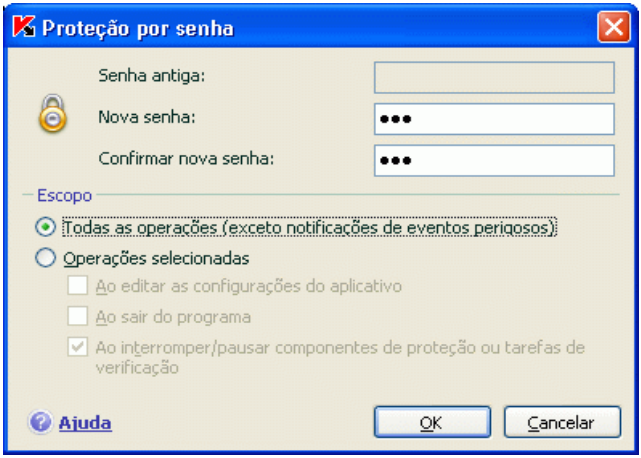


Figura 75. Configurações de proteção do programa por senha

15.9.3. Importando e exportando configurações do Kaspersky Anti-Virus

O Kaspersky Anti-Virus permite que você importe e exporte as configurações do aplicativo.

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 de configurações do programa e selecione a seção **Serviço** (veja a Figura 72).
2. Clique no botão **Salvar** na seção **Gerenciador de configurações**.
3. 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 de configurações do programa e selecione a seção **Serviço**.

2. Clique no botão **Carregar** e selecione o arquivo do qual deseja importar configurações do Kaspersky Anti-Virus.

15.9.4. Restaurando 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 de Configuração.

Para redefinir as configurações de proteção:

1. Abra a janela de configurações do programa e selecione a seção **Serviço** (veja a Figura 72).
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.

Alguns exemplos de configurações específicas seriam as listas de endereços confiáveis usadas pelo Antivírus da Web; as regras de exclusão criadas para os componentes do programa e as 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 de Configuração inicial será aberto (consulte a seção 3.2 na p. 34). Siga suas instruções.

Depois de concluir o Assistente de Configuração, o nível de segurança **Recomendado** será definido para todos os componentes de proteção, exceto pelas configurações que você decidiu manter. Além disso, as configurações feitas no Assistente de Configuração também serão aplicadas.

15.10. Suporte Técnico

Informações sobre o suporte técnico oferecido aos usuários da Kaspersky Lab estão disponíveis em **Suporte** (veja a Figura 76), na janela principal do aplicativo.

A seção superior apresenta informações gerais do aplicativo: versão, data de publicação do banco de dados e um resumo do sistema operacional do computador.

Se houver problemas ao executar o Kaspersky Anti-Virus, verifique primeiro se existem instruções para solução de problemas no sistema de ajuda ou na Base de Dados de Conhecimento, no site de Suporte Técnico da Kaspersky Lab. A Base de Dados de Conhecimento é uma seção independente do site de Suporte Técnico, com recomendações para os produtos da Kaspersky Lab e respostas às perguntas mais freqüentes. Tente usar esse recurso para encontrar uma resposta para sua pergunta ou uma solução para seu problema. Clique em Suporte pela Web para acessar a Base de Dados de Conhecimento.

O fórum de usuários da Kaspersky Lab é um outro recurso de informações sobre o aplicativo. Ele também consiste em uma seção independente do site de Suporte Técnico e contém perguntas, comentários e solicitações de usuários. Você pode exibir os temas principais, deixar comentários ou encontrar a resposta para uma pergunta. Clique em Fórum de usuários para acessar este recurso.

Se não encontrar uma solução para seu problema na Ajuda, na Base de Dados de Conhecimento ou no Fórum de Usuários, entre em contato com o Suporte Técnico da Kaspersky Lab.

É necessário ser um usuário registrado da versão comercial do Kaspersky Anti-Virus para obter suporte técnico. Os usuários de versões de teste não receberão suporte.

O registro do usuário é feito pelo Assistente de Ativação (consulte a seção 3.2.2 na p. 34), no caso de o aplicativo ser ativado com um código de ativação. No final do processo de registro, será atribuída uma identificação do cliente que pode ser visualizada em **Suporte** (veja a Figura 76), na janela principal. O número de cliente é uma identificação pessoal do usuário necessária para o suporte técnico telefônico ou baseado em formulários da Web.

Se for usado um arquivo de chave para a ativação, faça seu registro diretamente no site de Suporte Técnico.

Um novo serviço chamado Gabinete pessoal dá acesso a uma seção pessoal do site de Suporte Técnico. O Gabinete pessoal permite:

- enviar solicitações ao Suporte Técnico sem fazer logon;

- trocar mensagens com o Suporte Técnico sem usar o e-mail;
- monitorar as solicitações em tempo real;
- exibir o histórico completo das solicitações de Suporte Técnico;
- obter uma cópia de backup do arquivo de chave.

Use o link Criar solicitação para enviar uma solução pelo formulário on-line para o Suporte Técnico. Insira seu Gabinete pessoal no site de Suporte Técnico que será aberto e preencha o formulário de solicitação.

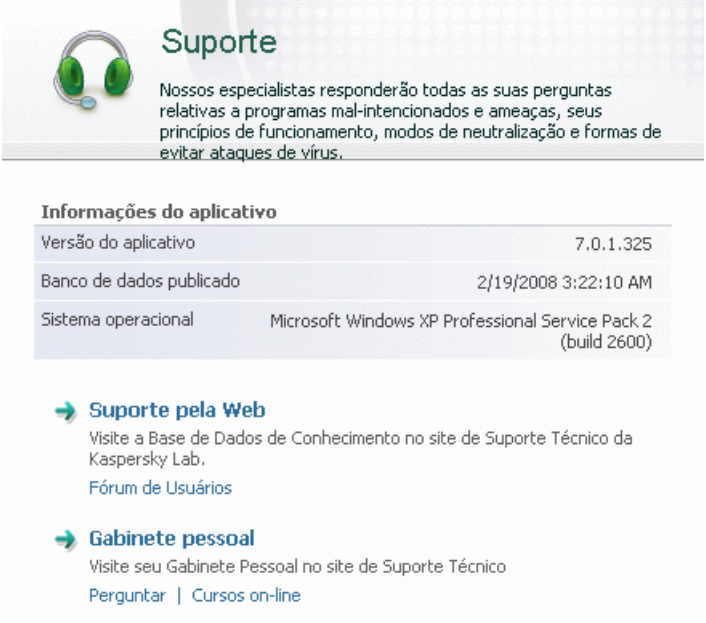


Figura 76. Informações de suporte técnico

Para obter assistência urgente, use os números de contato fornecidos no sistema de Ajuda (consulte a seção B.2 na p. 247). O suporte telefônico está disponível 24 horas por dia, 7 dias por semana em russo, inglês, francês, alemão e espanhol.

Use o link Cursos On-line para obter mais informações sobre eventos de treinamento nos produtos da Kaspersky Lab.

15.11. Fechando o aplicativo

Se for necessário desligar o Kaspersky Anti-Virus, selecione **Sair** no menu de contexto do aplicativo (consulte a seção 4.2 na p. 43). O aplicativo será descarregado da RAM, ou seja, o computador ficará desprotegido.

No caso de haver conexões de rede abertas no momento em que o aplicativo é desligado, aparecerá uma mensagem informando que as conexões foram desfeitas. Isso é necessário para que o aplicativo seja desligado corretamente. A desconexão é automática após 10 segundos ou ocorre ao clicar em **Sim**. A maioria dessas conexões é restabelecida após um período.

Observe que os downloads em andamento no momento em que as conexões são desfeitas são interrompidos, a menos que um gerenciador de download esteja sendo usado. O download deverá ser reiniciado para obter o arquivo.

Você pode evitar que as conexões sejam interrompidas, clicando em **Não** na janela de notificação. Assim, o aplicativo continuará em execução.

Se você fechou o aplicativo, a proteção poderá ser habilitada novamente reiniciando o Kaspersky Anti-Virus em **Iniciar** → **Programas** → **Kaspersky Anti-Virus 7.0** → **Kaspersky Anti-Virus 7.0**.

A proteção também será reiniciada automaticamente após a reinicialização do sistema operacional. Para habilitar este modo, selecione **Serviço** (veja a Figura 72) na janela de configurações do aplicativo e marque ☑ **Iniciar o aplicativo na inicialização** em **Carregamento automático**.

CAPÍTULO 16. TRABALHANDO COM O PROGRAMA A PARTIR DA LINHA DE COMANDO

Você pode usar o Kaspersky Anti-Virus a partir da linha 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 bancos de dados 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]
```

Acesse o programa do prompt de comando na pasta de instalação do programa ou especificando o caminho completo de avp.com.

As seguintes instruções podem ser usadas como **<comando>**:

ACTIVAE	Ativa o aplicativo pela Internet usando um código de ativação
ADDKEY	Ativa o aplicativo usando um arquivo de chave (o comando poderá ser executado somente se a senha atribuída na interface do programa for inserida)
START	Inicia um componente ou uma tarefa

PAUSE	Pausa um componente ou uma tarefa (o comando poderá ser executado somente se a senha atribuída pela interface do programa for inserida)
RESUME	Reinicia um componente ou uma tarefa
STOP	Interrompe um componente ou uma tarefa (o comando poderá ser executado somente se a senha atribuída pela interface do programa for inserida)
STATUS	Exibe o status atual do componente ou da tarefa na tela
STATISTICS	Exibe estatísticas do componente ou da tarefa na tela
HELP	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 última atualização do programa (o comando poderá ser executado somente se a senha atribuída pela interface do programa for inserida)
EXIT	Fecha o programa (este comando só pode ser executado com a senha atribuída na interface do programa)
IMPORT	Importa configurações do Kaspersky Anti-Virus (o comando poderá ser executado somente se a senha atribuída pela interface do programa for inserida)
EXPORT	Exporta configurações do Kaspersky Anti-Virus

Cada comando usa suas próprias configurações específicas daquele componente do Kaspersky Anti-Virus.

16.1. 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 (comando ADDKEY)

Sintaxe do comando:

```
ACTIVATE <código_de_ativação>
ADDKEY <nome_do_arquivo> /password=<sua_senha>
```

Descrição dos parâmetros:

<código_de_ativação>	Código de ativação do programa fornecido ao adquiri-lo.
<nome_do_arquivo>	Nome do arquivo de chave com a extensão *.key*.
<sua_senha>	Senha para acessar o Kaspersky Anti-Virus atribuída na interface do programa.
Não será possível executar o comando **ADDKEY** sem informar a senha.	

Exemplo:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key /password=<sua_senha>
```

16.2. Gerenciando tarefas e componentes do programa

Sintaxe do comando:

```
avp.com <comando> <perfil|nome_da_tarefa>
[/R[A]:<arquivo_de_relatório>]
avp.com STOP|PAUSE <perfil|nome_da_tarefa>
/password=<sua_senha> [/R[A]:<arquivo_de_relatório>]
```

Descrição dos parâmetros:

<comando>	Você pode gerenciar os componentes e as tarefas do Kaspersky Anti-Virus a partir do prompt de comando, com os seguintes comandos: **START** - carrega uma tarefa ou componente de proteção em tempo real. **STOP** - interrompe uma tarefa ou componente de proteção em tempo real.

	PAUSE - pausa uma tarefa ou componente de proteção em tempo real. **RESUME** - continua uma tarefa ou componente de proteção em tempo real. **STATUS** - exibe o status atual da tarefa ou componente de proteção em tempo real. **STATISTICS** - exibe na tela as estatísticas de operação da tarefa ou componente de proteção em tempo real. Não será possível executar os comandos **PAUSE** e **STOP** sem informar a senha.
<perfil|nome_da_tarefa>	Você pode especificar qualquer componente de proteção em tempo real, os módulos nos componentes, as tarefas de verificação por demanda ou as atualizações nos valores de <perfil> (os valores padrão usados no programa são mostrados na tabela a seguir). Você pode especificar o nome de qualquer tarefa de atualização ou verificação por demanda como valor de <nome_da_tarefa>.
<sua_senha>	Senha do Kaspersky Anti-Virus atribuída na interface do programa.
/R[A]:<arquivo_de_relatório>	**R:<arquivo_de_relatório>** – registra apenas os eventos importantes no relatório. **/RA:<arquivo_de_relatório>** – registra todos os eventos no relatório. Você pode usar um caminho absoluto ou relativo para o arquivo. Se o parâmetro não for definido, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.

Um dos seguintes valores é atribuído a **<perfil>**:

RTP	Todos os componentes de proteção O comando avp.com START RTP inicia todos os componentes de proteção em tempo real se a proteção estiver totalmente desabilitada (consulte

	a seção 6.1.2 na p. 60) ou pausada (consulte a seção 6.1.1 na p. 59). Esse comando também iniciará os componentes de proteção em tempo real que foram pausados na interface gráfica do usuário ou com o comando PAUSE do prompt de comando. Se o componente foi desabilitado na interface gráfica do usuário ou com STOP no prompt de comando, o comando avp.com START RTP não o iniciará. Para iniciá-lo, execute o comando avp.com START <perfil>, com o valor desse componente de proteção específico inserido em <perfil>. Por exemplo, avp.com START FM.
FM	Antivírus de Arquivos
EM	Antivírus de E-Mail
WM	Antivírus da Web Valores dos subcomponentes do Antivírus da Web: **httpscan** – verifica o tráfego HTTP **sc** – verifica os scripts
BM	Defesa Proativa Valores dos subcomponentes da Defesa Proativa: **pdm** – análise de atividade do aplicativo
UPDATER	Atualização
Rollback	Revertendo para a atualização anterior
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

SCAN_QUARANTINE	Verifica os objetos em quarentena
SCAN_ROOTKITS	Tarefa de verificação de rootkits
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>
```

16.3. 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>] [<tipos
de arquivos>] [<exclusões>] [<arquivo_configuração>]
[<configurações relatório>] [<configurações
avançadas>]
```

Para verificar objetos, você também pode iniciar uma das tarefas criadas no Kaspersky Anti-Virus do prompt de comando (consulte 16.1 na p. 211). 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	Caixas de correio
/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 **/i8**.	
/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.
/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 as caixas de correio
-e:m	Não verifica e-mails em texto sem formatação
-e:<máscara_arquivos>	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. O arquivo de configuração está no formato de texto, contendo um conjunto de parâmetros da linha de comando da verificação antivírus. 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:<nome_do_arquivo>	Usa os valores de configuração atribuídos no arquivo **<nome_do_arquivo>**
<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
<configurações avançadas> - configurações que definem o uso de tecnologias de verificação antivírus.	
/iChecker=<ativado|desativado>	Habilita / desabilita o iChecker
/iSwift=<ativado|desativado>	Habilita / desabilita o iSwift

Exemplos:

Iniciar a verificação da RAM, dos programas de inicialização, das caixas de correio, 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
```

Exemplo de arquivo de configuração:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt
/RA:scan.log
```

16.4. Atualizações do programa

A sintaxe para atualizar os bancos de dados e módulos do Kaspersky Anti-Virus a partir do prompt de comando é a seguinte:

```
avp.com UPDATE [<fonte_de_atualização>]
[/R[A]:<arquivo_de_relatório>] [/C:<nome_do_arquivo>]
[/APP=<on|off>]
```

Descrição dos parâmetros:

[<fonte_de_atualização>]	Servidor HTTP ou FTP ou pasta de rede para baixar as atualizações. Você pode especificar o caminho completo da fonte de atualização ou uma URL como valor para este parâmetro. Se não for selecionado um caminho, a fonte da atualização será obtida nas configurações da Atualização**.**
/R[A]:<arquivo_de_relatório>	**/R:<arquivo_de_relatório>** – registra somente os eventos importantes no relatório. **/RA:<arquivo_de_relatório>** registra todos os eventos no relatório. Você pode usar um caminho absoluto ou relativo para o arquivo. Se o parâmetro não for definido, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.
/C:<nome_do_arquivo>	Caminho do arquivo de configuração com as definições para atualizações do programa. O arquivo de configuração está no formato de texto, contendo um conjunto de parâmetros da linha de comando da verificação antivírus para a atualização do aplicativo. 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=<on|off>	Habilita / desabilita as atualizações de módulos do aplicativo

Exemplos:

Atualizar os bancos de dados do Kaspersky Anti-Virus 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=on /C:updateapp.ini
```

Exemplo de arquivo de configuração:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt
/app=on
```

16.5. Configurações de reversão

Sintaxe do comando:

```
ROLLBACK [/R[A]:<arquivo_de_relatório>]
[/password=<sua_senha>]
```

/R[A]:<arquivo_de_relatório>	/R:<arquivo_de_relatório> - registra somente os eventos importantes no relatório. /RA:<arquivo_de_relatório> - registra todos os eventos no relatório. Você pode usar um caminho absoluto ou relativo para o arquivo. Se o parâmetro não for definido, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.
<senha>	Senha para acessar o Kaspersky Anti-Virus atribuída na interface do programa.
Observe que não será possível executar este comando sem informar a senha.	

Exemplo:

```
avp.com ROLLBACK /RA:rollback.txt
/password=<sua_senha>
```

16.6. Exportando configurações de proteção

Sintaxe do comando:

```
avp.com EXPORT <perfil> <nome_do_arquivo>
```

Descrição dos parâmetros:

<perfil>	Componente ou tarefa com as configurações exportadas. Você pode usar qualquer valor em **<perfil>** que esteja listado em 16.2 na p. 212.
<nome_do_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. Este arquivo pode ser usado somente para especificar as configurações principais de funcionamento do programa.

Exemplo:

```
avp.com EXPORT c:\settings.dat
```

16.7. Importando configurações

Sintaxe do comando:

```
avp.com IMPORT <nome_arquivo> [/password=<senha>]
```

<nome_do_arquivo>	Caminho do arquivo do qual as configurações do Kaspersky Anti-Virus serão importadas. Você pode usar um caminho absoluto ou relativo. As configurações podem ser importadas somente de arquivos binários.
<sua_senha>	Senha do Kaspersky Anti-Virus atribuída na interface do programa.
Observe que não será possível executar este comando sem informar a senha.	

Exemplo:

```
avp.com IMPORT c:\ settings.dat /password=<sua_senha>
```

16.8. Iniciando o programa

Sintaxe do comando:

```
avp.com
```

16.9. Interrompendo o programa

Sintaxe do comando:

```
EXIT /password=<sua_senha>
```

<sua_senha>	Senha do Kaspersky Anti-Virus atribuída na interface do programa.
Observe que não será possível executar este comando sem informar a senha.	

16.10. Criando um arquivo de rastreamento

Talvez seja necessário criar um arquivo de rastreamento, no caso de problemas com o programa, de forma a solucioná-los de forma precisa juntamente com os especialistas do Suporte Técnico.

Sintaxe do comando:

```
avp.com TRACE [file] [on|off]
[<nível_de_rastreamento>]
```

Descrição dos parâmetros:

[on|off]	Habilitar/desabilitar a criação do rastreamento.
[file]	Colocar o rastreamento em arquivo.
<nível_de_rastreamento>	Este valor pode ser um número inteiro, de 0 (nível mínimo, apenas mensagens críticas) a 700 (nível máximo, todas as mensagens). O Suporte Técnico o informará sobre o nível de rastreamento necessário. Se não for especificado, é recomendável configurá-lo como 500.

Aviso!

É recomendável criar arquivos de rastreamento apenas para a solução de um problema específico. A utilização normal do rastreamento pode tornar o computador lento e encher o disco rígido.

Exemplos:

Para desabilitar a criação do arquivo de rastreamento:

```
avp.com TRACE file off
```

Para criar um arquivo de rastreamento para o Suporte Técnico com um nível de rastreamento máximo de 500:

```
avp.com TRACE file on 500
```

16.11. 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>
```

16.12. 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 17. MODIFICANDO, REPARANDO E REMOVENDO O PROGRAMA

O aplicativo pode ser desinstalado das maneiras a seguir:

- Usando o Assistente de Configuração do aplicativo (consulte a seção 17.2 na p. 228)
- Do prompt de comando (consulte a seção 17.2 na p. 228)

17.1. Modificando, reparando e removendo o programa usando o Assistente de Configuração

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:

1. Insira o CD de instalação utilizado para instalar o programa na unidade de CD/DVD-ROM. Se você instalou o Kaspersky Anti-Virus a partir de outra fonte (pasta compartilhada, pasta do disco rígido, etc.), verifique se o pacote de instalação está disponível na origem e se você tem acesso a ela.
2. Selecione **Iniciar** → **Programas** → **Kaspersky Anti-Virus 7.0** → **Modificar, reparar ou remover**.

Um assistente de configuração do programa será aberto. Vamos examinar mais detalhadamente as etapas necessárias para reparar, modificar ou excluir o programa.

Step 1. 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 você remover o programa, 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:

- *Informações de ativação* – arquivo de chave do aplicativo.
- *Bancos de dados do aplicativo* – 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 dos bancos de dados do aplicativo.
- *Configurações de proteção* – 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.

Step 2. 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**.

17.2. Desinstalando o programa da linha de comando

Para desinstalar o Kaspersky Anti-Virus da linha de comando, insira:

```
msiexec /i <nome_do_pacote>
```

O Assistente de Configuração será aberto. Você pode usá-lo para desinstalar o aplicativo (consulte a seção Capítulo 17 na p. 226).

Para desinstalar o aplicativo de forma não interativa sem reiniciar o computador (o computador deve ser reiniciado manualmente após a desinstalação), digite:

```
msiexec /i <nome_do_pacote> /qn
```

CAPÍTULO 18. 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 7.0 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 iSwift. 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 a ativação é necessária? O Kaspersky Anti-Virus funciona sem um arquivo de chave?

O Kaspersky Anti-Virus será executado sem uma chave, 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. Abra a janela de configurações do aplicativo e selecione **Serviço**.
5. Desmarque **Iniciar o aplicativo na inicialização** e clique em **OK**.
6. Reinicie o sistema operacional no modo normal.

Envie uma solicitação para o Suporte Técnico da Kaspersky Lab. Abra a janela principal do aplicativo, selecione **Suporte** e clique em Enviar solicitação. Descreva o problema e sua assinatura da forma mais detalhada possível.

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 a opção **Verificar programas e documentos (por extensão)** for selecionada como a opção de verificação ou a tarefa de verificação de vírus do Antivírus de Arquivos, os arquivos que tiverem as extensões listadas abaixo serão analisados quanto à presença de vírus. Estes tipos de arquivo também serão verificados pelo Antivírus de E-Mail se a verificação de anexos de mensagens estiver ativada:

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, como: *doc* – documento do Microsoft Office Word, *docx* – documento do Microsoft Office Word 2007 com suporte a XML, *docm* – documento do Microsoft Office Word 2007 com suporte de macro.

*dot** – modelo de documento do Microsoft Office Word, como *dot* – modelo de documento do Microsoft Office Word, *dotx* – modelo de documento do Microsoft Office Word 2007, *dotm* – modelo de documento do Microsoft Office Word 2007 com suporte de macro.

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, png – 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* – complemento do Microsoft Office Excel, *xlc* – diagrama, *xlt* – modelo de documento, *xlsx* – pasta de trabalho do Microsoft Office Excel 2007, *xltm* – pasta de trabalho do Microsoft Office Excel 2007 com suporte de macro, *xlsb* – Microsoft Office Excel 2007 em formato binário (não-XML), *xltx* – modelo do Microsoft Office Excel 2007, *xlsm* – modelo do Microsoft Office Excel 2007 com suporte de macro, *xlam* – complemento do Microsoft Office Excel 2007 com suporte de macro.

*pp** - documentos e arquivos do Microsoft Office PowerPoint, como: *pps* – slide do Microsoft Office PowerPoint, *ppt* – apresentação, *pptx* – apresentação do Microsoft Office PowerPoint 2007, *pptm* – apresentação do Microsoft Office PowerPoint 2007 com suporte de macro, *potx* – modelo de apresentação do Microsoft Office PowerPoint 2007, *potm* – modelo de apresentação do Microsoft Office PowerPoint 2007 com suporte de macro, *ppsx* – apresentação de slides do Microsoft Office PowerPoint 2007, *ppsm* – apresentação de slides do Microsoft Office PowerPoint 2007 com suporte de macro, *ppam* – complemento do Microsoft Office PowerPoint 2007 com suporte de macro.

*md** – documentos e arquivos do Microsoft Office Access, como: *mda* – grupo de trabalho do Microsoft Office Access, *mdb* – banco de dados, etc.

sldx – um slide do Microsoft PowerPoint 2007.

sldm – um slide do Microsoft PowerPoint 2007 com suporte de macro.

thmx – um tema do Microsoft Office 2007.

Lembre-se de que o formato real de um arquivo pode não corresponder ao formato indicado por sua extensão.

A.2. Máscaras de exclusão de arquivos válidos

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*.*** ou **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 *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 um tipo de ameaça excluído de acordo com a Enciclopédia de Vírus. Caso contrário, a ameaça especificada não será detectada em nenhum objeto. O uso dessas máscaras sem a seleção do tipo de ameaça 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. Máscaras de exclusão válidas de acordo com a classificação da Enciclopédia de Vírus

Ao adicionar ameaças com um determinado status na 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.

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 Lab News Agent

O News Agent destina-se ao envio oportuno de notícias publicadas pela Kaspersky Lab, de notificações sobre o status atual das atividades de vírus e notícias recentes. O programa lê a lista de feeds de notícias disponíveis e seu conteúdo no servidor de notícias da Kaspersky Lab com a freqüência especificada.

O News Agent permite:

- Ver a previsão de vírus atual na área de notificação da barra de tarefas
- Assinar e cancelar a assinatura de feeds de notícias
- Recuperar notícias de todos os feeds selecionados com a freqüência especificada e receber notificações sobre notícias recentes
- Examinar as notícias nos feeds selecionados
- Examinar a lista de feeds e seus status
- Abrir o texto completo do artigo no navegador

O News Agent é um aplicativo autônomo do Microsoft Windows que pode ser usado independentemente ou agregado com várias soluções integradas oferecidas pela Kaspersky Lab.

Kaspersky® OnLine Scanner

Este 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 sabem rapidamente as respostas às suas dúvidas referentes a possíveis infecções em seus computadores. Usando o serviço, os visitantes podem:

- Excluir arquivos comprimidos e bancos de dados de e-mail da verificação
- Selecionar bancos de dados 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 disponível para os visitantes do site corporativo da Kaspersky Lab. Ele oferece 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 padrão/estendido para a verificação
- Salvar um relatório sobre os resultados da verificação nos formatos txt ou html

Kaspersky® Internet Security 7.0

O Kaspersky® Internet Security 7.0 é uma solução integrada para a proteção de PCs contra as principais ameaças relacionadas a informações (vírus, hackers, spams e spyware). Os usuários podem configurar e gerenciar todos os componentes do programa em uma única interface.

Os recursos de proteção antivírus incluem:

- **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 (como Microsoft Office Outlook, Microsoft Outlook Express (Windows Mail) 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, pastas 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 monitora constantemente a atividade de aplicativos e 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 garantida pelo reconhecimento de ataques de phishing, o que ajuda a evitar vazamentos de dados confidenciais (principalmente todos os números de senhas, contas bancárias e cartões de crédito) e bloquear a execução de scripts perigosos em páginas da Web, janelas pop-up e banners de anúncios. O recurso de **bloqueio de discagem automática** ajuda a identificar softwares que tentam usar o modem para conexões não autorizadas ocultas com serviços telefônicos pagos e as bloqueia.

O Kaspersky Internet Security 7.0 **registra as tentativas de verificar as portas do computador** que freqüentemente antecedem ataques de rede, protegendo-o desses ataques com êxito. 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 o Modo Invisível, o sistema bloqueia toda a atividade de rede, exceto algumas transações permitidas nas regras definidas pelo usuário.

O programa utiliza uma abordagem inclusiva 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 aprendizagem
- Reconhecimento de spam enviado em arquivos de imagens

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 oferece verificações de vírus abrangentes, incluindo:

- **Verificação por demanda** da memória on-board do dispositivo móvel, de cartões de memória, pastas individuais ou arquivos específicos; se for detectado um arquivo infectado, ele será movido para a Quarentena ou excluído
- **Verificação em tempo real –** todos os arquivos enviados e recebidos são verificados automaticamente, assim como os arquivos acessados
- **Proteção contra spam em mensagens de texto**

Kaspersky Anti-Virus for File Servers

Este pacote de softwares oferece uma proteção confiável para sistemas de arquivos em servidores que executam o Microsoft Windows, Novell NetWare,

Linux e Samba contra todos os tipos de malware. O conjunto inclui os seguintes aplicativos da Kaspersky Lab:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server.
- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.
- Kaspersky Anti-Virus for Samba Server.

Recursos e funcionalidade:

- *Proteção dos sistemas de arquivos do servidor em tempo real*: Todos os arquivos do servidor são verificados ao serem abertos ou salvos no servidor
- *Prevenção de surtos de vírus*;
- *Verificações por demanda* de todo o sistema de arquivos ou de pastas e arquivos individuais;
- *Utilização de tecnologias de otimização* ao verificar objetos no sistema de arquivos do servidor;
- *Reversão do sistema após ataques de vírus*;
- *Escalabilidade do pacote de software* no escopo dos recursos do sistema disponíveis;
- *Monitoramento do balanceamento de carga do sistema*;
- *Criação de uma lista de processos confiáveis* cuja atividade no servidor não é controlada pelo pacote de software;
- *Administração remota* do pacote de software, incluindo a instalação, configuração e administração centralizada;
- *Gravação de cópias de backup de objetos infectados e excluídos* caso seja necessário restaurá-los;
- *Armazenamento de objetos suspeitos na Quarentena*;
- *Envio de notificações em eventos* de funcionamento do programa para o administrador do sistema;
- *Registro de relatórios detalhados*;
- *Atualização automática* dos bancos de dados do programa.

Kaspersky Open Space Security

O Kaspersky Open Space Security é um pacote de software com uma nova abordagem à segurança para as redes corporativas atuais de qualquer dimensão, oferecendo proteção centralizada dos sistemas de informação e suporte para escritórios remotos e usuários móveis.

O conjunto inclui quatro programas:

- Kaspersky WorkSpace Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

As especificidades de cada programa são apresentadas a seguir.

O **Kaspersky WorkSpace Security** é um programa para a proteção centralizada de estações de trabalho dentro e fora de redes corporativas contra todas as ameaças atuais da Internet (vírus, spyware, ataques de hackers e spam).

Recursos e funcionalidade:

- Proteção abrangente contra vírus, spyware, ataques de hackers e spam;
- Defesa Proativa contra novos programas mal-intencionados cujas assinaturas ainda não foram adicionadas ao banco de dados;
- Firewall Pessoal com sistema de detecção de intrusos e avisos sobre ataques de rede;
- Reversão de modificações mal-intencionadas ao sistema;
- Proteção contra ataques de phishing e lixo eletrônico;
- Redistribuição dinâmica de recursos durante as verificações completas do sistema;
- Administração remota do pacote de software, incluindo a instalação, configuração e administração centralizadas;
- Suporte para Cisco® NAC (Network Admission Control);
- Verificação de e-mails e do tráfego da Internet em tempo real;
- Bloqueio de janelas pop-up e banners de anúncios na Internet;
- Operação segura em qualquer tipo de rede, inclusive Wi-Fi;

- Ferramentas de criação de disco de recuperação que permitem restaurar o sistema após um surto de vírus;
- Um abrangente sistema de relatórios sobre o status da proteção;
- Atualizações automáticas do banco de dados;
- Suporte completo para sistemas operacionais de 64 bits;
- Otimização do desempenho do programa em notebooks (tecnologia Intel® Centrino® Duo);
- Recurso de desinfecção remota (Intel® Active Management, Intel® vPro™).

O **Kaspersky Business Space Security** oferece a proteção ideal para os recursos de informação de sua empresa contra as ameaças atuais da Internet. O Kaspersky Business Space Security protege estações de trabalho e servidores de arquivos de todos os tipos de vírus, cavalos de Tróia e worms, evita surtos de vírus e protege as informações, fornecendo acesso instantâneo aos recursos de rede.

Recursos e funcionalidade:

- Administração remota do pacote de software, incluindo a instalação, configuração e administração centralizadas;
- Suporte para Cisco® NAC (Network Admission Control);
- Proteção de estações de trabalho e servidores de arquivos de todos os tipos de ameaças da Internet;
- Tecnologia iSwift para evitar repetir a verificação de arquivos na rede;
- Distribuição de carga entre os processadores do servidor;
- Armazenamento de objetos suspeitos das estações de trabalho em quarentena;
- Reversão de modificações mal-intencionadas ao sistema;
- Escalabilidade do pacote de software no escopo dos recursos do sistema disponíveis;
- Defesa Proativa das estações de trabalho contra novos programas mal-intencionados cujas assinaturas ainda não foram adicionadas ao banco de dados;
- Verificação de e-mails e do tráfego da Internet em tempo real;
- Firewall Pessoal com sistema de detecção de intrusos e avisos sobre ataques de rede;

- Proteção ao usar redes Wi-Fi;
- Autodefesa contra programas mal-intencionados;
- Armazenamento de objetos suspeitos na Quarentena;
- Atualizações automáticas do banco de dados.

Kaspersky Enterprise Space Security

Este programa inclui componentes para a proteção de estações de trabalho e servidores conectados contra todas as ameaças atuais da Internet. Ele exclui vírus dos e-mails, mantendo as informações protegidas e fornecendo acesso seguro aos recursos de rede.

Recursos e funcionalidade:

- Proteção de estações de trabalho e servidores de arquivos contra vírus, cavalos de Tróia e worms;
- Proteção dos servidores de e-mail Sendmail, Qmail, Postfix e Exim;
- Verificação de todos os e-mails no Microsoft Exchange Server, incluindo as pastas compartilhadas;
- Processamento de e-mails, bancos de dados e outros objetos de servidores Lotus Domino;
- Proteção contra ataques de phishing e lixo eletrônico;
- Prevenção de envio de e-mails em massa e surtos de vírus;
- Escalabilidade do pacote de software no escopo dos recursos do sistema disponíveis;
- Administração remota do pacote de software, incluindo a instalação, configuração e administração centralizadas;
- Suporte para Cisco® NAC (Network Admission Control);
- Defesa Proativa das estações de trabalho contra novos programas mal-intencionados cujas assinaturas ainda não foram adicionadas ao banco de dados;
- Firewall Pessoal com sistema de detecção de intrusos e avisos sobre ataques de rede;
- Operação segura ao usar redes Wi-Fi;
- Verificação do tráfego da Internet em tempo real;
- Reversão de modificações mal-intencionadas ao sistema;

- Redistribuição dinâmica de recursos durante as verificações completas do sistema;
- Armazenamento de objetos suspeitos na Quarentena;
- Um abrangente sistema de relatórios sobre o status da proteção do sistema;
- Atualizações automáticas do banco de dados.

Kaspersky Total Space Security

Esta solução monitora todos os fluxos de dados enviados e recebidos (e-mail, Internet e todas as interações de rede). Ela inclui componentes para a proteção de estações de trabalho e dispositivo móveis, mantém as informações protegidas e oferece acesso seguro aos recursos de informação da empresa e à Internet, além de garantir comunicações seguras por e-mail.

Recursos e funcionalidade:

- Proteção abrangente contra vírus, spyware, ataques de hackers e spam em todos os níveis da rede corporativa, das estações de trabalho aos gateways da Internet;
- Defesa Proativa das estações de trabalho contra novos programas mal-intencionados cujas assinaturas ainda não foram adicionadas ao banco de dados;
- Proteção dos servidores de e-mail e servidores conectados;
- Verificação do tráfego da Internet (HTTP/FTP) que entra na rede local em tempo real;
- Escalabilidade do pacote de software no escopo dos recursos do sistema disponíveis;
- Bloqueio do acesso de estações de trabalho infectadas;
- Prevenção de surtos de vírus;
- Relatórios centralizados sobre o status da proteção;
- Administração remota do pacote de software, incluindo a instalação, configuração e administração centralizadas;
- Suporte para Cisco® NAC (Network Admission Control);
- Suporte para hardware de servidores proxy;
- Filtragem do tráfego da Internet usando uma lista de servidores, tipos de objetos e grupos de usuários confiáveis;

- Tecnologia iSwift para evitar repetir a verificação de arquivos na rede;
- Redistribuição dinâmica de recursos durante as verificações completas do sistema;
- Firewall Pessoal com sistema de detecção de intrusos e avisos sobre ataques de rede;
- Operação segura para usuários em qualquer tipo de rede, inclusive Wi-Fi;
- Proteção contra ataques de phishing e lixo eletrônico;
- Recurso de desinfecção remota (Intel® Active Management, Intel® vPro™);
- Reversão de modificações mal-intencionadas ao sistema;
- Autodefesa contra programas mal-intencionados;
- Suporte completo para sistemas operacionais de 64 bits;
- Atualizações automáticas do banco de dados.

Kaspersky Security for Mail Servers

Este programa protege servidores de e-mail e servidores conectados contra programas mal-intencionados e spam. O programa inclui aplicativos para a proteção de todos os servidores de e-mail padrão (Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix e Exim), além de permitir a configuração de um gateway de e-mail dedicado. A solução inclui:

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus for Lotus Notes/Domino.
- Kaspersky Anti-Virus for Microsoft Exchange.
- Kaspersky Anti-Virus for Linux Mail Server.

Seus recursos incluem:

- Proteção confiável contra programas mal-intencionados ou possivelmente perigosos;
- Filtragem de lixo eletrônico;
- Verificação de e-mails e anexos enviados e recebidos;
- Verificação de vírus em todos os e-mails no Microsoft Exchange Server, incluindo as pastas compartilhadas;

- Processamento de e-mails, bancos de dados e outros objetos de servidores Lotus Domino;
- Filtragem de e-mails por tipo de anexo;
- Armazenamento de objetos suspeitos na Quarentena;
- Sistema de administração fácil de usar;
- Prevenção de surtos de vírus;
- Monitoramento do status de proteção do sistema usando notificações;
- Sistema de relatórios de funcionamento do programa;
- Escalabilidade do pacote de software no escopo dos recursos do sistema disponíveis;
- Atualizações automáticas do banco de dados;

Kaspersky Security for Internet Gateways

Este programa oferece acesso seguro à Internet para todos os funcionários da organização, excluindo automaticamente os malwares e riskwares dos dados recebidos por HTTP/FTP. A solução inclui:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Proxy Server.
- Kaspersky Anti-Virus for Microsoft ISA Server.
- Kaspersky Anti-Virus for Check Point FireWall-1.

Seus recursos incluem:

- Proteção confiável contra programas mal-intencionados ou possivelmente perigosos;
- Verificação do tráfego da Internet (HTTP / FTP) em tempo real;
- Filtragem do tráfego da Internet usando uma lista de servidores, tipos de objetos e grupos de usuários confiáveis;
- Armazenamento de objetos suspeitos na Quarentena;
- Sistema de administração fácil de usar;
- Sistema de relatórios de funcionamento do programa;
- Suporte para hardware de servidores proxy;
- Escalabilidade do pacote de software no escopo dos recursos do sistema disponíveis;

- Atualizações automáticas do banco de dados.

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, onde monitora spams no tráfego de e-mail recebido, atua 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 em 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 Anti-Virus® for MIMESweeper

O Kaspersky Anti-Virus® for MIMESweeper fornece verificação em alta velocidade do tráfego em servidores que executam o Clearswift MIMESweeper for SMTP / Clearswift MIMEsweeper for Exchange / Clearswift MIMEsweeper for Web.

O programa é um plug-in e verifica vírus e processa 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	Internet: 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/DVD, 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/DVD, 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 7.0.

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/DVD-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 Você não poderá fornecer o código de ativação ou o arquivo da chave de licença a terceiros, nem permitir que terceiros tenham acesso a eles. O código de ativação e a chave de licença constituem-se em dados confidenciais.

1.1.8 A Kaspersky Lab pode solicitar que o Usuário instale a versão mais recente do Software (a versão e o pacote de manutenção mais recentes).

1.1.9 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).