KASPERSKY LAB

Kaspersky® Anti-Virus for Windows Workstations 6.0

MANUAL DO USUÁRIO

KASPERSKY ANTI-VIRUS FOR WINDOWS WORKSTATIONS 6.0

Manual do Usuário

http://www.kaspersky.com.br/

Data de revisão: julho de 2007

Sumário

CAPÍTULO 1. AMEAÇAS À SEGURANÇA DOS COMPUTADORES

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

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

Não são apenas as grandes empresas que correm riscos; usuários individuais também podem ser atacados. Os criminosos podem acessar dados pessoais (por exemplo, números e senhas de contas bancárias e de cartões de crédito) ou causar o mal funcionamento de um computador. Alguns tipos de ataques 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 quando você abre certas páginas da Web podem executar ações perigosas no seu computador, incluindo a

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

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

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

Intranet

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

E-mail

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

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

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

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

Mídia de armazenamento removível

As mídias removíveis (disquetes, CD-ROMs 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 for Windows Workstations.

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.

Quando um worm entra em um computador, ele verifica os endereços de rede dos outros computadores acessíveis localmente 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 a exclusão de informações em unidades, o travamento do sistema, o roubo de 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 computadores por si só. Eles são disseminados por hackers, que os disfarçam como softwares normais. Os danos causados por eles podem exceder em muito os ataques de vírus tradicionais.

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

Adware

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

Spyware

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

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

Riskware

O riskware inclui softwares que não possuem recursos mal-intencionados, mas que poderiam fazer parte do ambiente de desenvolvimento de programas mal-intencionados ou que 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

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

Rootkits

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

Outros programas perigosos

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

Ataques de hackers

Os ataques de hackers podem ser iniciados por hackers ou por programas mal-intencionados. Eles visam o roubo de informações residentes de um computador remoto, provocando o mau funcionamento do sistema ou controlando todos os recursos do mesmo. Você pode encontrar uma descrição detalhada dos tipos de ataques bloqueados pelo Kaspersky Anti-Virus for Windows Workstations na seção 12.9 na p. 167.

Alguns tipos de golpes on-line

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

solicitado que o usuário informe, por exemplo, o número do seu cartão de crédito e outras informações confidenciais.

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

Publicidade invasiva

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

Spam

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

Os spams aumentam significativamente a carga nos servidores de e-mail e o risco de perder dados importantes.

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

- *Reativo* – este método pesquisa arquivos mal-intencionados usando um banco de dados de assinaturas de ameaças atualizado periodicamente. Pelo menos uma infecção por vírus é necessária para implementar esse método, para que a assinatura da ameaça seja adicionada ao banco de dados e sua atualização seja distribuída.
- *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 de esses sintomas raramente indicarem a infecção do computador, é recomendável que, ao detectá-los, você execute uma verificação completa do computador (consulte a seção 5.2 na p. 65).

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 sistema operacional, criado na sua instalação.
4. Antes de qualquer coisa, faça o backup do seu trabalho em uma mídia de armazenamento removível (disquete, CD/DVD, unidade flash, etc.).
5. Instale o Kaspersky Anti-Virus for Windows Workstations, caso ainda o não tenha feito.
6. Atualize as assinaturas de ameaças do programa e os módulos do aplicativo (consulte a seção 5.6 na p. 69). Se possível, baixe as atualizações na Internet usando um outro computador não-infectado, por exemplo, de um amigo, em uma lan house ou no trabalho. É melhor usar outro computador, pois ao conectar um computador infectado à Internet, é possível que o vírus envie informações importantes para hackers ou dissemine o vírus para os endereços de seu catálogo de endereços. Por isso, se suspeitar que o computador está com vírus, desconecte-o imediatamente da Internet. Você também pode obter atualizações das assinaturas de ameaças em disquete junto à Kaspersky Lab ou seus distribuidores, e usá-las para fazer as atualizações.
7. Selecione o nível de segurança recomendado pelos especialistas da Kaspersky Lab.
8. Inicie uma verificação completa do computador (consulte a seção 5.2 na p. 65).

1.6. Evitando infecções

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

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.

As regras básicas de segurança são apresentadas a seguir. Siga essas regras para evitar ataques de vírus.

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

- Instale o Kaspersky Anti-Virus for Windows Workstations assim que possível.
- Atualize regularmente (consulte a seção 5.6 na p. 69) as assinaturas de ameaças do programa. No caso de surtos de vírus, atualize as assinaturas várias vezes por dia. Nessas situações, a Kaspersky Lab atualiza imediatamente as assinaturas de ameaças em seus servidores.
- Selecione as configurações de segurança recomendadas pela Kaspersky Lab para o seu computador. Você estará sempre protegido, desde o momento em que liga o computador, dificultando a infecção do mesmo por vírus.
- Selecione as configurações de verificação completa recomendadas pela Kaspersky Lab e programe verificações pelo menos uma vez por semana. Se ainda não tiver instalado o Anti-Hacker, é recomendável que o faça 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 5.4 na p. 67).
- 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 for Windows Workstations.
- Use seu bom-senso ao visitar sites da Web. Muitos sites estão infectados por vírus de script ou worms da Internet perigosos.

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

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

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

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

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

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

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

- Faça backup dos dados regularmente. No caso de perda de dados, o sistema poderá ser restaurado rapidamente, se você tiver cópias de backup. Guarde os disquetes, CDs, unidades flash e outras mídias de armazenamento de distribuição com software e informações importantes em um local seguro.
- Crie um Disco de Recuperação (consulte a seção 17.10 na p. 267) que possa ser usado para inicializar o sistema usando um sistema operacional limpo.

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

CAPÍTULO 2. KASPERSKY ANTI-VIRUS FOR WINDOWS WORKSTATIONS 6.0

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

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

2.1. Novidades do Kaspersky Anti-Virus for Windows Workstations 6.0

O Kaspersky Anti-Virus for Windows Workstations 6.0 representa uma 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, spam, ataques de hackers, ameaças desconhecidas, phishing e rootkits.

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

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

Vamos examinar os novos recursos do Kaspersky Anti-Virus for Windows Workstations mais detalhadamente:

Novos recursos de proteção

- O Kaspersky Anti-Virus for Windows Workstations o protege de programas mal-intencionados conhecidos e de programas ainda

desconhecidos. A Defesa Proativa (consulte a seção Capítulo 10 na p. 125) é a principal vantagem do programa. Ela analisa o comportamento dos aplicativos instalados no computador, monitorando as alterações do Registro do sistema, controlando as macros e combatendo ameaças ocultas. O componente usa um analisador heurístico para detectar e registrar vários tipos de atividade mal-intencionada; assim, as ações executadas por programas mal-intencionados podem ser revertidas e o sistema pode ser restaurado a seu estado anterior.

- O programa protege o computador de rootkits e discadores, bloqueia banners de anúncios, janelas pop-up e scripts mal-intencionados baixados de páginas da Web, além de detectar sites de phishing.
- A tecnologia do Antivírus de Arquivos foi aprimorada para diminuir a carga da CPU e aumentar a velocidade das verificações de arquivos. O iCheck™ e o iSwift™ ajudam a conseguir isso. 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.
- As áreas críticas do computador, cuja infecção afetaria seriamente a qualidade ou a segurança dos dados, possuem sua própria tarefa. Ela pode ser configurada para ser executada sempre que o sistema é iniciado.
- A proteção dos sistemas de e-mail contra spam e programas mal-intencionados foi aprimorada significativamente. O programa verifica e-mails contendo vírus e spam nestes protocolos:
    - IMAP, SMTP, POP3, independentemente do programa de e-mail utilizado
    - NNTP (somente verificação de vírus), independentemente do programa de e-mail
    - Independentemente do protocolo (MAPI, HTTP), ao usar plug-ins para o MS Outlook e o The Bat!
- Existem plug-ins específicos disponíveis para os programas de e-mail mais comuns, como o Outlook, o Microsoft Outlook Express (Windows Mail) e o The Bat!. Eles incorporam a proteção de e-mails contra vírus e spam diretamente no programa de e-mail.
- Agora, o Anti-Spam possui um modo de treinamento, baseado no algoritmo iBayes, que aprende através do monitoramento de como

você lida com seus e-mails. Ele também oferece o máximo de flexibilidade na configuração da detecção de spam; por exemplo, você pode criar uma lista negra e uma lista branca de destinatários e frases-chave que definem um e-mail como spam.

O Anti-Spam usa um banco de dados de phishing, que consegue filtrar os e-mails criados para obter informações financeiras confidenciais.

- O programa filtra o tráfego de entrada e de saída, rastreia e bloqueia ameaças de ataques de rede comuns e permite que você use a Internet no Modo Invisível.
- Ao usar uma combinação de redes, você também pode definir quais redes são totalmente confiáveis e quais devem ser monitoradas com extrema cautela.
- A função de notificação do usuário (consulte a seção 17.11.1 na p. 271) 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.
- Foi adicionada a verificação de dados transmitidos por conexões SSL seguras.
- Foram acrescentados ao programa recursos de autodefesa, incluindo proteção contra ferramentas de administração remota não autorizadas e configurações do programa protegidas por senha. Esses recursos ajudam a evitar que programas mal-intencionados, hackers e usuários não autorizados desabilitem a proteção.
- Você também pode criar um disco de recuperação, com o qual é possível reinicializar o sistema operacional após um ataque de vírus e verificar o computador quanto à presença de código mal-intencionado.
- Agora, o sistema de proteção tem a opção de administração remota centralizada, usando um administração adicional com interface pelo Kaspersky Administration Kit.

Recursos da nova interface do programa

- A nova interface do Kaspersky Anti-Virus for Windows Workstations 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 for Windows Workstations exibe mensagens informativas sobre o nível de proteção, acompanha sua operação com comentários e dicas, e inclui uma seção de Ajuda completa.

Novos recursos de atualização do programa

- Esta versão do programa inaugura o procedimento de atualização aprimorado: o Kaspersky Anti-Virus verifica automaticamente a fonte de atualizações. Se houver novas atualizações, o Anti-Virus 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.
- O programa possui um recurso de reversão da atualização que pode retornar para a versão anterior das assinaturas, se as assinaturas de ameaças estiverem danificadas ou se houver um erro na cópia.
- Foi adicionada uma ferramenta à Atualização que copia as atualizações em uma pasta local, para que outros computadores na rede possam acessá-las. Isso reduz o tráfego na Internet.

2.2. Os elementos da defesa do Kaspersky Anti-Virus for Windows Workstations

O Kaspersky Anti-Virus for Windows Workstations foi criado tendo em mente as fontes de ameaças. Em outras palavras, um componente separado do programa lida com cada ameaça, monitorando-a e tomando as medidas necessárias para evitar seus efeitos mal-intencionados sobre os dados do usuário. Isso torna o Security Suite flexível, com opções amigáveis para que cada componente se ajuste às necessidades de um usuário específico ou de uma empresa como um todo.

O Kaspersky Anti-Virus for Windows Workstations inclui:

- Componentes de proteção (consulte a seção 2.2.1 na p. 26), que fornecem uma defesa abrangente de todos os canais para transmissão e troca de dados no computador em tempo real.
- Tarefas de verificação de vírus (consulte 2.2.2 na p. 28) que verificam vírus na memória e no sistema de arquivos do computador, como arquivos individuais, pastas, discos ou regiões.

- Ferramentas de suporte (consulte 2.2.3 na p. 28) que dão suporte para o programa e ampliam sua funcionalidade.

2.2.1. Componentes de proteção

Estes componentes de proteção protegem seu computador em tempo real:

Antivírus de Arquivos

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

Antivírus de Arquivos é o componente que monitora o sistema de arquivos do computador. Ele verifica todos os arquivos que estão sendo abertos, executados ou salvos no computador e em todas as unidades de disco conectadas. Cada vez que um arquivo é acessado, o Kaspersky Anti-Virus o intercepta e o verifica quanto à presença de vírus conhecidos. Se, por algum motivo, não for possível desinfectar um arquivo, ele será excluído e uma cópia do mesmo será salva no Backup (consulte 17.2 na p. 237) ou ele será movido para a Quarentena (consulte 17.1 na p. 233).

Antivírus de E-Mail

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

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

Antivírus da Web

Ao abrir vários sites na Internet, existe o risco de infectar o computador com vírus instalados com scripts que estão armazenados nas páginas da Web. Você também pode baixar um arquivo perigoso para o computador.

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

Defesa Proativa

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

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

Anti-Spy

Programas que exibem publicidade não desejada (por exemplo, banners de anúncios e janelas pop-up), programas que ligam para números de serviços pagos da Internet sem a autorização do usuário, ferramentas de monitoração e administração remota, programas de piadas, etc. estão se tornando cada vez mais comuns.

O *Anti-Spy* rastreia essas ações no computador e as bloqueia. Por exemplo, o componente bloqueia banners de anúncios e janelas pop-up, bloqueia programas que tentam fazer discagens automáticas e analisa páginas da Web quanto à presença de conteúdo de phishing.

Anti-Hacker

Os hackers utilizarão qualquer possível brecha para invadir seu computador, seja uma porta aberta, a transmissão de dados entre computadores, etc.

O componente *Anti-Hacker* protege o computador enquanto você usa a Internet e outras redes. Ele monitora as conexões de entrada e de saída, e verifica portas e pacotes de dados.

Anti-Spam

Embora não representem uma ameaça direta ao seu computador, os spams sobrecarregam os servidores de e-mail, enchem a caixa de entrada de e-mail e desperdiçam seu tempo, representando um prejuízo para seus negócios.

O componente *Anti-Spam* se conecta ao programa de e-mail do computador e procura material sujeito a spam em todos os e-mails recebidos. O componente marca todos os spams com um cabeçalho específico. O Anti-Spam pode ser configurado para processar os spams da forma desejada (excluir automaticamente, mover para uma pasta específica, etc.).

2.2.2. Tarefas de verificação de vírus

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

O Kaspersky Anti-Virus for Windows Workstations configura, por padrão, as seguintes tarefas de verificação de vírus:

Áreas críticas

Verifica todas as áreas críticas do computador quanto à presença de vírus. Isso inclui a memória do sistema, os programas carregados na inicialização, os setores de inicialização no disco rígido e os diretórios do sistema do *Microsoft Windows*. Essa tarefa tem como objetivo detectar vírus ativos rapidamente 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 automaticamente na inicialização, além da RAM e dos setores de inicialização dos discos rígidos.

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

2.2.3. Ferramentas de programas

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

Atualização

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

O recurso de distribuição de atualizações salva atualizações de assinaturas de ameaças e de módulos do aplicativo recuperadas dos servidores de atualização da Kaspersky Lab em uma pasta local. Então, ele permite que outros computadores na rede as acessem, economizando largura de banda da Internet.

Arquivos de dados

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

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

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

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

Disco de Recuperação

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

Suporte

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

Usando estes links, é possível acessar o fórum de usuários da Kaspersky Lab e uma lista de perguntas freqüentes que podem ajudá-lo a resolver problemas. Além disso, ao preencher o formulário no site, você pode enviar uma mensagem para o Suporte Técnico sobre o erro ou a falha no funcionamento do aplicativo.

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

2.3. Requisitos de hardware e software do sistema

Para que o Kaspersky Anti-Virus for Windows Workstations 6.0 seja executado corretamente, o computador deve atender aos seguintes requisitos mínimos:

Requisitos gerais:

- 50 MB de espaço livre no disco rígido
- Unidade de CD-ROM (para instalar o Kaspersky Anti-Virus for Windows Workstations 6.0 de um CD de instalação)
- Microsoft Internet Explorer 5.5 ou superior (para atualizar as assinaturas de ameaças e módulos do programa pela Internet)
- Microsoft Windows Installer 2.0

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

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

Microsoft Windows 2000 Professional (Service Pack 4 ou superior), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 1 ou superior), Microsoft Windows XP Professional x64 Edition:

- Processador Intel Pentium 300 MHz ou 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 for Windows Workstations na caixa junto a nossos revendedores ou baixá-la de lojas da Internet, incluindo a seção **Loja Virtual** em www.kaspersky.com.br.

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

- Um envelope lacrado contendo um CD de instalação com os arquivos do programa
- Uma chave de licença fornecida com o pacote de instalação ou em um disquete específico, ou um código de ativação do aplicativo na embalagem do CD
- Um Manual do Usuário
- 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 for Windows Workstations 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 uma chave de licença ou 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 uma variedade de serviços que tornam o Kaspersky Anti-Virus for Windows Workstations mais efetivo para seus usuários registrados.

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

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

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

CAPÍTULO 3. INSTALANDO O KASPERSKY ANTI-VIRUS FOR WINDOWS WORKSTATIONS 6.0

Há diversas formas de instalar o Kaspersky Anti-Virus for Windows Workstations:

- Instalação local: instala o aplicativo em um único host. É necessário ter acesso direto a esse host para executar e concluir a instalação. É possível executar uma instalação local em um dos modos a seguir:
    - instalação interativa usando o Assistente para Instalação do aplicativo (consulte a seção 3.1 na p. 34); esse modo exige a participação do usuário para a continuidade da instalação;
    - instalação não interativa, executada da linha de comando, sem exigir a participação do usuário para a continuidade da instalação (consulte a seção 3.3 na p. 48).
- Instalação remota: instala o aplicativo nos aplicativos em rede remotamente, da estação de trabalho do administrador, usando:
    - o conjunto de software Kaspersky Administration Kit (consulte o Manual de Implantação do Kaspersky Administration Kit);
    - diretivas de domínio de grupo do Microsoft Windows Server 2000/2003 (consulte a seção 3.4 na p. 49).

É recomendável fechar todos os aplicativos em execução antes de instalar o Kaspersky Anti-Virus (inclusive na instalação remota).

No caso de o Kaspersky Anti-Virus 5.0 já estar instalado, ele será removido e atualizado para o Kaspersky Anti-Virus 6.0 ao executar o procedimento de instalação (para obter mais detalhes, consulte a seção 3.5 na p. 51). As atualizações para compilações mais recentes (versões secundárias) do Kaspersky Anti-Virus 6.0 são transparentes.

3.1. Procedimento de instalação usando o Assistente para Instalação

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

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

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

- **Avançar** – aceita uma ação e avança para a próxima etapa da instalação.
- **Voltar** – volta para a etapa anterior da instalação.
- **Cancelar** – cancela a instalação do produto.
- **Concluir** – conclui o procedimento de instalação do programa.

Vamos examinar as etapas do procedimento de instalação mais detalhadamente.

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

Antes de o programa ser instalado no computador, o sistema operacional e os pacotes de serviços necessários para a instalação do Kaspersky Anti-Virus for Windows Workstations são verificados no computador. 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 for Windows Workstations.

Etapa 2. Janela de boas-vindas da instalação

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

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

Etapa 3. Exibindo o Contrato de Licença do Usuário Final

A janela a seguir contém o Contrato de Licença do Usuário Final firmado 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 no botão **Cancelar**.

Etapa 4. Selecionando uma pasta de instalação

O próximo estágio da instalação do Kaspersky Anti-Virus for Windows Workstations determina o local onde o programa será instalado no computador. O caminho padrão é o seguinte:

- **<unidade> → Arquivos de Programas → Kaspersky Lab → Kaspersky Anti-Virus 6.0 for Windows Workstations** – para sistemas de 32 bits.
- **<unidade> → Arquivos de Programas (x86) → Kaspersky Lab → Kaspersky Anti-Virus 6.0 for Windows Workstations** – para sistemas de 64 bits.

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

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

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

Etapa 5. Usando as configurações de instalação salvas

Nesta etapa, é solicitado que você especifique se deseja usar as configurações de segurança, as assinaturas de ameaças e os bancos de dados do Anti-Spam

salvos anteriormente, caso eles tenham sido realmente salvos ao remover uma instalação anterior do Kaspersky Anti-Virus 6.0 do computador.

Vamos examinar mais detalhadamente como usar as opções descritas acima.

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

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

Também é recomendável usar a base de dados do Anti-Spam, se você a salvou ao desinstalar a versão anterior do programa. Dessa maneira, não será necessário treinar o Anti-Spam novamente. Para usar a base de conhecimento já criada, marque **Base de dados de conhecimento do Anti-Spam**.

Etapa 6. Selecionando um tipo de instalação

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

Completa. Se você selecionar esta opção, todos os componentes do Kaspersky Anti-Virus for Windows Workstations serão instalados. A instalação recomeçará com Etapa 8.

Personalizada. Se você selecionar esta opção, poderá selecionar os componentes do programa que deseja instalar. Para saber mais, consulte a Etapa 7.

Recursos antivírus. Esta opção instala apenas os componentes que o protegem contra vírus. O Anti-Hacker, o Anti-Spam e o Anti-Spy não serão instalados.

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

Etapa 7. Selecionando os componentes do programa a serem instalados

Esta etapa será executada somente se você selecionar o tipo de instalação **Personalizada**.

Se você selecionou a instalação Personalizada, poderá selecionar os componentes do Kaspersky Anti-Virus for Windows Workstations que deseja instalar. Por padrão, todos os componentes de proteção, assim como o conector

do Agente Administrativo para administração remota usando o Kaspersky Administration Kit são selecionados para a instalação.

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

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

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

Etapa 8. Desabilitando o firewall do Microsoft Windows

Você só passará por esta etapa se estiver instalando o componente Anti-Hacker do Kaspersky Anti-Virus for Windows Workstations em um computador com o firewall interno habilitado.

Nesta etapa, o Kaspersky Anti-Virus for Windows Workstations pergunta se você deseja desabilitar o Firewall do Windows, pois o componente Anti-Hacker do Kaspersky Anti-Virus for Windows Workstations fornece proteção de firewall integral.

Se desejar usar o Anti-Hacker como principal ferramenta de segurança da navegação, clique em **Avançar**. O Firewall do Windows será desabilitado automaticamente.

Se desejar usar o Firewall do Windows, selecione **Manter o Firewall do Windows habilitado**. Se esta opção for selecionada, o Anti-Hacker será instalado, mas ficará desabilitado para evitar conflitos nos programas.

Etapa 9. 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 for Windows Workstations.

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.

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

Etapa 10. Concluindo a instalação do programa

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

Ao instalar inicialmente o Kaspersky Anti-Virus 6.0, não é recomendável desmarcar ☑ **Habilitar Autodefesa antes da instalação**. A habilitação dos módulos de proteção permitirá que a instalação seja revertida corretamente, caso ocorram erros ao instalar o aplicativo. Se você tentar instalar o aplicativo novamente, é recomendável desmarcar esta 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 corretamente.

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

Aviso!

Ao instalar os componentes do Kaspersky Anti-Virus que interceptam o tráfego de rede, as conexões de rede atuais são desfeitas. A maioria delas será recuperada após algum tempo.

Etapa 11. Concluindo o procedimento de instalação

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

Para iniciar o Assistente para Instalação, clique no botão **Avançar** (consulte a seção 3.2 na p. 38).

Se a instalação for concluída com êxito, será necessário reiniciar o computador e uma mensagem na tela o informará.

3.2. Assistente para Instalação

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

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

Você pode ignorar este estágio de configurações iniciais ao instalar o programa, fechando a janela do Assistente. No futuro, você poderá executá-lo novamente a partir da interface do programa, se restaurar as configurações padrão do Kaspersky Internet Security (consulte 17.3 na p. 239).

3.2.1. Usando objetos salvos na Versão 5.0

Esta janela do assistente será exibida ao instalar o aplicativo sobre o Kaspersky Anti-Virus 5.0. Será solicitado que você selecione os dados usados pela verão 5.0 que deseja importar para a versão 6.0. Podem estar incluídos os arquivos da quarentena ou do backup, ou as configurações de proteção.

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

3.2.2. Ativando o programa

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

O programa é ativado pela instalação de uma chave de licença que será usada pelo Kaspersky Anti-Virus para verificar a licença e determinar sua data de validade.

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

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

3.2.2.1. Selecionando um método de ativação do programa

Dependendo de você possuir uma chave de licença do Kaspersky Anti-Virus ou precisar obtê-la do servidor da Kaspersky Lab, diferentes opções para ativar o programa estarão disponíveis:

- **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 completa do aplicativo durante a vigência do contrato de licença.
- **Ativar versão de teste.** Selecione esta opção de ativação para instalar a versão de teste do programa antes de decidir comprar a versão comercial. Você receberá uma chave de licença gratuita válida por um período especificado no contrato de licença da versão de teste.
- **Aplicar chave de licença existente**. Ativa o aplicativo usando um arquivo de chave de licença do Kaspersky Anti-Virus 6.0.
- **Ativar mais tarde**. Se você escolher esta opção, o estágio de ativação será ignorado. O Kaspersky Anti-Virus for Windows Servers 6.0 será instalado no computador e você terá acesso a todos os recursos do programa, exceto as atualizações (é possível atualizar as assinaturas de ameaças somente depois de instalar o programa).

As duas primeiras opções de ativação utilizam um servidor Web da Kaspersky Lab, o que exige uma conexão com a Internet. Antes da ativação, edite suas configurações de rede (consulte a seção 16.4.3 na p. 227) na janela que é aberta ao clicar em **Configurações da LAN**, se necessário. Para obter informações mais detalhadas sobre a configuração da rede, entre em contato com o administrador do sistema ou seu provedor.

Se não houver uma conexão com a Internet ao instalar o programa, você poderá ativar o aplicativo posteriormente (consulte 17.5 na p. 257) usando sua interface ou poderá utilizar o acesso à Internet de outro computador para se registrar no site de Suporte Técnico da Kaspersky Lab e obter a chave usando o código de ativação.

3.2.2.2. Inserindo o código de ativação

É necessário ter um código para ativar o programa. Ao comprar o programa pela Internet, você receberá o código de ativação por e-mail. Se comprou uma versão do programa na caixa, encontrará o código de ativação no envelope do CD-ROM de instalação.

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

Digite suas informações de contato na parte inferior da janela: nome completo, endereço de e-mail, país e cidade de residência. Essas informações poderão ser solicitadas para identificar um usuário registrado se, por exemplo, uma chave for

perdida ou roubada. Caso isso ocorra, suas informações de contato permitirão que você obtenha uma nova chave de licença.

3.2.2.3. Obtendo um arquivo de chave

O Assistente para Instalação se conecta aos servidores da Kaspersky Lab e envia seus dados de registro (o código de ativação e as informações pessoais), que são inspecionados no servidor.

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 para Instalação receberá o arquivo da chave de teste sem um código de ativação.

O arquivo recebido será instalado automaticamente para executar o programa e você verá uma janela de conclusão da ativação com informações detalhadas sobre a chave usada.

Se o código de ativação não passar na inspeção, você verá uma mensagem correspondente na tela. Se isso ocorrer, entre em contato com o fornecedor do software de quem você comprou o programa para obter mais informações.

3.2.2.4. Selecionando o arquivo da chave de licença

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

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

3.2.2.5. Concluindo a ativação do programa

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

3.2.3. Selecionando um modo de segurança

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

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

Interativo. Este modo fornece uma defesa mais personalizada dos dados do seu computador que a do Modo Básico. Ele controla tentativas de modificar as configurações do sistema, atividades suspeitas no sistema e atividades autorizadas na rede.

Todas essas atividades poderiam ter sido iniciadas por programas mal-intencionados ou ser uma atividade padrão de alguns dos programas usados no computador. Será necessário decidir caso a caso se essas atividades devem ser permitidas ou bloqueadas.

Se optar por este modo, especifique em que contextos ele deve ser usado:

- **Habilitar o modo de treinamento do Anti-Hacker** – solicita a confirmação do usuário quando programas instalados no computador tentarem se conectar a determinados recursos de rede. Você pode permitir ou bloquear essa conexão e configurar uma regra do Anti-Hacker para esse programa. Se o modo de treinamento for desabilitado, o Anti-Hacker será executado com configurações mínimas de proteção, ou seja, todos os aplicativos terão acesso aos recursos da rede.
- **Habilitar Proteção do Registro** – pergunta o que fazer ao serem detectadas tentativas de modificar 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 Defesa Proativa Estendida** – analisa todas as atividades suspeitas de aplicativos no sistema, incluindo a abertura de navegadores com configurações da linha de comando, infiltração em processos de aplicativos e interceptação de ganchos de janelas (por padrão, esta opção não é selecionada).

3.2.4. Configurando a atualização

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

- **Automaticamente**. O Kaspersky Anti-Virus verifica a fonte de atualizações em intervalos definidos. Durante os surtos de vírus, a freqüência dessa verificação pode aumentar, sendo diminuída ao final. Se houver novas atualizações, o Anti-Virus as baixa e instala no computador. Essa é a configuração padrão.
- **A cada 2 hora(s)**. As atualizações serão executadas automaticamente de acordo com a programação criada. Você pode configurar a programação clicando em **Editar**.
- **Manualmente**. Se escolher esta opção, você mesmo executará as atualizações do produto.

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

Para configurar as atualizações (configurar propriedades de rede, selecionar o recurso do qual as atualizações serão baixadas, configurar a tarefa de execução com uma determinada conta ou habilitar a opção de distribuição de atualizações), clique em **Configurações**.

3.2.5. Configurando uma programação de verificação de vírus

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

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

Objetos de inicialização

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

Áreas críticas

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

A configuração padrão dessa verificação automática é desabilitada.

Meu 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

O Kaspersky Anti-Virus permite que você proteja o programa por senha, pois várias pessoas com níveis diferentes de experiência em informática podem usar o mesmo computador e os programas mal-intencionados poderiam possivelmente desabilitar a proteção. O uso de uma senha pode proteger o programa de tentativas não-autorizadas de desabilitar a proteção ou alterar as configurações.

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

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

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

☑ **Ao interromper/pausar componentes de proteção ou tarefas de verificação de vírus** – solicita a senha se o usuário tentar pausar ou desabilitar completamente qualquer componente de proteção ou tarefa de verificação de vírus.

3.2.7. Configurando o Anti-Hacker

O Anti-Hacker é o componente do Kaspersky Anti-Virus for Windows Workstations que protege o computador em redes locais e na Internet. Neste estágio, o Assistente para Instalação pede que você crie uma lista de regras que direcionará o Anti-Hacker ao analisar a atividade de rede do computador.

3.2.7.1. Determinando o status de uma zona de segurança

Neste estágio, o Assistente para Instalação analisa o ambiente de rede do computador. Com base nessa análise, todo o espaço da rede é dividido em zonas:

Internet – a World Wide Web. Nessa zona, o Kaspersky Anti-Virus for Windows Workstations funciona como um firewall pessoal. Dessa forma, as regras padrão para filtragem de pacotes e aplicativos ajustam toda a atividade da rede para assegurar o máximo de segurança. Não é possível alterar as configurações de proteção ao trabalhar nessa zona, além de habilitar o Modo Invisível no computador para melhorar a segurança.

Zonas de segurança – determinadas zonas que correspondem, na maioria, às sub-redes que incluem seu computador (poderiam ser sub-redes locais em casa ou no trabalho). Por padrão, essas zonas têm um nível de risco médio. Você pode alterar o status dessas zonas com base na confiança que tem em uma determinada sub-rede, sendo possível configurar regras para a filtragem de pacotes e para aplicativos.

Todas as zonas detectadas serão exibidas em uma lista. Cada uma delas é mostrada com uma descrição, seu endereço e uma máscara de sub-rede, além do grau com o qual qualquer atividade de rede será permitida ou bloqueada pelo Anti-Hacker.

- **Internet**. Este é o status padrão atribuído à Internet pois, quando você está conectado a ela, seu computador está sujeito a todos os possíveis tipos de ameaças. Esse status também é recomendado para redes que não são protegidas por nenhum programa antivírus, firewall, filtro etc. Ao selecionar esse status, o programa garante o máximo de segurança enquanto você estiver usando essa zona, especificamente:

- bloqueando todas as atividades de rede do NetBios na sub-rede
- bloqueando regras para aplicativos e filtragem de pacotes que permitem a atividade do NetBios nessa sub-rede

Mesmo que você tenha criado uma pasta compartilhada, as informações contidas nela não estarão disponíveis aos usuários de sub-redes com esse status. Além disso, se esse status estiver selecionado para uma determinada sub-rede, você não poderá acessar os arquivos e impressoras dessa sub-rede.

- **Rede Local**. O programa atribui este status à maioria das zonas de segurança detectadas ao analisar o ambiente de rede do computador, exceto a Internet. É recomendável aplicar esse status às zonas com um fator de risco médio (por exemplo, redes locais corporativas). Se você selecionar esse status, o programa permitirá:
  - qualquer atividade de rede do NetBios na sub-rede
  - regras para aplicativos e filtragem de pacotes que permitem a atividade do NetBios nessa sub-rede

  Selecione este status para conceder acesso a determinadas pastas ou impressoras no computador e bloquear qualquer outra atividade externa.
- **Confiável (permitir todas as conexões).** Este status é concedido às redes que você considerar absolutamente seguras, de forma que o computador não estará sujeito a ataques e tentativas de obter acesso aos seus dados enquanto estiver nela. Ao usar este tipo de rede, toda a atividade de rede é permitida. Mesmo que você tenha selecionado Proteção Máxima e tiver criado regras de bloqueio, elas não funcionarão para computadores remotos de uma rede segura.

Você pode usar o *Modo Invisível* para aumentar a segurança ao usar redes rotuladas como **Internet**. Este recurso permite apenas a atividade de rede iniciada do computador, ou seja, ele se torna invisível para suas imediações. Esse modo não afeta o desempenho do computador na Internet.

O Modo Invisível não é recomendável ao usar o computador como servidor (por exemplo, um servidor de e-mail ou HTTP), pois os computadores que tentarem se conectar ao servidor não o verão como conectado.

Para alterar o status de uma zona ou para habilitar/desabilitar o Modo Invisível, selecione a zona na lista e use os links apropriados na caixa **Descrição da regra** abaixo da lista. É possível executar tarefas semelhantes e editar endereços e máscaras de sub-rede na janela **Configurações de zona**, que pode ser aberta clicando em **Editar**.

Uma nova zona pode ser adicionada à lista ao exibi-la. Para fazê-lo, clique em **Localizar**. O Anti-Hacker pesquisará as zonas disponíveis e, se detectar alguma, o programa solicitará que você selecione um status para elas. Além disso, você pode adicionar novas zonas à lista manualmente (se conectar o seu laptop a uma nova rede, por exemplo). Para fazê-lo, use o botão **Adicionar** e preencha as informações necessárias na janela **Configurações de zona**.

Para excluir uma rede da lista, clique no botão **Excluir**.

3.2.7.2. Criando uma lista de aplicativos de rede

O Assistente para Instalação analisa os softwares instalados no computador e cria uma lista de aplicativos que usam conexões de rede.

O Anti-Hacker cria uma regra para controlar a atividade de rede de cada um desses aplicativos. As regras são aplicadas usando modelos para aplicativos de rede comuns, criados na Kaspersky Lab e fornecidos com o software.

Você pode exibir a lista de aplicativos de rede e suas regras na janela de configurações do Anti-Hacker, que pode ser aberta clicando em **Listar**.

Para aumentar a segurança, é recomendável desabilitar o cache de DNS ao usar recursos da Internet. O cache de DNS reduz drasticamente o tempo que o computador fica conectado a este importante recurso da Internet; entretanto, ele também constitui uma vulnerabilidade perigosa que os hackers podem explorar para criar vazamentos de dados que não podem ser rastreados pelo firewall. Assim, para aumentar o grau de segurança do computador, é recomendável desabilitar o cache de DNS.

3.2.8. Concluindo o Assistente para Instalação

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

Alguns componentes do programa não funcionarão até a reinicialização.

3.3. Instalando o programa do prompt de comando

Para instalar o Kaspersky Anti-Virus 6.0 for Windows Workstations, digite o seguinte no prompt de comando:

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

O Assistente para Instalação será iniciado (consulte a seção 3.1 na p. 34). Depois que o programa for instalado, reinicie o computador.

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

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

Esta opção exigirá a reinicialização manual da máquina após a conclusão da instalação. Para executar a reinicialização automática da linha de comando, digite:

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

No modo não interativo, a reinicialização ocorrerá automaticamente (usando a chave /qn).

Para instalar o aplicativo com uma senha de desinstalação, digite:

`msiexec /i <nome_do_pacote> KLUNINSTPASSWD=******`, ao executar uma instalação interativa;

`msiexec /i <nome_do_pacote> KLUNINSTPASSWD=****** /qn`, ao executar uma instalação não interativa sem inicialização do sistema;

`msiexec /i <nome_do_pacote> KLUNINSTPASSWD=****** ALLOWREBOOT=1 /qn`, ao executar uma instalação não interativa com inicialização do sistema;

Se você instalar o Kaspersky Anti-Virus no modo não interativo, poderá acessar o arquivo *setup.ini*, que contém as configurações gerais para a instalação do aplicativo (consulte a seção A.4 na p. 327), a configuração *install.cfg* (consulte a seção 18.8 na p. 295) e o arquivo da chave de licença. Esses arquivos devem estar localizados na mesma pasta que o pacote de instalação do Kaspersky Anti-Virus.

3.4. Procedimento para a instalação do Objeto de Diretiva de Grupo

Há suporte para este recurso em computadores que executam o Microsoft Windows 2000 ou superior.

Com o **Editor de Objeto de Diretiva de Grupo**, você pode instalar, atualizar e desinstalar o Kaspersky Anti-Virus em estações de trabalho empresariais no domínio sem usar o Kaspersky Administration Kit.

3.4.1. Instalando o programa

Para instalar o Kaspersky Anti-Virus:

1. Crie uma pasta compartilhada no computador que é o controlador de domínio e copie o pacote de instalação *.msi* do Kaspersky Anti-Virus para ela.

   Você também pode copiar o arquivo *setup.ini*, que contém as configurações gerais para a instalação do aplicativo (consulte A.4 na p. 327), a configuração *install.cfg* (consulte 18.7 na p. 294) e o arquivo da chave de licença.

2. Abra o **Editor de Objeto de Diretiva de Grupo** via MMC (para obter informações mais detalhadas sobre o uso do Objeto de Diretiva de Grupo, consulte a ajuda do Microsoft Windows Server).

3. Crie um novo pacote. Para fazê-lo, na árvore do console, selecione **Objeto de Diretiva de Grupo** / **Configuração do Computador** / **Configurações de Software** / **Instalação de software** e use o comando **Novo** / **Pacote** no menu de contexto.

   Na janela que é aberta, especifique o caminho da pasta compartilhada no instalador do Anti-Virus (veja 1). Selecione **Atribuir** na caixa de diálogo **Selecione o Método de Implantação** e clique em **OK**.

A diretiva de grupo será imposta em cada estação de trabalho da próxima vez que o computador for registrado no domínio. Então, o Kaspersky Anti-Virus será instalado em todos os computadores.

3.4.2. Atualizando o programa

Para atualizar o Kaspersky Anti-Virus:

1. Copie o pacote do instalador que contém a atualização do Kaspersky Anti-Virus no formato .msi para a pasta compartilhada.
2. Abra o **Editor de Objeto de Diretiva de Grupo** e crie um novo pacote usando as etapas acima.
3. Selecione o novo pacote e, em seguida, o comando **Propriedades** no menu de contexto. Na janela de propriedades do pacote, vá para a guia **Atualizações** e especifique o pacote que contém o instalador da versão anterior do Kaspersky Anti-Virus. Para instalar a atualização do Kaspersky Anti-Virus e manter as configurações da proteção, selecione esta opção ao atualizar a versão anterior.

A diretiva de grupo será imposta em cada estação de trabalho da próxima vez que o computador for registrado no domínio.

Não é possível atualizar o Kaspersky Anti-Virus com o Editor de Objeto de Diretiva de Grupo em computadores que executam o Microsoft Windows 2000 Professional.

3.4.3. Desinstalando o programa

Para desinstalar o Kaspersky Anti-Virus:

1. Abra o **Editor de Objeto de Diretiva de Grupo**.
2. Para fazê-lo, na árvore do console, selecione **Objeto de Diretiva de Grupo** / Configuração do Computador / Configurações de Software / Instalação de software.

   Selecione o pacote do Kaspersky Anti-Virus na lista. Abra o menu de contexto e selecione o comando **Todas as Tarefas** / **Remover**.

   Na caixa de diálogo **Remover Software**, selecione **Desinstalar imediatamente o software dos usuários e computadores** para que o Kaspersky Anti-Virus seja desinstalado da próxima vez que o computador for reiniciado.

3.5. Atualizando da versão 5.0 para a versão 6.0

Se o Kaspersky Anti-Virus 5.0 for Windows Workstations estiver instalado no seu computador, você poderá atualizá-lo para o Kaspersky Anti-Virus 6.0.

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

Aviso!

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

CAPÍTULO 4. INTERFACE DO PROGRAMA

O Kaspersky Anti-Virus for Windows Workstations possui uma interface direta e amigável. Este capítulo aborda seus recursos básicos:

- Ícone da bandeja do sistema (consulte a seção 4.1 na p. 52)
- Menu de contexto (consulte a seção 4.2 na p. 53)
- Janela principal (consulte a seção 4.3 na p. 55)
- Janela de configurações do programa (consulte a seção 4.4 na p. 57)

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

- Microsoft Office Outlook – verificação de vírus (consulte a seção 8.2.2 na p. 110) e verificação de spam (consulte a seção 13.3.8 na p. 192)
- Microsoft Outlook Express (Windows Mail) (consulte a seção 13.3.9 na p. 195)
- The Bat! – verificações de vírus (consulte a seção 8.2.3 na p. 112) e verificações de spam (consulte a seção 13.3.10 na p. 196)
- Microsoft Internet Explorer (consulte Capítulo 11 na p. 140)
- Microsoft Windows Explorer (consulte a seção 14.2 na p. 200)

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

4.1. Ícone da bandeja do sistema

Logo após a instalação do Kaspersky Anti-Virus for Windows Workstations, o ícone do programa aparecerá na bandeja do sistema.

O ícone indica as funções do Kaspersky Anti-Virus for Windows Workstations. Ele reflete o status da proteção e mostra várias funções básicas executadas pelo programa.

Se o ícone estiver ativo (colorido), seu computador estará protegido. Se o ícone estiver inativo (preto e branco), isso indica que todos os componentes de proteção (consulte a seção 2.2.1 na p. 26) estão desabilitados.

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

	Os e-mails estão sendo verificados.
	Os scripts estão sendo verificados.
	Um arquivo que você ou algum programa está abrindo, salvando ou executando está sendo verificado.
	as assinaturas de ameaças e módulos do Kaspersky Anti-Virus for Windows Workstations estão sendo atualizados.
	Ocorreu um erro em algum componente do Kaspersky Anti-Virus.

O ícone também dá acesso aos principais itens da interface do programa: o menu de contexto (consulte a seção 4.2 na p. 53) e a janela principal (consulte a seção 4.3 na p. 55).

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

4.2. O menu de contexto

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

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

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

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

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

Figura 1. O menu de contexto

Atualização – inicia a atualização dos módulos do programa e das assinaturas de ameaças, e os instala no computador.

Monitor de Rede – exibe a lista de conexões estabelecidas, portas abertas e o tráfego de rede.

Ativar – ativa o programa. É necessário ativar sua versão do Kaspersky Internet Security 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 for Windows Workstations.

Abrir o Kaspersky Anti-Virus – abre a janela principal do programa (consulte 4.3 na p. 55).

Pausar a Proteção / Reiniciar a Proteção – desabilita temporariamente ou habilita os componentes de proteção (consulte 2.2.1 na p. 26). Este item do menu não afeta tarefas de atualização do programa ou de verificação de vírus.

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

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

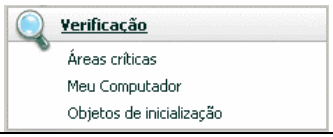
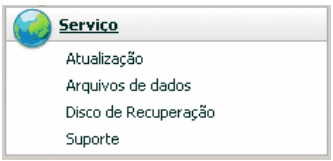
A janela principal do Kaspersky Anti-Virus for Windows Workstations (veja a Figura 2) pode ser dividido logicamente em duas partes:

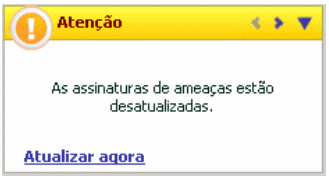
- à esquerda da janela, o painel de navegação o orienta de maneira rápida e fácil para qualquer componente, o desempenho da tarefa de atualização e verificação de vírus ou as ferramentas de suporte do programa;
- à direita da janela, o painel informativo contém informações sobre o componente de proteção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

Figura 2. Janela principal do Kaspersky Anti-Virus for Windows Workstations

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
Essencialmente, esta janela o informa sobre o status de proteção do seu computador. A seção **Proteção** foi criada exatamente para isso. 	Para obter informações gerais sobre o funcionamento do Kaspersky Anti-Virus, examine as estatísticas gerais de funcionamento do programa e verifique se todos os componentes estão funcionando corretamente, selecione a seção **Proteção** na área de navegação. Você também pode habilitar/desabilitar os componentes de proteção. Para exibir as estatísticas e configurações de um componente de proteção **específico,** basta selecionar o nome do componente sobre o qual deseja informações na seção **Proteção**.
Para verificar programas ou arquivos mal-intencionados no computador, use a seção **Verificação** específica na janela principal. 	Esta seção contém uma lista de objetos que podem ser verificados quanto à presença de vírus. As tarefas mais comuns e mais importantes são incluídas nesta seção. Elas incluem tarefas de verificação de vírus em áreas críticas, em programas de inicialização e a verificação completa do computador.
A seção **Serviço** inclui recursos adicionais do Kaspersky Anti-Virus for Windows Workstations. 	Aqui você pode atualizar o programa, exibir relatórios sobre o desempenho de qualquer componente ou tarefa do Kaspersky Anti-Virus for Windows Workstations, trabalhar com objetos em quarentena e cópias de backup, analisar informações de suporte técnico, criar um Disco de Recuperação e gerenciar chaves de licença.

Seção da janela principal	Finalidade
A seção de **comentários e dicas** o acompanha durante o uso do aplicativo. 	Esta seção fornece dicas de como elevar o nível de segurança do computador. Você também encontrará comentários sobre o desempenho atual do aplicativo e suas configurações. Os links nesta seção o orientam na execução das ações recomendadas para uma determinada seção ou para exibir informações mais detalhadas.

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

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

4.4. Janela de configurações do programa

Você pode abrir a janela de configurações do Kaspersky Anti-Virus for Windows Workstations a partir da janela principal (consulte 4.3 na p. 55). Para fazê-lo, clique em Configurações na parte superior da janela.

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 programa, às tarefas de atualização e de verificação de vírus e às ferramentas do programa;
- à direita da janela, existe uma lista detalhada de configurações do item selecionado à esquerda.

Ao selecionar qualquer seção, componente ou tarefa à esquerda da janela de configurações, a parte direita exibirá suas configurações básicas. Para definir configurações avançadas, você pode abrir janelas de configurações de segundo e terceiro níveis. Uma descrição detalhada das configurações do programa encontra-se nas seções correspondentes do Manual do Usuário.

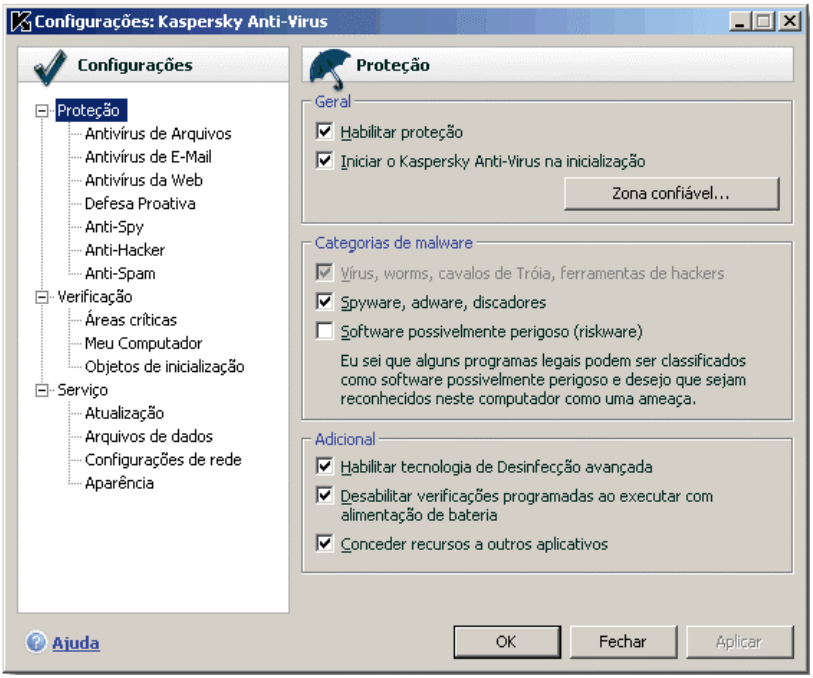


Figura 3. Janela de configurações do Kaspersky Anti-Virus for Windows Workstations

CAPÍTULO 5. INTRODUÇÃO

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

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

Para tornar mais fácil começar, combinamos todos os estágios preliminares de configuração em um Assistente para Instalação (consulte a seção 3.2 na p. 38) 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, proteger o acesso ao programa por senha e configurar o Anti-Hacker para que corresponda às propriedades de sua rede.

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

- Verifique o status de proteção atual (consulte 5.1 na p. 59) para certificar-se de que o Kaspersky Anti-Virus for Windows Workstations está sendo executado no nível apropriado.
- Treine o Anti-Spam (consulte a seção 5.5 na p. 67) com seus e-mails.
- Atualize o programa (consulte a seção 5.6 na p. 69) se o Assistente para Instalação não o fizer automaticamente depois de instalar o programa.
- Verifique o computador (consulte a seção 5.2 na p. 65) quanto à presença de vírus.

5.1. Qual é o status de proteção do computador?

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

O **status de proteção** exige o estado atual de proteção do computador usando indicadores especiais (consulte 5.1.1 na p. 60). As estatísticas (consulte 5.1.2 na p. 63) analisam a sessão atual do programa.

5.1.1. Indicadores de proteção

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

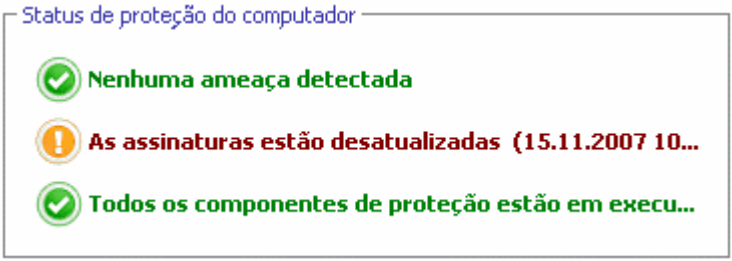


Figura 4. Indicadores que refletem o status de proteção do computador

Cada indicador tem três aparências possíveis:

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

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

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

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

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

	*Nenhuma ameaça detectada* O Kaspersky Anti-Virus for Windows Workstations não detectou nenhum arquivo ou programa perigoso no computador.
	Todas as ameaças foram neutralizadas O Kaspersky Anti-Virus for Windows Workstations neutralizou todos os arquivos e programas infectados, e excluiu os que não puderam ser neutralizados.
	*Foram detectadas ameaças* Existe risco de infecção no computador. O Kaspersky Anti-Virus for Windows Workstations detectou programas mal-intencionados (vírus, cavalos de Tróia, worms, etc.) que devem ser neutralizados. Para fazê-lo, use o link Neutralizar tudo. Clique no link Detalhes para ver informações mais detalhadas sobre os objetos mal-intencionados.

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

	*Assinaturas liberadas: (data, hora)* O aplicativo e as assinaturas de ameaças usadas pelo Kaspersky Anti-Virus for Windows Workstations são as versões mais recentes.
	*As assinaturas estão desatualizadas* Os módulos do programa e as assinaturas de ameaças do Kaspersky Anti-Virus for Windows Workstations não foram atualizados por vários dias. Você está correndo o risco de infectar o computador com novos programas mal-intencionados que apareceram desde a última atualização do programa. É recomendável atualizar o Kaspersky Anti-Virus for Windows Workstations. Para fazê-lo, use o link Atualização.
	As assinaturas estão parcialmente corrompidas Os arquivos de assinaturas de ameaças estão parcialmente corrompidos. Se isso ocorrer, é recomendável executar as atualizações do programa novamente. Se a mesma mensagem de erro aparecer novamente, entre em contato com o Serviço de Suporte Técnico da Kaspersky Lab.

	Reinicie o computador Reinicie o sistema para que o programa seja executado corretamente. Salve e feche todos os arquivos com os quais está trabalhando e use o link Reiniciar computador.
	As atualizações do programa estão desabilitadas O serviço de atualização das assinaturas de ameaças e de módulos do programa está desabilitado. Para manter a proteção em tempo real, é recomendável habilitar as atualizações.
	*As assinaturas estão obsoletas* O Kaspersky Anti-Virus for Windows Workstations não é atualizado há algum tempo. Os dados correm um grande risco. Atualize o programa assim que possível. Para fazê-lo, use o link Atualização.
	As assinaturas estão corrompidas Os arquivos de assinaturas de ameaças estão corrompidos. Se isso ocorrer, é recomendável executar as atualizações do programa novamente. Se a mesma mensagem de erro aparecer novamente, entre em contato com o Serviço de Suporte Técnico da Kaspersky Lab.

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

	*Todos os componentes de proteção estão em execução* O Kaspersky Anti-Virus for Windows Workstations está protegendo o computador em todos os canais pelos quais programas mal-intencionados poderiam entrar. Todos os componentes de proteção estão habilitados.
	A proteção não está instalada Quando o Kaspersky Anti-Virus for Windows Workstations foi instalado, nenhum dos componentes de monitoramento foi instalado. Isso significa que você pode apenas verificar vírus. Para obter segurança máxima, instale os componentes de proteção no computador.

	*Todos os componentes de proteção estão pausados* Todos os componentes de proteção foram pausados. Para restaurá-los, selecione **Continuar proteção** no menu de contexto, clicando no ícone da bandeja do sistema.
	Alguns componentes de proteção estão desabilitados Um ou vários componentes de proteção foram parados. Isso poderia levar à infecção do computador e à perda de dados. É fortemente recomendável habilitá-la. Para fazê-lo, selecione um componente inativo na lista e clique em ▶.
	Todos os componentes de proteção estão desabilitados A proteção está totalmente desabilitada. Nenhum componente está em execução. Para restaurá-los, selecione **Continuar proteção** no menu de contexto, clicando no ícone da bandeja do sistema.
	*Alguns componentes de proteção tiveram mau funcionamento* Um ou mais componentes do Kaspersky Anti-Virus for Windows Workstations têm erros internos. Se isso ocorrer, é recomendável habilitar o componente ou reiniciar o computador, pois é possível que os drivers dos componentes precisem ser registrados depois de serem atualizados.

5.1.2. Status dos componentes do Kaspersky Anti-Virus for Windows Workstations

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

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

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

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

- *Antivírus de Arquivos: em execução* – a proteção de arquivos está ativa para o nível selecionado (consulte 7.1 na p. 93).
- *Antivírus de Arquivos: em pausa* - o Antivírus de Arquivos está desabilitado por um determinado período. O componente continuará seu funcionamento automaticamente depois que o período atribuído expirar ou depois que o programa for reiniciado. Você também pode reiniciar a proteção de arquivos manualmente, clicando no botão ▶ localizado na barra de status.
- *Antivírus de Arquivos: interrompido* – o componente foi interrompido pelo usuário. Você pode reiniciar a proteção de arquivos manualmente, clicando no botão ▶ localizado na barra de status.
- *Antivírus de Arquivos: não executando* – por algum motivo, a proteção de arquivos não está disponível.
- *Antivírus de Arquivos: 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.

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

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

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

5.1.3. Estatísticas de desempenho do programa

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

Figura 5. A caixa de estatísticas gerais do programa

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

- Informações sobre objetos encontrados (consulte 17.3.2 na p. 243) e o status atribuído a eles
- Log de eventos (consulte 17.3.3 na p. 244)
- Estatísticas gerais de verificação (consulte 17.3.4 na p. 245) do computador
- Configurações de operação do programa (consulte 17.3.5 na p. 246)

5.2. Como verificar seu computador quanto à presença de vírus

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

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

Depois de selecionar a tarefa **Áreas críticas**, você poderá ver as estatísticas da verificação mais recente do computador e as configurações da tarefa: as estatísticas da verificação mais recente dessas áreas; as configurações da

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

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

1. Abra a janela principal do programa e selecione a tarefa **Áreas críticas** na seção **Verificação**.
2. Clique no botão **Verificação**.

Clique no botão **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 de andamento será ocultada, mas a verificação não será interrompida.

5.3. Como verificar áreas críticas do computador

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

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

Depois de selecionar a tarefa chamada **Áreas críticas**, o painel direito da janela principal exibirá o seguinte: as estatísticas da verificação mais recente dessas áreas; as configurações da tarefa; o nível de proteção selecionado e as ações que serão aplicadas às ameaças de segurança. Aqui, você também pode selecionar as áreas críticas que deseja verificar e iniciar imediatamente a verificação nessas áreas.

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

1. Abra a janela principal do programa e selecione a tarefa **Áreas críticas** na seção **Verificação**.
2. Clique no botão **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 de andamento será ocultada, mas a verificação não será interrompida.

5.4. 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 6).

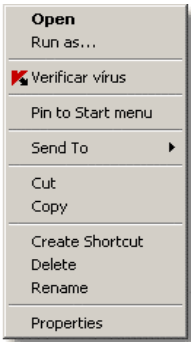


Figura 6. Verificando um objeto selecionado usando um menu de contexto padrão do Windows

Será iniciada então uma verificação do objeto selecionado e os detalhes serão mostrados em uma janela específica. Ao clicar no botão **Fechar**, a janela de andamento será ocultada, mas a verificação não será interrompida.

5.5. Como treinar o Anti-Spam

Uma etapa para começar é o treinamento do Anti-Spam para trabalhar com seus e-mails e filtrar o lixo eletrônico. O spam consiste em e-mails indesejados, apesar de ser difícil dizer o que constitui um spam para determinado usuário. Existem categorias de e-mails que podem ser aplicadas ao spam com bastante

precisão e generalidade (por exemplo, mensagens em massa, anúncios), mas esses e-mails poderiam fazer parte da caixa de entrada de alguns usuários.

Assim, solicitamos que você determine quais e-mails são e não são spam para você. O Kaspersky Anti-Virus for Windows Workstations perguntará, após a instalação, se deseja treinar o Anti-Spam para diferenciar os spams e os e-mails aceitos. Você pode fazê-lo por meio de botões específicos que funcionam junto com seu programa de e-mail (Microsoft Outlook, Outlook Express (Windows Mail), The Bat!) ou usando o assistente de treinamento específico.

Aviso!

Esta versão do Kaspersky Anti-Virus não fornece o plug-in Anti-Spam para o Microsoft Office Outlook no Microsoft Windows 98.

Para treinar o Anti-Spam usando os botões do plug-in no programa de e-mail,

1. Abra o programa de e-mail padrão do computador (por exemplo, o Microsoft Office Outlook). Você verá dois botões na barra de ferramentas: **Spam** e **Não spam**.
2. Selecione um e-mail aceito ou um grupo de e-mails que contenha e-mails aceitos e clique em **Não spam**. Deste ponto em diante, os e-mails dos endereços nos e-mails dos remetentes selecionados não serão mais processados como spam.
3. Selecione um e-mail, um grupo de e-mails ou uma pasta com e-mails que você considera spam e clique em **Spam**. O Anti-Spam analisará o conteúdo desses e-mails e, no futuro, considerará todos os e-mails com conteúdo semelhante como spam.

Para treinar o Anti-Spam usando o Assistente de Treinamento,

1. Abra a janela de configurações do aplicativo, selecione o componente Anti-Spam em **Proteção** e clique em **Assistente de Treinamento**.
2. Siga as instruções exibidas pelo Assistente de Treinamento do Anti-Spam (consulte a seção 13.2.1 na p. 177).

Quando chegar um e-mail na sua caixa de entrada, o Anti-Spam o verificará quanto ao conteúdo de spam e adicionará uma marca específica [Spam] à linha de assunto do spam. Você pode configurar uma regra específica para esses e-mails no programa de e-mail, como uma regra que os exclua ou mova para uma pasta específica.

5.6. Como atualizar o programa

A Kaspersky Lab atualiza as assinaturas de ameaças e módulos do Kaspersky Anti-Virus for Windows Workstations usando servidores de atualização dedicados.

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

Aviso!

Será necessária uma conexão com a Internet para atualizar o Kaspersky Anti-Virus for Windows Workstations.

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

Para atualizar o Kaspersky Anti-Virus for Windows Workstations manualmente,

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

Como resultado, o Kaspersky Anti-Virus for Windows Workstations 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 *desabilitado (erro de operação)*, tente reiniciar o Kaspersky Anti-Virus.

Se o problema não for resolvido ao reiniciar o programa, é recomendável corrigir possíveis erros usando o recurso de restauração do programa (consulte a seção Capítulo 19 na p. 298).

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

Para salvar o relatório em um arquivo:

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

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

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

ou

Clique em Todos os relatórios na janela de relatório de qualquer componente. Em seguida, a guia **Relatórios** relacionará os relatórios de todos os componentes do programa.

2. Clique no botão **Salvar como** e, na janela que é aberta, especifique o nome do arquivo do relatório de operação do programa.

CAPÍTULO 6. SISTEMA DE GERENCIAMENTO DA PROTEÇÃO

O Kaspersky Anti-Virus for Windows Workstations permite que você execute várias tarefas de gerenciamento da segurança dos computadores:

- Habilitar, desabilitar e pausar (consulte 6.1 na p. 71) o programa
- Definir os tipos de programas perigosos (consulte 6.2 na p. 76) dos quais o Kaspersky Anti-Virus for Windows Workstations protegerá seu computador
- Criar uma lista de exclusões (consulte 6.3 na p. 77) para a proteção
- Criar suas próprias tarefas de atualização e verificação de vírus (consulte 6.4 na p. 86)
- Configurar uma programação de verificação de vírus (consulte 6.5 na p. 87)
- Configurar a produtividade (consulte a seção 6.6 na p. 89) da proteção antivírus

6.1. Interrompendo e reiniciando a proteção do computador

Por padrão, o Kaspersky Anti-Virus é aberto na inicialização e protege o computador durante todo o tempo em que você o utiliza. As palavras *Kaspersky Anti-Virus 6.0* no canto superior direito da tela indicam que a proteção está ativa. Todos os componentes de proteção (consulte 2.2.1 na p. 25) estão sendo executados.

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

Aviso!

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

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

6.1.1. Pausando a proteção

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

Para pausar uma operação do Kaspersky Anti-Virus for Windows Workstations:

1. Selecione **Pausar proteção** no menu de contexto do programa (consulte a seção 4.2 na p. 53).
2. Na janela Pausar proteção que é aberta (veja a Figura 7), selecione em quanto tempo deseja que a proteção volte a funcionar:
   - **Em <período>** – a proteção continuará depois desse tempo. Use o menu suspenso para selecionar o intervalo de tempo.
   - **Na próxima reinicialização do programa** – a proteção será reiniciada se você abrir o programa no Menu Iniciar ou após reiniciar o computador (desde que o programa esteja definido para iniciar automaticamente ao ligar o computador (consulte a seção 6.1.5 na p. 75).
   - **Somente por solicitação do usuário** – a proteção será interrompida até que você mesmo a inicie. Para habilitar a proteção, selecione **Continuar proteção** no menu de contexto do programa.

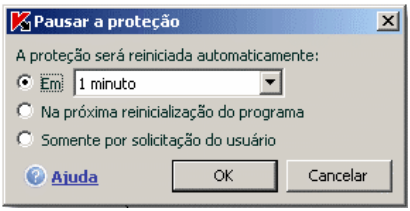


Figura 7. Janela Pausar a proteção

Dica:

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

- Clique no botão na seção **Proteção**.
- Selecione **Sair** no menu de contexto. Nesse caso, o programa será descarregado da memória do computador.

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

- Nomes inativos (cinza) dos componentes desabilitados na seção **Proteção** da janela principal.
- Ícone inativo (cinza) na bandeja do sistema.
- O terceiro indicador de proteção (consulte 5.1.1 na p. 60) no computador, que mostra que **Todos os componentes de proteção estão pausados**.

6.1.2. Interrompendo a proteção

Interromper a proteção significa desabilitar totalmente os componentes. 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 for Windows Workstations estiver em conflito com outros programas instalados no computador, você poderá pausar componentes individuais ou criar uma lista de exclusões (consulte 6.3 na p. 77).

Para interromper toda a proteção:

1. Abra a janela de configurações do Kaspersky Anti-Virus e selecione **Proteção**.
2. Desmarque **Habilitar proteção**.

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

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

- O terceiro indicador de proteção (consulte 5.1.1 na p. 60) no computador, que mostra que  **Todos os componentes de proteção estão desabilitados**.

6.1.3. Pausando / interrompendo tarefas e componentes de proteção

Existem várias maneiras de interromper um componente de proteção, verificação de vírus ou atualização. Antes de fazê-lo, é estritamente recomendável estabelecer o motivo da interrupção. É provável que o problema possa ser resolvido de outra maneira, por exemplo, alterando o nível de segurança. Se, por exemplo, você estiver trabalhando com um banco de dados que certamente não contém vírus, simplesmente adicione seus arquivos como uma exclusão (consulte a seção 6.3 na p. 77).

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

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

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

Ao pausar o um componente ou uma tarefa, as estatísticas do Kaspersky Anti-Virus referentes à sessão atual do Kaspersky Anti-Virus for Windows Workstations são salvas e continuarão sendo registradas após a atualização do componente ou tarefa.

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

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

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

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

6.1.4. Restaurando a proteção no computador

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

- *No menu de contexto*.

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

- *Na janela principal do programa*.

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

O status de proteção muda imediatamente para ***em execução***. O ícone do programa na bandeja do sistema fica ativo (colorido). O terceiro indicador de proteção (consulte 5.1.1 na p. 60) também informará que **Todos os componentes de proteção estão habilitados**.

6.1.5. Desligando o programa

Se for necessário desligar o Kaspersky Anti-Virus for Windows Workstations, selecione **Sair** no menu de contexto do programa (consulte 4.2 na p. 53). Isso fechará o programa, deixando seu computador desprotegido.

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

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

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

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

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

6.2. Tipos de programas mal-intencionados que serão monitorados

O Kaspersky Anti-Virus for Windows Workstations o protege de vários tipos de programas mal-intencionados. Independentemente das configurações atuais, o aplicativo sempre protegerá o computador contra os tipos mais perigosos de programas mal-intencionados, 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-intencionado dos quais o Kaspersky Anti-Virus for Windows Workstations o protegerá, selecione a seção **Proteção** na janela de configurações do programa (consulte 4.4 na p. 57).

A caixa **Categorias de malware** contém os tipos de ameaças (consulte a 1.1 na p. 11):

- ☑ **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 for Windows Workstations 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. Quando houver situações nas quais o Kaspersky Anti-Virus for Windows Workstations classifica um programa como possivelmente perigoso e você não o considerar como tal, é recomendável configurar uma exclusão para ele (consulte a seção 6.3 na p. 77).

6.3. Criando uma zona confiável

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

O usuário cria uma zona de proteção com base nas propriedades dos arquivos que usa e nos programas instalados no seu computador. Poderá ser necessário criar uma lista de exclusões se, por exemplo, o Kaspersky Anti-Virus for Windows Workstations 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 o status que o programa atribui aos objetos durante uma verificação.

Aviso!

Um objeto de exclusão não é verificado na verificação do disco ou da pasta no qual está localizado. Contudo, se você selecionar esse objeto especificamente, a regra de exclusão não será aplicada.

Para criar uma lista de exclusões,

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

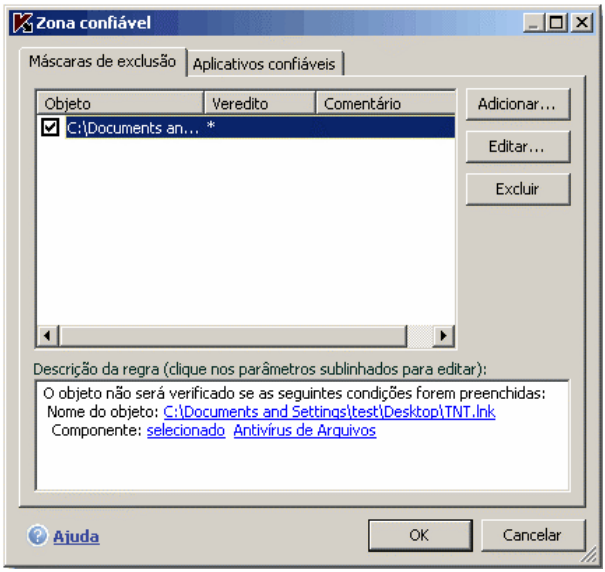


Figura 8. Criando uma zona confiável

6.3.1. Regras de exclusão

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

Você pode excluir da verificação arquivos de 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 seu veredito.

O *veredito* é o status que o Kaspersky Anti-Virus for Windows Workstations 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 possivelmente perigosos detectados pelo Kaspersky Anti-Virus for Windows

Workstations, consulte a Enciclopédia de Vírus 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 isso, especifique o veredito atribuído ao programa como uma máscara de exclusão.

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 for Windows Workstations 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 veredito.

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

*Para adicionar exclusões na guia **Regra de exclusão** tab:*

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

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

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

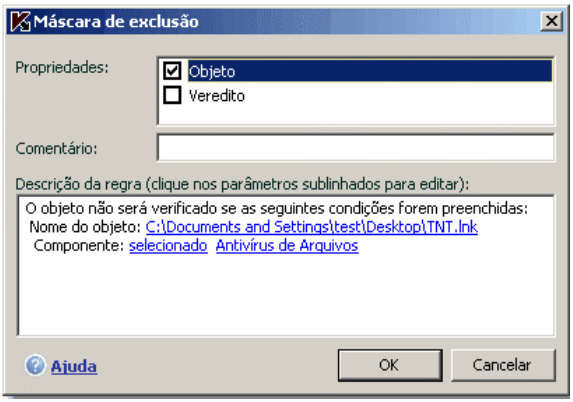


Figura 9. Criando uma regra de exclusão

Se você marcar as duas caixas ao mesmo tempo, será criada uma regra para aquele objeto com um determinado status conforme a classificação da Enciclopédia de Vírus. Nesse caso, as seguintes regras se aplicam:

- Se você especificar um determinado arquivo como **Objeto** e um determinado status na seção **Veredito**, o arquivo especificado será 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 **Veredito**, os objetos com esse status serão excluídos da verificação somente quando essa área ou pasta forem verificadas.

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. 327). 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 verificar as pastas aninhadas, o arquivo **winword.exe** será excluído da verificação se for encontrado em qualquer pasta sob **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. 327) para o **Veredito**.

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

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

     - *Internet*. Para esse veredito, você pode fornecer um nome, máscara ou caminho completo do objeto incorporado (por exemplo, um arquivo .dll) como uma condição de exclusão adicional.

- *Iniciando navegador da Internet*. Para esse veredito, você pode listar configurações de abertura do navegador como configurações de exclusão adicionais.
  Por exemplo, você bloqueou a abertura de navegadores com determinadas configurações na análise de atividade de aplicativos da Defesa Proativa. Contudo, deseja que o navegador possa ser aberto no domínio *www.kaspersky.com* com um link do Microsoft Office Outlook como uma regra de exclusão. Para fazê-lo, selecione o Microsoft Office Outlook como **Objeto** da exclusão e *Iniciando navegador da Internet* como **Veredito**, e insira uma máscara de domínio permitida no campo **Configurações avançadas**.

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

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

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

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**.

Figura 10. Notificação de detecção de objeto perigoso

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 11).
3. A janela de configurações da exclusão será aberta. Verifique se todas as configurações das regras de exclusão correspondem às suas necessidades. O programa preencherá o nome do objeto e o tipo de ameaça automaticamente com base nas informações do relatório. Para criar a regra, clique em **OK**.

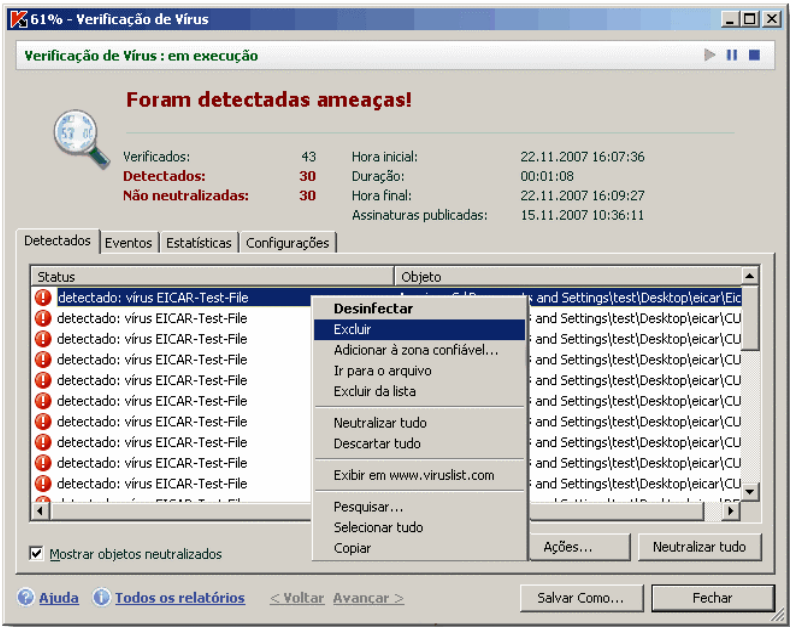


Figura 11. Criando uma regra de exclusão em um relatório

6.3.2. Aplicativos confiáveis

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

O Kaspersky Anti-Virus pode criar uma lista de aplicativos confiáveis, 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 Windows são seguros e não precisam ser verificados. Para excluir os objetos usados por esse processo da verificação, adicione o **Bloco de Notas** à lista de aplicativos confiáveis. Contudo, o arquivo executável e o processo do aplicativo confiável serão verificados quanto à presença de vírus, como anteriormente. Para excluir totalmente o aplicativo da verificação, use regras de exclusão (consulte 6.3.1 na p. 78).

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 for Windows Workstations 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 for Windows Workstations 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 12). Por padrão, essa lista contém os aplicativos que não serão monitorados com base nas recomendações da Kaspersky Lab ao instalar o Kaspersky Anti-Virus. Se você não confiar em um aplicativo da lista, desmarque a caixa de seleção correspondente. É possível editar a lista usando os botões **Adicionar**, **Editar** e **Excluir** à direita.

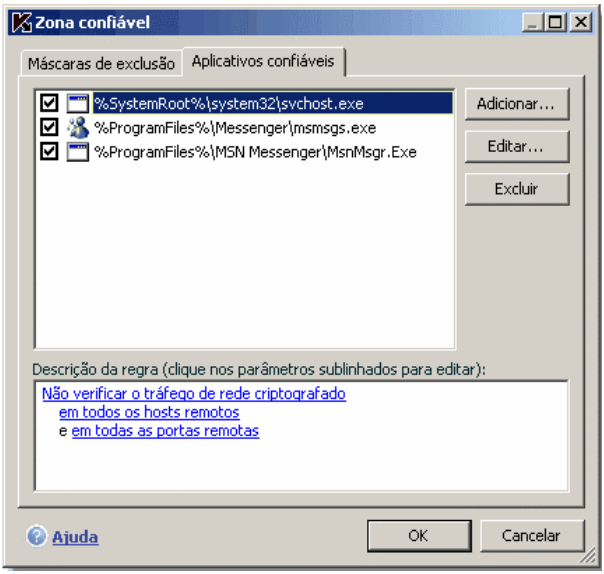


Figura 12. Lista de aplicativos confiáveis

Para adicionar um programa à lista de aplicativos confiáveis:

1. Clique no botão **Adicionar** à direita da guia **Aplicativos confiáveis**.

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

   Ao selecionar um programa, o Kaspersky Anti-Virus for Windows Workstations 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.

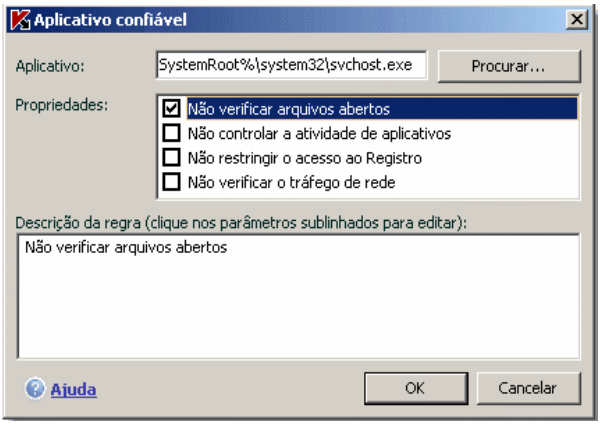


Figura 13. Adicionando um aplicativo à lista de aplicativos confiáveis

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 da rede** – exclui das verificações de vírus e spam o tráfego de rede iniciado pelo aplicativo confiável. Você pode excluir da verificação todo o tráfego de rede do aplicativo ou

o tráfego criptografado (SSL). Para fazê-lo, clique no link tudo. Ele mudará para criptografado. Além disso, você pode restringir a exclusão atribuindo uma porta/host remoto. Para criar uma restrição, clique em qualquer, que mudará para selecionado, e insira um valor para a porta/host remoto.

Observe que se **Não verificar o tráfego da rede** estiver marcado, o tráfego desse aplicativo será verificado apenas quanto à presença de vírus e spam. Contudo, isso não afeta a verificação do tráfego pelo Anti-Hacker. As configurações do Anti-Hacker controlam a análise da atividade de rede desse aplicativo.

6.4. Iniciando tarefas em outro perfil

O Kaspersky Anti-Virus for Windows Workstations 6.0 possui um recurso que permite iniciar tarefas de verificação com outro perfil de usuário. Por padrão, esse recurso está desabilitado e as tarefas são executadas no perfil com o qual você se conectou ao sistema.

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

Observe que esta opção não está disponível no Microsoft Windows 98/ME.

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 uma tarefa de verificação que é iniciada em outro perfil de usuário:

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

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

Se a tarefa não for executada por um usuário com os privilégios apropriados, a atualização programada será executada com os privilégios da conta de usuário atual. Se não houver um usuário conectado ao computador no momento, a execução das atualizações com outra conta de usuário não tiver sido configurada e as atualizações forem executadas automaticamente, elas o farão com os privilégios do sistema.

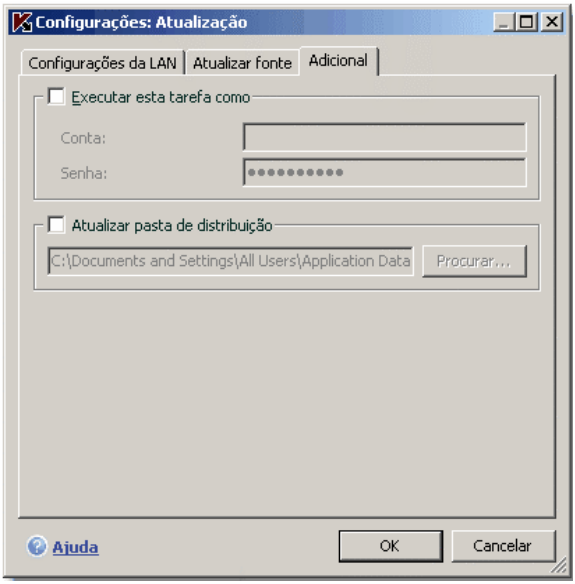


Figura 14. Configurando uma tarefa de atualização em outro perfil

6.5. Configurando notificações e tarefas programadas

As configurações de programação são idênticas para tarefas de verificação de vírus, atualizações do aplicativo e notificações de eventos do Kaspersky Anti-Virus.

Por padrão, as tarefas de verificação de vírus criadas na instalação do aplicativo estão desabilitadas. A exceção são os objetos de inicialização, que são verificados sempre que 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 não estiver satisfeito com essas configurações, poderá reconfigurar as programações de tarefas. Selecione uma tarefa pelo nome em **Verificação de vírus** (para tarefas de verificação de vírus) ou em **Serviço** (para atualizações e distribuição de atualizações) e abra a janela de configurações correspondente clicando em Configurações.

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

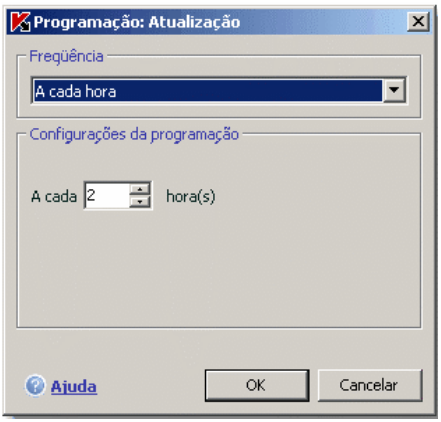


Figura 15. Configurando uma programação de tarefas

A principal configuração a ser definida é a freqüência de um evento (notificação ou execução da tarefa). Selecione a opção desejada em **Freqüência** (veja a Figura 15). Em seguida, especifique as configurações da opção selecionada em Configurações da atualização. As seguintes opções estão disponíveis:

- **Minutos.** O intervalo entre as verificações ou notificações será de vários minutos. Especifique o período em minutos nas configurações da programação. Ele não deve exceder 59 minutos.
- **Horas.** O intervalo entre as verificações ou notificações será de várias horas. Se esta opção estiver selecionada, especifique o intervalo nas configurações da programação: **A cada n horas** e especifique *n*. Por exemplo, insira **A cada 1 hora** se desejar que a tarefa seja executada a cada hora.
- **Dias.** A tarefa é iniciada ou a notificação é enviada com um intervalo de vários dias. Especifique o intervalo nas configurações da programação:

- Selecione **A cada n dias** e especifique o valor de n, se desejar um intervalo de vários dias.
- Selecione **Todos os dias da semana**, se desejar que a tarefa seja executada diariamente, de segunda a sexta-feira.
- **Todos os finais de semana** para executar a tarefa ou enviar a notificação somente aos sábados e domingos.

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

Semanas. A tarefa é iniciada ou a notificação é enviada em determinados dias da semana. Se você selecionar esta opção, marque os dias da semana nos quais deseja que a tarefa seja executada. Insira a hora do dia no campo **Hora**.

Mensal. A tarefa é iniciada ou a notificação é enviada uma vez por mês, na hora especificada.

Hora. Inicia 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 pode ser especificado um atraso com relação ao início do aplicativo para que uma tarefa seja executada.

Após cada atualização. A tarefa é iniciada após cada atualização da assinatura de ameaças (se aplica somente a tarefas de verificação de vírus).

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. Para fazê-lo, marque **Executar a tarefa se ignorado** na janela da programação.

6.6. Opções de energia

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

- Como às vezes as verificações de vírus e atualizações do programa exigem recursos consideráveis e podem levar algum tempo, é recomendável desabilitar a programação dessas tarefas, o que ajuda a economizar bateria. Se necessário, você mesmo pode atualizar o programa (consulte a seção 5.6 na p. 69) ou iniciar uma verificação de vírus (consulte a seção 5.2 na p. 65). Para usar o recurso de economia

de bateria, marque a caixa **Desabilitar verificações programadas ao executar com alimentação de bateria**.

- As verificações de vírus aumentam a carga nos subsistemas do processador central e do disco, fazendo os outros programas serem executados mais lentamente. Por padrão, se ocorrer essa situação, o programa pausará as verificações de vírus e liberará os recursos do sistema para os aplicativos do usuário.

Entretanto, há vários programas que podem ser iniciados assim que os recursos do processador forem liberados e executados em segundo plano. Para que as verificações de vírus não dependam do funcionamento desses programas, desmarque **Conceder recursos a outros aplicativos**.

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

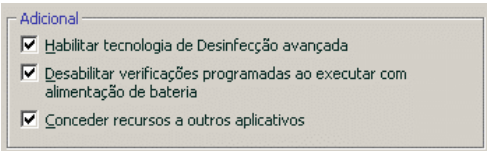


Figura 16. Configurando a energia

Para configurar a energia das tarefas de verificação de vírus:

Selecione a seção **Proteção** da janela principal do programa e clique em Configurações. Configure a energia na caixa **Avançado** (veja a Figura 16).

6.7. Tecnologia de Desinfecção Avançada

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

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

Para habilitar/desabilitar a Tecnologia de Desinfecção Avançada:

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

CAPÍTULO 7. ANTIVÍRUS DE ARQUIVOS

O componente do Kaspersky Anti-Virus for Windows Workstations 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 for Windows Workstations na bandeja do sistema, que tem a seguinte aparência  sempre que um arquivo está sendo verificado.

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

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

7.1. Selecionando um nível de segurança de arquivos

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

- **Alto** – o nível com o monitoramento mais abrangente dos arquivos abertos, salvos ou executados.
- **Recomendado** – a Kaspersky Lab recomenda este nível de configuração. As seguintes categorias de objetos serão verificadas:
  - Programas e arquivos por conteúdo
  - Objetos novos e modificados desde a última verificação
  - Objetos OLE incorporados
- **Baixo** – o nível com configurações que permitem usar tranqüilamente aplicativos que exigem recursos significativos do sistema, pois o escopo dos arquivos verificados é menor.

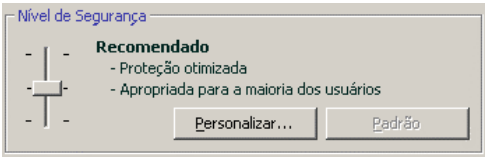


Figura 17. Nível de segurança do Antivírus de Arquivos

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

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

Para alterar o nível de segurança:

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

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

Exemplo:

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

Dica para selecionar um nível:

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

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

Para modificar as configurações de um nível de segurança:

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

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

7.2. Configurando o Antivírus de Arquivos

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

- Configurações que definem os tipos de arquivos (consulte a seção 7.2.1 na p. 95) que deverão ser verificados quanto à presença de vírus
- Configurações que definem o escopo da proteção (consulte a seção 7.2.2 na p. 97)
- Configurações que definem como o programa responderá a objetos perigosos (consulte a seção 7.2.5 na p. 102).

- Configurações adicionais do Antivírus de Arquivos (consulte a seção 7.2.3 na p. 99)

As seções a seguir abordarão esses grupos detalhadamente.

7.2.1. Definindo os tipos de arquivos que serão verificados

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

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

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

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

  > Observação:
  >
  > Há vários formatos de arquivos que têm um risco bem menor de conter código mal-intencionado infiltrado e, conseqüentemente, de estar ativados. Um exemplo são os arquivos .txt.
  >
  > Por outro lado, há formatos de arquivos que contêm ou podem conter código executável. 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. 323) que são verificados com essa opção.

Dica:

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

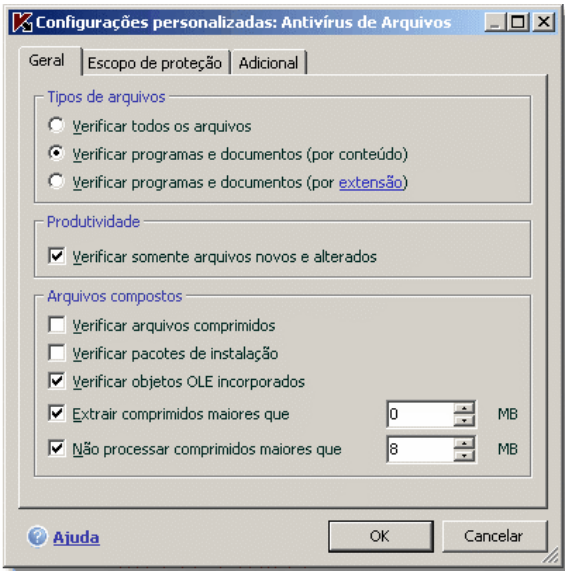


Figura 18. Selecionando os tipos de arquivos verificados quanto à presença de vírus

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 modificados. Esse modo se aplica a arquivos simples e compostos.

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

- **Verificar todos/somente novos arquivos comprimidos** – verifica arquivos comprimidos .zip, .cab, .rar e .arj.
- **Verificar todos/somente novos pacotes de instalação** – verifica arquivos comprimidos de extração automática quanto à presença de vírus.
- **Verificar tudo/somente novos objetos OLE incorporados** – verifica objetos incorporados em arquivos (por exemplo, planilhas ou macros do Microsoft Office Excel incorporados 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. Selecione **Antivírus de Arquivos** na janela principal e vá para a janela de configurações do componente clicando em Configurações.
2. Clique no botão **Configurações** e selecione a guia **Escopo de proteção** (veja a Figura 19) na janela que é aberta.

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

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

- Especifique somente as pastas, unidades e arquivos que precisam ser protegidos.
- Crie uma lista de objetos que não precisam ser protegidos (consulte a 6.3 na p. 77).
- Combine os dois métodos anteriores; crie um escopo de proteção que exclua vários objetos.

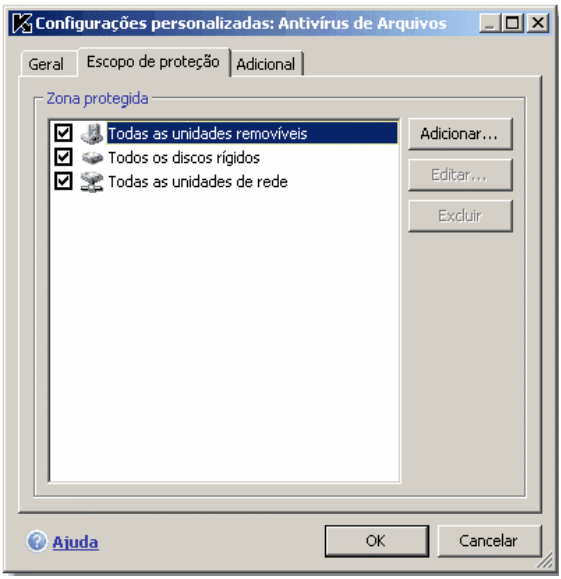


Figura 19. Definindo o escopo da proteção

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

- **C:\dir*.***, **C:\dir*** ou **C:\dir** - todos os arquivos na pasta *C:\dir*
- **C:\dir*.exe** - todos os arquivos com a extensão .exe na pasta *C:\dir*

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

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

Aviso!

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

7.2.3. Definindo as configurações avançadas

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

Para definir configurações adicionais do Antivírus de Arquivos:

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

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.

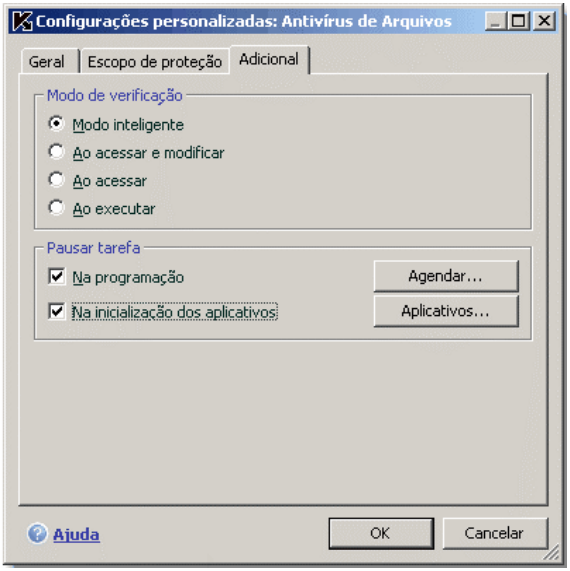


Figura 20. Definindo as configurações adicionais do Antivírus de Arquivos

- **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 21), clique em **Programação** para atribuir um período para desabilitar e reiniciar o componente. Para fazê-lo, insira um valor no formato HH:MM nos campos correspondentes.

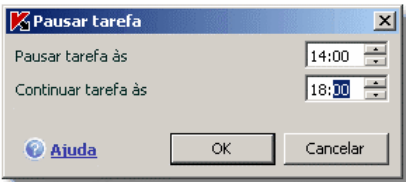


Figura 21. Pausando o componente

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

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.

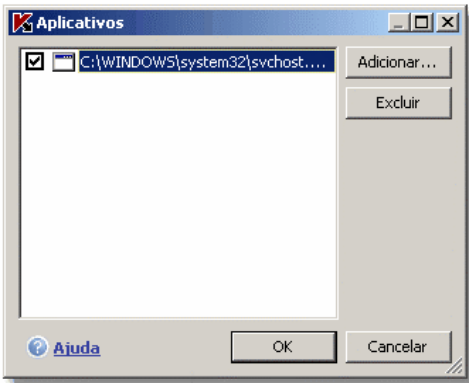


Figura 22. Criando uma lista de aplicativos

7.2.4. Restaurando as configurações padrão do Antivírus de Arquivos

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

Para restaurar as configurações padrão do Antivírus de Arquivos:

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

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

7.2.5. Selecionando ações para objetos

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

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

- Status de programa mal-intencionado (por exemplo, *vírus, cavalo de Tróia*) (consulte a 1.1 na p. 11)..
- *Possivelmente infectado*, quando a verificação não consegue determinar se o objeto está infectado. Isso significa que o programa detectou no arquivo uma seqüência de código de um vírus desconhecido ou de código modificado de um vírus conhecido.

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

Para editar uma ação para um objeto:

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

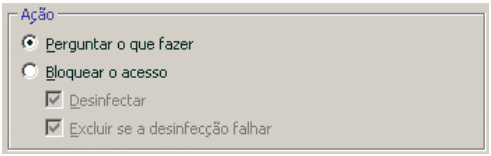


Figura 23. Possíveis ações do Antivírus de Arquivos para objetos perigosos

Se a ação selecionada for	Ao detectar um objeto perigoso
Perguntar o que fazer	O Antivírus de Arquivos emite uma mensagem de aviso com informações sobre o programa mal-intencionado que infectou, ou possivelmente infectou, o arquivo e permite que você escolha o que fazer. A opção pode variar dependendo do status do objeto.
Bloquear o acesso	O Antivírus de Arquivos bloqueia o acesso ao objeto. Essas informações são registradas no relatório (consulte a seção 17.3 na p. 239). 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 17.1 na p. 233). Essas informações são registradas no relatório. Posteriormente, você pode tentar desinfectar esse objeto.
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

Se a ação selecionada for	Ao detectar um objeto perigoso
	desinfectado, ele será excluído. Uma cópia do objeto será armazenada no Backup (consulte a seção 17.2 na p. 237).
Bloquear o acesso **Desinfectar** **Excluir**	O Antivírus de Arquivos bloqueará o acesso ao objeto e o excluirá.

Antes de desinfectar ou excluir o objeto, o Kaspersky Anti-Virus for Windows Workstations 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** na janela principal do programa e clique em qualquer local da caixa **Estatísticas**.
2. Selecione os objetos que o interessam na guia **Detectados** e clique no botão **Ação** → **Neutralizar tudo**.

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

CAPÍTULO 8. ANTIVÍRUS DE E-MAIL

O *Antivírus de E-Mail* é o componente do Kaspersky Anti-Virus for Windows Workstations 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 criptografadas (SSL) para POP3 e IMAP (SSL).

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

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

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

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

e-mail, informando que o mesmo foi processado pelo Kaspersky Anti-Virus for Windows Workstations.

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

É fornecido um plug-in específico (consulte 8.2.2 na p. 110) para o Microsoft Outlook que permite configurar a verificação de e-mails de maneira mais precisa.

Se você usar o The Bat!, o Kaspersky Anti-Virus for Windows Workstations 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. 112) são configuradas diretamente no The Bat! e sobrepõem as configurações de proteção de e-mail do Kaspersky Anti-Virus for Windows Workstations.

Aviso!

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

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 proteção de e-mails

O Kaspersky Anti-Virus for Windows Workstations protege seus e-mails em um dos seguintes níveis (veja a Figura 24):

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

Recomendado – os especialistas da Kaspersky recomendam este nível. São verificados os mesmos objetos que no nível **Alto**, com exceção

dos anexos ou dos e-mails que levarem mais de três minutos para serem verificados.

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

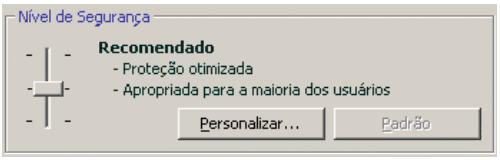


Figura 24. Selecionando um nível de segurança de e-mail

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

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

Para alterar o nível de segurança:

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

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

Exemplo:

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

Dica para selecionar um nível:

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

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

Para modificar as configurações do nível de segurança atual:

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

8.2. Configurando o Antivírus de E-Mail

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

- Configurações que definem o grupo de e-mails protegidos (consulte a seção 8.2.1 na p. 108)
- Configurações de verificação de e-mail do Microsoft Outlook (consulte 8.2.2 na p. 110) e do The Bat! (consulte 8.2.3 na p. 112)
- Configurações que definem ações para objetos de e-mail perigosos (consulte a seção 8.2.4 na p. 114)

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 com os parâmetros do nível de segurança **Recomendado**, que inclui a verificação de e-mails enviados e recebidos. Quando você começa a trabalhar no programa pela primeira vez, é recomendável verificar os e-mails enviados, pois é possível que haja worms no

computador que usam o e-mail para se distribuírem. Isso ajudará a evitar a possibilidade de enviar e-mails infectados em massa sem monitoramento do seu computador.

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

1. Selecione **Antivírus de E-Mail** na janela principal e vá para a janela de configurações do componente clicando em Configurações. Clique no botão **Personalizar** na janela de configurações do Antivírus de E-Mail.
2. Na janela **Configurações personalizadas: Antivírus de E-Mail** (veja a Figura 25), selecione **Somente e-mails recebidos** na seção **Escopo**.

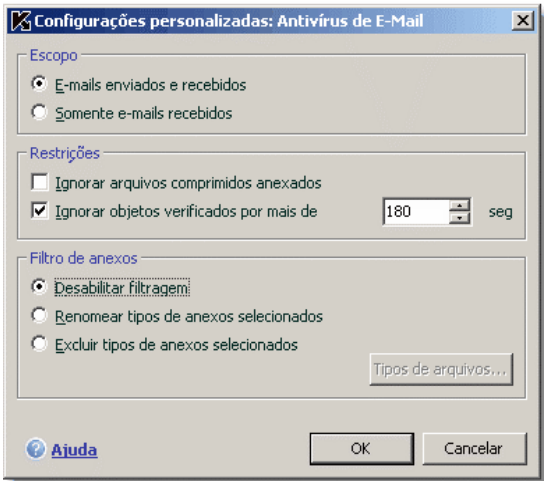


Figura 25. Configurações do Antivírus de E-Mail

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

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

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

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

- **Desabilitar filtragem** – não usa filtragem adicional de anexos.
- **Renomear tipos de anexos selecionados** – filtra um determinado formato de anexo e substitui o último caractere do nome do arquivo por um sublinhado. Você pode selecionar o tipo de arquivo clicando no botão Tipos de arquivos.
- **Excluir tipos de anexos selecionados** – filtra e exclui um determinado formato de anexo. Você pode selecionar o tipo de arquivo clicando no botão Tipos de arquivos.

Você pode obter mais informações sobre tipos de anexos filtrados na seção A.1 na p. 323.

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

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

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

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

Aviso!

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

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

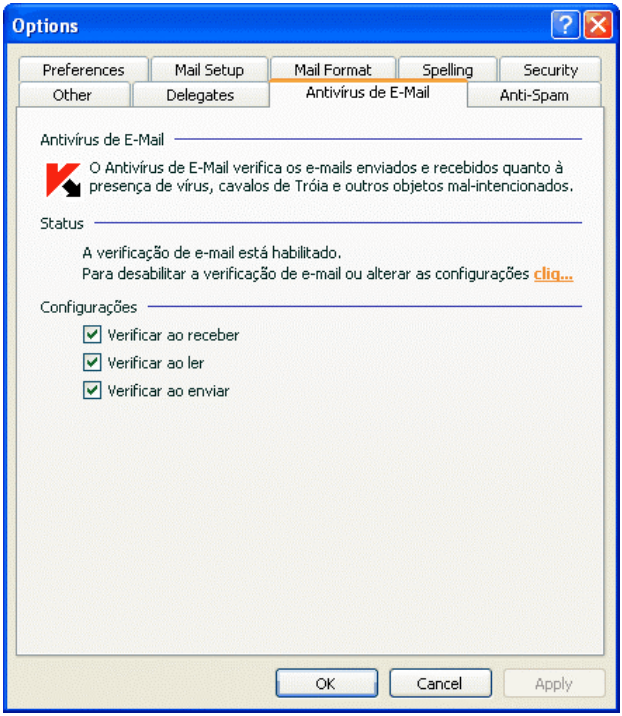


Figura 26. Configurando o Antivírus de E-Mail no Microsoft Outlook

Selecione um modo de verificação de e-mail:

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

Aviso!

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

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

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

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

> Aviso!
>
> As configurações do Antivírus de E-Mail que determinam se os e-mails enviados e recebidos são verificados, assim como as ações com relação a objetos de e-mail perigosos e exclusões são ignoradas. A única coisa que o The Bat! considera é a verificação de anexos com arquivos comprimidos e os limites de tempo da verificação de e-mails (consulte a seção 8.2.1 na p. 108).
>
> Esta versão do Kaspersky Anti-Virus não fornece plug-ins do Antivírus de E-Mail para o The Bat! de 64 bits.

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

1. Selecione **Settings** no menu **Properties** do programa de e-mail.
2. Selecione **Virus protection** na árvore de configurações.

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

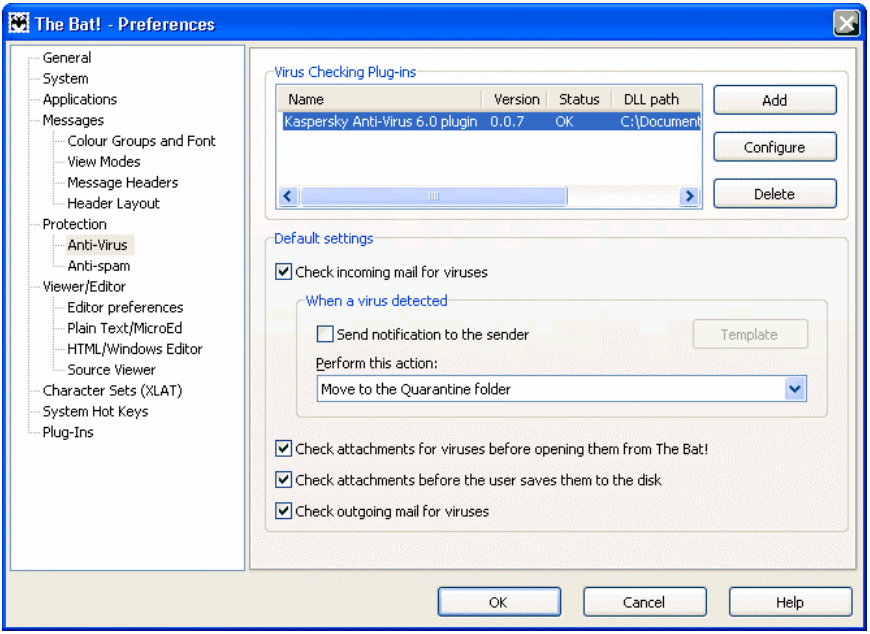


Figura 27. Configurando a verificação de e-mail no The Bat!

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:

  Attempt to disinfect infected parts – tenta neutralizar o objeto de e-mail infectado e, se o objeto não puder ser neutralizado, ele permanecerá no e-mail. O Kaspersky Anti-Virus for Windows Workstations 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.

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

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

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

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

8.2.5. Selecionando ações para objetos de e-mail perigosos

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

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

- Status de programa mal-intencionado (por exemplo, *vírus, cavalo de Tróia*; para obter mais detalhes, consulte 1.1 na p. 11).
- *Possivelmente infectado*, quando a verificação não consegue determinar se o objeto está infectado. Isso significa que o programa detectou no arquivo uma seqüência de código de um vírus desconhecido ou de código modificado de um vírus conhecido.

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

Para editar uma ação para um objeto:

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

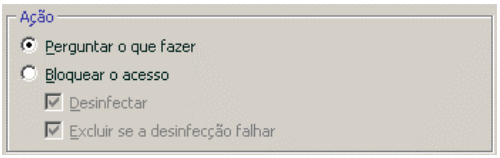


Figura 28. Selecionando ações para objetos de e-mail perigosos

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

Se a ação selecionada for	Ao detectar um objeto perigoso
Perguntar o que fazer	O Antivírus de E-Mail emitirá uma mensagem de aviso com informações sobre o programa mal-intencionado que infectou (ou possivelmente infectou) o arquivo e permite que você escolha uma das ações a seguir.
Bloquear o acesso	O Antivírus de E-Mail bloqueará o acesso ao objeto. Essas informações são registradas no relatório (consulte 17.3 na p. 239). Posteriormente, você pode tentar desinfectar esse objeto.

Se a ação selecionada for	Ao detectar um objeto perigoso
◉ **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 (consulte a seção 17.1 na p. 233). Essas informações são registradas no relatório. Posteriormente, você pode tentar desinfectar esse objeto.
◉ **Bloquear o acesso** ☑ **Desinfectar** ☑ **Excluir se a desinfecção falhar**[2]	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 desinfectado, ele será excluído. Uma cópia do objeto será armazenada no Backup. Os objetos com o status possivelmente infectado serão movidos para a Quarentena.
◉ **Bloquear o acesso** ☐ **Desinfectar** ☑ **Excluir**	Quando o Antivírus de E-Mail detecta um objeto infectado ou possivelmente infectado, ele o exclui sem informar o usuário.

Antes de desinfectar ou excluir o objeto, o Kaspersky Anti-Virus for Windows Workstations cria uma cópia de backup (consulte 17.2 na p. 237), 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 for Windows Workstations 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 17.7 na p. 261). As portas mais usadas para transmitir e-mails e tráfego HTTP estão listadas no pacote do programa. Se você usa portas que não estão nesta lista, adicione-as para proteger o tráfego que passa por elas.

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

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

Vamos examinar o funcionamento do componente mais detalhadamente.

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

- *Verificação de tráfego* – verifica objetos que entram no computador do usuário *via* HTTP.
- *Verificação de scripts* - verifica todos os scripts processados 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 for Windows Workstations. O ícone  na barra de ferramentas Padrão do navegador indica que ele foi

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

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

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

Os scripts são verificados de acordo com o seguinte algoritmo:

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

Aviso

Você deve habilitar o Antivírus da Web antes de se conectar com a web para que ele possa interceptar e verificar scripts e o tráfico http em busca de vírus.

9.1. Selecionando o nível de segurança da Web

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

Alto – o nível com o monitoramento mais abrangente de scripts e objetos recebidos via HTTP. O programa executa uma verificação completa de todos os objetos usando o conjunto total de assinaturas de ameaças. Este nível de proteção é recomendado para ambientes agressivos, quando nenhuma outra ferramenta de segurança de HTTP estiver sendo usada.

Recomendado – as configurações deste nível são as recomendadas pelos especialistas da Kaspersky Lab. Ele verifica os mesmos objetos do nível **Alto**, mas limita o tempo de cache para fragmentos do arquivo, o que acelera a verificação e retorna os objetos ao usuário mais rapidamente.

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

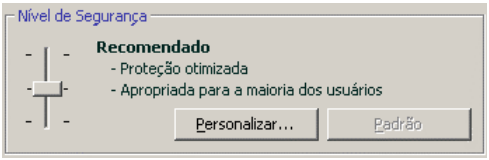


Figura 29. Selecionando um nível de segurança da Web

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

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

Para editar o nível de segurança:

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

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

Exemplo:

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

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

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

Dica para selecionar um nível:

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

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

Para modificar um nível de segurança pré-instalado:

clique no botão **Personalizar** na janela de configurações do Antivírus da Web. Na janela que é aberta, edite as configurações de proteção da Web (consulte 9.2 na p. 120) 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 (Java ou Visual Basic, etc.) executados.

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

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

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

As seções a seguir examinam estas configurações detalhadamente.

9.2.1. Configurando um método de verificação

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

- *Verificação contínua* – este método para a detecção de código mal-intencionado no tráfego de rede verifica os dados em trânsito: conforme o arquivo é baixado da Internet, o Antivírus da Web verifica as partes do arquivo, liberando o objeto verificado mais rápido para o usuário. Ao mesmo tempo, um conjunto limitado de assinaturas de ameaças é usado para executar verificações contínuas (apenas as ameaças mais ativas), o que reduz significativamente o nível de segurança para usar a Internet.
- *Verificação de buffering* – este método verifica objetos apenas depois de eles terem sido baixados integralmente para o buffer. Após a conclusão da verificação, o programa passa o objeto para o usuário ou o bloqueia.
  Ao usar este tipo de verificação, o conjunto completo de assinaturas de ameaças é usado, o que aumenta o nível de detecção de códigos mal-intencionados. Contudo, o uso desse algoritmo aumenta o tempo de processamento do objeto, tornando a navegação na Web mais lenta: ele também pode gerar problemas ao copiar e processar objetos grandes, pois a conexão com o cliente HTTP pode atingir o tempo limite.

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

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

Por padrão, o Antivírus da Web executa uma verificação de buffering nos os dados da Internet e usa o conjunto completo de assinaturas de ameaças.

Aviso!

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

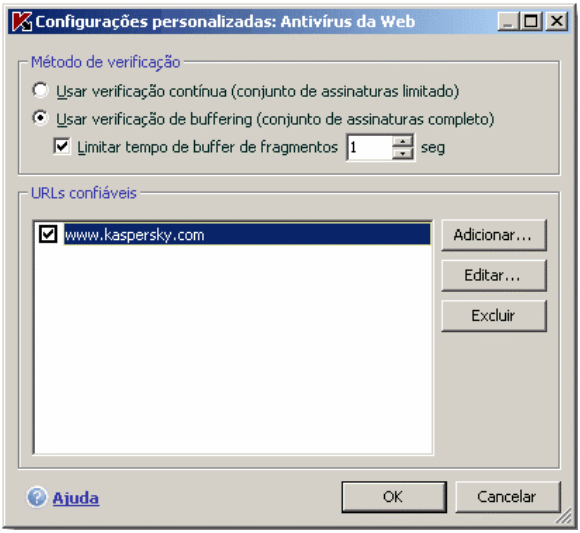


Figura 30. Configurando o Antivírus da Web

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. Este recurso poderá ser usado quando o Antivírus da Web impedir o download de um determinado arquivo, bloqueando-o.

Para criar uma lista de endereços confiáveis:

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

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

***** – qualquer combinação de caracteres.
Exemplo: Se você criar a máscara ***abc***, nenhuma URL que contém **abc**

será verificada. Por exemplo: www.virus.com/download_virus/page_0-9abcdef.html

? – qualquer caractere.

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

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

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

Para que o Kaspersky Anti-Virus for Windows Workstations não processe o **?** como um caractere curinga, coloque uma barra invertida (\) antes dele. Então, a URL que você está adicionando à lista de exclusões será a seguinte:

www.virus.com/download_virus/virus.dll\?virus_name=

9.2.3. Restaurando as configurações padrão do Antivírus da Web

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

Para restaurar as configurações padrão do Antivírus da Web:

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

9.2.4. Selecionando respostas para objetos perigosos

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

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

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

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

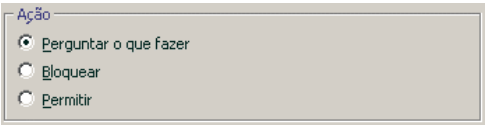


Figura 31. Selecionando ações para scripts perigosos

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

Se a ação selecionada for	Se um objeto perigoso for detectado no tráfego HTTP
Perguntar o que fazer	O Antivírus da Web emitirá uma mensagem de aviso com informações sobre o código mal-intencionado que possivelmente infectou o objeto e lhe dará opções de resposta.
Bloquear	O Antivírus da Web bloqueará o acesso ao objeto e exibirá uma mensagem na tela sobre o bloqueio. Informações semelhantes serão registradas no relatório (consulte a seção 17.3 na p. 239).
Permitir	O Antivírus da Web concederá o acesso ao objeto. Essas informações são registradas no relatório.

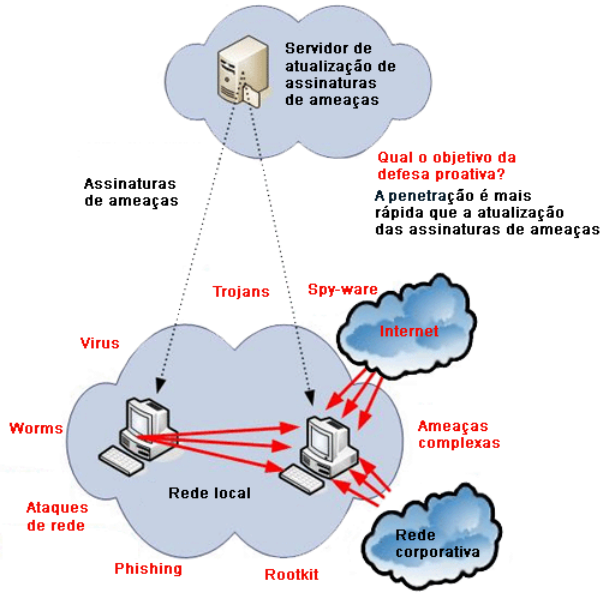
O Antivírus da Web sempre bloqueia scripts perigosos e emite mensagens pop-up que informam o usuário sobre a ação executada. Você não pode alterar a resposta a um script perigoso, além de desabilitar o módulo de verificação do script.

CAPÍTULO 10. DEFESA PROATIVA

Aviso!

Esta versão do aplicativo não tem o componente de defesa proativa **Proteção do Microsoft Office** para computadores que executam o Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista ou Microsoft Windows Vista x64.

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



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

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

As tecnologias preventivas fornecidas pela Defesa Proativa do Kaspersky Anti-Virus for Windows Workstations 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 assinaturas de ameaças, as tecnologias preventivas reconhecem uma nova ameaça no computador por meio da seqüência de ações executadas por um determinado programa. A instalação do aplicativo inclui um conjunto de critérios que podem ajudar a determinar a periculosidade da atividade de um programa. Se a análise da atividade determinar que as ações de um determinado programa são suspeitas, o Kaspersky Anti-Virus executará as ações atribuídas pela regra para esse tipo de atividade.

A atividade perigosa é definida pelas ações totais do programa. Por exemplo, forem executadas ações como o programa copiar a si mesmo para recursos de rede, a pasta de inicialização ou o Registro do sistema e, em seguida, várias cópias forem enviadas, é muito provável que trate-se 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 também controla todas as macros executadas em aplicativos do Microsoft Office.

A Defesa Proativa usa um conjunto de regras fornecidas com o aplicativo, além de regras definidas pelo usuário criadas durante o uso do mesmo. Uma *regra* é um conjunto de critérios que define o comportamento suspeito e como o Kaspersky Anti-Virus deve reagir a ele.

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

Vamos examinar os algoritmos da Defesa Proativa:

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

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

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

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

2. A análise é executada com base nas regras de *permissão* da Defesa Proativa (de acordo com os critérios relevantes, o comportamento é seguro) e nas regras de *bloqueio* (de acordo com os critérios relevantes, o comportamento é mal-intencionado).

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

    - Se a atividade não for definida como perigosa de acordo com os critérios relevantes (regras de *permissão* e *bloqueio*), ela será permitida.

    - Se a atividade for definida como perigosa de acordo com os critérios relevantes, as próximas etapas executadas pelo componente corresponderão às instruções especificadas na regra: geralmente, a atividade é bloqueada. Será exibida uma mensagem na tela especificando o programa perigoso, seu tipo de atividade e um histórico das ações executadas. Aceite a decisão, bloqueie ou permita essa atividade. Você pode criar uma regra para a atividade e cancelar as ações executadas no sistema.

10.1. Configurações da Defesa Proativa

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

- Se a atividade de aplicativos é monitorada no seu computador

Este recurso da Defesa Proativa é habilitado marcando a caixa **Habilitar Verificador de atividade do aplicativo**. Esse modo é habilitado por padrão, o que assegura que as ações de todos os programas abertos no seu computador sejam cuidadosamente controladas. Você pode configurar o procedimento de processamento do aplicativo (consulte a seção 10.1.1 na p. 129) para cada conjunto de atividades perigosas realçado. Também é possível criar exclusões da Defesa Proativa que interrompem a monitoração de aplicativos selecionados.

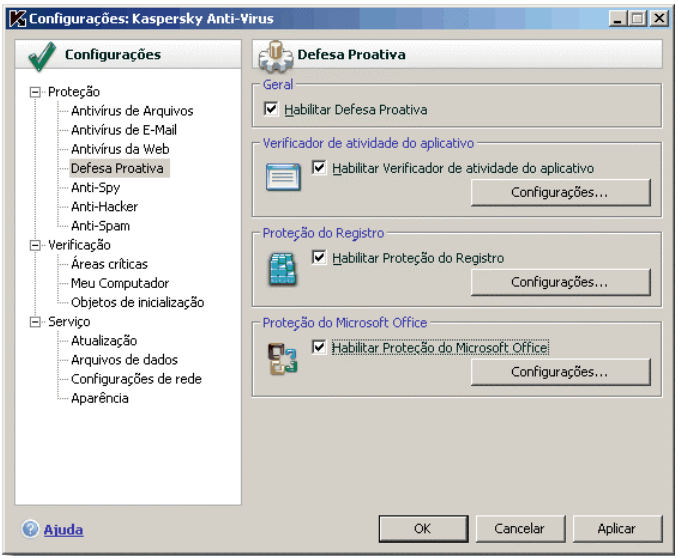


Figura 32. Configurações da Defesa Proativa

- 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 for Windows Workstations analisa todas as tentativas de alterar as chaves do Registro do sistema do Windows.

  Você pode criar suas próprias regras (consulte 10.1.3.2 na p. 138) para monitorar o Registro, dependendo da chave do Registro do Microsoft Windows.

- Se as *macros* são verificadas

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

Você pode selecionar quais macros são consideradas perigosas e o que fazer com elas (consulte 10.1.2 na p. 133).

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.

É possível configurar exclusões (consulte a seção 6.3.1 na p. 78) para os módulos da Defesa Proativa e criar uma lista de aplicativos confiáveis (consulte a seção 6.3.2 na p. 83).

As seções a seguir examinam estes aspectos mais detalhadamente.

10.1.1. Regras de controle de atividades

Observe que a configuração do controle de aplicativos no Microsoft Windows XP Professional x64 Edition, no Microsoft Windows Vista ou no Microsoft Windows Vista x64 é diferente do processo de configuração em outros sistemas operacionais.

Informações sobre a configuração do controle de atividade nesses sistemas operacionais são fornecidas no final desta seção.

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

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

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

- *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.

- *Processos ocultos (rootkit)*. Os rootkits são um conjunto de programas usados para mascarar 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 Windows, além dos utilitários instalados no computador. Ao tentar dissimular sua presença no sistema, os programas mal-intencionados copiam valores incorretos nas chaves do Registro. O Kaspersky Anti-Virus analisa as entradas do Registro do sistema quanto à presença de valores suspeitos.

- *Atividade do sistema suspeita*. O programa analisa as ações executadas pelo Microsoft Windows e exclui as atividades suspeitas. Um exemplo de atividade suspeita seria uma violação de integridade, que envolve a modificação de um ou vários módulos de um aplicativo monitorado desde sua última execução.

- *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.

- *Proteção do Gerenciador de Tarefas do Microsoft Windows*. O Kaspersky Anti-Virus protege o Gerenciador de Tarefas da infiltração de módulos mal-intencionados, quando esses objetivam o bloqueio do funcionamento do Gerenciador de Tarefas.

A lista de atividades perigosas pode ser ampliada automaticamente pelo processo de atualização do Kaspersky Anti-Virus for Windows Workstations, 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 6.3 na p. 77) relacionando os aplicativos com atividades que você não considera perigosas.

Para configurar o monitoramento de atividades,

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

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

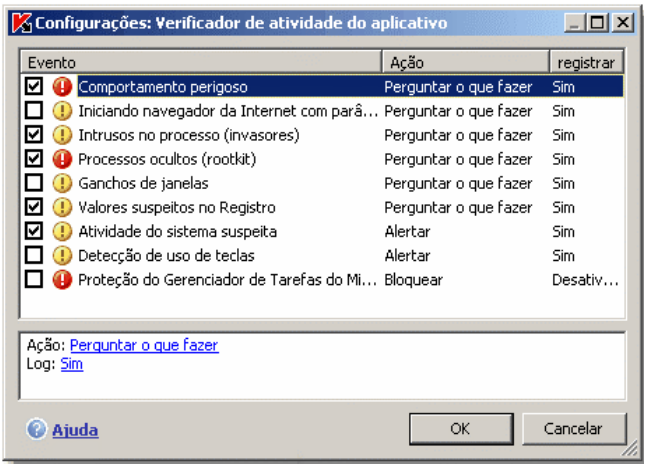


Figura 33. Configurando o controle da atividade de aplicativos

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

- Atribua a resposta da Defesa Proativa à atividade perigosa.

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

chegue ao valor desejado. Além de interromper o processo, você pode colocar o aplicativo que iniciou a atividade perigosa em Quarentena. Para fazê-lo, use o link Ligado / Desligado de acordo com a configuração apropriada. É possível atribuir um período para a freqüência com que a verificação será executada para detectar processos ocultos no sistema.

- Escolha se deseja gerar um relatório sobre a operação executada. Para fazê-lo, clique no link **Log** até ele mostrar Ligado ou Desligado, conforme o desejado.

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

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

Se você estiver executando um dos sistemas operacionais relacionados acima, apenas um tipo de evento do sistema será controlado, a *atividade perigosa*. O Kaspersky Anti-Virus for Windows Workstations 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 34). Por padrão, esta opção está desabilitada.

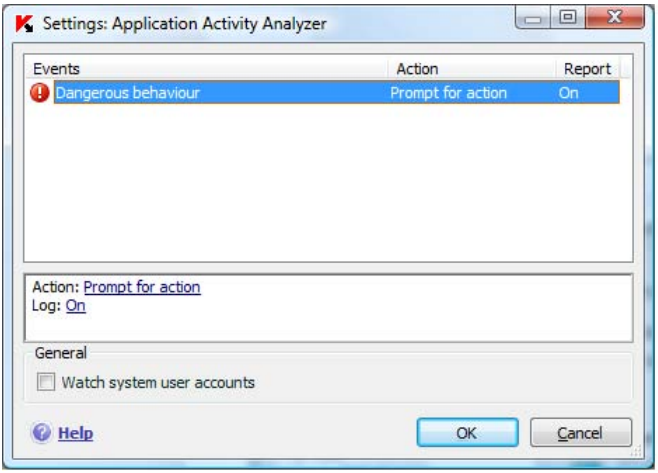


Figura 34. Configurando o controle de atividade de aplicativos no Microsoft Windows XP Professional x64 Edition, Microsoft Windows Vista e Microsoft Windows Vista x64

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.

10.1.2. Proteção do Microsoft Office

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

Você pode habilitar a verificação e o processamento de macros perigosas executadas no computador marcando **Habilitar Proteção do Microsoft Office**. Cada macro executada é verificada e, se estiver na lista de macros perigosas, será processada.

Exemplo:

> A macro *PDFMaker* é um plug-in da barra de ferramentas do Adobe Acrobat no Microsoft Office Word que pode criar um arquivo .pdf a partir de qualquer documento. A Defesa Proativa classifica a incorporação de elementos no software como uma ação perigosa. Se a Proteção do Microsoft Office estiver habilitada, quando uma macro for carregada, a Defesa Proativa emitirá um aviso na tela, informando que foi detectado um comando de macro perigoso. Você pode escolher encerrar a macro ou permitir que continue.

Você pode configurar as ações que o programa executa quando as macros assumem um comportamento suspeito. Se tiver certeza de que essa macro não é perigosa ao trabalhar com um arquivo específico, por exemplo, um documento do MS Word, é recomendável criar uma regra de exclusão. Se ocorrer uma correspondência com os termos da regra de exclusão, a ação suspeita executada pela macro não será processada pela Defesa Proativa.

Para configurar a Proteção do Microsoft Office:

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

As regras para o processamento de macros perigosas são configuradas na janela **Configurações: Proteção do Microsoft Office** (veja a Figura 35). Ela contém regras padrão para comportamentos classificados pela Kaspersky Lab

como perigosos, juntamente com a resposta a ser executada pela Defesa Proativa. Essas ações de macros perigosas incluem, por exemplo, a incorporação de módulos em programas e a exclusão de arquivos.

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

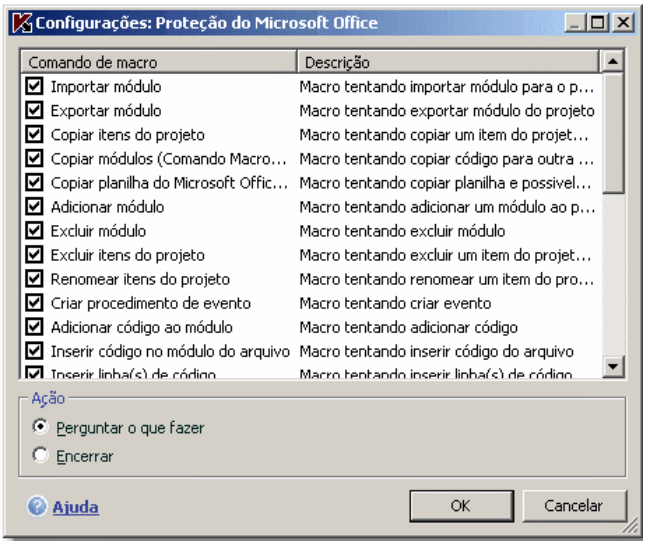


Figura 35. Configurando a Proteção do Microsoft Office

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

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

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

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

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

10.1.3. Proteção do Registro

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

Por exemplo, os programas mal-intencionados podem copiar suas informações na chave do Registro que faz os aplicativos abrirem automaticamente na inicialização. Assim, esses programas serão iniciados na inicialização do sistema operacional.

Para configurar o monitoramento do Registro do sistema:

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

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

A janela **Configurações: Proteção do Registro** (veja a Figura 36) 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.

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 10.1.3.1 na p. 136) 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 10.1.3.2 na p. 138) que se aplicará às chaves selecionadas na guia Chaves. Você pode criar várias regras e definir a ordem na qual elas são aplicadas.

Figura 36. Grupos de chaves do registro controlados

10.1.3.1. 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** mostra a lista de arquivos aos quais as regras se aplicam.

Para adicionar um arquivo do Registro do sistema:

1. Clique no botão **Adicionar** na janela **Editar...** (veja a Figura 37).

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.

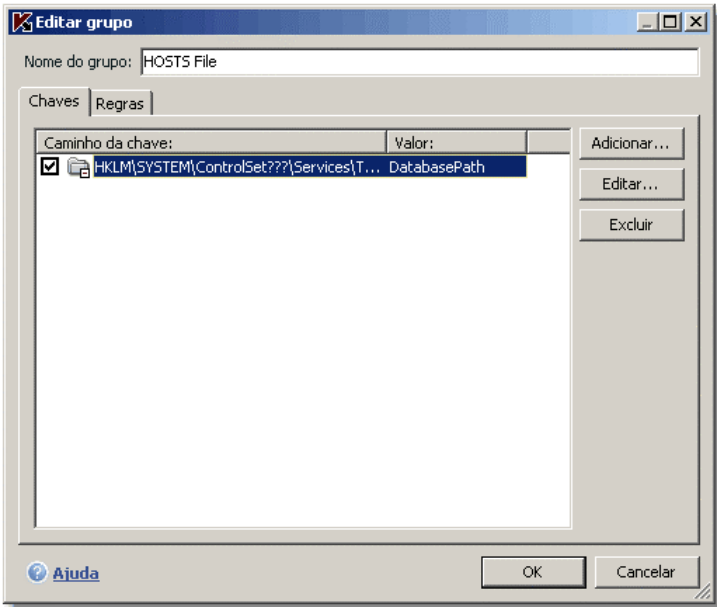


Figura 37. Adicionando chaves do Registro controladas

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

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

10.1.3.2. 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 38).
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.

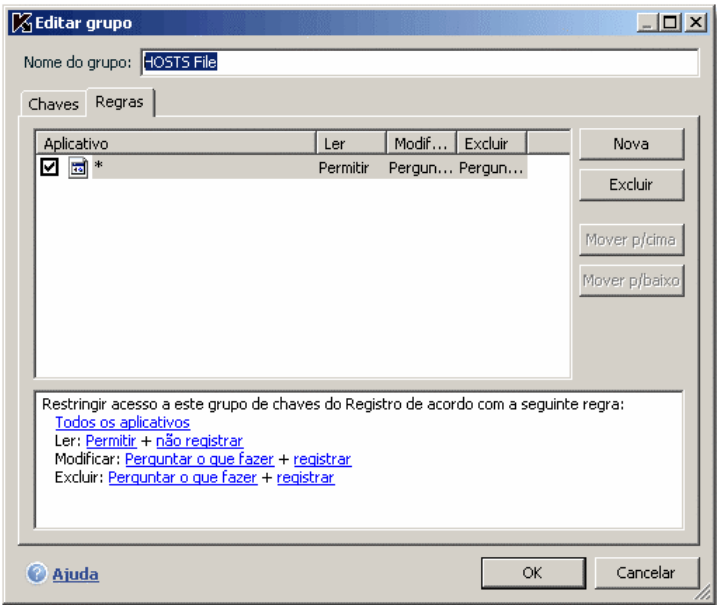


Figura 38. Criando uma regra de monitoramento de chaves do Registro

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. ANTI-SPY

O componente do Kaspersky Anti-Virus for Windows Workstations que o protege contra todos os tipos de malware é chamado *Anti-Spy*. Recentemente, cada vez mais os malwares incluem programas que têm como objetivo:

- Roubar suas informações confidenciais, incluindo senhas, números de cartões de crédito, documentos importantes, etc.
- Controlar suas ações no computador e analisar o software instalado nele.
- Inserir inadvertidamente conteúdo publicitário em navegadores da Web, janelas pop-up e banners em vários programas.
- Obter acesso não-autorizado à Internet pelo seu computador para vários sites.

O objetivo do phishing e dos registradores de uso do teclado é roubar suas informações; os discadores automáticos, programas de piadas e adware podem consumir seu tempo e dinheiro. O Anti-Spy foi criado para protegê-lo desses programas.

O Anti-Spy inclui os seguintes módulos:

- O *componente Anti-Phishing* o protege de ataques de phishing.

  Em geral, o phishing consiste em e-mails de supostas instituições financeiras com links para seus sites. O texto da mensagem convence o leitor a clicar em um link e digitar informações confidenciais em uma página da Web, por exemplo, um número de cartão de crédito ou um logon e senha de um site bancário real da Internet.

  Um exemplo comum de phishing é um e-mail supostamente enviado pelo banco contendo um link para o site oficial. Ao clicar no link, você é direcionado para uma cópia exata do site do banco e pode até ver o endereço na barra de endereço do navegador, embora esteja na página de um site falso. Desse momento em diante, todas as ações executadas no site são controladas e podem ser usadas para roubá-lo.

  Você pode receber um link para um site de phishing por e-mail ou por um programa de mensagens instantâneas. O Anti-Phishing controla as tentativas de abrir sites de phishing e as bloqueia.

  As assinaturas de ameaças do Kaspersky Anti-Virus for Windows Workstations incluem os endereços de todos os sites de phishing conhecidos no momento. Os especialistas da Kaspersky Lab alimentam a lista com endereços obtidos de uma organização internacional, o Anti-

Phishing Working Group. Sites são adicionados à lista através da atualização das assinaturas de ameaças.

- O componente *Popup Blocker* bloqueia as janelas pop-up que contêm anúncios com links para vários sites.

  Geralmente, as informações nessas janelas não trazem qualquer benefício. Elas são abertas automaticamente quando você abre um determinado site ou vai para outra janela usando um hiperlink. Elas contêm anúncios e outras informações que você não solicitou. O componente Popup Blocker bloqueia essas janelas e uma mensagem especial acima do ícone na bandeja do sistema o informa a respeito. É possível determinar diretamente nessa mensagem se você deseja bloquear a janela ou não.

  > O Popup Blocker funciona corretamente com o módulo de bloqueio de pop-ups no Microsoft Internet Explorer incluído no Service Pack 2 para Microsoft Windows XP. Ao instalar o Kaspersky Anti-Virus for Windows Workstations, é instalado um plug-in no navegador, com o qual você pode permitir janelas pop-up diretamente do navegador.

  Alguns sites usam janelas pop-up legitimamente, para fornecer informações com mais rapidez e conveniência. Se você usa esses sites com freqüência e as janelas pop-up são importantes para você, é possível adicioná-las à lista de sites confiáveis (consulte 11.1.1 na p. 142).

  Ao usar o Microsoft Internet Explorer, o ícone  aparecerá na barra de status do navegador quando uma janela pop-up for bloqueada. É possível desbloqueá-la ou adicionar o endereço à lista de endereços confiáveis, clicando nele.

- O componente *Anti-Banner* bloqueia os banners de anúncios em páginas da Web ou incorporados nas interfaces de programas instalados no computador.

  Os banners de anúncios são desprovidos de qualquer informação útil e, além disso, atrapalham seu trabalho e aumentam a quantidade de tráfego no computador. O Anti-Banner bloqueia os banners de anúncios mais comuns, com base em máscaras criadas pelo Kaspersky Anti-Virus for Windows Workstations. É possível desabilitar o bloqueio de banners ou criar suas próprias listas de banners permitidos e bloqueados.

Para integrar o Anti-Banner ao **Opera**, adicione a seguinte linha a *standard_menu.ini*, na seção **[Image Link Popup Menu]**:

Item, "New banner" = Copy image address & Execute program, "…\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Workstations\opera_banner_deny.vbs", "//nologo %C"

- O componente *Anti-Dialer* o protege contra conexões não autorizadas do modem.

O Anti-Dialer é executado no Microsoft Windows 2000, Microsoft Windows XP, Microsoft Windows XP x64, Microsoft Windows Vista e Microsoft Windows Vista x64.

Em geral, os discadores estabelecem conexões com sites específicos, como sites de material pornográfico. Então, você é forçado a pagar por um tráfego dispendioso que nunca desejou nem usou. Se desejar excluir um número da lista de bloqueados, coloque-o na lista de números confiáveis (consulte a seção 11.1.3 na p. 147).

11.1. Configurando o Anti-Spy

O Anti-Spy o protege de todos os programas conhecidos pela Kaspersky Lab capazes de roubar suas informações confidenciais ou seu dinheiro. É possível configurar o componente mais especificamente:

- Uma lista de sites confiáveis (consulte 11.1.1 na p. 142) cujas janelas pop-up você não deseja bloquear
- Uma lista negra e uma lista branca de banners (consulte 11.1.2 na p. 144)
- Criando listas de telefones confiáveis (consulte 11.1.3 na p. 147) para conexões discadas permitidas

11.1.1. Criando uma lista de endereços confiáveis no Popup Blocker

Por padrão, o Popup Blocker bloqueia a maioria das janelas pop-up automáticas. A exceção são as janelas pop-up dos sites pertencentes à lista de sites confiáveis no Microsoft Internet Explorer e sites da intranet da qual você faz parte.

Se estiver executando o Windows XP com Service Pack 2, o Internet Explorer já possui seu próprio bloqueador de pop-ups, que você pode configurar selecionando as janelas específicas que deseja bloquear ou não. O Popup Blocker é compatível com esse bloqueador, de acordo com o seguinte princípio: uma regra de bloqueio tem precedência, ou seja, se o Internet Explorer ou o Popup Blocker tiver uma regra de bloqueio para uma janela pop-up, ela será bloqueada. Por isso, é recomendável que o navegador e o Popup Blocker sejam configurados se você executar o Microsoft Windows XP Service Pack 2.

Se, por algum motivo, você desejar exibir uma janela pop-up, adicione-a à lista de endereços confiáveis. Para fazê-lo:

1. Abra a janela de configuração do Kaspersky Anti-Virus for Windows Workstations e selecione Anti-Spy na árvore de configurações.
2. Clique em **Sites confiáveis** na seção **Habilitar Bloqueio de Pop-ups**.
3. Clique em **Adicionar** na janela que é aberta (veja a Figura 39) e insira uma máscara para os sites cujas janelas pop-up você não deseja bloquear.

   Dica:

   Ao inserir uma máscara de endereços confiáveis, é possível usar os caracteres ***** ou **?**.

   Por exemplo, a máscara http://www.test* exclui pop-ups de qualquer site que comece com essa série de caracteres.

4. Especifique se os endereços na zona confiável do Internet Explorer ou os endereços da sua rede local serão excluídos da verificação. O programa os considera confiáveis por padrão e não bloqueia as janelas pop-up desses endereços.

A nova exclusão será adicionada ao início da lista de endereços confiáveis. Para interromper o uso da exclusão adicionada, desmarque a caixa ☑ ao lado de seu nome. Se desejar remover uma exclusão completamente, selecione-a na lista e clique em **Excluir**.

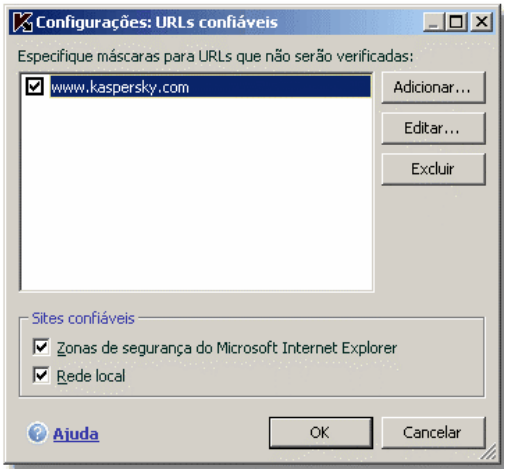


Figura 39. Criando uma lista de endereços seguros

Para bloquear pop-ups da sua intranet ou de sites incluídos na lista de sites confiáveis do Microsoft Internet Explorer, desmarque as caixas correspondentes na seção **Sites confiáveis**.

Quando as janelas pop-up que não estão na lista de endereços confiáveis tentarem abrir, será exibida uma mensagem sobre o ícone do programa informando que ela foi bloqueada. Existem links na mensagem que permitem cancelar o bloqueio e adicionar o endereço da janela à lista de endereços confiáveis.

Você também pode desbloquear janelas pelo Internet Explorer, se tiver o Windows XP Service Pack 2. Para fazê-lo, use o menu de contexto que pode ser aberto acima do ícone do programa que pisca no canto inferior do navegador quando as janelas pop-up são bloqueadas.

11.1.2. Lista de bloqueio de banners de anúncios

O *Anti-Banner* é o componente do Kaspersky Anti-Virus for Windows Workstations responsável pelo bloqueio de banners de anúncios. Os especialistas da Kaspersky Lab compilaram uma lista de máscaras dos banners de anúncios mais comuns com base em uma pesquisa específica e a incluíram no programa. Se o Anti-Banner não for desabilitado, ele bloqueará os banners de anúncios selecionados pelas máscaras nesta lista.

Você também pode criar uma lista branca e uma lista negra para permitir ou bloquear banners de anúncios.

Observe que, se a lista de banners bloqueados ou a lista negra contiver uma máscara para filtrar domínios, você ainda poderá acessar o site raiz.

Por exemplo, se a lista de banners bloqueados incluir uma máscara para **truehits.net**, você poderá acessar **http://truehits.net**, mas o acesso a **http://truehits.net/a.jpg** será bloqueado.

11.1.2.1. Configurando a lista de banners de anúncios padrão

O Kaspersky Anti-Virus for Windows Workstations inclui uma lista de máscaras para os banners de anúncios mais comuns em sites e interfaces de programas. Essa lista foi compilada pelos especialistas da Kaspersky Lab, sendo atualizada junto com as assinaturas de ameaças.

É possível selecionar quais máscaras de banners de anúncios padrão serão usadas com o Anti-Banner. Para fazê-lo:

1. Abra a janela de configuração do Kaspersky Anti-Virus for Windows Workstations e selecione Anti-Spy na árvore de configurações.
2. Clique no botão **Configurações** na seção Anti-Banner.
3. Abra a guia **Geral** (veja a Figura 40). O Anti-Banner bloqueará as máscaras de banners de anúncios relacionadas na guia. É possível usar caracteres curinga em um endereço de banner.

A lista de máscaras bloqueadas padrão não pode ser editada. Se não desejar bloquear um banner incluído em uma máscara padrão, desmarque a caixa ☑ ao lado da máscara.

Para analisar banners de anúncios que não correspondem às máscaras da lista padrão, marque ☑ **Usar métodos de análise heurística**. Assim, o aplicativo analisará as imagens carregadas quanto a sinais típicos de banners de anúncios. De acordo com essa análise, a imagem poderá ser identificada como um banner e ser bloqueada.

Também é possível criar suas próprias listas de banners permitidos e bloqueados. Para fazê-lo, use as guias **Lista branca** e **Lista negra**.

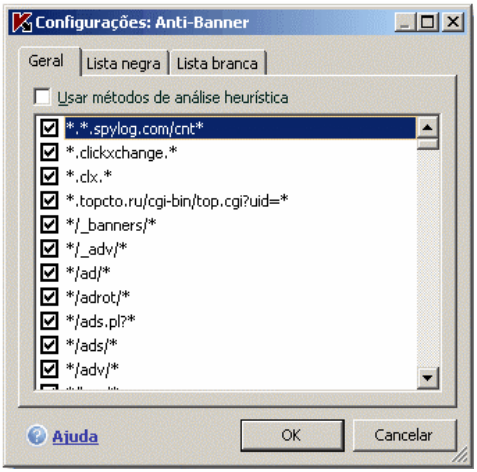


Figura 40. Lista de banners bloqueados

11.1.2.2. Listas brancas de banners de anúncios

Você pode criar uma lista branca de banners de anúncios para permitir que determinados banners sejam exibidos. Essa lista contém máscaras para os banners de anúncios permitidos.

Para adicionar uma nova máscara à lista branca:

1. Abra a janela de configuração do Kaspersky Anti-Virus for Windows Workstations e selecione Anti-Spy na árvore de configurações.
2. Clique no botão **Configurações** na seção Anti-Banner.
3. Abra a guia **Lista branca**.

Adicione a máscara de banners permitidos com o botão **Adicionar**. É possível especificar a URL completa do banner ou uma máscara para ela. No último caso, ao tentar carregar um banner, o programa verificará seu endereço de acordo com a máscara especificada.

Ao criar uma máscara, você pode usar os curingas ***** ou **?**(onde * representa uma seqüência de caracteres e ? representa qualquer caractere).

Para interromper o uso de uma máscara criada, você pode excluí-la da lista ou desmarcar a caixa ☑ ao seu lado. Em seguida, os banners incluídos nessa máscara serão revertidos para serem bloqueados.

Usando os botões **Importar** e **Exportar**, é possível copiar as listas de banners permitidos de um computador para outro.

11.1.2.3. Listas negras de banners de anúncios

Além da lista padrão de banners bloqueados (consulte a seção 11.1.2.1 na p. 145) pelo Anti-Banner, é possível criar sua própria lista. Para fazê-lo:

1. Abra a janela de configuração do Kaspersky Anti-Virus for Windows Workstations e selecione Anti-Spy na árvore de configurações.
2. Clique no botão **Configurações** na seção de banners bloqueados.
3. Abra a guia **Lista negra**.

Usando o botão **Adicionar**, insira uma máscara para o banner que o Anti-Banner deve bloquear. É possível especificar a URL completa do banner ou uma máscara para ela. No último caso, ao tentar carregar um banner, o programa verificará seu endereço de acordo com a máscara especificada.

Ao criar uma máscara, você pode usar os curingas ***** ou **?**(onde * representa uma seqüência de caracteres e ? representa qualquer caractere).

Para interromper o uso de uma máscara criada, você pode excluí-la da lista ou desmarcar a caixa ☑ ao seu lado.

Usando os botões **Importar** e **Exportar**, é possível copiar as listas de banners bloqueados de um computador para outro.

11.1.3. Criando uma lista de números confiáveis no Anti-Dialer

O componente *Anti-Dialer* monitora os telefones usados para conectar-se secretamente à Internet. A conexão é considerada secreta quando é configurada para não informar ao usuário sobre a conexão ou quando não é inicializada por ele.

Sempre que há uma tentativa de conexão secreta, o programa o notifica, emitindo uma mensagem específica na tela, solicitando que o usuário permita ou bloqueie a chamada telefônica. Se você não inicializou a conexão, é muito provável que ela tenha sido configurada por um programa mal-intencionado.

Se desejar permitir conexões com determinados números sem precisar confirmar a cada vez, adicione-os à lista de números confiáveis. Para fazê-lo:

1. Abra a janela de configuração do Kaspersky Anti-Virus for Windows Workstations e selecione Anti-Spy na árvore de configurações.
2. Clique em **Números confiáveis** na seção Anti-Dialer.
3. Clique em **Adicionar** na janela que é aberta (veja a Figura 41) e insira um número ou uma máscara para os números de telefones legítimos.

Dica:

Ao inserir uma máscara de números confiáveis, é possível usar os caracteres ***** ou **?**.

Por exemplo, *0???? 79787* abrangerá todos os números começados por 79787 com o código de área de quatro dígitos.*

O novo número de telefone será adicionado ao início da lista de números confiáveis. Para interromper o uso da exclusão do número adicionada, desmarque a caixa ☑ ao lado de seu nome. Se desejar remover uma exclusão completamente, selecione-a na lista e clique em **Excluir**.

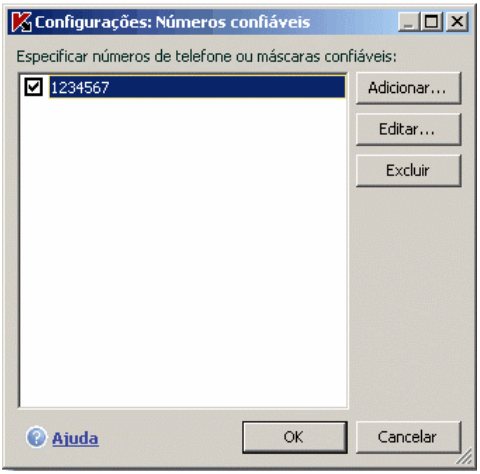
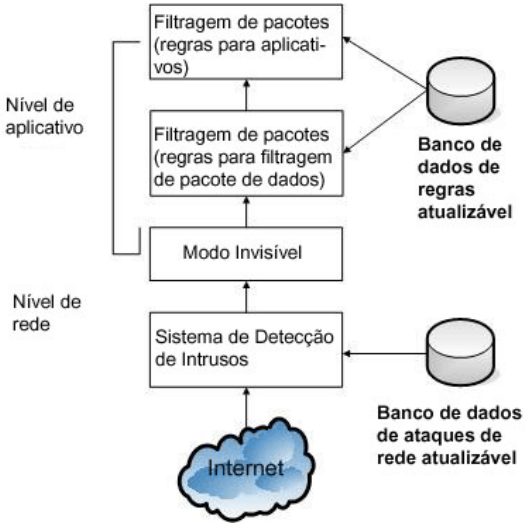


Figura 41. Criando uma lista de endereços confiáveis

CAPÍTULO 12. PROTEÇÃO CONTRA ATAQUES DE REDE

Atualmente, os computadores tornaram-se bastante vulneráveis quando conectados à Internet. Eles estão sujeitos a infecções por vírus e outros tipos de ataques que tiram proveito das vulnerabilidades nos sistemas operacionais e nos softwares.

O componente *Anti-Hacker* do Kaspersky Anti-Virus for Windows Workstations garante a segurança em redes locais e na Internet, protegendo o computador nos níveis de rede e de aplicativos, além de mascarar o computador na rede para evitar ataques. Vamos examinar mais detalhadamente como o Anti-Hacker funciona.



Você fica protegido no nível de rede por meio de regras globais de filtragem de pacotes, segundo as quais a atividade de rede é permitida ou bloqueada, com base em uma análise de configurações como: direção do pacote, o protocolo de transferência de dados e a porta dos pacotes enviados. As regras para pacotes de dados estabelecem o acesso à rede, independentemente dos aplicativos instalados no seu computador que usam a rede.

Além das regras para filtragem de pacotes, o *Sistema de Detecção de Intrusos* (SDI) fornece uma segurança adicional no nível de rede. O objetivo do SDI é analisar as conexões de entrada, detectar verificações de portas no computador

e filtrar pacotes de rede que visam explorar vulnerabilidades de software. Quando executado, o SDI bloqueia todas as conexões de entrada de um computador invasor por um determinado período e o usuário recebe uma mensagem informando que o computador sofreu uma tentativa de ataque de rede.

O Sistema de Detecção de Intrusos usa um banco de dados de ataques de rede específico (consulte a seção 12.9 na p. 167) na análise, que a Kaspersky Lab amplia periodicamente e que é atualizado juntamente com as assinaturas de ameaças.

O computador é protegido no nível de aplicativo fazendo os aplicativos instalados no computador seguirem as regras de aplicativos do Anti-Hacker para o uso dos recursos de rede. Assim como o nível de segurança de rede, o nível de segurança de aplicativos foi criado com base na análise de pacotes de dados quanto ao direcionamento, ao protocolo de transferência e às portas que usam. Entretanto, no nível de aplicativo, as ameaças de pacotes de dados e os aplicativos específicos que enviam e recebem os pacotes são considerados.

O uso de regras para aplicativos ajuda a configurar uma proteção específica permitindo, por exemplo, que um determinado tipo de conexão seja banido para alguns aplicativos mas não para outros.

Há dois tipos de regras do Anti-Hacker, baseadas nos seus dois níveis de segurança:

- *Regras para filtragem de pacotes* (consulte 12.3 na p. 157). Usadas para criar restrições gerais sobre a atividade de rede, independentemente dos aplicativos instalados. Exemplo: se você criar uma regra para filtragem de pacotes que bloqueie as conexões de entrada na porta 21, nenhum aplicativo que use essa porta (um servidor FTP, por exemplo) ficará acessível do exterior.
- *Regras para aplicativos* (consulte 12.2 na p. 152). Usadas para criar restrições sobre a atividade de rede para aplicativos específicos. Exemplo: se as conexões na porta 80 forem bloqueadas para todos os aplicativos, você poderá criar uma regra que permita conexões nessa porta somente para o Firefox.

Existem dois tipos de regras para filtragem de pacotes e para aplicativos: de *permissão* e de *bloqueio*. A instalação do programa inclui regras que ajustam a atividade de rede para os aplicativos mais comuns e que usam os protocolos e portas mais comuns. O Kaspersky Anti-Virus for Windows Workstations também inclui um conjunto de regras de permissão para aplicativos confiáveis, cuja atividade de rede não seja suspeita.

O Kaspersky Anti-Virus for Windows Workstations divide todo o espaço da rede em zonas para tornar as configurações e regras mais amigáveis: *Internet* e *zonas de segurança*, que correspondem em grande parte às sub-redes às quais

o seu computador pertence. É possível atribuir um status para cada zona (*Internet, rede local, zona de segurança*), que determina a política de aplicação de regras e do monitoramento da atividade de rede nessa zona (consulte a seção 12.5 na p. 162).

Um recurso específico do Anti-Hacker, o *Modo Invisível*, evita que o computador seja detectado do exterior, de forma que os hackers não possam detectar o computador para atacá-lo. Esse modo não afeta o desempenho do computador na Internet: é recomendável não usar o Modo Invisível se o computador estiver funcionando como servidor.

12.1. Selecionando um nível de segurança do Anti-Hacker

Quando você usa a rede, o Kaspersky Anti-Virus for Windows Workstations protege o computador em um dos seguintes níveis (veja a Figura 42):

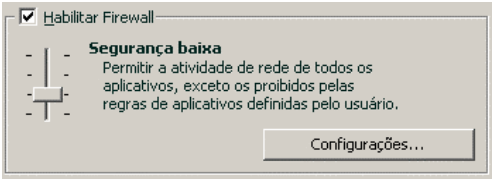


Figura 42. Selecionando um nível de segurança do Anti-Hacker

Segurança alta – passa apenas a atividade de rede permitida, usando regras de permissão fornecidas com o programa ou que você criou. O conjunto de regras fornecidas com o Kaspersky Anti-Virus for Windows Workstations inclui regras de permissão para aplicativos cuja atividade de rede não é suspeita e para pacotes de dados que são totalmente seguros para envio e recebimento. Entretanto, se houver uma regra de bloqueio com prioridade mais alta que a regra de permissão, o programa bloqueará a atividade de rede desse aplicativo.

> Aviso!
>
> Se você selecionar esse nível de segurança, toda a atividade de rede não registrada em uma regra de permissão do Anti-Hacker será bloqueada. Portanto, é recomendável usar esse nível somente se você tiver certeza de que todos os programas necessários são permitidos pelas regras para fazer conexões de rede e não planejar instalar novos softwares.

Modo de treinamento – nível de proteção no qual as regras do Anti-Hacker são criadas. Nesse nível, sempre que um programa tentar usar um recurso de rede, o Anti-Hacker verificará se existe uma regra para essa conexão. Se houver uma regra, o Anti-Hacker a aplicará. Se não houver uma regra, aparecerá uma mensagem na tela contendo uma descrição da conexão de rede (qual programa a iniciou, em qual porta, o protocolo, etc.). Você deve decidir se permitirá ou não a conexão. Usando um botão específico na janela da mensagem, é possível criar uma regra para essa conexão de forma que, no futuro, o Anti-Hacker aplique a nova regra para essa conexão sem emitir o aviso na tela.

Segurança baixa – bloqueia apenas a atividade de rede banida, usando regras de bloqueio instaladas com o programa ou que você criou. Entretanto, se houver uma regra de permissão para um aplicativo com prioridade mais alta que a regra de bloqueio, o programa permitirá a atividade de rede desse aplicativo.

Permitir tudo – permite toda a atividade de rede no computador. É recomendável definir a proteção nesse nível em casos extremamente raros, quando nenhum ataque de rede ativo foi observado e você confiar totalmente em toda a atividade de rede.

Você pode aumentar ou diminuir o nível de segurança de rede selecionando o nível existente desejado ou alterando as configurações do nível atual.

Para modificar um nível de segurança de rede:

1. Selecione **Anti-Hacker** na janela de configurações do Kaspersky Anti-Virus for Windows Workstations.
2. Ajuste o controle deslizante na seção **Habilitar Firewall** para indicar o nível de segurança desejado.

Para configurar o nível de segurança de rede:

1. Selecione o nível de segurança que melhor corresponde às suas preferências.
2. Clique no botão **Configurações** e edite as configurações de segurança de rede na janela exibida.

12.2. Regras para aplicativos

O Kaspersky Anti-Virus for Windows Workstations inclui um conjunto de regras para os aplicativos do Windows mais comuns. A atividade de rede desses programas foi analisada em detalhes pela Kaspersky Lab e definidos rigorosamente como perigosos ou confiáveis.

Dependendo do nível de segurança (consulte a seção 12.1 na p. 151) selecionado pelo Firewall e do tipo de rede (consulte a seção 12.5 na p. 162) na qual o computador é executado, é possível usar a lista de regras para programas de diversas maneiras. Por exemplo, com **Proteção máxima**, toda a atividade de rede dos aplicativos que não corresponder às regras de permissão será bloqueada.

Para trabalhar com a lista de regras para aplicativos:

1. Clique em **Configurações** na seção Firewall da janela de configurações do Anti-Hacker.
2. Na janela que é aberta, selecione a guia **Regras para aplicativos** (veja a Figura 43).

As regras nessa guia podem ser agrupadas de uma das seguintes maneiras:

- *Regras para aplicativos* Se **Agrupar regras por aplicativo** estiver marcado, cada aplicativo para o qual foram criadas regras será mostrado em uma única linha na lista. As seguintes informações são fornecidas para cada aplicativo: nome e ícone do aplicativo, prompt de comando, diretório raiz no qual o arquivo executável do aplicativo se localiza e o número de regras criadas para ele.

  Usando o botão **Editar**, você pode ir para a lista de regras para o aplicativo selecionado na lista e editá-la: adicionar uma nova regra, editar regras existentes e alterar sua prioridade relativa.

  Usando o botão **Adicionar**, você pode adicionar um novo aplicativo à lista e criar uma regra para ele.

  Os botões **Exportar** e **Importar** foram criados para transferir as regras para outros computadores, o que ajuda na rápida configuração do Anti-Hacker.

- *Lista geral de regras* Se **Agrupar regras por aplicativo** estiver desmarcado, cada linha na lista geral exibirá as informações completas de uma regra: o nome do aplicativo e o comando para iniciá-lo, se a atividade de rede deve ser permitida ou bloqueada, o protocolo de transferência de dados, a direção dos dados (de entrada ou saída) e outras informações.

  Usando o botão **Adicionar**, você pode criar uma nova regra e pode alterar uma regra existente, selecionando-a na lista e clicando no botão **Editar**. Também é possível editar as configurações básicas na parte inferior da guia.

  Você pode alterar sua prioridade relativa com os botões **Mover para cima** e **Mover para baixo**.

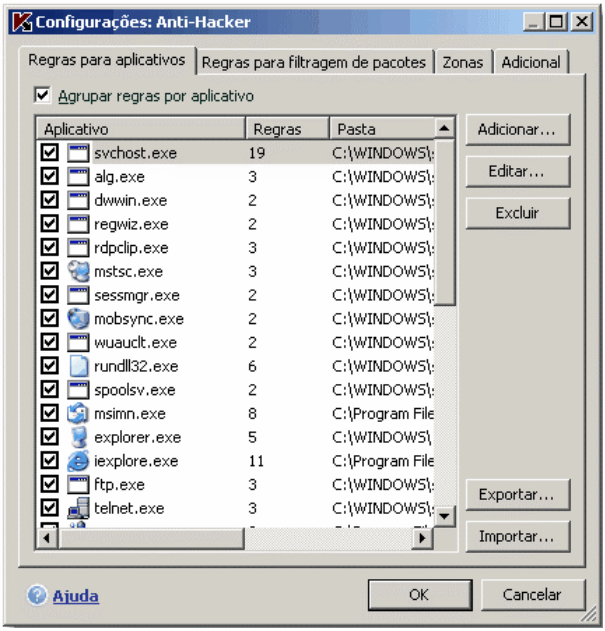


Figura 43. Lista de regras para os aplicativos instalados em um computador

12.2.1. Criando regras manualmente

Para criar uma regra para aplicativos manualmente:

1. Selecione o aplicativo. Para fazê-lo, clique no botão **Adicionar** na guia **Regras para aplicativos** (veja a Figura 43). Isso exibirá um menu de atalho que o levará a uma caixa de seleção de arquivos padrão com a opção **Procurar** ou para uma lista de aplicativos em execução com a opção **Aplicativos**, permitindo que você faça sua seleção. Uma lista de regras para o aplicativo selecionado será aberta. Se já existirem regras para ele, elas estarão relacionadas na parte superior da janela. Se não existirem regras, a janela de regras estará vazia.
2. Clique no botão **Adicionar** na janela de regras do aplicativo selecionado.

Você pode usar a janela **Nova regra** que é aberta para fazer o ajuste fino de uma regra (consulte a seção 12.6 na p.162).

12.2.2. Criando regras a partir de um modelo

O antivírus inclui modelos de regras prontos que podem ser usados para criar suas próprias regras.

Toda a variedade de aplicativos de rede existentes pode ser dividida em vários tipos: clientes de e-mail, navegadores da Web etc. Cada tipo se caracteriza por um conjunto de atividades específicas, como envio e recebimento de e-mails ou recebimento e exibição de páginas HTML. Cada tipo usa um determinado conjunto de portas e protocolos de rede. Por isso, os modelos de regras ajudam a definir, rápida e facilmente, as configurações iniciais das regras com base no tipo de aplicativo.

Para criar uma regra para aplicativos a partir de um modelo:

1. Marque **Agrupar regras por aplicativo** na guia **Regras para aplicativos**, se ainda não estiver marcado, e clique no botão **Adicionar**.
2. Isso exibirá um menu de atalho que o levará a uma caixa de seleção de arquivos padrão com a opção **Procurar** ou para uma lista de aplicativos em execução com a opção **Aplicativos**, permitindo que você faça sua seleção. Em seguida, será aberta uma caixa de diálogo com regras para o aplicativo selecionado. As regras do aplicativo serão exibidas na parte superior da janela. Se nenhuma regra tiver sido criada, a janela estará vazia.
3. clique em **Modelo** na janela de regras para aplicativos e selecione um dos modelos de regrar no menu de contexto (veja a Figura 44).

   Permitir tudo é uma regra que permite qualquer a atividade de rede para o aplicativo. **Bloquear tudo** é uma regra que bloqueia qualquer atividade de rede para o aplicativo. Todas as tentativas desse aplicativo de iniciar uma conexão de rede serão bloqueadas sem notificar o usuário.

   Outros modelos relacionados no menu de contexto criam regras típicas para os tipos de programas correspondentes. Por exemplo, o modelo **Cliente de e-mail** cria um conjunto de regras que permitem a atividade de rede padrão para programas de e-mail, como o envio de e-mail.

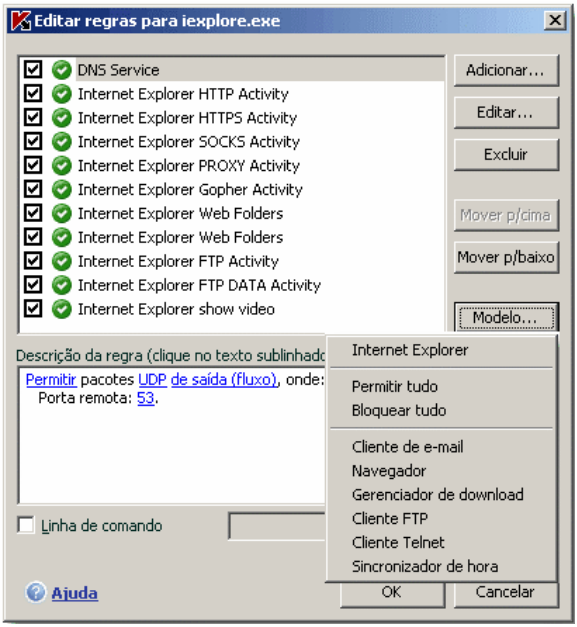


Figura 44. Selecionando um modelo para criar uma nova regra.

4. Edite as regras criadas para o aplicativo, se necessário. Você pode modificar ações, a direção da conexão de rede, o endereço remoto, as portas (local e remota) e o intervalo de tempo para a regra.

5. Se desejar que a regra se aplique a um programa aberto com determinadas configurações da linha de comando, marque ☑ **Linha de comando** e insira a seqüência de caracteres no campo à direita.

A regra ou o conjunto de regras criado será adicionado ao final da lista, com a classificação de prioridade mais baixa. É possível aumentar a prioridade da regra (consulte a seção 12.5 na p. 162).

Você pode criar uma regra da janela de alerta de detecção de atividade de rede (consulte a seção 12.10 na p. 170).

12.3. Regras para filtragem de pacotes

O pacote de instalação do Kaspersky Anti-Virus inclui um conjunto de regras usado para filtrar os pacotes de dados que entram e saem do computador. Você ou um programa instalado no computador podem iniciar a transferência de pacotes de dados. O programa inclui regras para filtragem de pacotes criadas pela Kaspersky Lab, que determinam se os pacotes de dados são perigosos ou não.

Dependendo do nível de segurança selecionado para o Firewall e o tipo de rede na qual o computador está sendo executado, a lista de regras pode ser usada de diversas maneiras. Por exemplo, no nível **Alto**, toda a atividade de rede que não corresponder às regras de permissão será bloqueada.

Importante!

As regras para as zonas de segurança (consulte a seção 12.6 na p. 162) são prioritárias com relação às regras de bloqueio de pacotes. Assim, por exemplo, se você selecionar o status **Rede local**, as trocas de pacotes serão permitidas e também o acesso a pastas compartilhadas, independentemente das regras de bloqueio de pacotes.

Para trabalhar com a lista de regras para filtragem de pacotes:

1. Clique em **Configurações** na seção Firewall da janela de configurações do Anti-Hacker.
2. Na janela que é aberta, selecione a guia **Regras para filtragem de pacotes** (veja a Figura 45).

As seguintes informações são fornecidas para cada regra de filtragem de pacotes: nome da regra, a ação (ou seja, permitir ou bloquear a transferência de pacotes), o protocolo de transferência de dados, a direção do pacote e as configurações da conexão de rede usada para transferir o pacote.

Se a caixa ao lado do nome da regra estiver marcada, a regra será usada.

É possível trabalhar com a lista de regras usando os botões à direita da lista.

Para criar uma nova regra para filtragem de pacotes:

Clique no botão **Adicionar** na guia **Regras para filtragem de pacotes**.

Na janela **Nova regra** que é aberta, existe um formulário que pode ser usado para ajustar uma regra precisamente (consulte a seção 12.4 na p. 158).

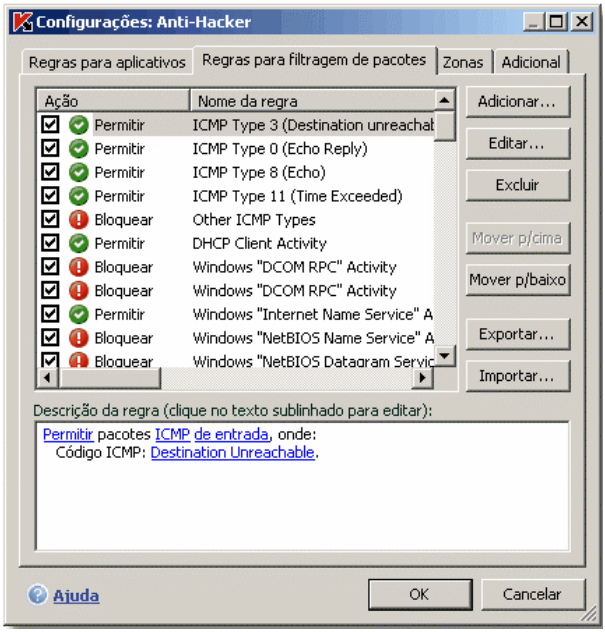


Figura 45. Lista de regras para filtragem de pacotes

12.4. Fazendo o ajuste fino de regras para aplicativos e filtragem de pacotes

Na prática, a janela **Nova regra** para configurações de regras avançadas é idêntica para aplicativos e pacotes de dados (veja a Figura 46).

Etapa um:

- Insira um nome para a regra. O programa usa um nome padrão que deve ser substituído.
- Selecione as configurações da conexão de rede para a regra: endereço IP remoto, porta remota, endereço IP local e a hora em que a regra foi aplicada. Marque todas as configurações que você deseja usar na regra.
- Defina as outras configurações para as notificações do usuário. Para que uma mensagem pop-up com um breve comentário apareça na tela

quando uma regra for usada, marque **Mostrar aviso**. Para que o programa registre as invocações da regra no relatório do Anti-Hacker, marque **Registrar evento**. A caixa não é marcada por padrão quando a regra é criada. É recomendável usar configurações adicionais ao criar regras de bloqueio.

Observe que, ao criar uma regra de bloqueio no modo de treinamento do Anti-Hacker, as informações sobre a regra aplicada serão automaticamente inseridas no relatório. Se não for necessário registrar essas informações, desmarque a caixa de seleção **Registrar evento** nas configurações dessa regra.

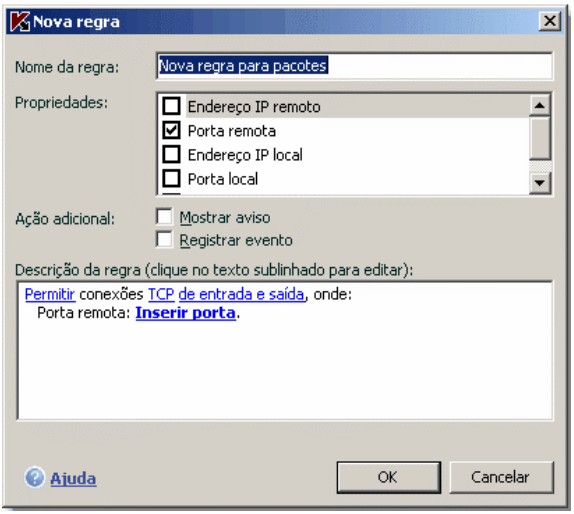


Figura 46. Criando uma nova regra para aplicativos

A Etapa dois da criação de uma regra consiste em atribuir valores aos parâmetros da regra e selecionar ações. Essas operações são executadas na seção **Descrição da regra**.

1. A ação padrão de toda nova regra é *permitir*. Para alterá-la para uma regra de *bloqueio*, clique no link Permitir na seção de descrição das regras. Ele será alterado para Bloquear.

   O Kaspersky Anti-Virus ainda verificará os programas e pacotes no tráfego de rede para os quais foi criada uma regra de permissão. Por isso, talvez os dados sejam transmitidos de forma mais lenta.

2. Se você não selecionou um aplicativo antes de criar a regra, precisará fazê-lo clicando em selecionar aplicativo. Clique no link e, na janela de

seleção de arquivos padrão que é aberta, selecione o arquivo executável do aplicativo para o qual você está criando a regra.

3. Determine a direção da conexão de rede para a regra. O valor padrão é uma regra para uma conexão de rede bidirecional (de entrada e de saída). Para alterar a direção, clique em de entrada e de saída e selecione a direção da conexão de rede na janela que é aberta.

   - **Fluxo de entrada**. A regra se aplica a conexões de rede abertas por um computador remoto.
   - **De entrada**. A regra se aplica aos pacotes de dados recebidos pelo computador, exceto os pacotes TCP.
   - **Fluxos de entrada e saída**. A regra se aplica ao tráfego de entrada e de saída, independentemente do computador que iniciou a conexão de rede, quer local ou remoto.
   - **Fluxo de saída**. A regra se aplica somente a conexões de rede abertas pelo seu computador.
   - **De saída**. A regra é aplicada a todos os pacotes de dados de saída enviados pelo computador, exceto os pacotes TCP.

   Se for importante, defina a direção dos pacotes especificamente na regra. Selecione se eles serão de entrada ou de saída. Se desejar criar uma regra para dados de fluxo contínuo, selecione o fluxo: de entrada, de saída ou ambos.

   A diferença entre a *direção do fluxo* e a *direção do pacote* é que, ao criar uma regra pra um fluxo, você define a direção da conexão. A direção dos pacotes ao transferir dados nesta conexão não é levada em consideração.

   Por exemplo, se você configurar uma regra para troca de dados com um servidor FTP executado no modo FTP passivo, permita um fluxo de saída. Para trocar dados com um servidor FTP no modo FTP ativo, permita os fluxos de saída e de entrada.

4. Se você selecionou um endereço remoto como propriedade de conexão de rede, clique em especifique o endereço e insira o endereço IP, um intervalo de endereços ou o endereço da sub-rede para a regra na janela que é aberta. Você pode usar um ou vários tipos de endereço IP para uma regra. Vários endereços de cada tipo podem ser especificados.

5. Defina o protocolo usado pela conexão de rede. O TCP é o protocolo padrão para a conexão. Se estiver criando uma regra para aplicativos, é possível selecionar um destes dois protocolos: TCP ou UDP. Para fazê-lo, clique no link com o nome do protocolo até atingir o valor necessário. Se estiver criando uma regra para filtragem de pacotes e

desejar alterar o protocolo padrão, clique em seu nome e selecione o protocolo necessário na janela que é aberta. Se você selecionar ICMP, talvez seja necessário indicar o tipo.

6. Se você selecionou as configurações de conexão de rede (endereço, porta, intervalo de tempo), também será necessário atribuir-lhes valores exatos.

Depois de adicionar a regra à lista de regras para o aplicativo, é possível configurá-la com mais detalhes (veja a Figura 47). Se desejar usá-la para um aplicativo aberto com determinadas configurações na linha de comando, marque ☑ **Linha de comando** e insira a seqüência de caracteres do parâmetro no campo à direita. Essa regra não se aplicará para aplicativos iniciados com outra linha de comando.

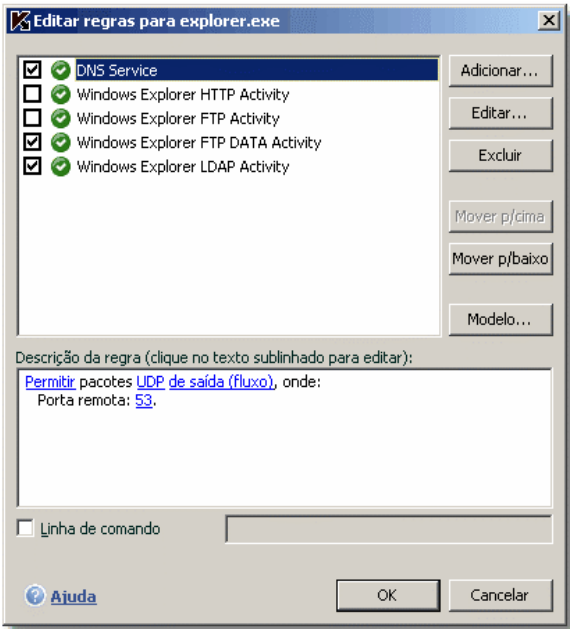


Figura 47. Configurações avançadas de nova regra

O Microsoft Windows 98 não tem a opção de configuração de início da linha de comando.

Você pode criar uma regra na janela de alerta de detecção de atividade de rede (consulte a seção 12.10 na p. 170).

12.5. Classificando a prioridade de regras

Cada aplicativo ou regra de pacotes possui uma prioridade de execução. Quando as outras condições forem iguais (por exemplo, as configurações de conexão de rede), a ação aplicada à atividade do programa será a regra com a prioridade mais alta.

A prioridade de uma regra é determinada por sua posição na lista de regras. A primeira regra na lista tem a prioridade mais alta. Cada regra criada manualmente é adicionada ao início da lista. As regras criadas a partir de um modelo ou de uma notificação são adicionadas ao final da lista.

Para priorizar as regras para aplicativos, execute as seguintes etapas:

1. Selecione o nome do aplicativo na guia **Regras para aplicativos** e clique no botão **Editar**.
2. Use os botões **Mover para cima** e **Mover para baixo** na guia de regras para aplicativos para mover as regras na lista, alterando sua classificação de prioridade.

Para priorizar regras para filtragem de pacotes, execute as seguintes etapas:

1. Selecione a regra na guia **Regras para filtragem de pacotes**.
2. Use os botões **Mover para cima** e **Mover para baixo** na guia de regras para filtragem de pacotes para mover as regras na lista, alterando sua classificação de prioridade.

12.6. Regras para zonas de segurança

Depois de instalar o Anti-Hacker no computador, ele analisará o ambiente de rede do mesmo. Com base na análise, ele divide todo o espaço de rede em zonas:

Internet – a World Wide Web. Nesta zona, o Kaspersky Anti-Virus for Windows Workstations funciona como um firewall pessoal, usando regras padrão para filtragem de pacotes e aplicativos para controlar

toda a atividade de rede e assegurar a segurança máxima. Não é possível alterar as configurações de proteção ao trabalhar nessa zona, além de habilitar o Modo Invisível no computador para melhorar a segurança.

Zonas de segurança – determinadas zonas convencionais que correspondem, em sua maioria, às sub-redes que nas quais o computador está registrado (podem ser sub-redes locais de sua residência ou trabalho). Geralmente, essas zonas têm um nível de risco médio. Você pode alterar o status dessas zonas com base na confiança que tem em uma determinada sub-rede, sendo possível configurar regras apropriadas para a filtragem de pacotes e para aplicativos.

Se o Modo de treinamento do Anti-Hacker estiver habilitado, será aberta uma janela sempre que o computador se conectar a uma nova zona, exibindo uma descrição básica sobre ela. Atribua um status à zona; a atividade de rede será permitida com base nesse status. Os valores de status possíveis são os seguintes:

- **Internet**. Este é o status padrão atribuído à Internet pois, quando você está conectado a ela, seu computador está sujeito a todos os possíveis tipos de ameaças. Esse status também é recomendado para redes que não são protegidas por nenhum programa antivírus, firewall, filtro etc. Ao selecionar esse status, o programa garante o máximo de segurança enquanto você estiver usando essa zona, especificamente:

    - Bloqueando qualquer atividade de rede do NetBios na sub-rede.

    - Bloqueando as regras para aplicativos e filtragem de pacotes que permitem a atividade do NetBios na sub-rede.

    Mesmo que você tenha criado uma pasta compartilhada, as informações contidas nela não estarão disponíveis aos usuários de sub-redes com esse status. Além disso, se esse status estiver selecionado para uma determinada sub-rede, você não poderá acessar os arquivos e impressoras dessa sub-rede.

- **Rede Local**. O programa atribui esse status a todas as zonas detectadas ao analisar o ambiente de rede do computador, exceto a Internet. Esse status é recomendado para zonas com uma fator de risco médio (por exemplo, redes locais corporativas). Se você selecionar esse status, o programa permitirá:

    - Qualquer atividade de rede do NetBios na sub-rede.

    - Regras para aplicativos e filtragem de pacotes que permitam atividade do NetBios na sub-rede.

Selecione esse status para conceder acesso a determinadas pastas ou impressoras no computador, mas bloquear qualquer outra atividade externa.

- **Confiável**. Este status é recomendado apenas para zonas que você tem certeza de que são absolutamente seguras e que seu computador não estará sujeito a ataques ou invasões. Se você selecionar esse status, toda a atividade de rede será permitida. Mesmo que a opção Proteção máxima esteja selecionada e você tenha criado regras de bloqueio, elas não funcionarão para computadores remotos de uma zona segura.

Observe que todas as restrições ou acesso aos arquivos só entrará em vigor sem essa sub-rede.

Você pode usar o Modo Invisível para aumentar a segurança ao usar uma rede rotuladas como **Internet**. Este recurso permite apenas a atividade de rede iniciada do computador, ou seja, ele se torna invisível para suas imediações. Esse modo não afeta o desempenho do computador na Internet.

O Modo Invisível não é recomendável ao usar o computador como servidor (por exemplo, um servidor de e-mail ou HTTP), pois os computadores que tentarem se conectar ao servidor não o verão como conectado.

A lista de zonas nas quais o computador está registrado é exibida na guia **Zonas** (veja a Figura 48). Cada uma delas recebeu um status, uma breve descrição da rede e se o Modo Invisível é usado.

Para alterar o status de uma zona ou para habilitar/desabilitar o Modo Invisível, selecione a zona na lista e use os links apropriados na caixa **Descrição da regra** abaixo da lista. É possível executar tarefas semelhantes e editar endereços e máscaras de sub-rede na janela **Configurações de zona**, que pode ser aberta clicando em **Editar**.

Uma nova zona pode ser adicionada à lista ao exibi-la. Para fazê-lo, clique em **Atualizar**. O Anti-Hacker pesquisará possíveis zonas para registrar e, se alguma for detectada, o programa solicitará que você selecione um status para ela. Além disso, é possível adicionar novas zonas à lista manualmente (por exemplo, se você conectar seu laptop a uma nova rede). Para fazê-lo, use o botão **Adicionar** e preencha as informações necessárias na janela **Configurações de zona**.

Para excluir uma rede da lista, selecione-a e clique no botão **Excluir**.

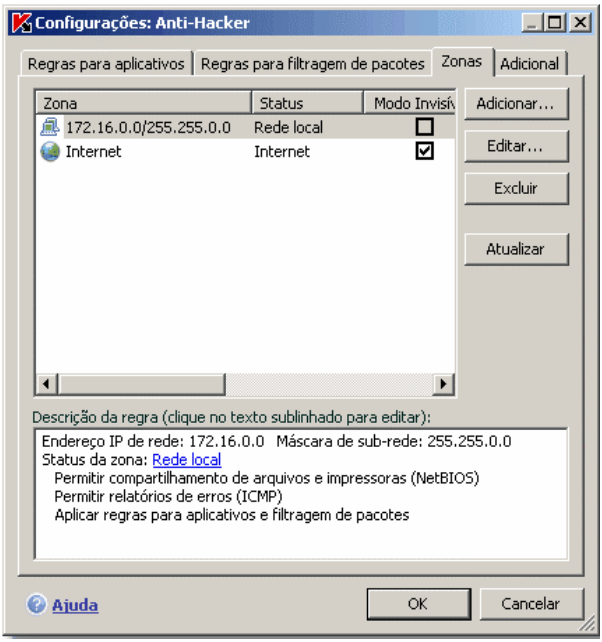


Figura 48. Lista de regras para zonas

12.7. Modo Firewall

O modo firewall (veja Figura 49) controla a compatibilidade do Anti-Hacker com programas que estabelecem várias conexões de rede e também jogos em rede.

Compatibilidade máxima – o Firewall assegura que o Anti-Hacker funcionará de maneira ideal com programas que estabelecem várias conexões de rede, por exemplo, programas de rede de compartilhamento de arquivos. Contudo, este modo pode causar um tempo de reação maior em jogos em rede. Se houver problemas com isso, é recomendável usar a Velocidade máxima.

Velocidade máxima – o Firewall assegura o melhor tempo de resposta possível durante jogos em rede. Entretanto, programas de compartilhamento de arquivos em rede ou outros aplicativos de rede podem ter conflitos nesse modo. Para resolver o problema, desabilite o Modo Invisível.

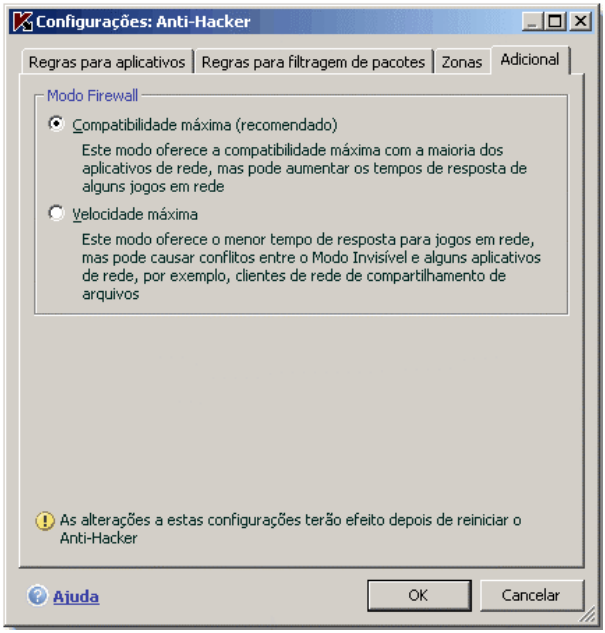


Figura 49. Selecionando um modo do Anti-Hacker

Para selecionar um modo de Firewall:

1. Abra a janela de configurações do aplicativo e selecione **Anti-Hacker** em **Proteção**.
2. Clique em **Configurações** na seção Firewall da janela de configurações do Anti-Hacker.
3. Selecione a guia **Adicional** na janela que é aberta e escolha o modo desejado, **Compatibilidade máxima** ou **Velocidade máxima**.

As alterações nas configurações do Firewall só terão efeito depois de reiniciar o Anti-Hacker.

12.8. Configurando o Sistema de Detecção de Intrusos

Todos os ataques de rede conhecidos no momento que poderiam ameaçar o computador estão relacionados nas assinaturas de ameaças, sendo atualizados

nas atualizações de assinaturas. Por padrão, o Kaspersky Anti-Virus não atualiza as assinaturas de ataques (consulte 16.4.2 na p.225).

O Sistema de Detecção de Intrusos controla a atividade de rede normal de ataques de rede e, se detectar uma tentativa de invasão do computador, bloqueia toda a atividade de rede entre o computador remoto e o seu por uma hora. Um aviso aparecerá na tela informando que ocorreu uma tentativa de ataque de rede, com informações específicas sobre o computador que o atacou.

Você pode configurar o Sistema de Detecção de Intrusos. Para fazê-lo:

1. Abra a janela de configurações do aplicativo e selecione **Anti-Hacker** em **Proteção**.
2. Clique em **Configurações** na seção **Sistema de Detecção de Intrusos**.
3. Na janela que é aberta (veja a Figura 50), determine se deseja bloquear um computador invasor e, em caso afirmativo, por quanto tempo. O tempo padrão de bloqueio é de 60 minutos. Você pode aumentar ou diminuir o tempo de bloqueio, alterando o valor no campo ao lado de **Bloquear o computador atacante por... min**. Se desejar interromper o bloqueio do tráfego de um computador invasor direcionado ao computador, desmarque essa caixa.

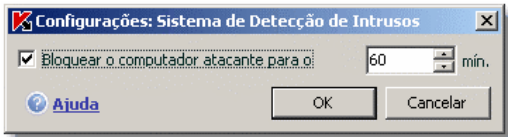


Figura 50. Configurando o tempo de bloqueio de invasores

12.9. Lista de ataques de rede detectados

Atualmente, existem vários ataques de rede que utilizam vulnerabilidades do sistema operacional e de outros softwares, sistemas ou outros, instalados no seu computador. Os malfeitores estão constantemente aperfeiçoando seus métodos de ataque, aprendendo a roubar informações confidenciais, provocando o mal funcionamento do seu sistema ou assumindo o controle total sobre o seu computador para usá-lo como parte de uma rede de zumbis e realizar novos ataques.

Para assegurar a segurança do computador, você precisa conhecer os tipos de ataques de rede que pode encontrar. Os ataques de rede conhecidos podem ser divididos em três grupos principais:

- **Verificação de portas** – essa ameaça não é um ataque em si, mas geralmente precede um, já que é uma das maneiras comuns de obter informações sobre um computador remoto. As portas UDP/TCP usadas pelos programas de rede são verificadas para descobrir seu estado (fechadas ou abertas).

  As verificações de portas informam ao hacker sobre os tipos de ataque que funcionarão ou não naquele sistema. Além disso, as informações obtidas pela verificação permitirão que o hacker determine qual sistema operacional é usado no computador remoto. Isso, por sua vez, restringe ainda mais o número de possíveis ataques e, portanto, o tempo gasto para executá-los. Isso também ajuda um hacker na tentativa de usar as vulnerabilidades específicas daquele sistema operacional.

- **Ataques DoS (Denial of Service)** – são ataques que levam o sistema atacado a entrar em um estado instável ou totalmente inoperável. Esses ataques podem danificar ou corromper os recursos de informações objetivados, impossibilitando seu uso.

  Há dois tipos básicos de ataques DoS:

  - O envio de pacotes criados especificamente que o computador não espera e que podem fazer o sistema reiniciar ou parar.
  - O envio ao computador-alvo vários pacotes em um uma velocidade que ele não seja capaz de processar, causando um colapso nos recursos do sistema.

  Os ataques a seguir são exemplos comuns deste tipo de ataque:

  - O *ping da morte* envia um pacote ICMP maior que o máximo de 64 KB. Esse ataque pode causar a falha de alguns sistemas operacionais.
  - O *ataque por terra* envia uma solicitação para uma porta aberta nos computador para estabelecer uma conexão consigo mesma. O computador é levado a entrar em um ciclo que intensifica a carga do processador e pode terminar na falha do sistema operacional.
  - A *inundação ICMP* envia uma grande quantidade de pacotes ICMP ao computador. O computador é forçado a responder a cada pacote de entrada, sobrecarregando seriamente o processador.
  - A *inundação SYN* envia uma grande quantidade de consultas ao computador para estabelecer uma conexão falsa. O sistema reserva determinados recursos para cada uma dessas conexões, esgotando totalmente os recursos do sistema e

fazendo o computador parar de reagir a outras tentativas de conexão.

- **Ataques de intrusos**, cujo objetivo é assumir o controle do computador. Esse é o tipo mais perigoso de ataque pois, quando bem-sucedido, permite ao hacker assumir completamente o controle do computador.

  Os hackers usam esse ataque para obter informações confidenciais de um computador remoto (por exemplo, números de cartões de crédito ou senhas) ou para usar seus recursos posteriormente com propósitos mal-intencionados (por exemplo, usando o sistema capturado em redes de zumbis ou como plataforma para novos ataques).

  Esse grupo contém mais tipos diferentes de ataques que qualquer outro. Eles podem ser divididos em três subgrupos, com base no sistema operacional: ataques do Microsoft Windows, do Unix e um grupo para serviços de rede executados em qualquer sistema operacional.

  Os tipos de ataques mais comuns que usam as ferramentas de rede do sistema operacional são:

  - *Ataques de estouro do buffer* – um tipo de vulnerabilidade de software que surge por controle insuficiente para lidar com quantidades maciças de dados. É um dos tipos de vulnerabilidade mais antigos e mais fácil de ser explorado pelos hackers.
  - *Ataques de seqüência de formato* – um tipo de vulnerabilidade de software que surge pela falta de controle de valores de entrada para funções de E/S como *printf()*, *fprintf()*, *scanf()* e outras da biblioteca C padrão. Se um programa tiver essa vulnerabilidade, um hacker, usando consultas criadas com uma técnica específica, pode obter o controle completo do sistema.

O Sistema de Detecção de Intrusos analisa e bloqueia automaticamente as tentativas de explorar vulnerabilidades nas ferramentas de rede mais comuns (FTP, POP3, IMAP) em execução no computador do usuário.

Os ataques do Microsoft Windows se baseiam no aproveitamento das vulnerabilidades de softwares instalados no computador (por exemplo, programas como o Microsoft SQL Server, Microsoft Internet Explorer, Messenger e componentes de sistema que podem ser acessados pela rede: DCom, SMB, Wins, LSASS, IIS5).

O Anti-Hacker protege o computador de ataques que usam as seguintes vulnerabilidades de software conhecidas (esta lista de vulnerabilidades é citada no sistema de numeração da Base de Dados de Conhecimento da Microsoft):

(**MS03-026**) Vulnerabilidade RPC DCOM (worm Lovesan)

(**MS03-043**) Saturação de buffer no serviço do Microsoft Messenger

(**MS03-051**) Saturação de buffer nas extensões do Microsoft FrontPage 2000 Server

(**MS04-007**) Vulnerabilidade ASN.1 do Microsoft Windows

(**MS04-031**) Saturação do buffer remoto não autenticada do serviço Microsoft NetDDE

(**MS04-032**) Saturação de heap de metarquivo do Microsoft Windows XP (.emf)

(**MS05-011**) Controle de resposta de transação de cliente SMB do Microsoft Windows

(**MS05-017**) Vulnerabilidade de saturação de buffer na fila de mensagens do Microsoft Windows

(**MS05-039**) Saturação remota do serviço plug-and-play do Microsoft Windows

(**MS04-045**) Saturação de heap remoto do WINS (Windows Internet Naming Service) do Microsoft Windows

(**MS05-051**) Modificação da memória de coordenação de transações distribuídas do Microsoft Windows

Além disso, existem incidentes isolados de ataques de invasão usando vários scripts mal-intencionados, incluindo scripts processados pelo Microsoft Internet Explorer e worms do tipo Helkern. A base desse tipo de ataque é o envio de um tipo específico de pacotes UDP para um computador remoto que pode executar código mal-intencionado.

Lembre-se de que, enquanto estiver conectado à rede, o computador estará constantemente correndo o risco de ser atacado por um hacker. Para assegurar a segurança do seu computador, habilite o Anti-Hacker ao usar a Internet e atualize regularmente as assinaturas de ataques de hackers (consulte 16.4.2 na p. 225).

12.10. Bloqueando e permitindo a atividade de rede

Se o nível de segurança do Firewall estiver definido como **Modo de treinamento**, aparecerá um aviso específico na tela sempre que houver uma tentativa de conexão de rede sem regras.

Por exemplo, após abrir o Microsoft Outlook, ele baixará seus e-mails de um servidor remoto do Exchange. Para exibir sua Caixa de Entrada, o programa se conectará ao servidor de e-mail. O Anti-Hacker sempre controla esse tipo de

atividade de rede. Será exibida uma mensagem na tela (veja a Figura 51), contendo:

- *Descrição da atividade* – nome do aplicativo e uma breve descrição da conexão que está sendo iniciada, em geral incluindo o tipo de conexão, a porta local da qual ela está sendo iniciada, a porta remota e o endereço que está sendo conectado. Clique em qualquer local dessa área para obter informações detalhadas sobre a conexão, o processo que a iniciou e o distribuidor do aplicativo.
- *Ação* – uma série de operações relacionadas à atividade de rede detectada executadas pelo Anti-Hacker.

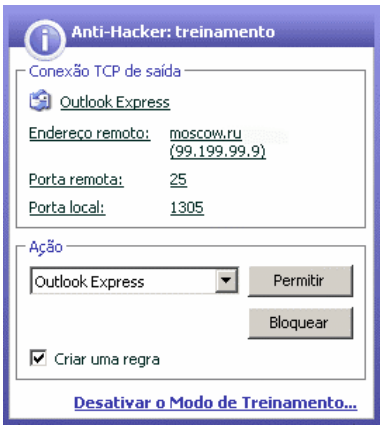


Figura 51. Notificação de atividade de rede

Analise cuidadosamente as informações sobre a atividade de rede e somente então selecione as ações para o Anti-Hacker. Ao decidir, é recomendável seguir estas dicas:

1. Antes de qualquer coisa, decida se irá permitir ou bloquear a atividade de rede. É possível que, nessa situação, um conjunto de regras já criado para esse aplicativo ou pacote o ajude (supondo que ele tenha sido criado). Para fazê-lo, use o link **Editar regras**. Em seguida, uma janela será aberta com uma lista completa das regras criadas para o aplicativo ou pacote de dados.
2. Decida se deseja executar essa ação uma vez ou automaticamente sempre que essa atividade for detectada.

Para executar a ação somente essa vez:

desmarque ☑ **Criar uma regra** e clique no botão com o nome da ação, por exemplo, **Permitir**.

Para executar automaticamente a ação selecionada sempre que essa atividade for iniciada no seu computador:

1. Certifique-se de que **Criar regra** esteja selecionado.
2. Selecione o tipo de atividade ao qual você deseja que a ação seja aplicada na lista suspensa na seção **Ação**:
   - **Qualquer atividade** – toda a atividade de rede iniciada por esse aplicativo.
   - **Personalizada** – uma única atividade que você terá de definir na caixa de diálogo de regras (consulte a seção 12.2.1 na p. 154).
   - **<Modelo>** – nome do modelo que inclui o conjunto de regras típicas da atividade de rede do programa. Este tipo de atividade aparecerá na lista se o Kaspersky Anti-Virus for Windows Workstations incluir um modelo apropriado para o aplicativo que iniciou a atividade de rede (consulte 12.2.2 na p. 155). Nesse caso, não será necessário personalizar as atividades que serão permitidas ou bloqueadas. Use o modelo e um conjunto de regras será criado automaticamente para o aplicativo.
3. Clique no botão com o nome da ação (**Permitir** ou **Bloquear**).

Lembre-se de que a regra criada será usada somente se houver correspondência com todos os parâmetros de conexão. Essa regra não se aplica a uma conexão estabelecida de uma porta local diferente, por exemplo.

Para desativar a exibição de mensagens do Anti-Hacker quando algum aplicativo tentar estabelecer conexões de rede, clique em Desabilitar modo de treinamento. Isso colocará o Anti-Hacker no modo Permitir tudo, em que todas as conexões de rede, exceto aquelas claramente proibidas pelas regras, serão permitidas.

CAPÍTULO 13. PROTEÇÃO CONTRA E-MAILS INDESEJADOS

O componente do Kaspersky Anti-Virus for Windows Workstations que detecta spam, o processa de acordo com um conjunto de regras e economiza seu tempo ao usar o e-mail é chamado *Anti-Spam*.

O Anti-Spam usa o seguinte método para determinar se um e-mail é um spam:

1. O endereço do remetente é verificado em uma lista negra e uma lista branca de endereços.
    - Se o endereço do remetente estiver na lista branca, o e-mail será marcado como *aceito*.
    - Caso esteja na lista negra, o e-mail será marcado como *spam*. A continuação do processamento depende da ação selecionada (consulte a seção 13.3.7 na p. 191).
2. Se o endereço do remetente não for encontrado em nenhuma das listas, o e-mail será analisado usando a tecnologia PDB (consulte a seção 13.3.2 na p. 182).
3. O Anti-Spam examina o texto do e-mail detalhadamente e verifica linhas contidas na lista negra ou na lista branca.
    - Se o texto do e-mail contiver linhas da lista branca, o e-mail será marcado como *aceito*.
    - Caso sejam encontradas frases da lista negra, o e-mail será marcado como *spam*. O restante do processamento depende da ação especificada.
4. Se o e-mail não contiver frases presentes em nenhuma das listas, ele será analisado para saber se não contém phishing. Se o texto do e-mail contiver um endereço do banco de dados de anti-phishing, o e-mail será marcado como *spam*. O restante do processamento depende da ação especificada.
5. Se o e-mail não contiver linhas de phishing, ele será verificado com tecnologias específicas quanto a indícios de spam:
    - Análise de imagem usando a tecnologia GSG

- Análise do texto da mensagem usando o algoritmo iBayes para reconhecimento de spam

6. Em seguida, o e-mail será verificado por fatores avançados de filtragem de spam (consulte a seção 13.3.5 na p. 189) especificado pelo usuário na instalação do Anti-Spam. Isso poderia incluir a verificação de marcas HTML, tamanho de fonte ou caracteres ocultos corretos.

Você pode habilitar ou desabilitar cada um dos estágios da análise.

O Anti-Spam funciona como um plug-in para os seguintes programas de e-mail:

- Microsoft Outlook (consulte a seção 13.3.8 na p. 192)
- Microsoft Outlook Express (Windows Mail) (consulte a seção 13.3.9 na p. 195)
- The Bat! (consulte a seção 13.3.10 na p. 196)

Esta versão do Kaspersky Anti-Virus não dá suporte ao plug-in do Anti-Hacker para o Microsoft Office Outlook no Microsoft Windows 98.

O painel de tarefas dos programas Microsoft Office Outlook e Microsoft Outlook Express (Windows Mail) possui dois botões, **Spam** e **Não spam**, que podem configurar o Anti-Spam para detectar spams diretamente na sua caixa de correio. No The Bat!, esses botões não existem: o programa pode ser treinado usando os itens especiais **Mark as spam** e **Mark as NOT spam** no menu **Special**. Além disso, parâmetros especiais de processamento (consulte a seção 13.3.1 na p. 181) de spam são adicionados a todas as configurações dos programas de e-mail.

O Anti-Spam usa um algoritmo de autotreinamento iBayes modificado que permite que, ao longo do tempo, o componente diferencie com mais precisão os *spams* de *e-mails aceitos*. A fonte de dados do algoritmo é o conteúdo dos e-mails.

Há certos casos em que o iBayes não consegue classificar um determinado e-mail como spam ou e-mail aceito com muita precisão. Esses e-mails são marcados como *possível spam*.

Para reduzir a quantidade de e-mails marcados como possível spam, é recomendável realizar um treinamento adicional do Anti-Spam (consulte 13.2 na p. 176) com esses e-mails. Para fazê-lo, especifique quais desses e-mails devem ser marcados como *spam* e como *aceitos*.

Os e-mails que são *spam* ou *possível spam* são modificados: as marcas **[!! SPAM]** ou **[?? Possível spam]** são adicionadas à linha de assunto.

As regras para o processamento de spam ou possível spam para o Microsoft Office Outlook, o Microsoft Outlook Express (Windows Mail) ou o The Bat! são

especificadas em componentes de plug-in específicos nos próprios programas de e-mail. Para outros programas de e-mail, é possível configurar regras de filtragem que pesquisam a linha de assunto modificada que contém **[!! SPAM]** ou **[?? Possível spam]** e movem os e-mails para uma pasta designada. Para obter mais informações sobre o mecanismo de filtragem, consulte a documentação do seu programa de e-mail.

13.1. Selecionando o nível de sensibilidade do Anti-Spam

O Kaspersky Anti-Virus for Windows Workstations o protege de spams em um dos seguintes níveis (veja a Figura 52):

Bloquear tudo – o nível mais rigoroso de sensibilidade, no qual apenas as mensagens que contêm frases da lista branca de frases (consulte a seção 13.3.4.1 na p. 185) e remetentes relacionados na lista branca são aceitas. todo o resto é marcado como spam. Nesse nível, o e-mail é analisado apenas com relação às listas brancas. Todos os outros recursos são desabilitados.

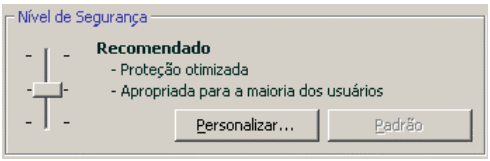


Figura 52. Selecionando o nível de segurança do Anti-Spam

Alto – um nível rigoroso que, quando ativado, aumenta a probabilidade de que alguns e-mails que não são spam sejam marcados como *spam*. Nesse nível, o e-mail é comparado com as listas branca e negra, e também usando as tecnologias PDB e GSG e o algoritmo iBayes (consulte a seção 13.3.2 na p. 182).

Esse nível deve ser aplicado em casos onde há uma grande probabilidade de que o endereço do destinatário seja desconhecido dos remetentes de spam. Por exemplo, quando o destinatário não é assinante de listas de envio de mensagens em massa e não possui um endereço de e-mail em servidores de e-mail gratuitos/não-corporativos.

Recomendado – o nível de configuração universal padrão para a classificação de e-mail.

Nesse nível, é possível que alguns spams não sejam detectados. Isso mostra que o Anti-Spam não foi suficientemente treinado. É recomendável

realizar um treinamento adicional do módulo usando o Assistente de Treinamento (consulte a seção 13.2.1 na p. 177) ou os botões **Spam/NÃO Spam** (ou os itens do menu correspondentes no The Bat!), no caso de e-mails marcados incorretamente.

Baixo – o nível de configuração mais flexível. Recomendável para usuários cujas mensagens recebidas contêm um número significativo de palavras reconhecidas pelo Anti-Spam como spam, quando na verdade não o são. Isso pode ocorrer devido à atividade do destinatário, que o força a usar termos profissionais que são comuns nos spams na sua correspondência com colegas. Nesse nível, todas as tecnologias de detecção de spam são usadas na análise de e-mails.

Ignorar tudo – o nível de sensibilidade mais baixo. Apenas os e-mails com frases contidas na lista negra ou de remetentes contidos na lista negra de endereços são marcados como spam. Nesse nível, os e-mails são processados apenas usando a lista negra e todos os outros recursos estão desabilitados.

Por padrão, o nível de sensibilidade do Anti-Spam é definido como **Recomendado**. É possível aumentar ou reduzir o nível, ou editar a configuração do nível atual.

Para modificar o nível de proteção:

Na seção Sensibilidade, mova o controle deslizante para cima ou para baixo, de acordo com a configuração desejada. Ao ajustar o nível de sensibilidade, você define a correlação entre os fatores de spam, possível spam e e-mail aceito (consulte a seção 13.3.3 na p. 183).

Para modificar as configurações do nível atual:

Na janela Configurações do aplicativo, clique em **Anti-Spam** para mostrar as configurações dos componentes. Clique no botão **Personalizar** na seção Sensibilidade. Na janela que é aberta, edite o fator de spam e clique em **OK**.

O nome do nível de segurança mudará para **Personalizado**.

13.2. Treinando o Anti-Spam

O Anti-Spam é fornecido com um banco de dados de e-mails pré-instalado que contém cinqüenta exemplos de spam. É recomendável que o módulo Anti-Spam seja mais treinado usando seus próprios e-mails.

Há várias abordagens para treinar o Anti-Spam:

- Usar o Assistente de Treinamento (consulte a seção 13.2.1 na p. 177)

- Treinar o Anti-Spam com os e-mails enviados (consulte a seção 13.2.2 na p. 178)
- Treinar diretamente ao trabalhar com o e-mail (consulte a seção 13.2.3 na p. 178) usando botões especiais nos itens de menu ou no painel de ferramentas do programa de e-mail
- Treinamento nos relatórios do Anti-Spam (consulte a seção 13.2.4 na p. 179)

O melhor método é usar o Assistente de Treinamento desde o início da utilização do Anti-Spam, pois ele pode ser treinado com um grande número de e-mails.

Observe que não é possível treinar o Anti-Spam com mais de 50 e-mails por pasta. Se houver mais e-mails na pasta, o programa utilizará cinqüenta deles para o treinamento.

O treinamento adicional usando botões específicos na interface do programa de e-mail é preferível ao trabalhar diretamente com e-mail.

13.2.1. Assistente de Treinamento

O Assistente de Treinamento treina o Anti-Spam indicando as pastas da caixa de correio que contêm spams e mensagens aceitas.

Para abrir o Assistente de Treinamento:

1. Abra a janela de configurações do aplicativo e selecione **Anti-Spam** em **Proteção**.
2. Clique no botão **Assistente de Treinamento** na seção Treinamento da janela de configurações.

O Assistente de Treinamento inclui procedimentos passo a passo para treinar o Anti-Spam. Use os botões **Voltar** e **Avançar** para navegar entre as etapas.

A Etapa um do Assistente de Treinamento envolve a seleção de pastas que contêm e-mails aceitos. Nesse estágio, selecione apenas as pastas cujo conteúdo é totalmente confiável.

A Etapa dois do Assistente de Treinamento consiste na seleção de pastas que contêm spam. Caso seu programa de e-mail não tenha pastas para spam, ignore esta etapa.

Na Etapa três, o Anti-Spam é treinado automaticamente usando as pastas selecionadas. Os e-mails contidos nessas pastas preenchem o banco de dados do Anti-Spam. Os remetentes de e-mails aceitos são adicionados automaticamente à lista branca de endereços.

Na Etapa quatro, os resultados do treinamento devem ser salvos usando um dos métodos a seguir: adicione os resultados do treinamento ao banco de dados atual do Anti-Spam ou substitua o banco de dados atual pelos resultados do treinamento. Lembre-se de que o programa deve ser treinado com pelo menos 50 e-mails aceitos e 50 e-mails indesejados para que o iBayes funcione com precisão.

Para economizar tempo, o Assistente de Treinamento usa apenas 50 e-mails de cada pasta selecionada para o treinamento.

13.2.2. Treinando com e-mails enviados

Você pode treinar o Anti-Spam usando e-mails enviados do programa de e-mail. Em seguida, a lista branca de endereços do Anti-Spam será preenchida analisando as mensagens enviadas. Apenas os primeiros 50 e-mails são usados para o treinamento, quando ele estará concluído.

Para treinar o Anti-Spam com e-mails enviados:

1. Abra a janela de configurações do aplicativo e selecione **Anti-Spam** em **Proteção**.
2. Marque **Treinar usando e-mails enviados** na seção **Treinamento**.

Aviso!

O Anti-Spam se treinará com e-mails enviados pelo protocolo MAPI somente se você marcar **Verificar ao enviar** no plug-in do Antivírus de E-Mail do Microsoft Outlook (consulte a seção 13.3.8 na p. 192).

13.2.3. Treinando com o programa de e-mail

Para treinar ao usar sua caixa de correio, utilize os botões específicos no painel de ferramentas do programa de e-mail.

Ao instalar o Anti-Spam no computador, são instalados plug-ins para os seguintes programas de e-mail:

- Microsoft Outlook
- o Outlook Express (Windows Mail)
- The Bat!

Por exemplo, o painel de tarefas do Outlook possui dois botões, **Spam** e **Não spam**, e uma guia de configurações do **Kaspersky Anti-Spam** (consulte 13.3.8 na p. 192) na caixa de diálogo Opções (item de menu **Serviço** → **Opções**). Outlook Express, além dos botões **Spam** e **Não spam**, adiciona um botão **Configurações** ao painel de tarefas, que abre uma janela com ações (consulte a seção 13.3.9 na p. 195) ao detectar um spam. No The Bat! esses botões não existem, embora o programa possa ser treinado usando os itens específicos **Mark as spam** e **Mark as NOT spam** no menu **Special**.

Se você decidir que o e-mail aberto é um spam, clique no botão **Spam**. Caso contrário, clique em **Não spam**. Depois disso, o Anti-Spam será treinado usando o e-mail. Se você selecionar vários e-mails, todos serão usados para o treinamento.

Aviso!

Quando for necessário selecionar imediatamente vários e-mails ou se você tiver certeza de que uma determinada pasta contém somente e-mails de um grupo (spam ou não spam), será possível adotar uma abordagem abrangente para o treinamento com o Assistente de Treinamento (consulte 13.2.1 na p. 177).

13.2.4. Treinando com relatórios do Anti-Spam

É possível treinar o Anti-Spam usando seus próprios relatórios.

Para exibir os relatórios do componente:

1. Selecione o componente **Anti-Spam** na seção **Proteção** da janela principal do programa.
2. Clique na caixa **Estatísticas** (veja a Figura 53).

Os relatórios do componente podem ajudá-lo a tirar uma conclusão sobre a precisão de sua configuração e, se necessário, fazer algumas correções.

Para marcar um determinado e-mail como spam ou não spam:

1. Selecione-o na lista de relatório na guia **Eventos** e use o botão **Ações**.
2. Selecione uma das quatro opções:
   - **Marcar como spam**
   - **Marcar como não spam**
   - **Adicionar à lista branca**
   - **Adicionar à lista negra**

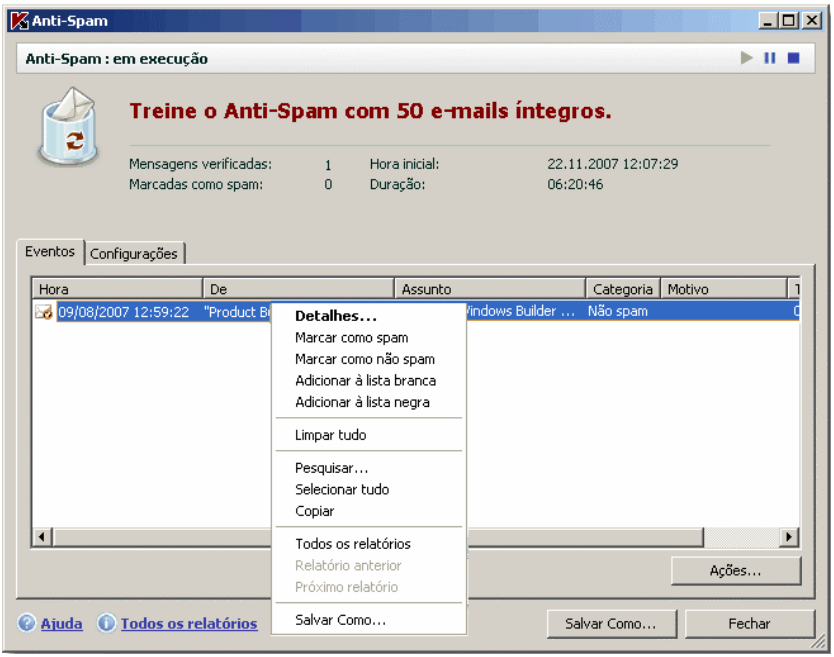


Figura 53. Treinando o Anti-Spam com relatórios

O Anti-Spam continuará o treinamento com base nesse e-mail.

13.3. Configurando o Anti-Spam

É essencial fazer o ajuste fino do Anti-Spam para que o recurso de segurança de spam funcione. Todas as configurações de funcionamento do componente estão localizadas na janela de configurações do Kaspersky Anti-Virus for Windows Workstations e permitem:

- Determine as particularidades de funcionamento do Anti-Spam (consulte a seção 13.3.1 na p. 181)
- Escolha as tecnologias de filtragem de spam que serão utilizadas (consulte a seção 13.3.2 na p. 182)
- Ajuste a precisão do reconhecimento de spam e possível spam (consulte a seção 13.3.3 na p. 183)
- Crie listas brancas e negras para remetentes e frases-chave (consulte a seção 13.3.4 na p. 184)

- Configure os recursos adicionais de filtragem de spam (consulte a seção 13.3.5 na p. 189)
- Reduza ao máximo a quantidade de spams na sua Caixa de Entrada através da visualização com o Mail Dispatcher (consulte a seção 13.3.6 na p. 190)

As seções a seguir examinarão estas configurações detalhadamente.

13.3.1. Configurando a verificação

Você pode definir as seguintes configurações de verificação:

- Se o tráfego dos protocolos POP3 e IMAP será verificado. Por padrão, o Kaspersky Anti-Virus verifica os e-mails em todos esses protocolos.
- Se os plug-ins do Outlook, Outlook Express (Windows Mail) e The Bat! devem ser ativados.
- Se os e-mails são visualizados pelo POP3 no Mail Dispatcher (consulte a seção 13.3.6 na p. 190) antes de serem baixados do servidor de e-mail para a Caixa de Entrada do usuário.

Para definir estas configurações:

1. Abra a janela de configurações do aplicativo e selecione **Anti-Spam** em **Proteção**.
2. Marque ou desmarque as caixas na seção Conectividade, que correspondem às três opções abordadas anteriormente (veja a Figura 54).
3. Se necessário, edite as configurações de rede.

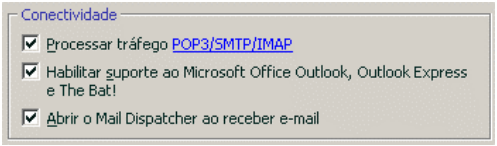


Figura 54. Configurando a verificação

Aviso!

Se você usa o Microsoft Outlook Express, deverá reiniciá-lo quando alterar o status da caixa Habilitar suporte para Outlook, Outlook Express e The Bat!.

13.3.2. Selecionando as tecnologias de filtragem de spam

Os spams são verificados nos e-mails usando tecnologias avançadas de filtragem:

- **iBayes**, baseada no teorema de Bayes, analisa o texto do e-mail para detectar frases que o identifiquem como spam. A análise usa as estatísticas obtidas com o treinamento do Anti-Spam (consulte a seção 13.2 na p. 176).
- **GSG**, que analisa os elementos gráficos nos e-mails usando assinaturas específicas para a detecção de spam em gráficos.
- **PDB**, que analisa os cabeçalhos dos e-mails e os classifica como spam com base em um conjunto de regras heurísticas.

Por padrão, todas essas tecnologias de filtragem estão habilitadas, verificando os e-mails quanto à presença de spams da forma mais completa possível.

Para desabilitar alguma das tecnologias de filtragem:

1. Abra a janela de configurações do aplicativo e selecione **Anti-Spam** em **Proteção**.
2. Clique no botão **Personalizar** na seção **Sensibilidade** e, na janela que é aberta, selecione a guia **Reconhecimento de spam** (veja a Figura 55).
3. Desmarque as caixas ao lado das tecnologias de filtragem que não deseja usar para detecção de spam.

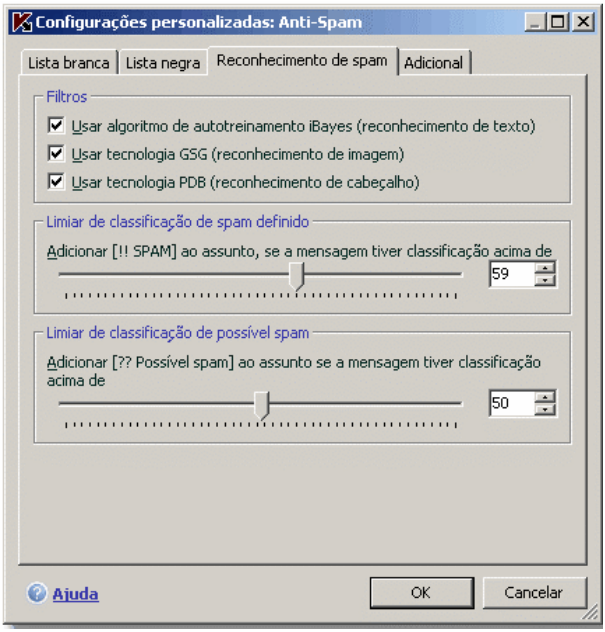


Figura 55. Configurando o reconhecimento de spam

13.3.3. Definindo os fatores de spam e possível spam

Os especialistas da Kaspersky Lab configuraram o Anti-Spam de forma ideal para reconhecer spam e possível spam.

O reconhecimento de spam funciona com tecnologias avançadas de filtragem (consulte a seção 13.3.2 na p. 182) e com o treinamento do Anti-Spam para reconhecer precisamente spam, possível spam e e-mails aceitos usando os e-mails da sua Caixa de Entrada.

O Anti-Spam é treinado usando o Assistente de Treinamento e através dos programas de e-mail. Durante o treinamento, é atribuído um peso a cada elemento individual dos e-mails aceitos ou spams. Quando um e-mail entra na caixa de entrada, o Anti-Spam verifica com o iBayes os elementos de spam ou e-mail aceito. Os fatores de cada elemento são calculados, e o e-mail recebe um *fator de spam* e um *fator de e-mail aceito*.

O fator de possível spam define a probabilidade de o e-mail ser classificado como possível spam. Se o nível **Recomendado** for usado, qualquer e-mail terá

entre 50 e 59% de probabilidade de ser considerado como *possível spam*. Os e-mails íntegros ser referem àqueles que, após a verificação, possuem um fator de spam menor que 50%.

O fator de spam determina a probabilidade de o Anti-Spam classificar um e-mail como spam. Qualquer e-mail com probabilidade superior à indicada acima será considerado spam. O fator de spam padrão no nível **Recomendado** é de 59%. Isso significa que qualquer e-mail com uma probabilidade superior a 59% será marcado como *spam*.

No total, há cinco níveis de sensibilidade (consulte a seção 13.1 na p. 175), sendo três deles (**Alto, Recomendado** e **Baixo**) baseados em diversos valores de fatores de spam e possível spam.

Você pode editar o algoritmo do Anti-Spam. Para fazê-lo:

1. Abra a janela de configurações do aplicativo e selecione **Anti-Spam** em **Proteção**.
2. Na caixa **Nível de sensibilidade** à direita da janela, clique em **Personalizar**.
3. Na janela que é aberta, ajuste os fatores de spam e possível spam nas respectivas seções da guia **Reconhecimento de spam** (veja a Figura 55).

13.3.4. Criando listas brancas e negras manualmente

Os usuários podem criar listas brancas e negras manualmente usando o Anti-Spam com seus e-mails. Essas listas armazenam informações sobre endereços de usuários que são considerados seguros ou fontes de spam, além de várias frases e palavras-chave que os identificam como spam ou e-mail aceito.

A principal aplicação das listas de palavras-chave e, em particular, da lista branca, é que você pode coordenar assinaturas contendo uma determinada frase com destinatários confiáveis (por exemplo, seus colegas). Você poderia usar, por exemplo, uma assinatura PGP como assinatura de e-mail. É possível usar caracteres curinga nas assinaturas e nos endereços: * e ?. Um * representa qualquer seqüência de caracteres de qualquer tamanho. Um ponto de interrogação representa qualquer caractere.

Se houver de asteriscos e pontos de interrogação na assinatura, para evitar erros no processamento pelo Anti-Spam, eles devem ser precedidos de uma barra invertida. Então, são usados dois caracteres em vez um: * e \?.

13.3.4.1. Listas brancas de endereços e frases

A lista branca contém frases-chave de e-mails marcados como *aceitos* e endereços de remetentes confiáveis que não enviariam spam. A lista branca é preenchida manualmente, enquanto a lista de endereços de remetentes é criada automaticamente durante o treinamento do componente Anti-Spam. Você pode editar essa lista.

Para configurar a lista branca:

1. Abra a janela de configurações do aplicativo e selecione **Anti-Spam** em **Proteção**.
2. Clique no botão **Configurações** à direita da janela de configurações.
3. Abra a guia **Lista branca** (veja a Figura 56).

A guia é dividida em duas seções: a parte superior contém os endereços dos remetentes de e-mails confiáveis, enquanto a parte inferior contém palavras-chave desses e-mails.

Para habilitar as listas brancas de frases e endereços durante a filtragem de spam, marque as caixas correspondentes nas seções **Remetentes permitidos** e **Frases permitidas**.

Você pode editar as listas usando os botões em cada seção.

É possível atribuir endereços e máscaras de endereços na lista de endereços. Ao inserir um endereço, o uso de maiúsculas é ignorado. Vamos examinar alguns exemplos de máscaras de endereços:

- *ivanov@test.ru* – os e-mails desse endereço sempre serão classificados como aceitos.
- **@test.ru* – os e-mails de qualquer remetente no domínio *test.ru* serão aceitos, por exemplo: *petrov@test.ru*, *sidorov@test.ru*;
- *ivanov@** – um remetente com este nome, independentemente do domínio, terá seus e-mails aceitos sempre, por exemplo: *ivanov@test.ru*, *ivanov@mail.ru*;
- **@test** – os e-mails de qualquer remetente em um domínio iniciado com *test* não serão considerados spam, por exemplo: *ivanov@test.ru*, *petrov@test.com*;
- *ivan.*@test.???* – os e-mails de remetentes que começam com ivan. e cujo nome de domínio começa com *test* e termina com quaisquer três caracteres serão sempre aceitos, por exemplo: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

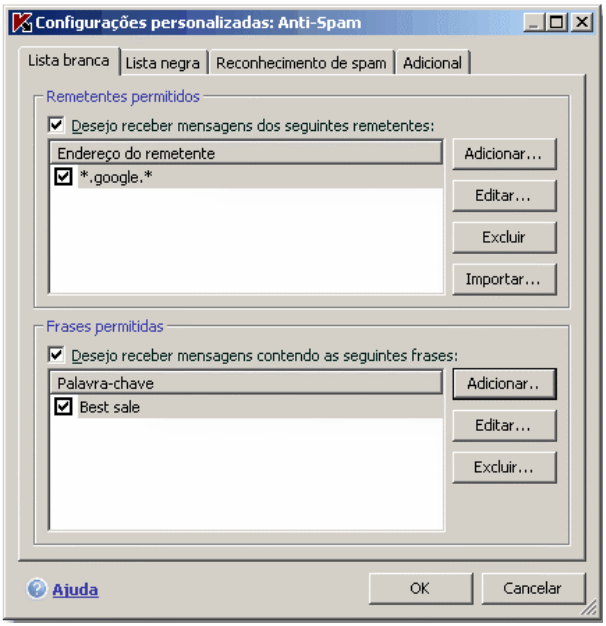


Figura 56. Configurando listas brancas de endereços e frases

Você também pode usar máscaras para frases. Ao inserir uma frase, o uso de maiúsculas é ignorado. Seguem alguns exemplos:

- *Oi, Ivan!* – um e-mail que contém apenas este texto é aceito. Não é recomendável usar uma frase como esta como frase da lista branca.
- *Oi, Ivan!** – um e-mail que começa com a frase *Oi, Ivan!* é aceito.
- *Oi, *! ** – os e-mails começando com a saudação *Oi* e um ponto de exclamação em qualquer local do e-mail não serão tratados como spam.
- * *Ivan?* * – os e-mails contendo uma saudação a um usuário com o nome *Ivan*, cujo nome é seguido de qualquer caractere, não são considerados spam.
- * *Ivan\?* * – os e-mails contendo a frase *Ivan?* são aceitos.

Para desabilitar o uso de um determinado endereço ou frase como atributo de um e-mail íntegro, é possível excluí-lo usando o botão Excluir ou a caixa ao lado do texto pode ser desmarcada para desabilitá-lo.

Você pode importar arquivos no formato CSV para as listas brancas de endereços.

13.3.4.2. Listas negras de endereços e frases

A lista negra de remetentes armazena frases-chave de e-mails considerados *spam* e os endereços desses remetentes. A lista é preenchida manualmente.

Para preencher a lista negra:

1. Selecione **Anti-Spam** na janela de configuração do Kaspersky Anti-Virus for Windows Workstations.
2. Clique no botão **Configurações** à direita da janela de configurações.
3. Abra a guia **Lista negra** (veja a Figura 57).

A guia é dividida em duas seções: a parte superior contém os endereços dos remetentes de spam, enquanto a parte inferior contém palavras-chave desses e-mails.

Para habilitar as listas negras de frases e endereços durante a filtragem de spam, marque as caixas correspondentes nas seções **Remetentes bloqueados** e **Frases bloqueadas**.

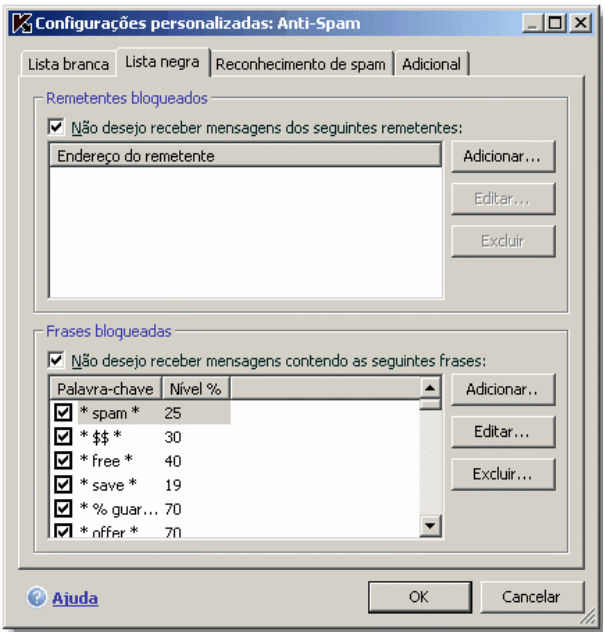


Figura 57. Configurando listas negras de endereços e frases

Você pode editar as listas usando os botões em cada seção.

É possível atribuir endereços e máscaras de endereços na lista de endereços. Ao inserir um endereço, o uso de maiúsculas é ignorado. Vamos examinar alguns exemplos de máscaras de endereços:

- *ivanov@test.ru* – os e-mails desse endereço sempre serão classificados como aceitos.
- **@test.ru* – os e-mails de qualquer remetente no domínio *test.ru* serão aceitos, por exemplo: *petrov@test.ru*, *sidorov@test.ru*;
- *ivanov@** – um remetente com este nome, independentemente do domínio, terá seus e-mails aceitos sempre, por exemplo: *ivanov@test.ru*, *ivanov@mail.ru*;
- **@test** – os e-mails de qualquer remetente em um domínio iniciado com *test* não serão considerados spam, por exemplo: *ivanov@test.ru*, *petrov@test.com*;
- *ivan.*@test.???* – – os e-mails de remetentes que começam com ivan. e cujo nome de domínio começa com *test* e termina com quaisquer três caracteres serão sempre aceitos, por exemplo: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

Você também pode usar máscaras para frases. Ao inserir uma frase, o uso de maiúsculas é ignorado. Seguem alguns exemplos:

- *Oi, Ivan!* – um e-mail que contém apenas este texto é aceito. Não é recomendável usar uma frase como esta como frase da lista branca.
- *Oi, Ivan!** – um e-mail que começa com a frase *Oi, Ivan!* é aceito.
- *Oi, *! ** – os e-mails começando com a saudação *Oi* e um ponto de exclamação em qualquer local do e-mail não serão tratados como spam.
- ** Ivan? ** – os e-mails contendo uma saudação a um usuário com o nome *Ivan*, cujo nome é seguido de qualquer caractere, não são considerados spam.
- ** Ivan\? ** – os e-mails contendo a frase *Ivan?* são aceitos.

Para desabilitar o uso de um determinado endereço ou frase como atributo de spam, é possível excluí-lo usando o botão Excluir ou a caixa ao lado do texto pode ser desmarcada para desabilitá-lo.

13.3.5. Recursos adicionais da filtragem de spam

Além dos principais recursos usados para filtrar spam (a criação de listas brancas e negras, análise de phishing e tecnologias de filtragem), o Kaspersky Anti-Virus for Windows Workstations fornece recursos avançados.

Para configurar recursos avançados de filtragem de spam:

1. Abra a janela de configurações do aplicativo e selecione **Anti-Spam** em **Proteção**.
2. Clique no botão **Personalizar** na seção Sensibilidade da janela de configurações.
3. Abra a guia **Adicional** (veja a Figura 58).

A guia relaciona uma série de indicadores que classificarão os e-mails com mais probabilidade de ser spam.

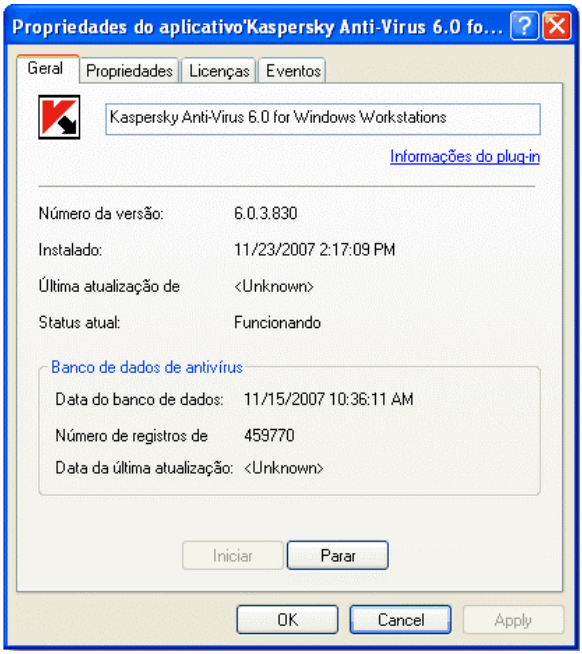


Figura 58. Configurações avançadas de reconhecimento de spam

Para usar um indicador de filtragem adicional, marque o sinalizador ao lado dele. Cada fator também exige que você configure um fator de spam (em pontos percentuais), que define a probabilidade de um e-mail ser classificado como spam. O valor padrão do fator de spam é 80%. Os e-mails serão marcados como spam se a soma das probabilidades de todos os fatores adicionais exceder 100%.

Os spams podem ser e-mails vazios (sem assunto ou corpo), e-mails contendo links para imagens ou com imagens incorporadas, com texto formatado na cor de fundo ou com texto utilizando uma fonte muito pequena. Os spams também podem ser e-mails com caracteres invisíveis (o texto coincide com a cor de fundo), e-mails contendo elementos ocultos (que não são exibidos) ou com marcações HTML incorretas, além de e-mails contendo scripts (séries de instruções executadas ao abrir o e-mail).

Se você ativar um filtro para capturar “mensagens não endereçadas a mim”, precisará criar uma lista de endereços confiáveis que pode ser acessada pelo botão **Meus endereços**. O endereço do destinatário será verificado na análise do e-mail. Se o endereço não corresponder aos endereços da lista, ele será rotulado como *spam*.

Você pode criar e editar uma lista de endereços em **Meus endereços** usando os botões **Adicionar**, **Editar** e **Excluir**.

Para excluir os e-mails encaminhados pela intranet (por exemplo, mensagens corporativas) da verificação de spam, marque ☑ **Não verificar mensagens nativas do MS Exchange**. Os e-mails serão considerados correspondência interna se todos os computadores da rede usarem o Microsoft Office Outlook como programa de e-mail e se as caixas de e-mail do usuário estiverem localizadas no servidor Exchange ou esses servidores deverão estar conectados por conectores X400. Para que o Anti-Spam analise esses e-mails, desmarque a caixa de seleção.

13.3.6. Mail Dispatcher

Aviso!

O Mail Dispatcher estará disponível somente se você receber e-mails pelo protocolo POP3.

O Mail Dispatcher foi criado para exibir a lista de mensagens de e-mail no servidor baixá-las para o computador. Isso permite que você não aceite mensagens, economizando tempo e dinheiro quando estiver trabalhando com o e-mail e diminuindo a probabilidade de baixar spams e vírus para o computador.

O Mail Dispatcher será aberto se a janela de configurações do **Anti-Spam** ☑ **Abrir o Mail Dispatcher ao receber e-mail** estiver marcada.

Para excluir e-mails do servidor sem baixá-los para o computador:

marque as caixas à esquerda dos e-mails que deseja excluir e clique no botão **Excluir**. Os e-mails marcados serão excluídos do servidor. Os demais serão baixados para o computador assim que a janela do Mail Dispatcher for fechada.

Às vezes, pode ser difícil decidir se você deve aceitar um determinado e-mail, analisando apenas o remetente e a linha de assunto do e-mail. Nesses casos, o Mail Dispatcher fornece mais informações, baixando os cabeçalhos do e-mail.

Para exibir os cabeçalhos dos e-mails:

selecione o e-mail na lista de e-mails recebidos. Os cabeçalhos do e-mail serão exibidos na parte inferior do formulário.

Os cabeçalhos do e-mail não têm um tamanho significativo, geralmente algumas dezenas de bytes, e não contêm código mal-intencionado.

Segue um exemplo de quando pode ser útil exibir os cabeçalhos de um e-mail: os remetentes de spam instalaram um programa mal-intencionado no computador de um colega, que envia spams para toda a lista de contatos do programa de e-mail usando o nome dele. A probabilidade de você estar na lista de contatos do seu colega é muito grande e, sem dúvida, sua caixa de entrada ficará repleta dos spams vindos dele. É impossível dizer apenas pelo endereço do remetente se o e-mail foi enviado por seu colega ou por um remetente de spam. Contudo, os cabeçalhos do e-mail mostrarão essas informações, permitindo que você verifique quem enviou o e-mail, quando, qual o seu tamanho, sendo possível rastrear o caminho do e-mail do remetente até seu servidor de e-mail. Todas essas informações devem estar nos cabeçalhos do e-mail. Então, você pode decidir se é realmente necessário baixar esses e-mails do servidor ou se é melhor excluí-los.

Observação:

Você pode classificar os e-mails por qualquer coluna da lista de e-mails. Para classificar, clique no cabeçalho da coluna. As linhas serão classificadas em ordem ascendente. Para alterar a ordem de classificação, clique novamente no cabeçalho da coluna.

13.3.7. Ações para spams

Se, depois da verificação, você achar que um e-mail é spam ou possível spam, as próximas etapas do Anti-Spam dependerão do status do objeto e da ação selecionada. Por padrão, os e-mails marcados como *spam* ou *possível spam* são modificados: as marcas **[!! SPAM]** ou **[?? Possível spam]** são adicionadas à linha de assunto.

Você pode selecionar outras ações para spams e possíveis spams. Para fazê-lo, são fornecidos plug-ins específicos para o Microsoft Outlook, Outlook Express (Windows Mail) e The Bat!. Você pode configurar regras de filtragem para os outros programas de e-mail.

13.3.8. Configurando o processamento de spams no Microsoft Office Outlook

Observe que não há um plug-in de spam para o Microsoft Outlook, se o aplicativo for executado no Windows 9x.

Por padrão, os e-mails classificados pelo Anti-Spam como *spam* ou *possível spam* recebem marcas específicas **[!! SPAM]** ou **[?? Possível spam]** na linha de **Assunto**.

Outras ações sobre spam e possível spam no Outlook podem ser encontradas na guia específica **Anti-Spam** do menu **Serviço** → **Opções** (veja a Figura 59).

Ele abre automaticamente quando o programa de e-mail é aberto pela primeira vez após a instalação do programa e pergunta se você deseja configurar o processamento de spams.

Você pode atribuir as seguintes regras de processamento para spams e possíveis spams:

Mover para a pasta – o spam é movido para a pasta especificada.

Copiar para a pasta – é criada uma cópia do e-mail e essa cópia é movida para a pasta especificada. O e-mail original permanece na sua Caixa de Entrada.

Excluir – exclui o spam da caixa de correio do usuário.

Ignorar – deixa o e-mail na sua Caixa de Entrada.

Para fazê-lo, selecione o valor apropriado na lista suspensa na seção **Spam** ou **Possível spam**.

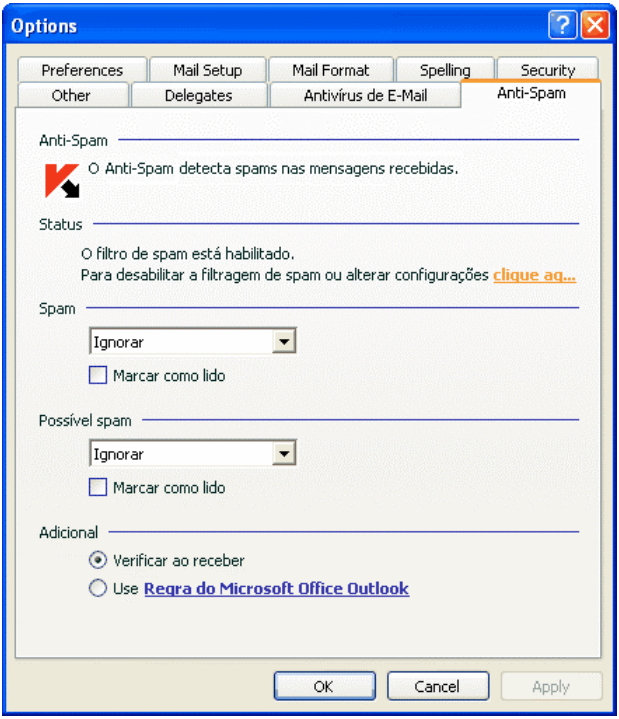


Figura 59. Configurando o processamento de spams no Microsoft Office Outlook

Você também pode configurar o Microsoft Office Outlook e o Anti-Spam para funcionarem em conjunto:

- **Verificar ao receber**. Todos os e-mails que entrarem na caixa de entrada do usuário serão processados inicialmente de acordo com as regras do Outlook. Terminado o processamento, o plug-in do Anti-Spam processa as mensagens que não se encaixam em nenhuma dessas regras. Em outras palavras, os e-mails são processados de acordo com a prioridade das regras. Às vezes, a seqüência de prioridades pode ser ignorada se, por exemplo, um grande número de e-mails chegar na sua Caixa de Entrada ao mesmo tempo. Nesse caso, podem acontecer situações em que informações sobre um e-mail processadas por uma regra do Outlook são registradas no relatório do Anti-Spam como *spam*. Para evitar isso, é recomendável configurar o plug-in do Anti-Spam como uma regra do Outlook.
- **Usar regra do Microsoft Office Outlook**. Com essa opção, as mensagens recebidas são processadas com base na hierarquia das regras do Outlook

criadas. Uma delas deve ser uma regra sobre o processamento de e-mails pelo Anti-Spam. Essa é a melhor configuração. Ela não causará conflitos entre o Outlook e o plug-in do Anti-Spam. Seu único inconveniente é que você deverá criar e excluir regras de processamento de spams pelo Outlook manualmente.

O plug-in do Anti-Spam não poderá ser usado como regra do Outlook no Microsoft Office XP, se você estiver utilizando o 9x/ME/NT4, devido a um erro no Outlook XP.

Para criar uma regra de processamento de spams:

1. Abra o Microsoft Office Outlook e vá para **Serviço** → **Regras e alertas** no menu principal. O comando para abrir o Assistente depende da sua versão do Microsoft Office Outlook. Este Manual do Usuário descreve como criar uma regra usando o Microsoft Office Outlook 2003.
2. Na janela **Regras e alertas** que é aberta, clique em **Nova regra** na guia **Regras de e-mail** para abrir o Assistente de Regras. O **Assistente de Regras** o guiará pelas seguintes janelas e etapas:

   Etapa um

   Você pode optar por criar uma regra a partir do zero ou a partir de um modelo. Selecione **Iniciar de uma regra em branco** e **Verificar mensagens quando chegarem**. Clique no botão **Avançar**.

   Etapa dois

   Na janela **Condições da regra**, clique em **Avançar** sem marcar nenhuma caixa. Confirme na caixa de diálogo que você deseja aplicar essa regra a todos os e-mails recebidos.

   Etapa três

   Na janela para selecionar as ações a serem aplicadas às mensagens, marque **Executar ação personalizada** na lista de ações. Na parte inferior da janela, clique em ação personalizada. Na janela que é aberta, selecione **Kaspersky Anti-Spam** no menu suspenso e clique em **OK**.

   Etapa quatro

   Na janela para selecionar exceções à regra, clique em **Avançar** sem marcar nenhuma caixa.

   Etapa cinco

   Na janela para concluir a criação da regra, você pode editar o nome da regra (o padrão é **Kaspersky Anti-Spam**). Verifique se **Ativar esta regra** está marcado e clique em **Concluir**.

3. Por padrão, a nova regra ocupa a primeira posição na lista de regras da janela **Regras de e-mail**. Se preferir, mova a regra para o final da lista, de forma que ela seja aplicada por último ao e-mail.

Todos os e-mails recebidos são processados de acordo com essas regras. A ordem na qual as regras são aplicadas dependem de sua prioridade, com as regras no início da lista tendo uma prioridade mais alta que as do final. Você pode alterar a prioridade de aplicação das regras aos e-mails.

Se não quiser que a regra do Anti-Spam continue a processar os e-mails depois da aplicação de uma regra, marque a opção **Parar de processar mais regras** na configuração das regras (consulte a Etapa três da criação de uma regra).

Se você tiver experiência na criação de regras de processamento de e-mails no Outlook, poderá criar sua própria regra para o Anti-Spam com base na configuração sugerida.

13.3.9. Configurando o processamento de spams no Outlook Express (Windows Mail)

Por padrão, os e-mails classificados pelo Anti-Spam como *spam* ou *possível spam* recebem marcas específicas **[!! SPAM]** ou **[?? Possível spam]** na linha de **Assunto**.

Outras ações para spam e possível spam no Outlook Express (Windows Mail) podem ser encontradas na janela de configurações que é aberta (veja a Figura 60) ao clicar no botão **Configuração**, perto dos botões **Spam** e **Não spam** no painel de tarefas.

Ele abre automaticamente quando o programa de e-mail é aberto pela primeira vez após a instalação do programa e pergunta se você deseja configurar o processamento de spams.

Você pode atribuir as seguintes regras de processamento para spams e possíveis spams:

Mover para a pasta – o spam é movido para a pasta especificada.

Copiar para a pasta – é criada uma cópia do e-mail e essa cópia é movida para a pasta especificada. O e-mail original permanece na sua Caixa de Entrada.

Excluir – exclui o spam da caixa de correio do usuário.

Ignorar – deixa o e-mail na sua Caixa de Entrada.

Para atribuir estas regras, selecione o valor apropriado na lista suspensa da seção **Spam** ou **Possível spam**.

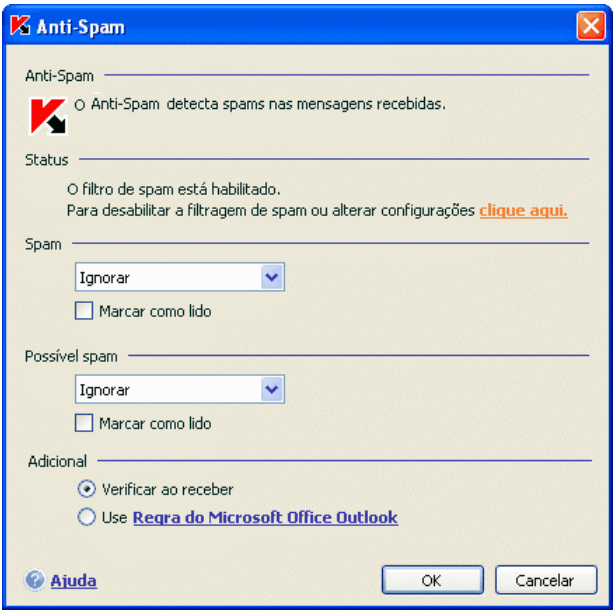


Figura 60. Configurando o processamento de spams no Microsoft Outlook Express

13.3.10. Configurando o processamento de spams no The Bat!

O programa de e-mail deve ser reiniciado depois de habilitar/desabilitar o plug-in do Microsoft Outlook Express.

As ações para spams e possíveis spams no The Bat! são definidas pelas ferramentas do próprio programa.

Para configurar as regras de processamento de spams no The Bat!:

1. Selecione **Settings** no menu **Properties** do programa de e-mail.
2. Selecione **Anti-spam** na árvore de configurações (veja a Figura 61).

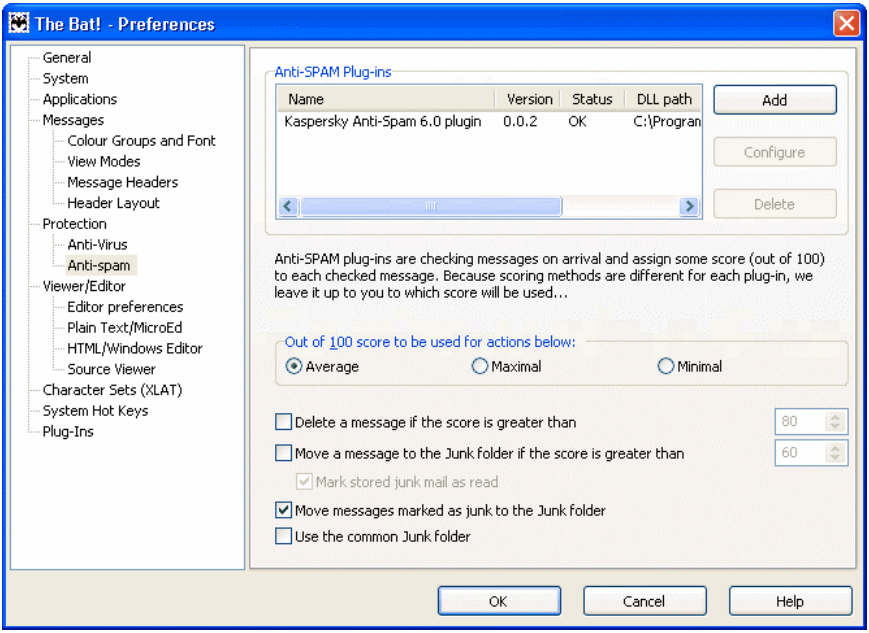


Figura 61. Configurando o reconhecimento e o processamento de spams no The Bat!

As configurações de proteção contra spams apresentadas estendem-se a todos os módulos anti-spam instalados no computador que funcionam com o The Bat!

É necessário definir o nível de classificação e especificar como responder aos e-mails com uma determinada classificação (no caso do Anti-Spam, a probabilidade do e-mail ser spam):

- Excluir os e-mails com uma classificação superior a um determinado valor.
- Mover os e-mails em um determinado intervalo de classificações para uma pasta específica de spams.
- Mover os spams marcados com cabeçalhos específicos para a pasta de spams.
- Deixar os spams na sua Caixa de Entrada.

Aviso!

Após o processamento de um e-mail, o Kaspersky Anti-Virus for Windows Workstations atribui o status de spam ou possível spam a ele, com base em um fator (consulte 13.3.3 na p. 183) com um valor que você pode ajustar. O The Bat! tem seu próprio método para classificação de spams, também baseado em um fator de spam. Para assegurar que não haja discrepâncias entre os fatores de spam do Kaspersky Anti-Virus for Windows Workstations e do The Bat!, todos os e-mails verificados pelo Anti-Spam receberão uma classificação de acordo com as categorias de status de e-mails usada pelo The Bat!: *e-mail aceito* – 0%, *possível spam – 50 %*, spam – *100 %*.

Dessa forma, a classificação de spams no The Bat! corresponderá não ao fator de e-mail atribuído pelo Anti-Spam, mas ao fator do status correspondente.

Para obter mais detalhes sobre regras de processamento e classificação de spams, consulte a documentação do The Bat!.

CAPÍTULO 14. VERIFICANDO O COMPUTADOR QUANTO A PRESENÇA DE VIRUS

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

O Kaspersky Anti-Virus for Windows Workstations 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.

As configurações padrão dessas tarefas são as recomendadas. É possível editar essas configurações (consulte 14.4 na p. 203) ou criar uma programação (consulte 6.5 na p. 87) para a execução das tarefas.

Você também pode criar suas próprias tarefas (consulte a seção 14.3 na p. 202) e criar uma programação para elas. Por exemplo, é possível programar uma tarefa de verificação semanal dos bancos de dados de e-mail ou uma tarefa de verificação de vírus na pasta **Meus Documentos**.

Além disso, você pode verificar qualquer objeto quanto à presença de vírus (por exemplo, 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 for Windows Workstations ou com as ferramentas padrão do sistema operacional Windows (por exemplo, na janela do programa **Explorer** ou na **Área de Trabalho**).

Você pode exibir uma lista completa das tarefas de verificação de vírus no computador clicando em **Verificação** no painel esquerdo da janela principal do programa.

14.1. Gerenciando tarefas de verificação de vírus

Você pode executar uma tarefa de verificação de vírus manual ou automaticamente por meio de uma programação (consulte 6.5 na p. 87).

Para iniciar uma tarefa de verificação de vírus manualmente:

Marque a caixa ao lado do nome da tarefa na seção **Verificação** da janela principal do programa e clique no botão na barra de status.

As tarefas em execução (incluindo aquelas criadas com o Kaspersky Administration Kit) são exibidas no menu de contexto clicando com o botão direito do mouse no ícone da bandeja do sistema.

Para pausar uma tarefa de verificação:

Clique no botão na barra de status. O status da tarefa mudará para *em pausa*. A verificação será pausada até ser iniciada manualmente ou ela iniciará automaticamente de acordo com a programação.

Para interromper uma tarefa de verificação:

Clique no botão na barra de status. O status da tarefa mudará para *interrompida*. A verificação será interrompida até ser iniciada manualmente ou ela iniciará automaticamente de acordo com a programação. Na próxima vez que você executar a tarefa, o programa perguntará se deseja continuar a tarefa do ponto em que foi interrompida ou iniciá-la novamente.

14.2. Criando uma lista de objetos para verificação

Para exibir uma lista dos objetos que devem ser verificados por uma determinada tarefa, selecione o nome da tarefa (por exemplo, **Meu Computador**) na seção **Verificação** da janela principal do programa. A lista de

objetos será exibida à direita da janela, abaixo da barra de status (veja a Figura 62).

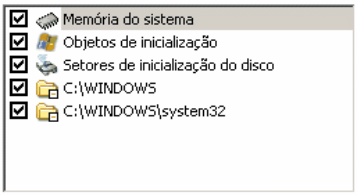


Figura 62. Lista de objetos a serem verificados

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 em uma área de verificação, você pode editar a recursão selecionando um item na lista de verificação, abrindo um menu de atalho e usando a opção **Incluir subpastas**.

Para excluir um objeto, selecione-o na lista (ao fazê-lo, o nome do objeto será realçado em cinza) e clique no botão **Excluir**. É possível desabilitar temporariamente a verificação de objetos individuais para qualquer tarefa sem excluí-los da lista. Para fazê-lo, desmarque a caixa ao lado do objeto que não deseja verificar.

Para iniciar uma tarefa de verificação, clique no botão **Verificação**, selecione **Iniciar** no menu que é aberto ao clicar no botão **Ações**.

Além disso, você pode selecionar um objeto para ser verificado usando as ferramentas padrão do sistema operacional Windows (por exemplo, na janela do programa Explorer ou na Área de Trabalho, etc.) (veja a Figura 63). Para fazê-lo, selecione o objeto, abra o menu de contexto do Windows clicando com o botão direito do mouse e selecione **Verificar vírus**.

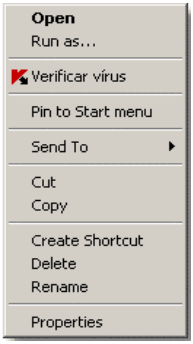


Figura 63. Verificando objetos a partir do menu de contexto do Windows

14.3. Criando tarefas de verificação de vírus

Para verificar objetos no computador quanto à presença de vírus, você pode usar as tarefas de verificação internas incluídas no programa e criar suas próprias tarefas. As novas tarefas de verificação são criadas usando tarefas existentes como modelo.

Para criar uma nova tarefa de verificação de vírus:

1. Selecione a tarefa com as configurações mais próximas do necessário na seção **Verificação** da janela principal do programa.
2. Abra o menu de contexto clicando com o botão direito do mouse no nome da tarefa ou clique no botão **Ações** à direita da lista de objetos para verificação e selecione **Salvar como...**.
3. Insira o nome da nova tarefa na janela que é aberta e clique em **OK**. Uma tarefa com esse nome aparecerá na lista de tarefas na seção **Verificação** da janela principal do programa.

Aviso!

O número de tarefas que podem ser criadas pelo usuário é limitado. O máximo são quatro tarefas.

A nova tarefa é uma cópia daquela na qual foi baseada. É necessário continuar sua configuração por meio da criação de uma lista de objetos para verificação (consulte 14.2 na p. 200), da configuração de propriedades que controlarão a tarefa (consulte 14.4 na p. 203) e, se necessário, da configuração de uma programação (consulte 6.5 na p. 87) para executar a tarefa automaticamente.

Para renomear uma tarefa criada:

Selecione a tarefa na seção **Verificação** da janela principal do programa. Clique com o botão direito do mouse no nome da tarefa para abrir o menu de contexto ou clique no botão **Ações** à direita da lista de objetos para verificação e selecione **Renomear**.

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

Para excluir uma tarefa criada:

Selecione a tarefa na seção **Verificação** da janela principal do programa. Clique com o botão direito do mouse no nome da tarefa para abrir o menu de contexto ou clique no botão **Ações** à direita da lista de objetos para verificação e selecione **Excluir**.

Você deverá confirmar que deseja excluir a tarefa. A tarefa será então excluída da lista de tarefas na seção **Verificação**.

Aviso!

É possível renomear e excluir somente as tarefas criadas por você.

14.4. 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 e selecione uma tarefa pelo nome em **Verificação**.

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

- selecionar o nível de segurança que será usado pela tarefa (consulte a seção 14.4.1 na p. 204)
- editar configurações avançadas:
    - definir os tipos de arquivos que devem ser verificados quanto à presença de vírus (consulte a seção 14.4.2 na p. 205)
    - configurar o início da tarefa usando um perfil de usuário diferente (consulte 6.4 na p. 86)

- definir as configurações avançadas de verificação (consulte 14.4.5 na p. 211)

- restaurar as configurações padrão de verificação (consulte a seção 14.4.3 na p. 208)
- selecionar uma ação que o programa aplicará ao detectar um objeto infectado ou suspeito (consulte 14.4.4 na p. 208)
- criar uma programação (consulte 6.5 na p. 87) para executar tarefas automaticamente
- além disso, você pode definir configurações globais (consulte a seção 14.4.6 na p. 212) para executar todas as tarefas

As seções a seguir examinam detalhadamente as configurações de tarefas listadas acima.

14.4.1. Selecionando um nível de segurança

É possível atribuir um nível de segurança a cada tarefa de verificação de vírus (veja a Figura 64):

Alto – a verificação mais completa de todo o computador ou de discos, pastas ou arquivos individuais. É recomendável usar este nível no caso de suspeita de que um vírus infectou o computador.

Recomendado – os especialistas da Kaspersky Lab recomendam este nível. Serão verificados os mesmos arquivos que na configuração **Alto**, exceto pelos bancos de dados de e-mails.

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

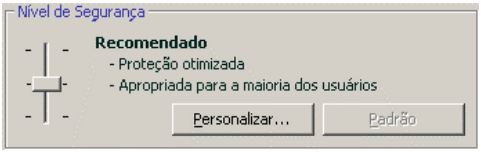


Figura 64. Selecionando um nível de segurança de verificação de vírus

Por padrão, o nível de verificação 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 da verificação. Para fazê-lo, selecione o nível mais próximo do necessário como ponto inicial e edite suas configurações. Se o fizer, o nível será renomeado para **Personalizado**.

Para modificar as configurações de um nível de segurança:

clique no botão **Configurações** na janela de configurações de tarefas. Edite as configurações de verificação na janela que é aberta e clique em **OK**.

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

14.4.2. 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 65). 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. 323).

Dica:

Não esqueça que alguém pode enviar para o seu computador um vírus com a extensão .txt que, na verdade, é um arquivo executável renomeado como .txt. Se você selecionar a opção **Programas e documentos (por extensão)**, a verificação ignorará esse arquivo. Se a opção **Verificar programas e documentos (por conteúdo)** for selecionada, o programa analisará os cabeçalhos dos arquivos, descobrindo que o arquivo é um arquivo .exe e o verificando extensivamente quanto à presença de vírus.

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

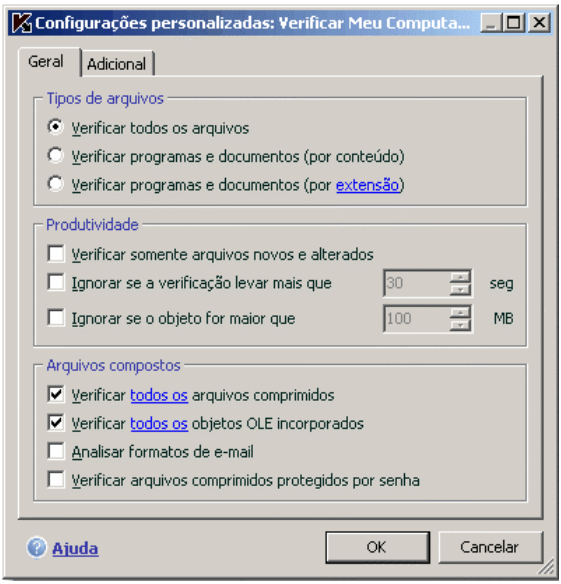


Figura 65. Configurando a verificação

Você também pode definir limites de tempo e de tamanho de arquivo para a verificação na seção **Produtividade**.

Ignorar se a verificação levar mais que... seg. Marque esta opção e insira o tempo máximo de verificação de um objeto. Se esse tempo for excedido, o objeto será removido da fila de verificação.

Ignorar se o objeto for maior que... MB. Marque esta opção e insira o tamanho máximo de um objeto. Se esse tamanho for excedido, o objeto será removido da fila de verificação.

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

Verificar todos os/somente novos arquivos comprimidos – verifica arquivos comprimidos .rar, .arj, .zip, .cab, .lha, .jar e .ice.

Aviso!

O Kaspersky Anti-Virus não exclui automaticamente os arquivos comprimidos em formatos aos quais ele não dá suporte (por exemplo, .ha, .uue, .tar), mesmo se você optar pela neutralização ou exclusão automática no caso de não ser possível neutralizar os objetos.

Para excluir esses arquivos comprimidos, clique no link Excluir arquivos comprimidos na notificação de detecção de objetos perigosos. Essa notificação será exibida na tela depois que o programa inicia o processamento dos objetos detectados na verificação. Você também pode excluir os arquivos comprimidos infectados manualmente.

Verificar todos os/somente novos objetos OLE incorporados - verifica objetos incorporados em arquivos (por exemplo planilhas do Excel ou uma macro incorporada em um arquivo do Microsoft Word, anexos de e-mail, etc.).

Você pode selecionar e verificar todos os arquivos ou somente os novos de cada tipo de arquivo composto. Para fazê-lo, use o link ao lado do nome do objeto. Ele muda seu valor quando você clica nele. Se a seção **Produtividade** tiver sido configurada para verificar somente arquivos novos e modificados, você não poderá selecionar o tipo de arquivos compostos que serão verificados.

Analisar formatos de e-mail – verifica arquivos e bancos de dados de e-mails. Se esta caixa de seleção estiver habilitada, o Kaspersky Anti-Virus separará o arquivo com formato de e-mail e analisará cada componente (corpo, anexos, etc.) quanto à presença de vírus. Se a caixa não estiver marcada, o arquivo será verificado como um único objeto.

Observe que, ao verificar bancos de dados de e-mail protegidos por senha:

- O Kaspersky Anti-Virus for Windows Workstations detecta código mal-intencionado em bancos de dados do Microsoft Outlook 2000, mas não os neutraliza;
- O Kaspersky Anti-Virus for Windows Workstations 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.

14.4.3. Restaurando configurações de verificação padrão

Ao definir as configurações de tarefas de verificação, é sempre possível retornar para as configurações recomendadas. A Kaspersky Lab as considera ideais e as combinou no nível de segurança **Recomendado**.

Para restaurar as configurações de verificação padrão:

1. Selecione o nome da tarefa na seção **Verificação** da janela principal e use o link Configurações para abrir a janela de configurações da tarefa.
2. Clique no botão **Padrão** na seção **Nível de segurança**.

14.4.4. Selecionando ações para objetos

Se, durante uma verificação, for descoberto que um arquivo está infectado ou é suspeito, as próximas etapas do programa dependerão do status do objeto e da ação selecionada.

Um dos seguintes status pode ser atribuído ao objeto após a verificação:

- Status de programa mal-intencionado (por exemplo, *vírus, cavalo de Tróia*).
- *Possivelmente infectado*, quando a verificação não consegue determinar se o objeto está infectado. Isso significa que o código do arquivo contém uma seção que se assemelha a um vírus conhecido

mas modificado ou é remanescente da estrutura de uma seqüência de vírus.

Por padrão, todos os arquivos infectados são desinfectados e, se estiverem possivelmente infectados, serão enviados para a Quarentena.

Para editar uma ação para um objeto:

selecione o nome da tarefa na seção **Verificação** da janela principal do programa e use o link Configurações para abrir a janela de configurações da tarefa. Todas as respostas possíveis são exibidas nas seções apropriadas (veja a Figura 66).

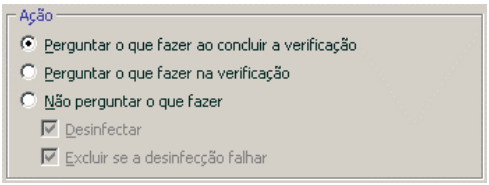


Figura 66. Selecionando ações para objetos perigosos

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.

Se a ação selecionada for	Ao detectar um objeto mal-intencionado ou possivelmente infectado
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 17.1 na p. 233). Essas informações são registradas no relatório (consulte a seção 17.3 na p. 239). 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.

Antes de desinfectar ou excluir um objeto, o Kaspersky Anti-Virus for Windows Workstations cria uma cópia de backup do mesmo e a envia para o Backup (consulte 17.2 na p. 237), caso seja necessário restaurá-lo ou surja uma oportunidade de neutralizá-lo posteriormente.

14.4.5. Outras configurações de verificação de vírus

Além de definir as configurações básicas de verificação de vírus, você também pode usar configurações avançadas (veja a Figura 67):

- **Habilitar tecnologia iChecker** – usa a tecnologia que pode aumentar a velocidade de verificação por meio da exclusão de determinados objetos. Um objeto é excluído da verificação usando um algoritmo específico que leva em conta a data de lançamento das assinaturas de ameaças, a data mais recente em que o objeto foi verificado e as modificações das configurações de verificação.

  Por exemplo, você tem um arquivo armazenado que o programa verificou e ao qual atribuiu o status de *não infectado*. Na próxima verificação, o programa ignorará esse arquivo, a menos que ele tenha sido modificado ou que as configurações de verificação tenham sido alteradas. Mas o programa verificará o arquivo comprimido novamente se sua estrutura tiver mudado porque foi adicionado um novo objeto a ele, se as configurações de verificação tiverem sido alteradas ou se as assinaturas de ameaças tiverem sido atualizadas.

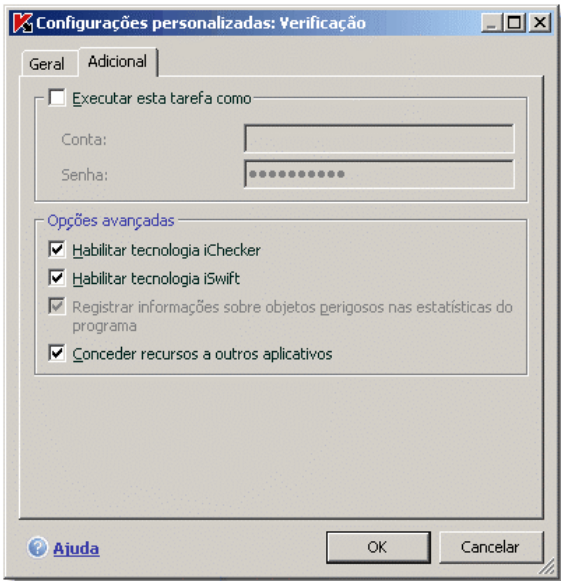


Figura 67. Configurações avançadas de verificação

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 for Windows Workstations (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.

A tecnologia iSwift não está disponível em computadores com o Microsoft Windows 98SE/ME/XP64.

Registrar informações sobre objetos perigosos nas estatísticas do programa - salva informações sobre objetos perigosos detectados nas estatísticas gerais do programa e exibe uma lista de ameaças detectadas durante a verificação na guia **Detectados** da janela do relatório (consulte a 17.3.2 na p. 243). Se esta opção ficar desmarcada, as informações sobre objetos perigosos não serão exibidas no relatório e será impossível processar dados.

Conceder recursos a outros aplicativos – pausa a tarefa de verificação de vírus se o processador estiver ocupado com outros aplicativos.

14.4.6. Definindo configurações globais de verificação para todas as tarefas

Cada tarefa de verificação é executada de acordo com suas próprias configurações. Por padrão, as tarefas criadas ao instalar o programa no computador usam as configurações recomendadas pela Kaspersky Lab.

Você pode definir configurações globais de verificação para todas as tarefas. Como ponto de partida, você usará um conjunto de propriedades utilizadas para verificar vírus em um objeto individual.

Para atribuir configurações globais de verificação para todas as tarefas:

1. Selecione a seção **Verificação** à esquerda da janela principal do programa e clique em Configurações.
2. Na janela de configurações que é aberta, defina as configurações de verificação: Selecione o nível de segurança (consulte 14.4.1 na p. 204), defina as configurações de nível avançado e selecione uma ação (consulte 14.4.4 na p. 208) 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 15. 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.

15.1. O vírus de teste da EICAR e suas variações

O vírus de teste foi especialmente desenvolvido pela eicar (The European Institute for Computer Antivirus Research) pra testar a funcionalidade dos antivírus.

O vírus de teste NÃO É UM VÍRUS e não contém nenhum código de programa que possa danificar seu computador. Contudo, a maioria dos programas antivírus o identificarão como um vírus.

Nunca use vírus reais para testar a funcionalidade de um antivírus!

Você pode baixar o vírus de teste do site oficial da **EICAR**: http://www.eicar.org/anti_virus_test_file.htm.

O arquivo que é baixado do site da **EICAR** contém o corpo de um vírus de teste padrão. O Kaspersky Anti-Virus o detectará, o rotulará como um **vírus** e executará a ação definida para esse tipo de objeto.

Para testar as reações do Kaspersky Anti-Virus quando diferentes tipos de objetos são detectados, você pode modificar o conteúdo do vírus de teste padrão, adicionando um dos prefixos mostrados na tabela.

Prefixo	Status do vírus de teste	Ação correspondente quando o aplicativo processar o objeto
Sem prefixo, vírus de teste padrão	O arquivo contém um vírus de teste. Não é possível desinfectar o objeto.	O aplicativo identificará o objeto como sendo mal-intencionado e não passível de neutralização, e o excluirá.

Prefixo	Status do vírus de teste	Ação correspondente quando o aplicativo processar o objeto
CORR–	Corrompido.	O aplicativo poderia acessar o objeto, mas não verificá-lo, pois ele está corrompido (por exemplo, a estrutura do arquivo foi violada ou tem um formato de arquivo inválido).
SUSP– WARN–	O arquivo contém um vírus de teste (modificação). Não é possível desinfectar o objeto.	Esse objeto é uma modificação de um vírus conhecido ou desconhecido. No momento da detecção, os bancos de dados de assinaturas de ameaças não contêm uma descrição do procedimento para neutralizar esse objeto. O aplicativo o colocará na Quarentena para que seja processado posteriormente com assinaturas de ameaças atualizadas.
ERRO–	Erro de processamento.	Ocorreu um erro ao processar o objeto: o aplicativo não pode acessar o objeto que está sendo verificado, pois a integridade do mesmo foi violada (por exemplo, não existe um final em um arquivo comprimido com vários volumes) ou não é possível conectá-lo (se o objeto estiver sendo verificado em uma unidade de rede).
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.

Prefixo	Status do vírus de teste	Ação correspondente quando o aplicativo processar o objeto
DELE–	O arquivo contém um vírus de teste. Não é possível desinfectar o objeto.	Esse objeto contém um vírus que não pode ser desinfectado ou que é um cavalo de Tróia. O aplicativo exclui esses objetos.

A primeira coluna da tabela contém os prefixos que precisam ser adicionados ao início da seqüência de caracteres de um vírus de teste padrão. A segunda coluna descreve o status e a reação do Kaspersky Anti-Virus aos vários tipos de vírus de teste. A terceira coluna contém informações sobre objetos com o mesmo status que o aplicativo processou.

Os valores das configurações de verificação de vírus determinam a medida tomada sobre cada um dos objetos.

15.2. Testando o Antivírus de Arquivos

Para testar a funcionalidade do Antivírus de Arquivos;

1. Crie uma pasta em um disco; copie o vírus de teste baixado do site oficial da organização (consulte a seção 15.1 na p. 213) e as modificações do vírus de teste que você criou para essa pasta.
2. Permita que todos os eventos sejam registrados de forma que o arquivo de relatório mantenha os dados de objetos corrompidos e objetos não verificados devido a erros. Para fazê-lo, marque **Registrar eventos não críticos** na janela de configurações do relatório.
3. Execute o vírus de teste ou uma de suas modificações.

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

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.

15.3. 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 15.1 na p. 213) 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 14.3 na p. 202) e selecione a pasta que contém o conjunto de vírus de teste para ser verificada (consulte a seção 14.2 na p. 200).
3. Permita que todos os eventos sejam registrados de forma que o arquivo de relatório mantenha os dados de objetos corrompidos e objetos não verificados devido a erros. Para fazê-lo, marque **Registrar eventos não críticos** na janela de configurações do relatório.
4. Execute a tarefa de verificação de vírus (consulte a seção 14.1 na p. 200).

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:

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 16. 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:

- **Assinaturas de ameaças, assinaturas de ataques de rede e drivers de rede**

  As informações no computador são protegidas usando um banco de dados que contém assinaturas de ameaças e perfis de ataques de rede. Os componentes que oferecem proteção usam o banco de dados de assinaturas de ameaças para pesquisar e desinfectar objetos nocivos no computador. As assinaturas são completadas a cada hora, com registros de novas ameaças e métodos para combatê-las. Assim, é recomendável atualizá-las periodicamente.

  Além das assinaturas de ameaças e do banco de dados de ataques de rede, 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. Com o Kaspersky Anti-Virus for Windows Workstations, você não precisa se preocupar com a seleção do conjunto de assinaturas de ameaças apropriado. Agora, nossos produtos usam assinaturas de ameaças que o protegem de objetos mal-intencionados e possivelmente perigosos, e de ataques de hackers.

- **Módulos do aplicativo**

  Além das assinaturas, você pode atualizar os módulos do Kaspersky Anti-Virus. Novas atualizações do aplicativo surgem periodicamente.

As principais fontes de atualização do Kaspersky Anti-Virus for Windows Workstations 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.

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 ou +7 (495) 956-70-00 e solicitar informações de contato dos parceiros da Kaspersky Lab que podem fornecer atualizações compactadas em disquetes ou CDs.

É possível baixar as atualizações de um dos seguintes modos:

- *Automaticamente*. O Kaspersky Anti-Virus verifica a fonte de atualizações em intervalos definidos. Durante os surtos de vírus, a freqüência dessa verificação pode aumentar, sendo diminuída ao final. Se houver novas atualizações, o Anti-Virus as baixa e instala no computador. Essa é a configuração padrão.
- *Na programação*. A atualização é programada para iniciar em uma hora especificada.
- *Manualmente*. Com esta opção, você inicia a Atualização manualmente.

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

Antes de atualizar as assinaturas de ameaças, o Kaspersky Anti-Virus for Windows Workstations cria cópias delas, que podem ser usadas se for necessário executar uma reversão (consulte 16.2 na p. 220). Se, por exemplo, o processo de atualização corromper as assinaturas de ameaças e inutilizá-las, você poderá facilmente reverter para a versão anterior e tentar atualizar as assinaturas mais tarde.

Você pode distribuir as atualizações recuperadas em uma fonte local enquanto atualiza o aplicativo (consulte 16.4.4 na p.229). Esse recurso permite atualizar os bancos de dados e os módulos usados pelos aplicativos 6.0 em computadores em rede para economizar largura de banda.

16.1. 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 16.4.1 na p. 222).

Você pode iniciar a Atualização:

- do menu de contexto (consulte a seção 4.2 na p. 53)
- da janela principal do programa (consulte a seção 4.3 na p. 55)

Para iniciar a Atualização no menu de atalho:

1. Clique com o botão direito do mouse no ícone do aplicativo na bandeja do sistema para abrir o menu de atalho.
2. Selecione **Atualização**.

Para iniciar a Atualização na janela principal do programa:

1. Selecione **Atualização** na seção **Serviço**.
2. Clique no botão **Atualizar agora** no painel direito da janela principal ou use o botão na barra de status.

O andamento da atualização será exibido em uma janela específica, que pode ser ocultada clicando em **Fechar**. A atualização continuará com a janela oculta.

As atualizações são distribuídas para a fonte local durante o processo de atualização, desde que esse serviço esteja habilitado (consulte a seção 16.4.4 na p. 229).

16.2. Revertendo para a atualização anterior

Sempre que você iniciar a Atualização, o Kaspersky Anti-Virus for Windows Workstations criará uma cópia de backup das assinaturas de ameaças atuais antes de começar o download das atualizações. Dessa forma, você poderá voltar a usar a versão anterior das assinaturas, se a atualização falhar.

Para reverter para a versão anterior das assinaturas de ameaças:

1. Selecione o componente **Atualização** na seção **Serviço** da janela principal do programa.

2. Clique no botão **Reverter** no painel direito da janela principal do programa.

16.3. Criando tarefas de atualização

O Kaspersky Anti-Virus possui uma tarefa de atualização interna para atualizar módulos do programa e assinaturas de ameaças. Você também pode criar suas próprias tarefas de atualização com várias configurações e programações de início.

Por exemplo, você instalou o Kaspersky Anti-Virus em um laptop que usa em casa e no escritório. Em casa, você atualiza o programa dos servidores de atualização da Kaspersky Lab e, no escritório, de uma pasta local que armazena as atualizações necessárias. Use duas tarefas diferentes para não precisar alterar as configurações de atualização a cada vez que mudar de local.

Para criar uma tarefa de atualização avançada:

1. Selecione **Atualização** na seção **Serviço** da janela principal do programa, abra o menu de contexto clicando com o botão direito do mouse e selecione **Salvar como**.

2. Insira o nome da tarefa na janela que é aberta e clique em **OK**. Uma tarefa com esse nome aparecerá então na seção **Serviço** da janela principal do programa.

Aviso!

O Kaspersky Anti-Virus tem um limite para o número de tarefas de atualização que podem ser criadas pelo usuário. O máximo são duas tarefas.

A nova tarefa herda todas as propriedades da tarefa na qual foi baseada, exceto as configurações de programação. A configuração padrão dessa verificação automática é desabilitada.

Depois de criar a tarefa, defina as configurações avançadas: especifique a fonte de atualização (consulte a seção 16.4.1 na p. 222), as configurações de rede (consulte a seção 16.4.3 na p. 227) e, se necessário, habilite as tarefas em outro perfil (consulte a seção 6.4 na p. 86) e configure a programação (consulte a seção 6.5 na p. 87).

Para renomear uma tarefa:

Selecione a tarefa na seção **Serviço** da janela principal do programa, abra o menu de contexto clicando com o botão direito do mouse e selecione **Renomear**.

Insira o novo nome da tarefa na janela que é aberta e clique em **OK**. O nome da tarefa será mudado então na seção **Serviço**.

Para excluir uma tarefa:

Selecione a tarefa na seção **Serviço** da janela principal do programa, abra o menu de contexto clicando com o botão direito do mouse e selecione **Renomear**.

Confirme se você deseja excluir a tarefa na janela de confirmação. A tarefa será então excluída da lista de tarefas na seção **Serviço**.

Aviso!

É possível renomear e excluir somente as tarefas criadas por você.

16.4. Configurando a atualização

As configurações da Atualização especificam os seguintes parâmetros:

- A fonte para o download e a instalação das atualizações (consulte a seção 16.4.1 na p. 222);
- O modo de atualização do aplicativo e os itens específicos atualizados (consulte a 16.4.2 na p. 225);
- A freqüência da atualização, caso as atualizações sejam executadas por programação (consulte a 6.5 na p. 87);
- A conta na qual a atualização será executada (consulte 6.4 na p. 86);
- O requisito para copiar as atualizações baixadas em um diretório local (consulte a seção 16.4.4 na p. 229);
- As ações que devem ser executadas após a conclusão da atualização (consulte a seção 16.4.5 na p. 230).

As seções a seguir examinam estes aspectos detalhadamente.

16.4.1. Selecionando uma fonte de atualização

A *fonte de atualização* é algum recurso que contém as atualizações das assinaturas das ameaças e dos módulos do aplicativo Kaspersky Anti-Virus.

Você pode usar as seguintes fontes de atualização:

- *Servidor de Administração* – um repositório de atualizações centralizado que reside no Servidor Administrativo do Kaspersky

Administration Kit (para obter mais detalhes, consulte o Manual do Usuário do Administrador do Kaspersky Administration Kit).

- *Servidores de atualização da Kaspersky Lab* – sites específicos que contêm atualizações disponíveis de assinaturas de ameaças e módulos dos aplicativos de todos os produtos da Kaspersky Lab.
- *Servidor FTP ou HTTP, pasta local ou de rede* – pasta ou servidor local que contém as atualizações mais recentes.

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 a sede da Kaspersky Lab pelos telefones +7 (495) 797-87-00, +7 (495) 645-79-39 ou +7 (495) 956-70-00 para solicitar informações de contato dos parceiros da Kaspersky Lab, que podem fornecer atualizações compactadas em disquetes ou CDs.

Aviso!

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

Você pode copiar as atualizações de um disco e carregá-las em um site FTP ou HTTP, ou salvá-las em uma pasta local ou de rede.

Selecione a fonte de atualização na guia **Fonte de atualização** (veja a Figura 68).

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. Durante a atualização, o Kaspersky Anti-Virus for Windows Workstations 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.

Para baixar atualizações de outro site FTP ou HTTP:

1. Clique em **Adicionar**.
2. Na caixa de diálogo **Selecionar fonte de atualização**, selecione o site FTP ou HTTP de destino ou especifique o endereço IP, o nome do caractere ou endereço da URL desse site no campo **Fonte**. Ao selecionar um site FTP como fonte de atualização, insira as configurações de autenticação na URL do servidor, no formato ftp://usuário:senha@servidor.

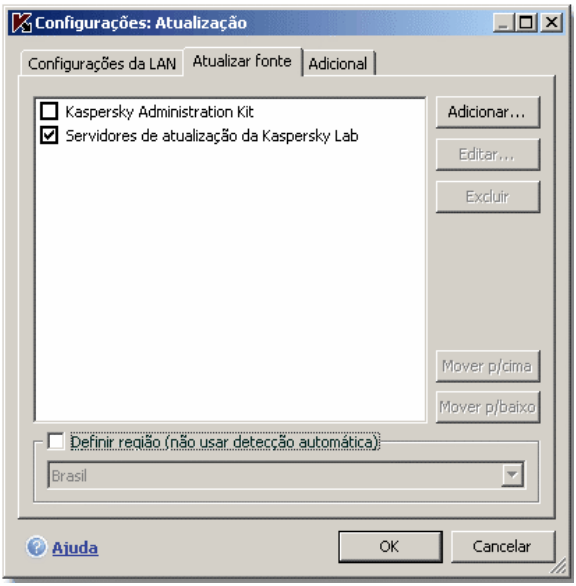


Figura 68. Selecionando uma fonte de atualização

Aviso!

Se você selecionou um recurso fora da rede local para as atualizações, será necessária uma conexão com a Internet para recuperar as atualizações.

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 for Windows Workstations adiciona novas fontes de atualização ao início da lista e habilita a fonte automaticamente, marcando a caixa ao lado do nome da fonte.

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.

16.4.2. Selecionando um método de atualização e o que atualizar

Ao definir as configurações de atualização, é importante especificar o que será atualizado e qual método de atualização será usado.

Objetos de atualização (veja a Figura 69) são os componentes que serão atualizados:

- Assinaturas de ameaças
- drivers de rede que permitem que os componentes de proteção interceptem o tráfego de rede
- bancos de dados de ataques de rede usados pelo Anti-Hacker
- Módulos do programa

As assinaturas de ameaças, drivers de rede e bancos de dados de ataques de rede são atualizados sempre, enquanto os módulos do aplicativo são atualizados somente se o modo correspondente estiver selecionado.

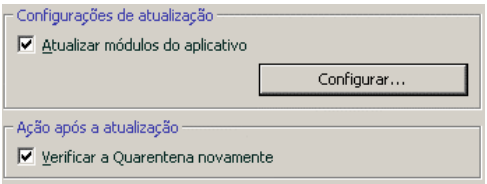


Figura 69. Selecionando objetos de atualização

Se desejar baixar e instalar atualizações dos módulos do programa:

Marque **Atualizar módulos do programa** na caixa de diálogo **Configurações da Atualização** do serviço **Atualização**.

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 programa anteriores sejam instaladas, somente as assinaturas de ameaças serão atualizadas.

O método de atualização (veja a Figura 70) define como a Atualização será iniciada. Você pode selecionar um desses métodos na seção **Modo de execução**:

Automaticamente. O Kaspersky Anti-Virus verifica a fonte de atualizações em intervalos definidos. Se houver novas atualizações, o Anti-Virus 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 for Windows Workstations 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 de assinaturas de ameaças, ataques de rede e módulos do software oportunamente, excluindo assim a possibilidade de invasão do computador por software mal-intencionado.

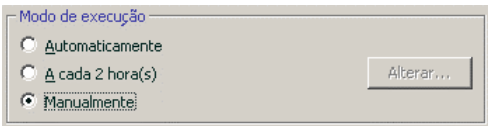


Figura 70. Selecionando um modo de execução da atualização

Na programação. A atualização é programada para iniciar em uma hora especificada. Por padrão, as atualizações programadas ocorrerão a cada 2 horas. 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 6.5 na p. 87).

Manualmente. Com esta opção, você inicia a Atualização manualmente. O Kaspersky Anti-Virus for Windows Workstations o notificará quando precisar ser atualizado:

- Uma mensagem pop-up informando que a atualização é necessária aparece acima do ícone do aplicativo na bandeja do sistema (se as notificações estiverem habilitadas; consulte a seção 17.11.1 na p. 271)
- O segundo indicador na janela principal do programa informa que seu computador está desatualizado (consulte 5.1.1 na p. 60)
- Uma recomendação de que é necessário atualizar o aplicativo aparece na seção de mensagens na janela principal do programa (consulte 4.3 na p. 55)

16.4.3. Configurando a conexão

Se você configurar o programa para recuperar atualizações dos servidores de atualização da Kaspersky Lab ou de outros sites FTP ou HTTP, é recomendável verificar primeiro suas configurações de conexão.

Todas as configurações estão agrupadas em uma guia específica – **Configurações da LAN** (veja a Figura 71).

Marque **Se possível, usar modo de FTP passivo** se você baixar as atualizações de um servidor FTP no modo passivo (por exemplo, através de um firewall). Se estiver trabalhando no modo FTP ativo, desmarque essa caixa de seleção.

No campo **Tempo limite da conexão… (seg)**, atribua o tempo alocado para a conexão com o servidor de atualização. Se a conexão falhar e esse período tiver acabado, o programa tentará conectar-se ao próximo servidor de atualização. Isso continuará até que uma conexão seja bem-sucedida ou até que se tenha tentado todos os servidores de atualização disponíveis.

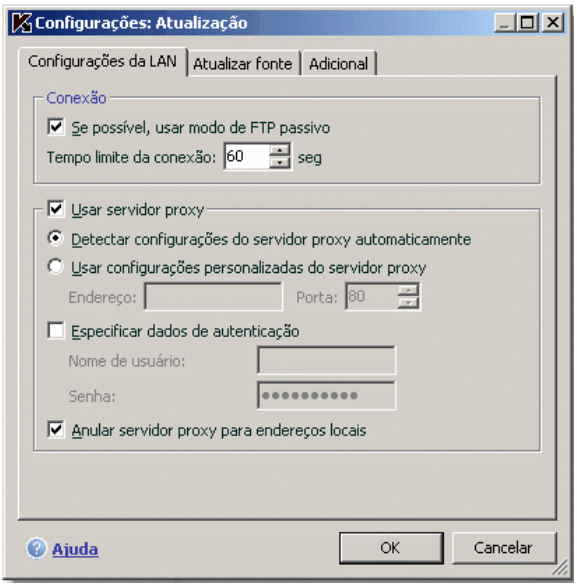


Figura 71. Definindo as configurações de atualização de rede

Marque **Usar servidor proxy** se estiver usando um servidor proxy para acessar a Internet e, se necessário, selecione as configurações a seguir:

- Selecione as configurações do servidor proxy que serão usadas durante a atualização:

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

  Usar configurações de proxy personalizadas - Usa um proxy diferente daquele especificado nas configurações de conexão do navegador. No campo **Endereço**, digite o endereço IP ou o nome simbólico do servidor proxy e especifique o número da porta proxy no campo Porta.

- Especifique se o servidor proxy requer autenticação. *Autenticação* é o processo de verificação dos dados de registro do usuário para fins de controle de acesso.

Se a autenticação for necessária para conectar-se ao servidor proxy, marque **Especificar dados de autenticação** e defina o nome de usuário e a senha nos campos a seguir. Nesse caso, serão tentadas primeiro a autenticação NTLM e depois a autenticação BASIC.

Se esta caixa de seleção não estiver marcada ou se os dados não forem inseridos, será tentada a autenticação NTLM utilizando a conta de usuário que foi usada para iniciar a atualização (consulte a seção 6.4 na p. 86).

Se o servidor proxy exigir autenticação e você não inseriu o nome de usuário e a senha ou se, por algum motivo, os dados especificados não foram aceitos pelo servidor proxy, uma janela pop-up será exibida ao iniciar as atualizações, solicitando um nome de usuário e uma senha para autenticação. Se a autenticação for bem-sucedida, o nome de usuário e a senha serão usados nas próximas atualizações. Caso contrário, as configurações de autenticação serão solicitadas novamente.

Para evitar o uso de um proxy quando a fonte de atualização for uma pasta local, selecione **Anular servidor proxy para endereços locais**.

Este recurso não está disponível no Windows 9X/NT 4.0. Entretanto, por padrão, o servidor proxy não é usado para endereços locais.

16.4.4. Distribuição de atualizações

O recurso de cópia de atualizações torna possível otimizar a carga na rede empresarial. As atualizações são copiadas em dois estágios:

1. Um dos computadores na rede recupera um pacote de atualização do aplicativo e da assinatura de ameaças nos servidores da Kaspersky Lab ou de outros recursos da Web que hospedem um conjunto de atualizações. As atualizações recuperadas são colocadas em uma pasta de acesso público.
2. Os outros computadores da rede acessam essa pasta para recuperar as atualizações do aplicativo.

Para habilitar a distribuição de atualizações, marque a caixa de seleção **Pasta de distribuição de atualizações** na guia **Adicional** (veja a Figura 72) 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.

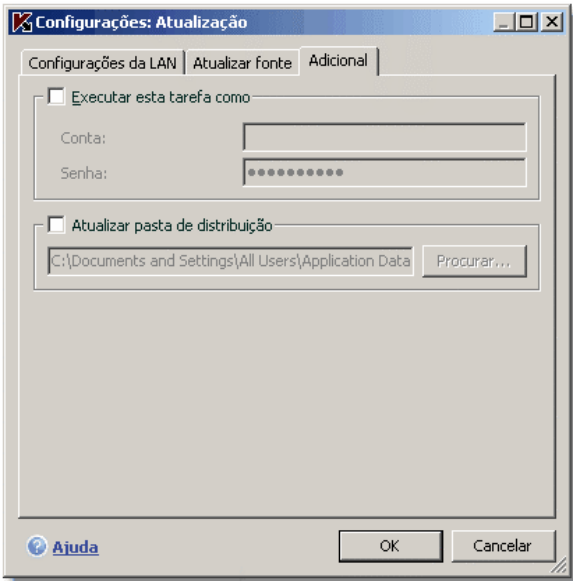


Figura 72. Configurações da ferramenta de cópia de atualizações

Observe que o Kaspersky Anti-Virus 6.0 recupera apenas os pacotes de atualização para aplicativos da versão 6.0 dos servidores de atualização da Kaspersky Lab. É recomendável copiar atualizações para outros aplicativos da Kaspersky Lab através do Kaspersky Administration Kit.

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.

16.4.5. Ações após a atualização do programa

Cada atualização de assinaturas de ameaças contém novos registros que protegem seu computador das ameaças mais recentes.

A Kaspersky Lab recomenda verificar os *objetos em quarentena* e os *objetos de inicialização* sempre que o banco de dados for atualizado.

Por que esses objetos devem ser verificados?

A área de quarentena contém objetos que foram sinalizados pelo programa como suspeitos ou possivelmente infectados (consulte a seção 17.1 na p. 233). Usando a versão mais recente das assinaturas de ameaças, talvez o Kaspersky Anti-Virus for Windows Workstations possa identificar a ameaça e eliminá-la.

Por padrão, o aplicativo verifica os objetos em quarentena depois de cada atualização das assinaturas de ameaças. Também é recomendável verificar periodicamente os objetos em quarentena porque o status dos mesmos pode mudar após várias verificações. Alguns objetos podem ser então restaurados para os locais anteriores e você poderá continuar trabalhando com eles.

Para desabilitar as verificações de objetos em quarentena, desmarque  **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 for Windows Workstations possui uma tarefa interna de verificação de objetos de inicialização (consulte Capítulo 14 na p. 199). É recomendável configurar uma programação para essa tarefa de forma que ela seja iniciada automaticamente depois de cada atualização das assinaturas de ameaças (consulte 6.5 na p. 87).

CAPÍTULO 17. OPÇÕES AVANÇADAS

O Kaspersky Anti-Virus for Windows Workstations 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 for Windows Workstations alterou ou excluiu (consulte 17.2 na p. 237). Se não foi possível recuperar integralmente um objeto que continha informações importantes para você durante o processamento do antivírus, sempre é possível restaurá-lo a partir de sua cópia de backup.

- A Quarentena contém objetos possivelmente infectados que não puderam ser processados usando as assinaturas de ameaças atuais (consulte 17.1 na p. 233).

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 for Windows Workstations (consulte 17.6 na p. 260) A Kaspersky fornece vários canais de suporte, incluindo o suporte on-line e um fórum de perguntas e comentários para usuários dos programas.

- O recurso de Notificações configura as notificações do usuário sobre momentos-chave no Kaspersky Anti-Virus for Windows Workstations (consulte 17.11.1 na p. 271). Podem ser eventos de natureza informativa ou sobre erros críticos que devem ser eliminados imediatamente.

- A Autodefesa protege os próprios arquivos do programa contra modificações ou danos provocados por hackers, bloqueia o uso dos recursos do programa pela administração remota e restringe a realização de determinadas ações no Kaspersky Anti-Virus for Windows Workstations por outros usuários (consulte 17.11.1.2 na p. 274). Por exemplo, alterar o nível de proteção pode influir significativamente sobre a segurança das informações no computador.

- O Gerenciador de Chaves de Licença pode obter informações detalhadas sobre a licença usada, ativar sua cópia do programa e gerenciar arquivos de chave de licença (consulte 17.5 na p. 257).

O programa também fornece uma seção de Ajuda (consulte a seção 17.4 na p. 256) e relatórios detalhados (consulte a seção 17.3 na p. 239) sobre a operação de todos os componentes de proteção e tarefas de atualização e verificação de vírus.

A criação da lista de portas monitoradas pode controlar quais módulos do Kaspersky Anti-Virus for Windows Workstations controlam os dados transferidos nas portas selecionadas (consulte a seção 17.7 na p. 261).

O Disco de Recuperação permite restaurar a funcionalidade do computador após uma infecção (consulte a seção 17.10 na p. 267). 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 for Windows Workstations e personalizar a interface do programa (consulte 17.9 na p. 265).

As seções a seguir abordam estes recursos mais detalhadamente.

17.1. Quarentena de objetos possivelmente infectados

A **Quarentena** é uma área de armazenamento específica que mantém os objetos possivelmente infectados.

Os **objetos possivelmente infectados** são aqueles que se suspeita estarem infectados com vírus ou modificações deles.

Por que *possivelmente infectados*? Por vários motivos, nem sempre é possível determinar se um objeto está infectado:

- O código do objeto verificado se parece com uma ameaça conhecida, mas está parcialmente modificado.

  As assinaturas de ameaças contêm ameaças que já foram estudadas pela Kaspersky Lab. Se um programa mal-intencionado for modificado por um hacker mas essas alterações ainda não tiverem sido inseridas nas assinaturas, o Kaspersky Anti-Virus for Windows Workstations classificará o objeto infectado com esse programa mal-intencionado como possivelmente infectado e indicará a ameaça com a qual a infecção se parece.

- O código do objeto detectado se parece, estruturalmente, com um programa mal-intencionado; contudo, não há nada semelhante registrado nas assinaturas de ameaças.

  É bastante possível que se trate de um novo tipo de ameaça, então o Kaspersky Anti-Virus for Windows Workstations classifica o 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.

17.1.1. Ações sobre objetos em quarentena

O número total de objetos em Quarentena é exibido selecionando o item **Arquivos de dados** na área **Serviço** da janela principal do aplicativo. À direita da tela, a seção *Quarentena* exibe:

- o número de objetos possivelmente infectados detectados durante a operação do Kaspersky Anti-Virus for Windows Workstations;
- o tamanho atual da Quarentena.

Você pode excluir todos os objetos da quarentena com o botão **Esvaziar**. Observe que, ao fazê-lo, os arquivos de Backup e de relatório também serão excluídos.

Para acessar os objetos na Quarentena:

clique em qualquer parte da seção **Quarentena**.

As seguintes ações podem ser executadas na guia **Quarentena** (veja a Figura 73):

- 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*.

Se um arquivo for armazenado manualmente na quarentena e uma verificação posterior mostrar que ele não está infectado, seu status após a verificação não será mudado imediatamente para *OK*. Isso ocorrerá somente se a verificação ocorrer decorrido um determinado período (pelo menos três dias) do armazenamento do arquivo na quarentena.

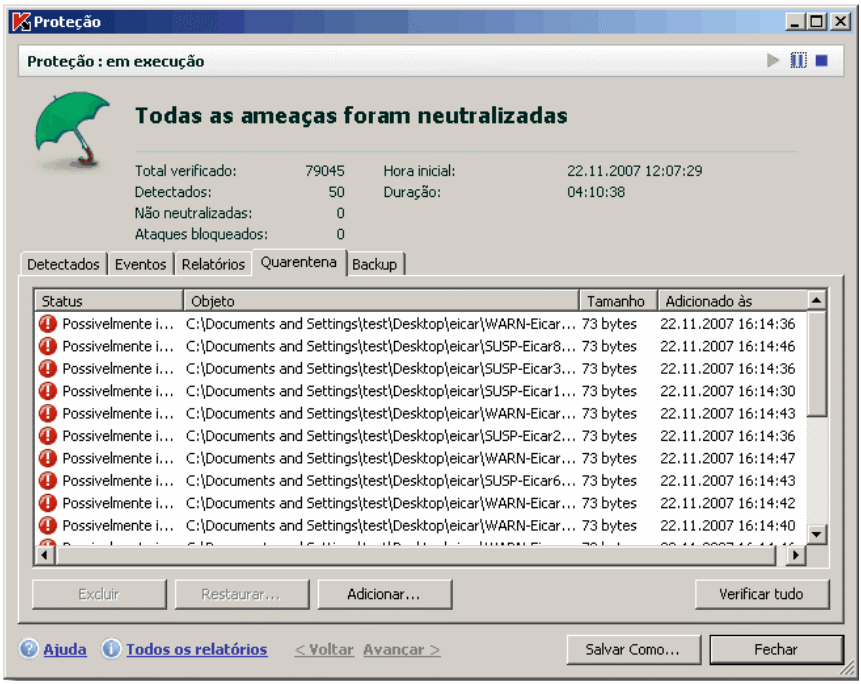


Figura 73. Lista de objetos em quarentena

- Verificar e desinfectar todos os objetos possivelmente infectados na Quarentena usando as assinaturas de ameaças atuais, clicando em **Verificar tudo**.

  Depois de verificar e desinfectar qualquer objeto em quarentena, seu status pode mudar para *infectado, possivelmente infectado, falso positivo, OK,* etc.

  O status *infectado* significa que o objeto foi identificado como infectado, mas não pôde ser neutralizado. É recomendável excluí-lo.

  Todos os objetos marcados como *falso positivo* podem ser restaurados, pois seu status *possivelmente infectado* anterior não foi confirmado pelo programa após nova verificação.

- Restaurar os arquivos para uma pasta selecionada pelo usuário ou para sua pasta original antes da Quarentena (padrão). Para restaurar um objeto, selecione-o na lista e clique em **Restaurar**. Ao restaurar objetos de arquivos comprimidos, bancos de dados de e-mails e arquivos em formato de e-mail da Quarentena, selecione também o diretório no qual serão restaurados.

  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**.

17.1.2. Configurando a Quarentena

Você pode configurar o layout e o funcionamento da Quarentena, mais especificamente:

- Configurar verificações automáticas de objetos em Quarentena após cada atualização das assinaturas de ameaças (para obter mais detalhes, consulte 16.4.4 na p. 229).

  Aviso!

  O programa não poderá verificar objetos em quarentena imediatamente após a atualização das assinaturas de ameaças, se você estiver acessando a área de Quarentena.

- Definir o tempo máximo de armazenamento na Quarentena.

  O tempo de armazenamento padrão é de 30 dias e, ao término dele, os objetos são excluídos. Você pode alterar o tempo de armazenamento da Quarentena ou desabilitar totalmente esta restrição.

Para fazê-lo:

1. Abra a janela de configurações do Kaspersky Anti-Virus for Windows Workstations clicando em Configurações na janela principal do programa.
2. Selecione **Arquivos de dados** na árvore de configurações.

3. Na seção **Quarentena e Backup** (veja a Figura 74), insira o período depois do qual os objetos na Quarentena serão excluídos automaticamente. Alternativamente, desmarque a caixa de seleção para desabilitar a exclusão automática.

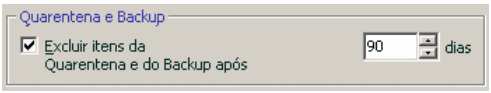


Figura 74. Configurando o período de armazenamento na Quarentena

17.2. 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.

17.2.1. Ações sobre cópias de backup

O número total de cópias de objetos no Backup é exibido em **Arquivos de dados**, na seção **Serviço** da janela principal do aplicativo. À direita da tela, a seção *Backup* exibe:

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

Aqui, você pode excluir todas as cópias do Backup com o botão **Esvaziar**. Observe que, ao fazê-lo, os objetos na Quarentena e arquivos de relatório também serão excluídos.

Para acessar as cópias de objetos perigosos:

clique em qualquer parte da seção **Backup**.

Uma lista de cópias de backup será exibida na guia Backup (veja a Figura 75). As seguintes informações são exibidas para cada cópia: o nome e o caminho do objeto, o status do objeto atribuído pela verificação e seu tamanho.

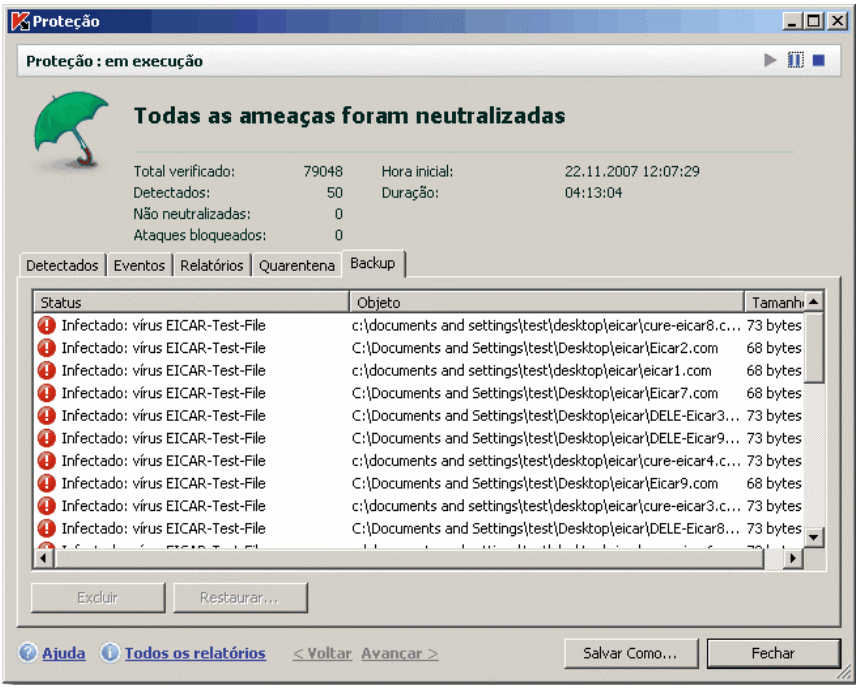


Figura 75. Lista de objetos do backup

Você pode restaurar cópias selecionadas usando o botão **Restaurar**. O objeto é restaurado do Backup com o mesmo nome que tinha antes da desinfecção.

Se houver um objeto com esse nome no local original (isto é possível se foi feita uma cópia do objeto que está sendo restaurado antes da desinfecção), será exibido um aviso. Você pode alterar o local do objeto restaurado ou renomeá-lo.

É recomendável verificar os objetos de backup quanto à presença de vírus imediatamente após sua restauração. É possível que, com as assinaturas atualizadas, você consiga desinfectá-lo sem perder a integridade do arquivo.

É recomendável **não** restaurar cópias de backup de objetos, exceto quando absolutamente necessário. Isto pode levar à infecção do computador.

É recomendável examinar a área de Backup e esvaziá-la usando o botão **Excluir** periodicamente. Você também pode configurar o programa de modo a

excluir automaticamente as cópias mais antigas de Backup (consulte a seção 17.2.2 na p. 239).

17.2.2. Configurando o Backup

Você pode definir o tempo máximo que as cópias permanecem na área de Backup.

O tempo de armazenamento padrão do Backup é 30 dias e, ao término dele, as cópias são excluídas. Você pode alterar o tempo de armazenamento ou remover totalmente esta restrição. Para fazê-lo:

1. Abra a janela de configurações do Kaspersky Anti-Virus for Windows Workstations clicando em Configurações na janela principal do programa.
2. Selecione **Arquivos de dados** na árvore de configurações.
3. Defina a duração do armazenamento de cópias de backup no repositório na seção **Quarentena e backup** (veja a Figura 74) à direita da tela. Alternativamente, desmarque a caixa de seleção para desabilitar a exclusão automática.

17.3. Relatórios

As ações dos componentes, as tarefas de verificação de vírus e as atualizações do Kaspersky Anti-Virus for Windows Workstations são registradas em relatórios.

O número total de relatórios criados pelo programa e seu tamanho total são exibidos clicando em **Arquivos de dados**, na seção **Serviço** da janela principal do programa. As informações são exibidas na caixa *Relatórios*.

Para exibir relatórios:

Clique em qualquer local da caixa *Relatórios* para abrir a janela Proteção, que resume a proteção fornecida pelo aplicativo. Será aberta uma janela na guia **Relatórios** (veja a Figura 76).

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

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**.

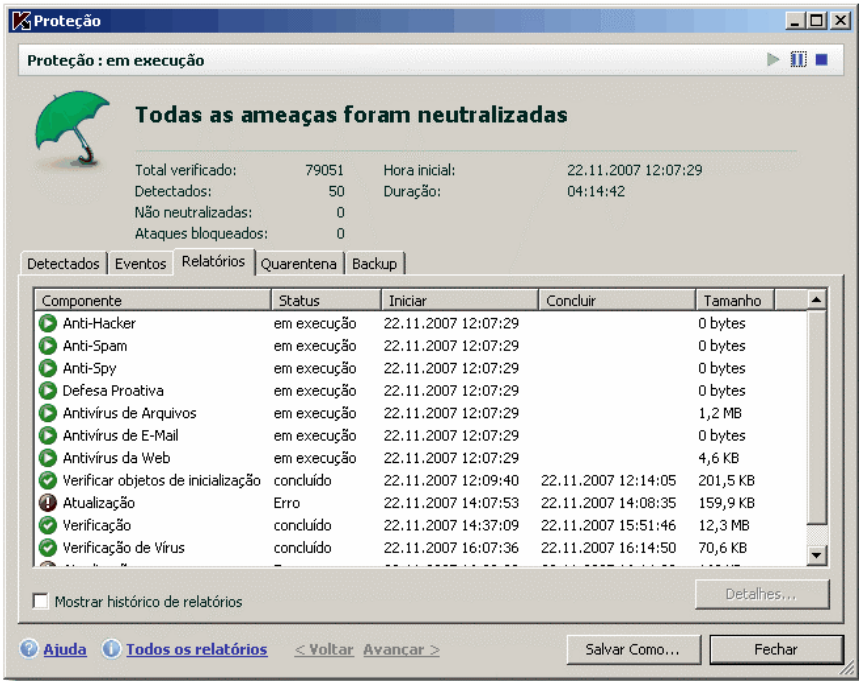


Figura 76. Relatórios de funcionamento do componente

Uma janela será aberta, contendo informações detalhadas sobre o desempenho do componente da ou tarefa selecionada. As estatísticas de desempenho resultantes são exibidas na parte superior da janela e informações detalhadas são fornecidas nas guias. Dependendo do componente ou tarefa, as guias podem variar:

- A guia **Detectados** contém uma lista de objetos perigosos detectados por um componente ou uma tarefa de verificação de vírus.
- A guia **Eventos** exibe os eventos de componentes ou tarefas.
- A guia **Estatísticas** contém estatísticas detalhadas de todos os objetos verificados.

- A guia **Configurações** exibe as configurações usadas pelos componentes de proteção, verificações de vírus ou atualizações de assinaturas de ameaças.
- As guias **Macros** e **Registro** aparecem apenas no relatório da Defesa Proativa e contêm informações sobre todas as macros que tentaram executar no computador e todas as tentativas de modificar o Registro do sistema operacional.
- As guias **Phishing**, **Pop-ups**, **Banners** e **Discagens** aparecem apenas no relatório do Anti-Spy. Elas contêm informações sobre todos os ataques de phishing detectados e todas as janelas pop-up, banners de anúncios e tentativas de discagem automática bloqueadas durante essa sessão do programa.
- As guias **Ataques de rede**, **Hosts banidos**, **Atividade do aplicativo** e **Filtragem de pacotes** são encontradas apenas no relatório do Anti-Hacker. Elas incluem informações sobre todas as tentativas de ataque de rede no computador, hosts banidos após ataques, descrições da atividade de rede de aplicativos que correspondem às regras de atividades existentes e todos os pacotes de dados que correspondem às regras de filtragem de pacotes do Anti-Hacker.
- As guias **Conexões efetuadas**, **Portas abertas** e **Tráfego** também cobrem a atividade de rede no computador, exibindo as atuais conexões estabelecidas, as portas abertas e a quantidade de tráfego de rede que o computador enviou e recebeu.

Você pode exportar todo o relatório como um arquivo de texto. Este recurso é útil quando ocorre um erro que você não consegue eliminar sozinho e você precisa de assistência do Suporte Técnico. Se isso acontecer, o relatório deve ser enviado como um arquivo .txt para o Suporte Técnico, para que nossos especialistas possam estudar o problema detalhadamente e solucioná-lo assim que possível.

Para exportar um relatório como arquivo de texto:

Clique em **Salvar como** e especifique o local onde deseja salvar o arquivo do relatório.

Depois de terminar o trabalho com o relatório, clique em **Fechar**.

Existe um botão **Ações** em todas as guias (exceto em **Configurações** e **Estatísticas**) que você pode usar para definir respostas aos objetos na lista. Ao clicar nele, um menu de contexto é aberto, com uma seleção dos seguintes itens de menu (i menu é diferente dependendo do componente; todas as opções possíveis estão relacionadas a seguir):

Desinfectar – tenta desinfectar um objeto perigoso. Se o objeto não for desinfectado com êxito, você pode deixá-lo nesta lista para que seja

verificado posteriormente com assinaturas de ameaças atualizadas ou excluí-lo. É possível aplicar essa ação a um objeto na lista ou a vários objetos selecionados.

Descartar – exclui o registro de detecção do objeto da lista.

Adicionar à zona confiável – exclui o objeto da proteção. Será aberta uma janela com uma regra de exclusão para o objeto.

Ir para o arquivo – abre a pasta na qual o objeto está localizado no Windows Explorer.

Neutralizar tudo – neutraliza todos os objetos da lista. O Kaspersky Anti-Virus for Windows Workstations tentará processar os objetos usando as assinaturas de ameaças.

Descartar tudo – limpa o relatório sobre objetos detectados. Ao usar esta função, todos os objetos perigosos detectados permanecem no computador.

Pesquisar www.viruslist.com – vai para uma descrição do objeto na Enciclopédia de Vírus no site da Kaspersky Lab.

Pesquisar www.google.com – localiza informações sobre o objeto usando este mecanismo de pesquisa.

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

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

17.3.1. Configurando relatórios

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

1. Abra a janela de configurações do Kaspersky Anti-Virus for Windows Workstations clicando em Configurações na janela principal do programa.
2. Selecione **Arquivos de dados** na árvore de configurações.
3. Edite as configurações na caixa **Relatórios** (veja a Figura 77) 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.

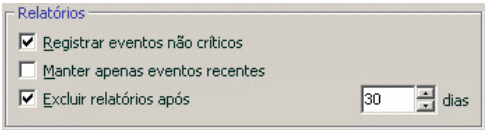


Figura 77. Configurando relatórios

17.3.2. A guia *Detectados*

Esta guia (veja a Figura 78) contém uma lista de objetos perigosos detectados pelo Kaspersky Anti-Virus for Windows Workstations. 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**.

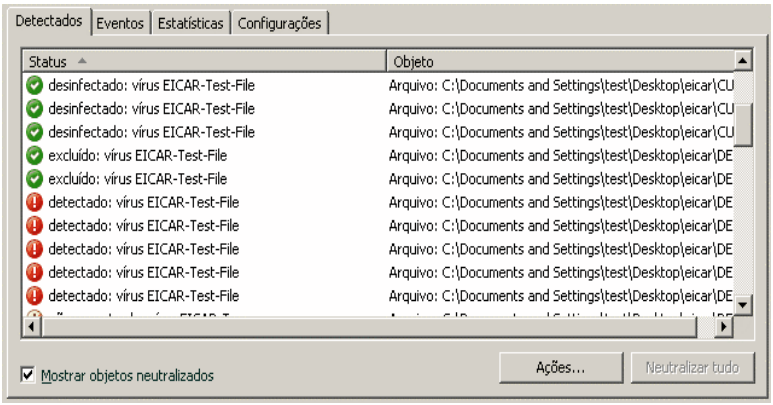


Figura 78. Lista de objetos perigosos detectados

Para processar objetos perigosos detectados pelo Kaspersky Anti-Virus, pressione o botão **Neutralizar** (para um objeto ou grupo de objetos

selecionados) ou **Neutralizar 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.

17.3.3. A guia *Eventos*

Esta guia (veja a Figura 79) fornece uma lista completa de todos os eventos importantes no funcionamento do componente de proteção, nas verificações de vírus e nas atualizações das assinaturas de ameaças que não foram substituídos por uma regra de controle de atividade (consulte a seção 10.1.1 na p. 129).

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.

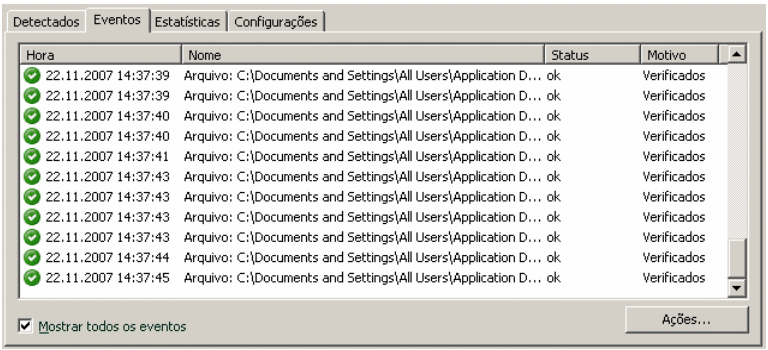


Figura 79. Eventos que ocorrem no funcionamento do componente

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.

Você também pode treinar o Anti-Spam enquanto visualiza o relatório, usando o menu de contexto específico. Para fazê-lo, selecione o nome do e-mail e abra o menu de contexto clicando com o botão direito do mouse; selecione **Marcar como spam**, se o e-mail for spam, ou **Marcar como Não spam**, se o e-mail selecionado for aceito. Além disso, com base nas informações obtidas através da análise do e-mail, você pode adicioná-lo às listas branca se negra do Anti-Spam. Para fazê-lo, use os itens correspondentes no menu de contexto.

17.3.4. A guia *Estatísticas*

Esta guia (veja a Figura 80) fornece estatísticas detalhadas sobre os componentes e tarefas de verificação de vírus. Aqui, você pode descobrir:

- Quantos objetos foram verificados quanto a indícios perigosos nesta sessão de um componente ou após a conclusão de uma tarefa. É exibido o número de arquivos comprimidos, arquivos compactados e arquivos protegidos por senha verificados, e de objetos corrompidos.
- Quantos objetos perigosos foram detectados, não desinfectados, excluídos e colocados em Quarentena.

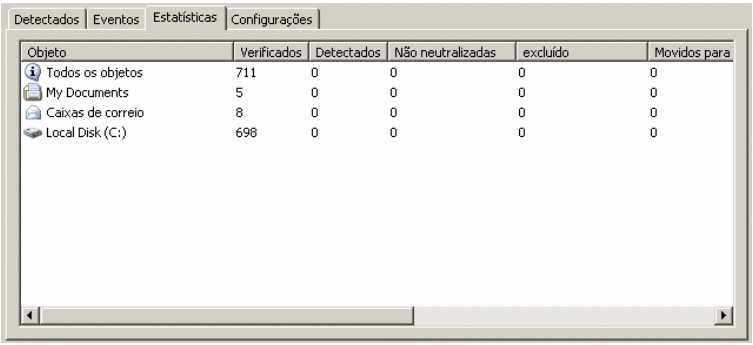


Figura 80. Estatísticas do componente

17.3.5. A guia *Configurações*

A guia **Configurações** (veja a Figura 81) exibe uma visão geral completa das configurações de componentes de proteção, 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.

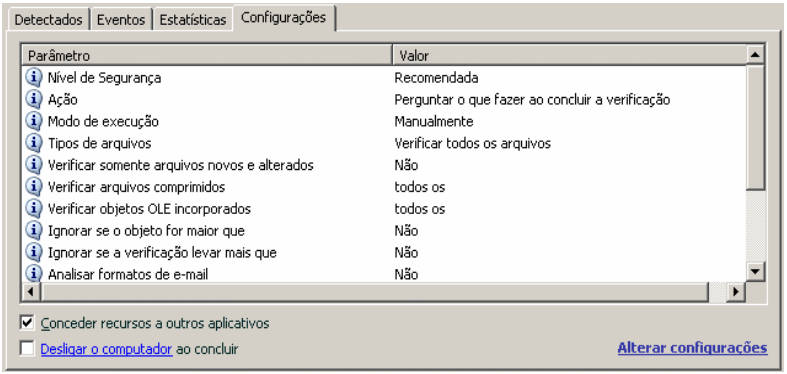


Figura 81. Configurações do componente

- 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.

17.3.6. A guia *Macros*

Todas as macros que tentaram ser executadas durante a sessão atual do Kaspersky Anti-Virus for Windows Workstations estão listadas na guia **Macros** (veja a Figura 82). Aqui, você encontrará o nome completo de cada macro, a hora em que foi executada e seu status após o processamento.

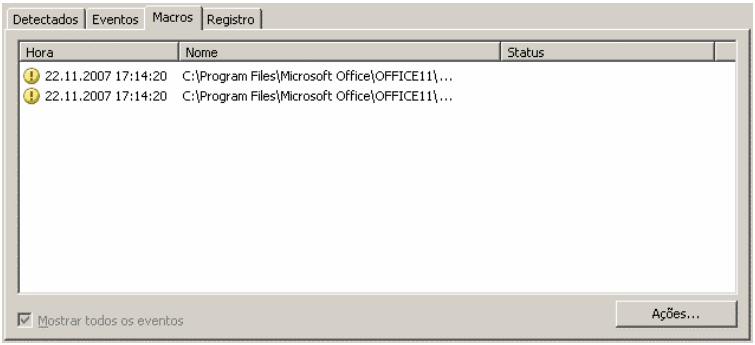


Figura 82. Macros perigosas detectadas

Você pode escolher o modo de exibição desta guia. Se não desejar ver eventos informativos, desmarque **Mostrar todos os eventos**.

17.3.7. A guia *Registro*

O programa registra as operações com chaves do registro que foram tentadas desde que o programa foi iniciado na guia **Registro** (veja a Figura 83), a menos que proibido por uma regra (consulte a seção 10.1.3.2 na p. 138).

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.

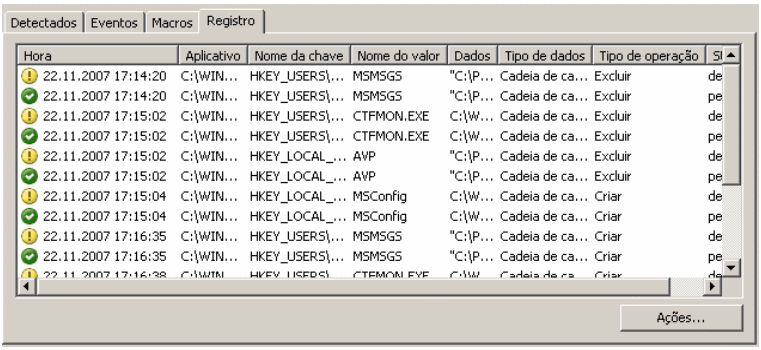


Figura 83. Ler e modificar eventos do registro do sistema

17.3.8. A guia *Sites de Phishing*

Esta guia do relatório (veja a Figura 84) exibe todas as tentativas de phishing executadas durante a sessão atual do Kaspersky Anti-Virus for Windows Workstations. O relatório mostra um link para o site de phishing detectado no e-mail (ou em outra fonte), a data e a hora em que o ataque foi detectado e o status do mesmo (se foi bloqueado).

Figura 84. Ataques de phishing bloqueados

17.3.9. A guia *Pop-ups*

Esta guia do relatório (veja a Figura 85) relaciona os endereços de todas as janelas pop-up que o Anti-Spy bloqueou. Geralmente, essas janelas são abertas em sites.

O endereço e a data e hora em que o Popup Blocker bloqueou a janela são registrados para cada pop-up.

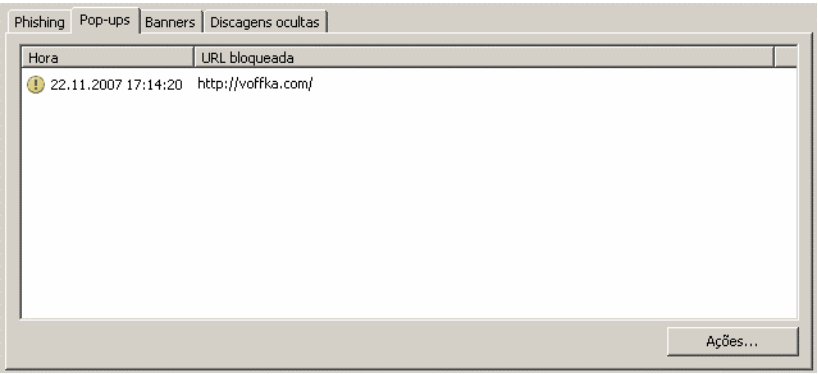


Figura 85. Lista de janelas pop-up bloqueadas

17.3.10. A guia *Banners*

Esta guia do relatório (veja a Figura 86) contém os endereços dos banners de anúncios que o Kaspersky Anti-Virus for Windows Workstations detectou na sessão atual. O endereço de cada banner de anúncio é relacionado, junto com o status do processamento (banner bloqueado ou exibido).

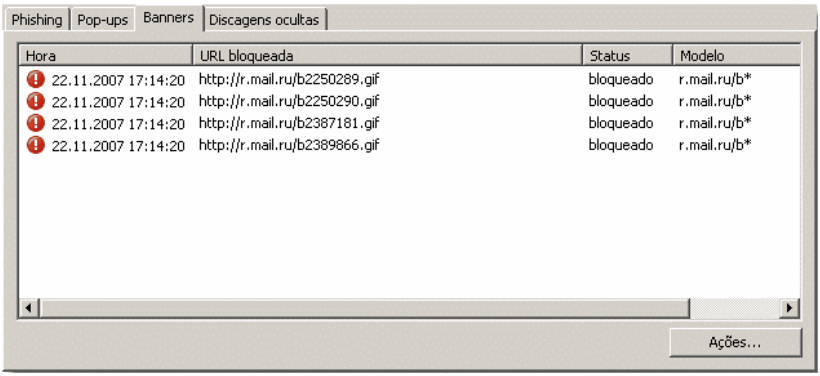


Figura 86. Lista de banners de anúncios bloqueados

Você pode permitir que os banners de anúncios bloqueados sejam exibidos. Para fazê-lo, selecione o objeto desejado na lista e clique em **Ações** → **Permitir**.

17.3.11. A guia *Discagens*

Esta guia (veja a Figura 87) exibe todas as tentativas secretas de discagem para conectar sites pagos. Em geral, essas tentativas são executadas por programas mal-intencionados instalados no seu computador.

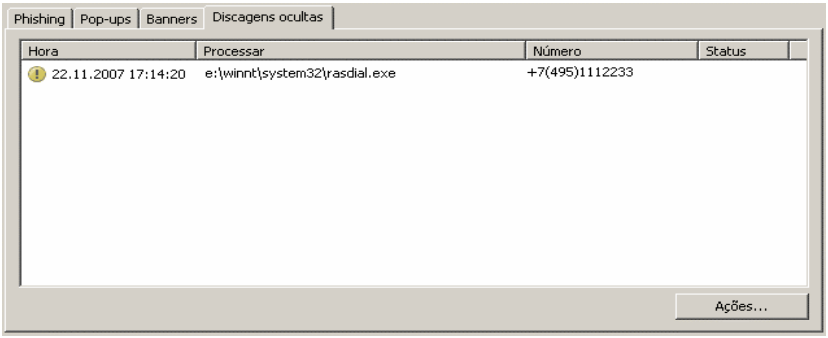


Figura 87. Lista de tentativas de discagem

No relatório, você pode exibir o programa que tentou discar o número para conectar a Internet e se a tentativa foi bloqueada ou permitida.

17.3.12. A guia *Ataques de rede*

Esta guia (veja a Figura 88) exibe uma visão geral dos ataques de rede no seu computador. Se habilitada, essas informações são registradas no Sistema de Detecção de Intrusos, que monitora todas as tentativas de ataque ao seu computador.

A guia **Ataques de rede** relaciona as seguintes informações sobre os ataques:

- Origem do ataque. Pode ser um endereço IP, host, etc.
- Porta local pela qual o ataque ao computador foi tentado.
- Breve descrição do ataque.
- A hora da tentativa de ataque.

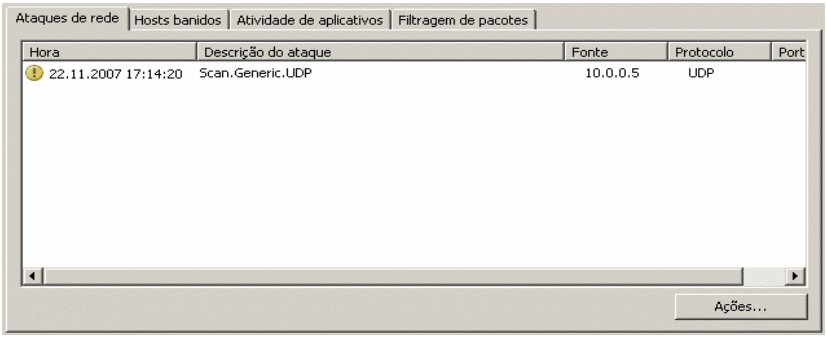


Figura 88. Lista de ataques de rede bloqueados

17.3.13. A guia *Hosts banidos*

Todos os hosts bloqueados depois que um ataque foi detectado pelo Sistema de Detecção de Intrusos estão relacionados nesta guia do relatório (veja a Figura 89).

O nome de cada host e a hora em que ele foi bloqueado são mostrados. Você pode desbloquear um host nesta guia. Para fazê-lo, selecione o host na lista e clique no botão **Ações** → **Desbloquear**.

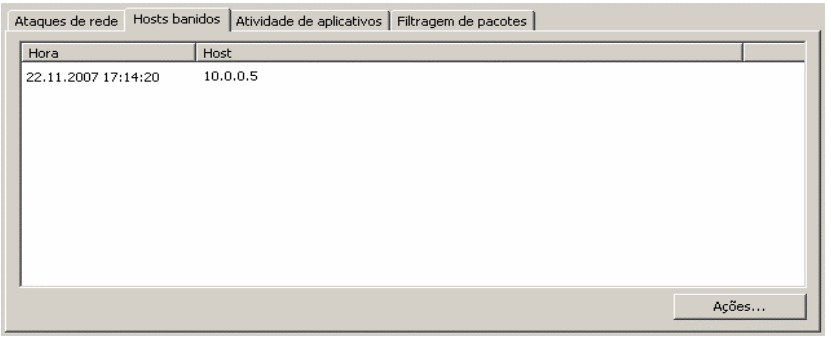


Figura 89. Lista de hosts bloqueados

17.3.14. A guia *Atividade de aplicativos*

Todos os aplicativos cuja atividade corresponde às regras de aplicativos e que foram registrados pelo módulo *Firewall* durante a sessão atual do Anti-Hacker estão relacionados na guia **Atividade do aplicativo** (veja a Figura 90).

A atividade é registrada apenas se o sinalizador **Registrar evento** estiver marcado na regra. Nas regras para aplicativos incluídas no Kaspersky Anti-Virus for Windows Workstations, esse sinalizador estará desmarcado por padrão.

Esta guia exibe as propriedades básicas de cada aplicativo (nome, PID, nome da regra) e um breve resumo de sua atividade (protocolo, direção do pacote, etc.) Também são relacionadas informações sobre o bloqueio ou não da atividade do aplicativo.

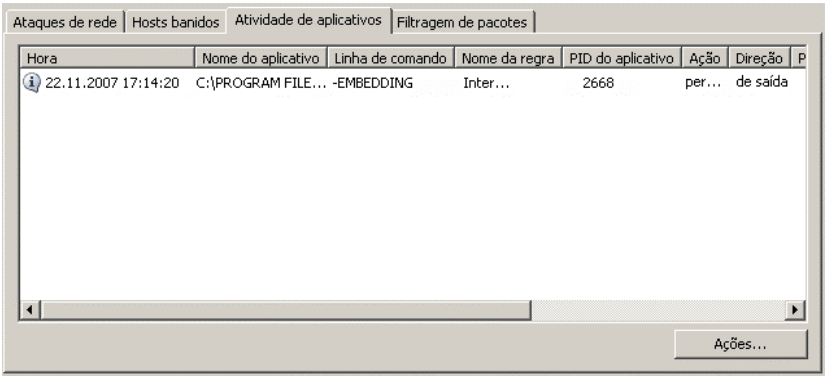


Figura 90. Atividade do aplicativo monitorada

17.3.15. A guia Filtragem de pacotes

A guia **Filtragem de pacotes** contém informações sobre o envio e o recebimento de pacotes que correspondem a regras de filtragem e que foram registrados durante a sessão atual do aplicativo (veja a Figura 91).

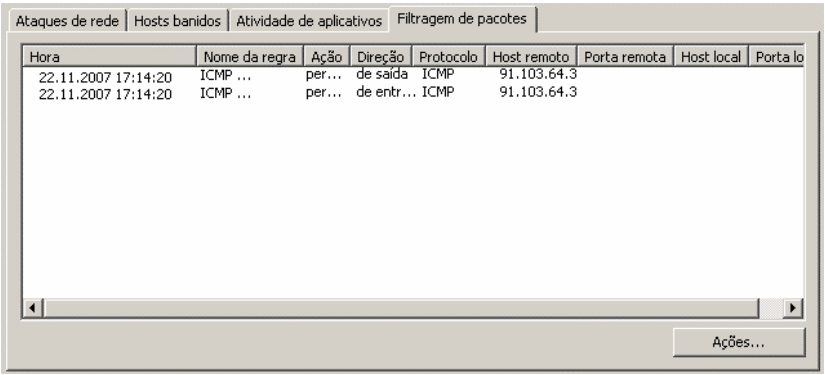


Figura 91. Pacotes de dados monitorados

A atividade é registrada apenas se **Registrar evento** estiver marcado na regra. Por padrão, estará desmarcado nas regras para filtragem de pacotes incluídas no Kaspersky Anti-Virus for Windows Workstations.

O nome resultado da filtragem (se o pacote foi bloqueado), a direção do pacote, o protocolo e outras configurações da conexão de rede para envio e recebimento de pacotes são indicados para cada pacote.

17.3.16. A guia *Conexões efetuadas*

Todas as conexões de rede ativas estabelecidas no computador estão listadas na guia **Conexões efetuadas** (veja a Figura 92). Aqui você encontrará o nome do aplicativo que iniciou a conexão, o protocolo usado, a direção da conexão (de entrada ou de saída) e as configurações da conexão (portas locais e remotas e endereços IP). Também é possível ver por quanto tempo uma conexão ficou ativa e o volume de dados enviados e recebidos. Você pode criar ou excluir regras para a conexão. Para fazê-lo, use as opções apropriadas no menu de contexto.

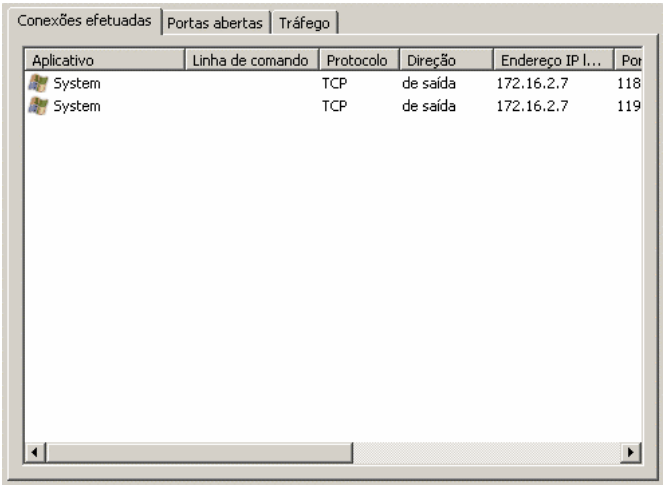


Figura 92. Lista de conexões estabelecidas

17.3.17. A guia *Portas abertas*

Todas as portas abertas para conexões de rede no computador no momento estão relacionadas na guia *Portas abertas* (veja a Figura 93). Para cada porta estão relacionados o número da porta, o protocolo de transferência de dados, o nome do aplicativo que usa a porta e há quanto tempo a porta está aberta.

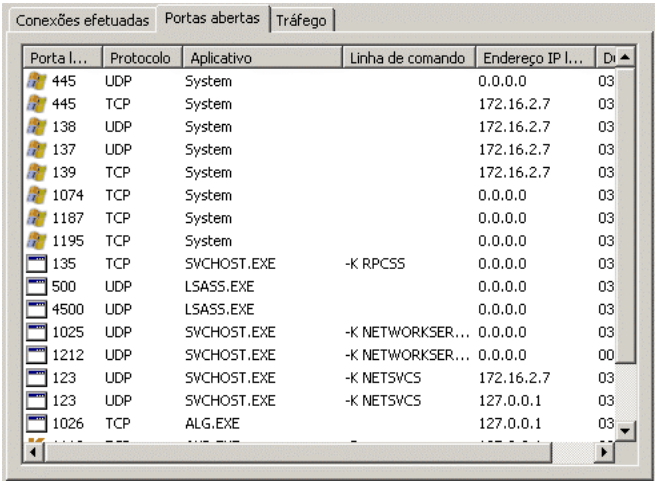


Figura 93. Lista de portas abertas em um computador

Essas informações poderão ser úteis durante surtos de vírus e ataques de rede, se você souber exatamente qual porta está vulnerável. É possível descobrir se a porta está aberta no computador e tomar as medidas necessárias para protegê-lo (por exemplo, habilitando a Detecção de Intrusos, fechando a porta vulnerável ou criando uma regra para ela).

17.3.18. A guia *Tráfego*

Esta guia (veja a Figura 94) contém informações sobre todas as conexões de entrada e de saída estabelecidas entre o seu computador e outros, incluindo servidores da Web, servidores de e-mail, etc. As seguintes informações são fornecidas para cada conexão: nome e endereço IP do host conectado, e o volume de tráfego enviado e recebido.

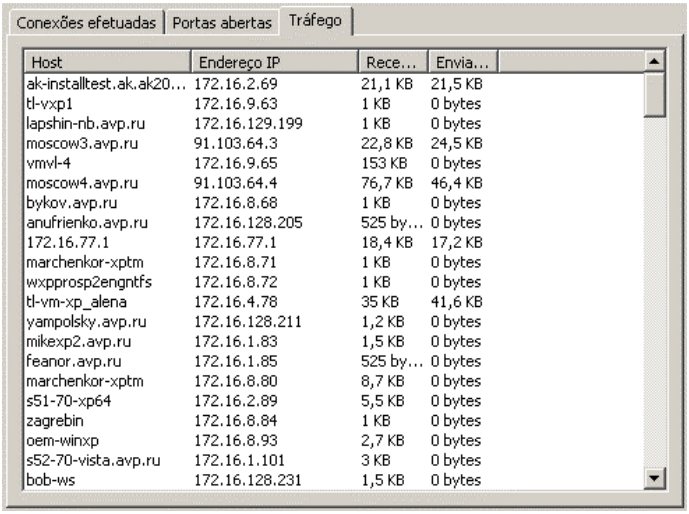


Figura 94. Tráfego nas conexões de rede estabelecidas

17.4. Informações gerais sobre o programa

Você pode exibir informações gerais sobre o programa na seção **Serviço** da janela principal (veja a Figura 95).

Todas as informações estão divididas em três seções:

- A versão do programa, a data da última atualização e o número de ameaças conhecidas até o momento são exibidos na caixa **Informações do produto**.
- As informações básicas sobre o sistema operacional instalado no computador são mostradas na caixa **Informações do sistema**.
- Informações básicas sobre a licença do Kaspersky Anti-Virus que você comprou estão na caixa **Informações da licença**.

Você precisará de todas essas informações quando entrar em contato com o Suporte Técnico da Kaspersky Lab (consulte 17.6 na p. 260).

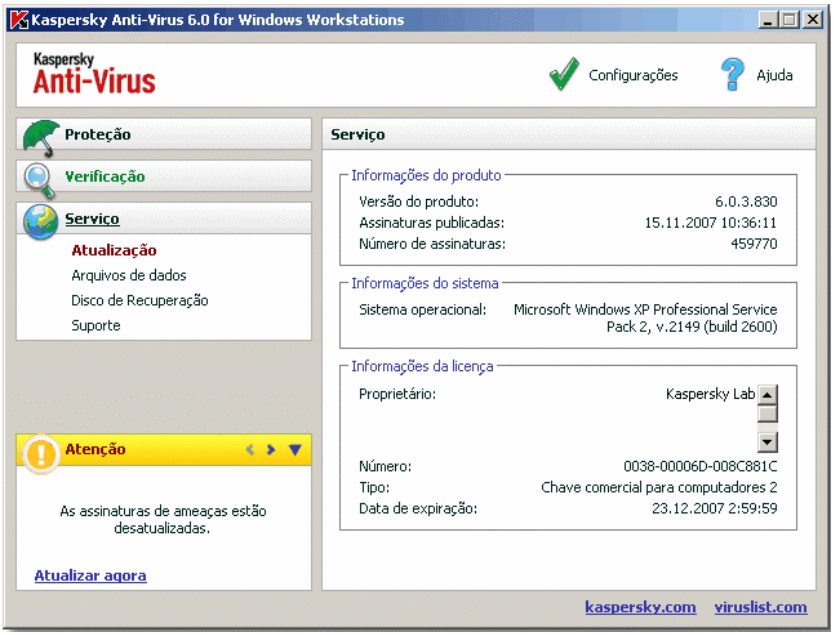


Figura 95. Informações sobre o programa, a licença e o sistema em que está instalado

17.5. Gerenciando licenças

O Kaspersky Anti-Virus for Windows Workstations precisa de uma *chave de licença* para funcionar. Você recebe a chave ao comprar o produto, e ela lhe dá o direito de usar o programa a partir da data de sua instalação.

Sem uma chave de licença, a menos que uma versão de teste do aplicativo tenha sido ativada, o Kaspersky Anti-Virus será executado no modo de uma atualização. O programa não baixará novas atualizações.

Se uma versão de teste do programa tiver sido ativada, 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 as assinaturas de ameaças. Como antes, você poderá verificar seu computador quanto à presença de vírus e usar os componentes de proteção, mas apenas com as assinaturas de ameaças que você tinha antes de a licença expirar. Não podemos garantir que você estará protegido contra os vírus que surgirem depois que a licença do programa expirar.

Para evitar infectar o computador com novos vírus, é recomendável estender a licença do Kaspersky Anti-Virus for Windows Workstations. O programa o notificará duas semanas antes da expiração da licença e, durante essas semanas, essa mensagem será exibida sempre que for aberto.

Para renovar a licença, compre e instale uma nova chave de licença ou digite o código de ativação do aplicativo. Para fazê-lo:

Entre em contato com o fornecedor do produto e adquira uma chave de licença ou um código do aplicativo.

ou:

Adquira uma chave de licença ou um código de ativação diretamente da Kaspersky Lab, clicando em Comprar licença na caixa de diálogo da chave de licença (veja a Figura 96). Preencha o formulário apropriado na página que é aberta. Depois que o pagamento for feito, será enviado um link para o e-mail que você inseriu no formulário de pedido. Esse link permitirá que você baixe uma chave de licença do aplicativo ou obtenha um código de ativação.

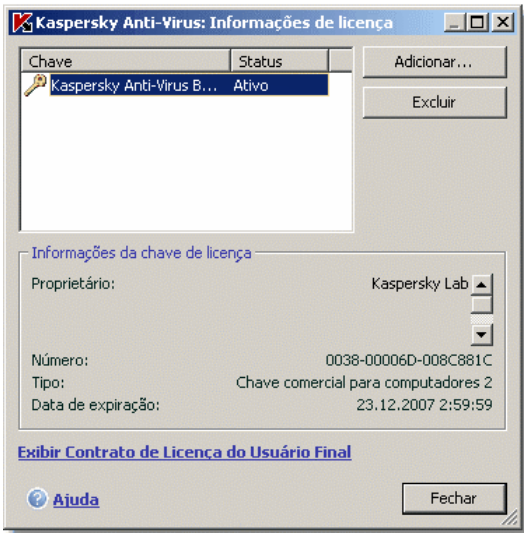


Figura 96. Informações da licença

Periodicamente, a Kaspersky Lab lança ofertas de extensões de licença de nossos produtos. Verifique as ofertas no site da Kaspersky Lab, em **Products → Sales and special offers**.

Existem informações sobre a chave de licença atual disponíveis na caixa **Informações da licença** da seção **Serviço** na janela principal do aplicativo. Para ir para a janela do gerenciador de licenças, clique em qualquer local da caixa. Na janela que é aberta (veja a Figura 96), é possível exibir informações sobre a chave atual, adicionar ou excluir uma chave.

Ao selecionar uma chave na lista da caixa **Informações da licença**, serão exibidas informações sobre o número, o tipo e a data de expiração da licença. Para adicionar uma nova chave de licença, clique em **Adicionar** e ative o aplicativo com o assistente de ativação (consulte 3.2.2 na p. 39). Para excluir uma chave da lista, pressione o botão **Excluir**.

Para examinar os termos do contrato de licença, clique em Exibir Contrato de Licença do Usuário Final. Para obter uma licença através do formulário no site da Kaspersky Lab, clique em Comprar licença.

17.6. Suporte Técnico

O Kaspersky Anti-Virus for Windows Workstations fornece uma grande variedade de opções para dúvidas e problemas relacionados com o funcionamento do programa. Elas estão localizadas em **Suporte** (veja a Figura 97), na seção **Serviço**.

Dependendo do problema, fornecemos vários serviços de suporte técnico:

Fórum de usuários. Este recurso é uma seção dedicada do site da Kaspersky Lab com perguntas, comentários e sugestões de usuários do programa. Você pode examinar os tópicos básicos do fórum e deixar um comentário. Talvez também encontre a resposta para sua pergunta.

Para acessar este recurso, use o link Fórum de usuários.

Base de dados de conhecimento. Este recurso também é uma seção dedicada do site da Kaspersky Lab e contém recomendações de Suporte Técnico para o uso do software da Kaspersky Lab e respostas para perguntas freqüentes. Tente encontrar uma resposta para sua pergunta ou uma solução para seu problema com este recurso.

Para obter suporte técnico on-line, clique no link Base de dados de conhecimento.

Comentários sobre a operação do programa. Este serviço foi criado para postar comentários sobre o funcionamento do programa ou descrever um problema que apareceu durante sua operação. É necessário preencher um formulário específico no site da empresa, descrevendo a situação detalhadamente. Para lidar com o problema da melhor forma, a Kaspersky Lab precisará de algumas informações sobre o seu computador. Você pode descrever a configuração do sistema sozinho ou usar o coletor de informações automático no seu computador.

Para ir para o formulário de comentários, use o link Enviar um relatório de erro ou uma sugestão.

Suporte técnico. Se precisar de ajuda ao usar o Kaspersky Anti-Virus, clique no link localizado na caixa **Serviço de Suporte Local**. O site da Kaspersky Lab será aberto com informações sobre como contatar nossos especialistas.

Figura 97. Informações sobre o suporte técnico

17.7. Criando uma lista de portas monitoradas

Os componentes de proteção como o Antivírus de E-Mail, Antivírus da Web, Anti-Spy e Anti-Spam monitoram fluxos de dados transmitidos usando determinados protocolos e que passam por determinadas portas abertas no computador. Assim, por exemplo, o Antivírus de E-Mail analisa informações transferidas usando o protocolo SMTP e o Antivírus da Web analisa informações transferidas usando HTTP.

A lista de portas padrão que geralmente são usadas para transmitir tráfego de e-mail e HTTP é fornecida com o pacote do programa. Você pode adicionar uma nova porta ou desabilitar a monitoração de uma determinada porta, desabilitando assim a detecção de objetos perigosos para o tráfego que passa por essa porta.

Para editar a lista de portas monitoradas, execute as seguintes etapas:

1. Abra a janela de configurações do Kaspersky Anti-Virus for Windows Workstations clicando no link Configurações na janela principal.
2. Selecione **Configurações de rede** na seção **Serviço** da árvore de configurações do programa.
3. Clique em **Configurações de porta** à direita da janela de configurações.
4. Edite a lista de portas monitoradas na janela que é aberta (veja a Figura 98).

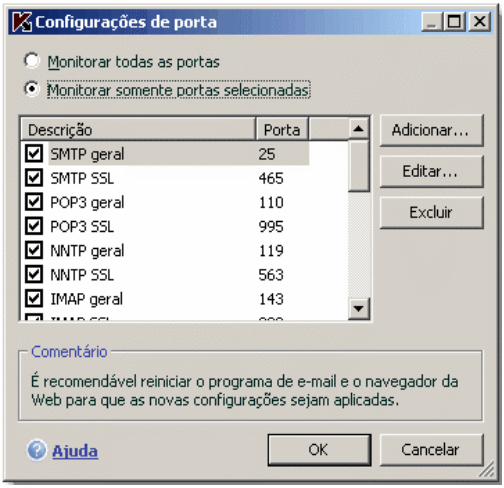


Figura 98. Lista de portas monitoradas

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**.

Não é recomendável selecionar a opção **Monitorar todas as portas** ao administrar o Kaspersky Anti-Virus 6.0 com o Kaspersky Administration Kit, se instalado em um computador com o Microsoft Windows 98. Isso pode causar problemas de acesso a recursos de rede e à Internet.

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 for Windows Workstations 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 for Windows Workstations e o firewall de outra empresa simultaneamente, configure esse firewall para permitir o acesso do processo *avp.exe* (o processo interno do Kaspersky Anti-Virus for Windows Workstations) a 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 for Windows Workstations 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.

17.8. Verificando conexões criptografadas

Conectar-se usando o protocolo SSL protege a troca de dados pela Internet. O protocolo SSL identifica as partes que trocam dados usando certificados eletrônicos, codifica os dados que são transferidos e assegura sua integridade durante a transferência.

Esses recursos do protocolo são usados por hackers para disseminar programas mal-intencionados, pois a maioria dos programas antivírus não verifica o tráfego SSL.

O Kaspersky Anti-Virus 6.0 possui a opção de verificar vírus no tráfego SSL. Quando for feita uma tentativa de conexão segura a um recurso da Web, uma notificação aparecerá na tela (veja a Figura 99) perguntando o que fazer.

A notificação contém informações sobre o programa que iniciou a conexão segura, junto com o endereço remoto e a porta. O programa solicita que você decida se a conexão deve ser verificada quanto à presença de vírus:

- **Processar** – verifica o tráfego quanto à presença de vírus ao conectar-se ao site de maneira segura.

  É recomendável sempre verificar o tráfego SSL se você estiver usando um site suspeito ou se uma transferência de dados SSL começar quando você passa para outra página. É bastante provável que isso seja um sinal de transferência de um programa mal-intencionado em um protocolo seguro.

- **Ignorar** – continua a conexão segura com o site, sem verificar o tráfego quanto à presença de vírus.

Para aplicar a ação selecionada a todas as tentativas de estabelecer conexões SSL, marque **Aplicar a todos**.

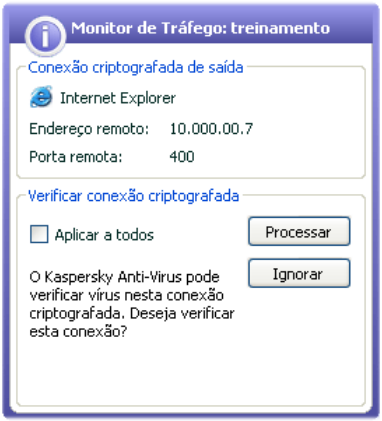


Figura 99. Notificação de detecção de conexão SSL

Para verificar conexões criptografadas, o Kaspersky Anti-Virus substitui o certificado de segurança solicitado por um certificado assinado por ele mesmo. Em alguns casos, os programas que estão estabelecendo conexões não aceitarão esse certificado e nenhuma conexão será estabelecida. É recomendável desabilitar a verificação de tráfego SSL nos seguintes casos:

- Ao conectar-se a um recurso da Web confiável, como a página do seu banco, na qual você gerencia sua conta pessoal. Nesse caso, é importante receber a confirmação da autenticidade do certificado do banco.

- Se o programa que está estabelecendo a conexão verificar o certificado do site acessado. Por exemplo, o MSN Messenger verifica a autenticidade da assinatura digital da Microsoft Corporation ao estabelecer uma conexão com o servidor.

Você pode configurar a verificação de SSL na guia **Conexão criptografada** da janela de configurações do programa:

Verificar todas as conexões criptografadas – verifica vírus em todo o tráfego de entrada no protocolo SSL.

Perguntar ao usuário quando uma nova conexão criptografada for detectada – exibe uma mensagem que pergunta o que fazer sempre que uma conexão SSL é estabelecida.

Não verificar conexões criptografadas – não verifica vírus no tráfego de entrada do protocolo SSL.

17.9. Configurando a interface do Kaspersky Anti-Virus for Windows Workstations

O Kaspersky Anti-Virus for Windows Workstations lhe dá a opção de alterar a aparência do programa, criando e usando capas. Você também pode configurar o uso dos elementos de interface ativos, como o ícone da bandeja do sistema e as mensagens pop-up.

Para configurar a interface do programa, execute as seguintes etapas:

1. Abra a janela de configurações do Kaspersky Anti-Virus for Windows Workstations clicando no link Configurações na janela principal.
2. Selecione **Aparência** na seção **Serviço** da árvore de configurações do programa (veja a Figura 100).

À direita da janela de configurações, você pode determinar:

- Se o indicador de proteção do Kaspersky Anti-Virus for Windows Workstations será exibido quando o sistema operacional for iniciado.

  Por padrão, esse indicador aparece no canto superior direito da tela quando o programa é carregado. Ele informa se o computador está protegido de todos os tipos de ameaça. Se não desejar usar o indicador de proteção, desmarque ☑ **Mostrar ícone sobre a janela de logon do Microsoft Windows**.

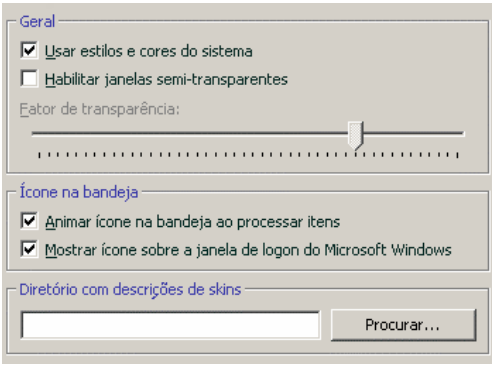


Figura 100. Configurando a aparência do programa

- Se a animação será usada no ícone da bandeja do sistema.

  Dependendo da operação do programa realizada, o ícone da bandeja do sistema muda. Por exemplo, se um script estiver sendo verificado, uma pequena ilustração de um script aparecerá no plano de fundo do ícone e, se um e-mail estiver sendo verificado, um envelope. Por padrão, a animação do ícone está ativada. Se desejar desativar a animação, desmarque **Animar ícone na bandeja ao processar itens**. Em seguida, o ícone indicará apenas o status de proteção do computador. Se a proteção estiver habilitada, o ícone ficará colorido e, se a proteção for pausada ou desabilitada, o ícone ficará cinza.

- Grau de transparência das mensagens pop-up.

  Todas as operações do Kaspersky Anti-Virus for Windows Workstations que devem ser informadas a você imediatamente ou que exigem que você tome uma decisão são apresentadas como mensagens pop-up acima do ícone da bandeja do sistema. As janelas de mensagem são transparentes, de modo a não interferir no seu trabalho. Se você mover o cursor sobre a mensagem, a transparência desaparecerá. Você pode alterar o grau de transparência dessas mensagens. Para fazê-lo, ajuste a escala do **Fator de transparência** para a posição desejada. Para remover a transparência da mensagem, desmarque **Habilitar janelas semi-transparentes.**

  Este recurso não está disponível no Windows 98/NT 4.0/ME.

- Use suas próprias capas para a interface do programa.

  Todas as cores, fontes, ícones e textos usados na interface do Kaspersky Anti-Virus for Windows Workstations podem ser alterados. Você pode criar seus próprios elementos gráficos para o programa ou localizá-los

em outro idioma. Para usar uma capa, especifique o diretório com suas configurações no campo **Diretório com descrições de capas**. Use o botão **Procurar** para selecionar o diretório.

Por padrão, as cores e estilos do sistema são usados na capa do programa. Você pode removê-los, desmarcando **Usar estilos e cores do sistema**. Então, os estilos especificados nas configurações do tema da tela serão usados.

Observe que as configurações da interface do Kaspersky Anti-Virus for Windows Workstations não serão salvas se você restaurar as configurações de operação padrão ou desinstalar o programa.

17.10. Disco de Recuperação

O Kaspersky Anti-Virus for Windows Workstations 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 do programa Kaspersky Anti-Virus for Windows Workstations
- Arquivos contendo assinaturas de ameaças

Para criar um disco de recuperação:

1. Abra a janela principal do programa e selecione **Disco de recuperação** na seção **Serviço**.
2. Clique no botão **Iniciar Assistente** para iniciar o processo de criação do disco.

Um Disco de Recuperação se destina ao computador no qual foi criado. O uso do disco em outros computadores poderia ter conseqüências imprevisíveis, pois ele contém informações sobre os parâmetros de um determinado computador (informações sobre os setores de inicialização, por exemplo).

Você pode criar um disco de recuperação somente no Windows XP e no Microsoft Windows Vista. O disco de recuperação não pode ser criado em computadores que executam o Microsoft Windows XP Professional x64 Edition ou o Microsoft Windows Vista x64.

17.10.1. Criando um disco de recuperação

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

Etapa 1. Preparando-se para gravar o disco

Para criar um disco de recuperação, especifique o caminho para as seguintes pastas:

- Pasta do programa PE Builder
- Pasta na qual os arquivos do disco de recuperação serão salvos antes de gravar o CD

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

  Observe que uma versão anterior dos arquivos do disco de recuperação conterá assinaturas de ameaças desatualizadas. Para analisar o computador quanto à presença de vírus e restaurar o sistema de forma ideal, é recomendável atualizar as assinaturas de ameaças e criar uma nova versão do disco de recuperação.

- CD de instalação do Microsoft Windows XP Service Pack 2

Para criar um disco de recuperação que possa inicializar o sistema operacional em um computador remoto, verificar e processar código mal-intencionado usando o Kaspersky Anti-Virus, marque  **Permitir administração remota do computador verificado**.

Observe que, para usar este recurso, o computador remoto deve dar suporte à Intel® vPRO™ ou à Intel® Active Management Technology (iAMT). Essas tecnologias permitem que os administradores trabalhem com todos os computadores conectados à rede remotamente, incluindo os que estão

desligados e aqueles cujos sistemas operacionais ou discos rígidos não estão funcionando.

Depois de inserir os caminhos para as pastas necessárias, clique em **Avançar**. O PE Builder será iniciado e o processo de criação do disco de recuperação começará. Aguarde até o processo ser concluído. Isto pode levar vários minutos.

Etapa 2. Criando um arquivo .iso

Depois que o PE Builder tiver concluído a criação dos arquivos do disco de recuperação, uma janela **Criar arquivo ISO** será aberta.

O arquivo .iso é uma imagem em CD do disco, salva como um arquivo. A maioria dos programas para gravação de CDs reconhece corretamente os arquivos .iso (o Nero, por exemplo).

Se esta não for a primeira vez que você cria um disco de recuperação, você poderá selecionar o arquivo .iso no disco anterior. Para fazê-lo, selecione **Arquivo ISO existente**.

Etapa 3. Gravando o disco

Esta janela do Assistente solicitará que você decida gravar os arquivos do disco de recuperação no CD agora ou depois.

Se você optar por gravar o disco imediatamente, especifique se deseja formatar o CD antes de gravá-lo. Para fazê-lo, marque a caixa correspondente. Esta opção estará disponível somente se você estiver usando um CD-RW.

O CD começará a ser gravado quando você clicar no botão **Avançar**. Aguarde até o processo ser concluído. Isto pode levar vários minutos.

Etapa 4. Concluindo a criação de um disco de recuperação

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

17.10.2. Usando o disco de recuperação

Observe que o Kaspersky Anti-Virus funcionará no modo de recuperação do sistema somente se a janela principal estiver aberta. Ao fechar a janela principal, o programa será fechado.

O Bart PE, o programa padrão, não dá suporte a arquivos .chm, nem a navegadores da Internet; portanto, você não poderá exibir a Ajuda do Kaspersky Anti-Virus, nem os links na interface do programa no Modo de Recuperação.

Se um ataque de vírus impossibilitar o carregamento do sistema operacional, execute as seguintes etapas:

1. Crie um disco de inicialização de emergência usando o Kaspersky Anti-Virus for Windows Workstations 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.

   O Bart PE possui suporte a rede interno para usar sua LAN. Quando o programa é iniciado, ele pergunta se você deseja habilitá-lo. Habilite o suporte à rede se planeja atualizar as assinaturas de ameaças na rede local antes de verificar o computador. Se a atualização não for necessária, cancele o suporte à rede.
3. Para abrir o Kaspersky Anti-Virus, clique em **Iniciar→Programas→Kaspersky Anti-Virus 6.0 for Windows Workstations →Iniciar**.

   A janela principal do Kaspersky Anti-Virus for Windows Workstations será aberta. No modo de recuperação do sistema, você pode acessar apenas as verificações de vírus e as atualizações de assinaturas de ameaças na rede local (se você tiver habilitado o suporte à rede no Bart PE).
4. Inicie a verificação de vírus.

Observe que, por padrão, são usadas as assinaturas de ameaças da data em que o disco de recuperação é criado. Por isso, é recomendável atualizar as assinaturas de ameaças antes de iniciar a verificação.

Observe também que o aplicativo usará apenas as assinaturas de ameaças atualizadas somente durante a sessão atual com o disco de recuperação, antes de reiniciar o computador.

Aviso!

Se foram detectados objetos infectados ou possivelmente infectados ao verificar o computador, e eles foram processados e movidos para a Quarentena ou o Backup, é recomendável concluir o processamento desses objetos durante a sessão atual com um disco de recuperação.

Caso contrário, eles serão perdidos ao reiniciar o computador.

17.11. Usando serviços adicionais

O Kaspersky Anti-Virus for Windows Workstations fornece os seguintes recursos avançados:

- Notificações sobre determinados eventos que ocorrem no programa.
- Autodefesa do Kaspersky Anti-Virus for Windows Workstations contra a desabilitação, exclusão ou edição de módulos, além da proteção do programa por senha.
- Resolução de conflitos com o Kaspersky Anti-Virus 6.0 ao usar outros aplicativos.

Para configurar estes recursos:

1. Abra a janela de configuração do programa com o link Configurações na janela principal.
2. Selecione **Serviço** na árvore de configurações.

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

17.11.1. Notificações de eventos do Kaspersky Anti-Virus for Windows Workstations

Vários tipos de eventos ocorrem no Kaspersky Anti-Virus for Windows Workstations. 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 for Windows Workstations, você pode usar o recurso de notificação.

Os avisos podem ser entregues de várias formas:

- Mensagens pop-up acima do ícone de programa, na bandeja do sistema
- Mensagens sonoras
- E-mails
- Registro de informações no log de eventos

Para usar este recurso:

1. Marque **Habilitar notificações** na caixa **Interação com o usuário** (veja a Figura 101).

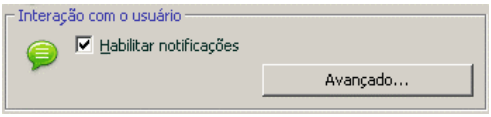


Figura 101. Habilitando notificações

2. Defina os tipos de eventos do Kaspersky Anti-Virus for Windows Workstations sobre os quais você deseja ser notificado e o método de entrega das notificações (consulte a seção 17.11.1.1 na p. 272).
3. Configure a entrega de notificações por e-mail, se esse for o método de notificação usado (consulte a seção 17.11.1.2 na p. 274).

17.11.1.1. Tipos de eventos e métodos de entrega de notificações

Durante o funcionamento do Kaspersky Anti-Virus for Windows Workstations, ocorrem os seguintes tipos de eventos:

Notificações críticas envolvem eventos de importância crítica. As notificações são altamente recomendadas, pois indicam problemas no funcionamento do programa ou vulnerabilidades do computador. Por exemplo, *assinaturas de ameaças corrompidas* ou *licença expirada*.

Notificações de erro se referem a eventos que fazem o aplicativo não funcionar. Por exemplo, quando não existe uma licença ou assinaturas de ameaças.

Notificações importantes são eventos que devem ser investigados, pois refletem situações importantes no funcionamento do programa. Por exemplo, *proteção desabilitada* ou *não é feita uma verificação de vírus no computador há muito tempo*.

Notificações secundárias são do tipo de referência, que geralmente não contêm informações importantes. Por exemplo, *todos os objetos perigosos foram desinfectados*.

Para especificar quais eventos o programa deve notificar e de que forma:

1. Clique no link Configurações na janela principal do programa.
2. Na janela de configurações do programa, selecione **Serviço**, marque **Habilitar notificações** e edite as configurações detalhadas, clicando no botão **Configurações**.

Você pode configurar os seguintes métodos de notificação dos eventos listados acima, na janela **Configurações de notificação** que é aberta (veja a Figura 102):

- *Mensagens pop-up* acima do ícone de programa, na bandeja do sistema, que contêm uma mensagem informativa sobre o evento que ocorreu.

  Para usar esse tipo de notificação, marque na seção **Balão** para o evento sobre o qual você deseja ser informado.

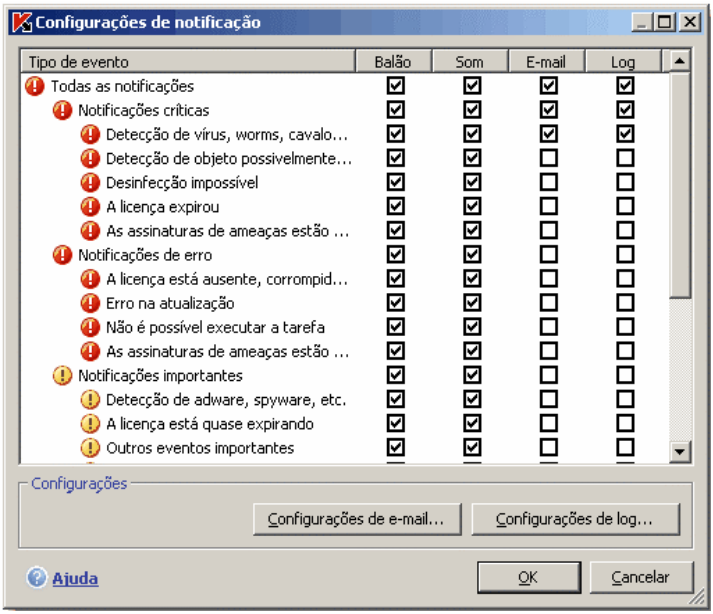


Figura 102. Eventos do programa e métodos de notificação de eventos

- *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 17.11.1.2 na p. 274).

- *Registro de informações no log de eventos*

  Para registrar no log informações sobre os eventos ocorridos, marque na coluna **Log** e configure o log de eventos (consulte a seção 17.11.1.3 na p. 275).

17.11.1.2. Configurando a notificação por e-mail

Depois de selecionar os eventos (consulte a seção 17.11.1.1 na p. 272) sobre os quais você deseja receber notificações por e-mail, configure a entrega de notificações. Para fazê-lo:

1. Abra a janela de configuração do programa com o link Configurações na janela principal.
2. Selecione **Serviço** na árvore de configurações.
3. Clique em **Avançado** na caixa **Interação com o usuário** à direita da tela.
4. Na guia **Configurações de notificação** (veja a Figura 102), marque a caixa de seleção na imagem de **E-mail** para os eventos que devem acionar uma mensagem de e-mail.
5. Na janela que é aberta ao clicar em **Configurações de notificação**, configure o seguinte para o envio de notificações por e-mail:
   - Atribua a configuração de notificação de envio para **De: endereço de e-mail**.
   - Especifique o endereço de e-mail para o qual os avisos serão enviados em **Para: endereço de e-mail**.
   - Atribua um método de entrega de notificações por e-mail em **Modo de envio**. Se desejar que o programa envie um e-mail assim que o evento ocorrer, selecione **Imediatamente na ocorrência do evento**. Para notificações sobre eventos após de um determinado período, preencha a programação de envio de e-mails informativos clicando em **Editar**. Notificações diárias são o padrão.

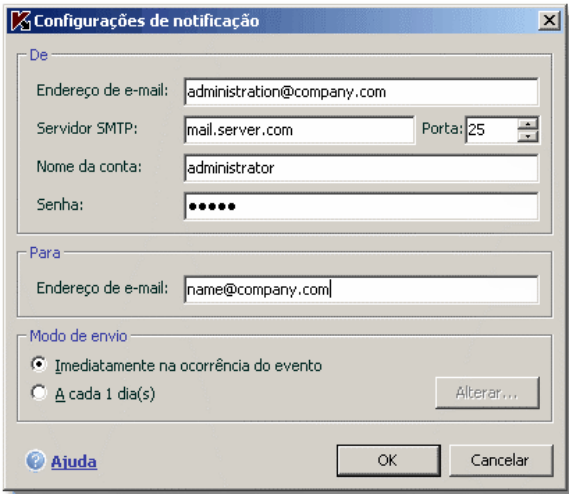


Figura 103. Configurando a notificação por e-mail

17.11.1.3. Configurando o log de eventos

Para configurar o log de eventos:

1. Abra a janela de configuração do aplicativo com o link Configurações na janela principal.
2. Selecione **Serviço** na árvore de configurações.
3. Clique em **Avançado** na seção **Interação com o usuário**, à direita da tela.

Na janela **Configurações de notificação**, selecione a opção de registrar informações de um evento e clique no botão **Configurações do log**.

O Kaspersky Anti-Virus permite registrar informações sobre eventos ocorridos durante a execução do programa, no log de eventos geral do MS Windows (**Aplicativo**) ou em um log de eventos dedicado do Kaspersky Anti-Virus (**Log de Eventos Kaspersky**).

No Microsoft Windows 98/ME, não é possível registrar no log de eventos. No Microsoft Windows NT 4.0, não é possível registrar no **Log de Eventos Kaspersky**.

Essas limitações se devem aos recursos dos sistemas operacionais.

Os logs podem ser exibidos em Visualizar Eventos da MS, que pode ser aberto em **Iniciar** → **Configurações** → **Painel de Controle** → **Ferramentas Administrativas** →**Visualizar eventos**.

17.11.2. Autodefesa e restrição de acesso

O Kaspersky Anti-Virus for Windows Workstations garante a segurança do computador contra programas mal-intencionados e, por isso, ele próprio pode ser alvo de programas mal-intencionados que tentam bloqueá-lo ou excluí-lo do computador.

Além disso, várias pessoas, com níveis diferentes de experiência em informática, podem usar um computador. Permitir o acesso ao programa e suas configurações pode diminuir bastante a segurança do computador como um todo.

Para assegurar a estabilidade do sistema de segurança do computador, os mecanismos de Autodefesa, defesa contra acesso remoto e proteção por senha foram adicionados ao programa.

Se você estiver executando o Kaspersky Anti-Virus no Microsoft Windows 98/ME, o recurso de autodefesa do aplicativo não ficará disponível.

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 configuração do programa com o link Configurações na janela principal.
2. Selecione **Serviço** na árvore de configurações.
3. Defina as seguintes configurações na caixa **Autodefesa** (veja a Figura 104):

   ☑ **Habilitar Autodefesa**. Se esta caixa estiver marcada, o programa protegerá seus próprios arquivos, processos na memória e entradas no registro do sistema contra exclusão e modificação.

   ☑ **Desabilitar controle de serviço externo**. Se esta caixa estiver marcada, qualquer programa de administração remota que tentar usar o programa será bloqueado.

Se houver alguma tentativa de executar as ações relacionadas, aparecerá uma mensagem sobre o ícone do programa na bandeja do sistema (se o serviço de notificação não tiver sido desabilitado pelo usuário).

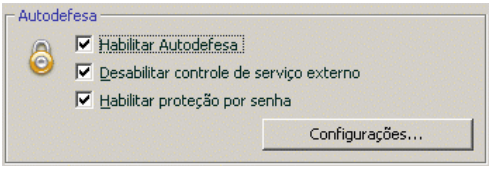


Figura 104. Configuração da defesa do programa

Para proteger o programa por senha, marque **Habilitar proteção por senha**. Clique no botão **Configurações** para abrir a janela **Proteção por senha** e insira a senha e a área a ser coberta pela restrição de acesso (veja a Figura 105). 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 for Windows Workstations
- Desabilitar ou pausar a proteção do computador

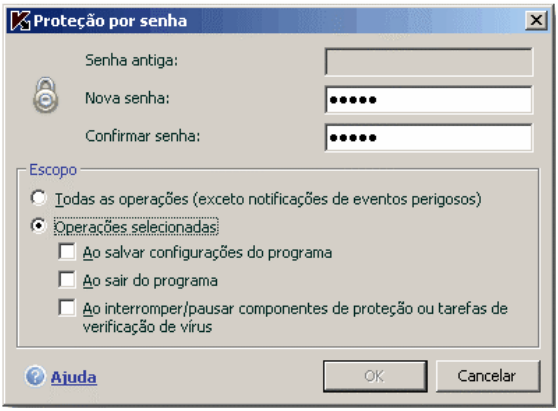


Figura 105. Configurações de proteção do programa por senha

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.

17.11.3. Resolvendo conflitos com outros aplicativos

Em alguns casos, o Kaspersky Anti-Virus pode causar conflitos com outros aplicativos instalados em um computador. Isso ocorre porque esses programas possuem mecanismos de autodefesa internos que são ativados quando o Kaspersky Anti-Virus tenta inspecioná-los. Esses aplicativos incluem o plug-in do Authentica para Acrobat Reader, que verifica o acesso a arquivos .pdf, o Oxygen Phone Manager II e alguns jogos que possuem ferramentas de gerenciamento de direitos digitais.

Para corrigir este problema, marque **Modo de compatibilidade para programas que usam métodos de autoproteção** na seção **Serviço** da janela de configurações do aplicativo. Reinicie o sistema operacional para que esta alteração tenha efeito.

Quando o Kaspersky Anti-Virus está instalado no computador com o Microsoft Windows Vista ou o Microsoft Windows Vista x64, não é possível resolver problemas de compatibilidade com outros aplicativos.

Entretanto, se você marcar esta caixa de seleção, alguns recursos do Kaspersky Anti-Virus, especificamente a Proteção do Microsoft Office e o Anti-Dialer, não funcionarão. Se você habilitar qualquer um desses componentes, a compatibilidade com a autodefesa do aplicativo será desabilitada automaticamente. Uma vez habilitados, esses componentes serão executados somente depois que você reiniciar o aplicativo.

17.12. Importando e exportando as configurações do Kaspersky Anti-Virus for Windows Workstations

O Kaspersky Anti-Virus for Windows Workstations permite que você importe e exporte suas configurações.

Esse recurso é útil quando, por exemplo, o programa é instalado no seu computador doméstico e no seu escritório. Você pode configurar o programa da maneira desejada em casa, salvar as configurações em um disco e, usando o recurso de importação, carregá-las no computador do trabalho. As configurações são salvas em um arquivo de configuração específico.

Para exportar as configurações atuais do programa:

1. Abra a janela principal do Kaspersky Anti-Virus for Windows Workstations.
2. Selecione a seção **Serviço** e clique em Configurações.
3. Clique no botão **Salvar** na seção **Gerenciador de configurações**.
4. Insira um nome para o arquivo de configuração e selecione um destino para salvá-lo.

Para importar configurações de um arquivo de configuração:

1. Abra a janela principal do Kaspersky Anti-Virus for Windows Workstations.
2. Selecione a seção **Serviço** e clique em Configurações.
3. Clique no botão **Carregar** e selecione o arquivo do qual deseja importar configurações do Kaspersky Anti-Virus for Windows Workstations.

17.13. Redefinindo as configurações padrão

Sempre é possível retornar às configurações padrão do programa, que são consideradas ideais e recomendadas pela Kaspersky Lab. Isso pode ser feito usando o Assistente para Instalação.

Para redefinir as configurações de proteção:

1. Selecione a seção **Serviço** e clique em Configurações para ir para a janela de configurações do programa.
2. Clique no botão **Redefinir** na seção **Gerenciador de configurações**.

A janela que é aberta solicita que você defina as configurações que devem ser restauradas para seus valores padrão.

A janela lista os componentes do programa cujas configurações foram alteradas pelo usuário ou que o programa acumulou durante o treinamento (Anti-Hacker ou Anti-Spam). Se tiverem sido criadas configurações específicas para algum componente, elas também serão mostradas na lista.

Exemplos de configurações específicas seriam as listas brancas e negras de frases e endereços usadas pelo Anti-Spam, listas de endereços confiáveis e listas de números de telefones de provedores confiáveis usados pelo Antivírus da Web e pelo Anti-Spy, regras de exclusão criadas por componentes do

programa, regras de aplicativos e filtragem de pacotes do Anti-Hacker e regras de aplicativos da Defesa Proativa.

Geralmente, essas listas são preenchidas gradualmente através do uso extensivo do programa, com base em requisitos de segurança e tarefas individuais e muitas vezes sua criação leva algum tempo. Portanto, é recomendável salvá-las antes de redefinir as configurações do programa.

Por padrão, o programa salva todas as configurações personalizadas na lista (elas estão desmarcadas). Se você não precisar salvar uma das configurações, marque a caixa correspondente.

Depois de concluir a configuração, clique no botão **Avançar**. O Assistente para Instalação inicial será aberto (consulte a seção 3.2 na p. 38). Siga suas instruções.

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

CAPÍTULO 18. TRABALHANDO COM O PROGRAMA NO PROMPT DE COMANDO

Você pode usar o Kaspersky Anti-Virus a partir do prompt de comando. É possível executar as seguintes operações:

- Iniciar, interromper, pausar e reiniciar a atividade dos componentes do aplicativo
- Iniciar, interromper, pausar e reiniciar as verificações de vírus
- Obter informações sobre o status atual dos componentes, das tarefas e das estatísticas
- Verificar objetos selecionados
- Atualizar assinaturas de ameaças e módulos do programa
- Acessar a Ajuda sobre a sintaxe do prompt de comando
- Acessar Ajuda sobre a sintaxe de comandos

A sintaxe do prompt de comando é a seguinte:

```
avp.com <comando> [configurações]
```

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>**:

ADDKEY	Ativa o aplicativo usando um arquivo de chave de licença (o comando poderá ser executado somente se a senha atribuída pela interface do programa for inserida)
ACTIVATE	Ativa o aplicativo on-line usando um código de ativação
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 for Windows Workstations (o comando poderá ser executado somente se a senha atribuída pela interface do programa for inserida)
EXPORT	Exporta configurações do Kaspersky Anti-Virus for Windows Workstations

Cada comando usa suas próprias configurações específicas do componente do Kaspersky Anti-Virus for Windows Workstations.

18.1. Ativando o aplicativo

Existem duas formas de ativar o aplicativo:

- on-line, usando um código de ativação (comando ACTIVATE)

- usando um arquivo de chave de licença (comando ADDKEY).

Sintaxe do comando:

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

Descrição dos parâmetros:

<nome_do_arquivo>	Nome do arquivo da chave de licença com a extensão *.key*.
<código_de_ativação>	O código de ativação do aplicativo fornecido na compra.
<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 ACTIVATE 11AA1-11AAA-1AA11-1A111
avp.com ADDKEY 1AA111A1.key /password=<sua_senha>
```

18.2. Gerenciando tarefas e componentes do programa

Sintaxe do comando:

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

Parâmetros:

<comando>	O Kaspersky Anti-Virus oferece gerenciamento de tarefas e componentes da linha de comando usando os seguintes comandos: **START** – inicia 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 as estatísticas de tempo de execução da tarefa ou componente de proteção em tempo real. Observe que PAUSE e STOP são protegidos por senha.
<perfil|nome_da_tarefa>	Ao parâmetro **<perfil>** pode ser atribuído qualquer módulo ou componente de segurança em tempo real do aplicativo, tarefa de verificação por demanda ou atualização como um valor (os valores padrão usados pelo aplicativo são mostrados a seguir). Os valores válidos para o parâmetro **<nome_da_tarefa>** incluem o nome de qualquer atualização ou tarefa de verificação por demanda definida pelo usuário.
<sua_senha>	A senha do Kaspersky Anti-Virus definida pela interface do programa.
/R[A]:<arquivo_de_relatório>	**R:<arquivo_de_relatório>**: registra apenas eventos importantes. **/RA:<arquivo_de_relatório>**: registra todos os eventos. Pode ser usado um caminho absoluto ou relativo de um 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. 73) ou pausada (consulte a seção 6.1.1 na p. 72). Esse comando também iniciará os componentes de proteção em tempo real que foram pausados usando o botão ❚❚ da interface gráfica do usuário ou o comando PAUSE no prompt de comando. Se o componente foi desabilitado usando o botão ■ da interface gráfica do usuário ou o comando 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: **og** – verifica macros do Microsoft Office **pdm** – análise de atividade do aplicativo
ASPY	Anti-Spy Valores dos subcomponentes do Anti-Spy:

	AdBlocker – Bloqueio de anúncios **antidial** – Anti-Dialer **antiphishing** – Anti-Phishing **popupchk** – Bloqueio de pop-ups
AH	Anti-Hacker Valores dos subcomponentes do Anti-Hacker: **fw** – Firewall **ids** – Sistema de Detecção de Intrusos
AS	Anti-Spam
UPDATER	Atualização
RetranslationCfg	Distribuição de atualizações para uma fonte local
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
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>
```

18.3. 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 for Windows Workstations do prompt de comando (consulte 18.1 na p. 282). A tarefa será executada de acordo com as configurações definidas na interface do programa.

Descrição dos parâmetros.

<objeto verificado> - este parâmetro fornece a lista de objetos que serão verificados quanto à presença de código mal-intencionado. Pode incluir vários valores da seguinte lista, separados por espaços.	
<arquivos>	Lista dos caminhos dos arquivos e/ou pastas a serem verificados. Você pode inserir caminhos absolutos ou relativos. Os itens da lista são separados por um espaço. Observações: • Se o nome do objeto contiver um espaço, será necessário colocá-lo entre aspas • Se você selecionar uma pasta específica, todos os arquivos contidos nela serão verificados.
/MEMORY	Objetos da memória do sistema

/STARTUP	Objetos de inicialização
/MAIL	Bancos de dados de e-mail
/REMDRIVES	Todas as unidades de mídia removíveis
/FIXDRIVES	Todas as unidades internas
/NETDRIVES	Todas as unidades de rede
/QUARANTINE	Objetos em quarentena
/ALL	Verificação completa
/@:<filelist.lst>	Caminho para o arquivo que contém uma lista de objetos e pastas a serem incluídos na verificação. O arquivo deve estar no formato de texto e cada objeto da verificação deve iniciar uma nova linha. Você pode inserir um caminho absoluto ou relativo para o arquivo. Se contiver espaços, o caminho deverá estar entre aspas.
<ação> - este parâmetro define as respostas para objetos mal-intencionados detectados durante a verificação. Se este parâmetro não for definido, o valor padrão será **/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 bancos de dados de e-mail
-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 é um arquivo de texto que contém um grupo de configurações de prompt de comando para verificações 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 for Windows Workstations.	
/C:<nome_do_arquivo>	Use os valores de configuração atribuídos no arquivo de configuração **<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, dos bancos de dados de e-mail, dos diretórios **Meus Documentos** *e* **Arquivos de Programas** *e do arquivo* **test.exe***:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and
Settings\Todos os Usuários\Meus Documentos"
"C:\Arquivos de Programas" "C:\Downloads\test.exe"
```

Pausar a verificação de objetos selecionados e iniciar uma verificação completa do computador; continuar a verificação de vírus nos objetos selecionados:

```
avp.com PAUSE SCAN_OBJECTS /password=<sua_senha>
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

Verificar a RAM e os objetos relacionados no arquivo ***object2scan.txt****: Use o arquivo de configuração* ***scan_setting.txt****. Após a verificação, gerar um relatório que registre todos os eventos:*

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

Exemplo de arquivo de configuração:

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

18.4. Atualizações do programa

A sintaxe para atualizar os módulos do programa e as assinaturas de ameaças do Kaspersky Anti-Virus for Windows Workstations a partir do prompt de comando é a seguinte:

```
avp.com UPDATE [<caminho/URL>]
[/R[A]:<arquivo_relatório>]
[/C:<arquivo_configurações>] [/APP=<on|off>]
```

Descrição dos parâmetros:

<fonte_de_atualização>	Servidor HTTP ou FTP ou diretório de rede para baixar as atualizações. O valor do parâmetro pode estar no formato de um caminho completo para uma fonte de atualização ou uma URL. Se nenhum caminho for especificado, uma fonte de atualização será copiada das configurações de atualização do aplicativo.

/R[A]:<arquivo_de_relatório>	**/R:<arquivo_relatório>** – registra somente os eventos importantes no relatório. **/R[A]:<arquivo_relatório>** – registra todos os eventos no relatório. Você pode usar um caminho absoluto ou relativo para o arquivo. Se o parâmetro não for definido, os resultados da verificação serão exibidos na tela e todos os eventos serão mostrados.
/C:<nome_do_arquivo>	Caminho do arquivo de configuração com as definições para atualizações do programa. O arquivo de configuração é um arquivo de texto que contém um grupo de configurações de prompt de comando para atualizar o programa. Você pode inserir um caminho absoluto ou relativo para o arquivo. Se este parâmetro não for definido, serão usados os valores especificados na interface do Kaspersky Anti-Virus for Windows Workstations.
/APP=<on|off>	Habilita / desabilita as atualizações de módulos do aplicativo

Exemplos:

Atualizar as assinaturas de ameaças e registrar todos os eventos no relatório:

```
avp.com UPDATE /RA:avbases_upd.txt
```

*Atualizar os módulos do programa Kaspersky Anti-Virus for Windows Workstations 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
```

18.5. Configurações de reversão

Sintaxe do comando:

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

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

Exemplo:

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

18.6. Exportando configurações

Sintaxe do comando:

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

Descrição dos parâmetros:

<perfil>	Componente ou tarefa com as configurações exportadas. Em **<perfil>**, você pode usar qualquer valor que esteja listado em 18.2 na p. 283.
<nome_do_arquivo>	O arquivo de configuração pode ser salvo como um arquivo de texto. Para fazê-lo, especifique a extensão *.txt* no nome do arquivo. Você também pode salvar o arquivo em qualquer formato binário. O arquivo de configuração é salvo no formato binário (*.dat*), a menos que seja especificado outro formato ou se o formato não for atribuído, 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. Não é possível importar configurações de proteção de um arquivo de texto. Este arquivo pode ser usado somente para especificar as configurações principais de funcionamento do programa.

Exemplo:

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

18.7. Importando configurações

Sintaxe do comando:

```
avp.com IMPORT <nome_do_arquivo>
[/password=<sua_senha>]
```

<nome_do_arquivo>	O arquivo de configuração pode ser salvo como um arquivo de texto. Para fazê-lo, especifique a extensão *.dat* no nome do arquivo. As configurações podem ser importadas somente de arquivos binários. Se você instalar o programa no modo oculto usando o prompt de comando ou o Editor de Objeto de Diretiva de Grupo, o nome que consta no arquivo de configuração deverá ser *install.cfg*. Caso contrário, o programa não o reconhecerá.
<sua_senha>	Senha do Kaspersky Anti-Virus atribuída na interface do programa.
Observe que este comando não será aceito sem uma senha.	

Exemplo:

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

18.8. Iniciando o programa

Sintaxe do comando:

```
avp.com
```

18.9. Interrompendo o programa

Sintaxe do comando:

```
avp.com EXIT /password=<sua_senha>
```

<sua_senha>	Senha do Kaspersky Anti-Virus for Windows Workstations atribuída na interface do programa.
Observe que este comando não será aceito sem uma senha.	

Observe que não será possível executar este comando sem informar a senha.

18.10. Obtendo um arquivo de rastreamento

Talvez seja necessário um arquivo de rastreamento, no caso de problemas em tempo de execução do aplicativo, para que os especialistas do Suporte Técnico possam trabalhar em uma solução de problemas mais direcionada.

Sintaxe do comando:

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

[on|off]	Habilita/desabilita a geração do arquivo de rastreamento.
[file]	Obtém um rastreamento e salva em arquivo.
<nível_de_rastreamento>	Este parâmetro pode ter valores numéricos de 0 (nível mais baixo, somente para eventos críticos) a 700 (nível mais alto, todos os eventos). Quando uma solicitação é enviada para o Suporte Técnico, um especialista deve especificar o nível de rastreamento necessário. Se não for especificado, o nível recomendado será 500.
Cuidado! A geração do arquivo de rastreamento deve estar habilitada somente para solucionar um problema específico. A ativação contínua da funcionalidade de rastreamento pode reduzir o desempenho do computador e fazer o disco rígido ficar cheio.	

Exemplos:

Desabilitar rastreamento:

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

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

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

18.11. 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>
```

18.12. 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 19. MODIFICANDO, REPARANDO E REMOVENDO O PROGRAMA

O aplicativo pode ser desinstalado das maneiras a seguir:

- Usando o Assistente para Instalação do aplicativo (consulte a seção 19.2 na p. 301)
- Do prompt de comando (consulte 19.2 na p. 301)
- Usando o Kaspersky Administration Kit (consulte o Manual de Implementação do Kaspersky Administration Kit)
- Usando as diretivas de domínio de grupo do Microsoft Windows Server 2000/2003 (consulte a 3.4.3 na p. 50).

19.1. Modificando, reparando e removendo o programa usando o Assistente para Instalação

Talvez seja necessário reparar o programa, se você detectar erros no funcionamento depois de uma configuração incorreta ou da corrupção de arquivos.

A modificação do programa pode resultar na instalação de componentes ausentes do Kaspersky Anti-Virus for Windows Workstations e na exclusão de componentes indesejados.

Para reparar ou modificar componentes ausentes do Kaspersky Anti-Virus for Windows Workstations ou excluir o programa:

1. Saia do programa. Para fazê-lo, clique no ícone do programa na bandeja do sistema e selecione **Sair** no menu de contexto.
2. Insira o CD de instalação utilizado para instalar o programa na unidade de CD-ROM. Se você instalou o Kaspersky Anti-Virus for Windows Workstations de outra fonte (pasta de acesso público, pasta no disco rígido, etc.), verifique se o pacote de instalação se encontra na pasta e se você tem acesso a ela.

3. Selecione **Iniciar** → **Programas** → **Kaspersky Anti-Virus 6.0 for Windows Workstations** → **Modificar, reparar ou remover**.

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

Etapa 1. Janela de boas-vindas da instalação

Se você executar todas as etapas descritas acima, necessárias para reparar ou modificar o programa, a janela de boas-vindas da instalação do Kaspersky Anti-Virus for Windows Workstations aparecerá. Para continuar, clique no botão **Avançar**.

Etapa 2. Selecionando uma operação

Neste estágio, selecione a operação que deseja executar. Você pode modificar os componentes do programa, reparar os componentes instalados ou remover componentes ou o programa todo. Para executar a operação desejada, clique no botão apropriado. A resposta do programa dependerá da operação selecionada.

A modificação do programa se assemelha à instalação personalizada do mesmo (consulte a seção Etapa 7. na p. 36), na qual você pode especificar os componentes que deseja instalar e 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 for Windows Workstations, selecione **Desinstalação completa**. Para salvar os dados, selecione **Salvar objetos do aplicativo** e especifique os objetos que não deverão ser excluídos da lista:

- *Dados de ativação* – arquivo da chave de licença necessário para o funcionamento do aplicativo.
- *Assinaturas de ameaças* – conjunto completo de assinaturas de programas perigosos, vírus e outras ameaças da atualização mais recente.
- *Base de dados de conhecimento do Anti-Spam* – banco de dados usado para detectar e-mails indesejados. Esse banco de dados contém informações detalhadas sobre quais e-mails são spams ou não.

- *Arquivos de backup* – cópias de backup dos objetos excluídos ou desinfectados. É recomendável salvar esses arquivos, caso possam ser restaurados posteriormente.
- *Arquivos da Quarentena* – arquivos possivelmente infectados por vírus ou suas modificações. Esses arquivos contêm códigos semelhantes ao código de um vírus conhecido, mas é difícil determinar se eles são mal-intencionados. É recomendável salvá-los, pois eles podem não estar infectados ou talvez possam ser desinfectados após a atualização das assinaturas de ameaças.
- *Configurações do aplicativo* – configurações de todos os componentes do programa.
- *Dados do iSwift* – banco de dados com informações sobre os objetos verificados nos sistemas de arquivos NTFS, que podem aumentar a velocidade de verificação. Ao usar esse banco de dados, o Kaspersky Anti-Virus for Windows Workstations verifica somente os arquivos modificados desde a última verificação.

Aviso!

Se passar muito tempo entre a desinstalação de uma versão do Kaspersky Anti-Virus for Windows Workstations e a instalação de outra, não é recomendável usar o banco de dados do *iSwift* de uma instalação anterior. Um programa perigoso poderia invadir o computador durante este período e seus efeitos não seriam detectados pelo banco de dados, o que poderia resultar em uma infecção.

Para iniciar a operação selecionada, clique no botão **Avançar**. O programa começará a copiar os arquivos necessários para o computador ou a excluir os componentes e dados selecionados.

Etapa 3. Concluindo a modificação, o reparo ou a remoção do programa

O processo de modificação, reparo ou remoção será exibido na tela, sendo informado a seguir sobre sua conclusão.

Em geral, a remoção do programa exige a reinicialização do computador, pois é necessário informar essas modificações ao sistema. O programa perguntará se deseja reiniciar o computador. Clique em **Sim** para reiniciar imediatamente. Para reiniciar mais tarde, clique em **Não**.

19.2. Desinstalando o programa do prompt de comando

Para desinstalar o Kaspersky Anti-Virus 6.0 for Windows Workstations do prompt de comando, digite:

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

O Assistente para Instalação será aberto. Você pode usá-lo para desinstalar o aplicativo (consulte a seção Capítulo 19 na p. 298).

Para desinstalar o aplicativo no modo não interativo sem reiniciar o computador (o computador deverá ser reiniciado manualmente após a desinstalação), digite:

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

Para desinstalar o aplicativo no modo não interativo e reiniciar o computador, digite:

```
msiexec /x <nome_do_pacote> ALLOWREBOOT=1 /qn
```

Se você optou pela proteção da desinstalação do programa por senha ao instalá-lo, será necessário inserir essa senha de proteção. Caso contrário, o programa não poderá ser desinstalado.

Para remover o aplicativo inserindo uma senha como prova do privilégio de remoção, digite:

`msiexec /x <nome_do_pacote> KLUNINSTPASSWD=******` – para remover o aplicativo no modo interativo;

`msiexec /x <nome_do_pacote> KLUNINSTPASSWD=****** /qn` – para remover o aplicativo no modo não interativo;

CAPÍTULO 20. ADMINISTRANDO O PROGRAMA COM O KASPERSKY ADMINISTRATION KIT

O **Kaspersky Administration Kit** é um sistema para gerenciar centralmente as principais tarefas administrativas na operação do sistema de segurança de uma rede corporativa, com base nos aplicativos incluídos no Kaspersky Anti-Virus Business Optimal.

O Kaspersky Anti-Virus 6.0 for Windows Workstations é um dos produtos da Kaspersky Lab que pode ser administrado de sua própria interface, da linha de comando (esses métodos estão descritos acima, neste Manual do Usuário) ou usando o Kaspersky Administration Kit (se o computador fizer parte de um sistema de administração remota centralizada).

Execute as seguintes etapas para gerenciar o Kaspersky Anti-Virus 6.0 for Windows Workstations usando o Kaspersky Administration Kit:

- implemente o *Servidor de Administração* na rede; instale o *Console* de Administração no local de trabalho do administrador (para obter mais detalhes, consulte o Manual do Administrador para instalar o Kaspersky Administration Kit 6.0);
- implemente o Kaspersky Anti-Virus 6.0 for Windows Workstations e o *Agente Administrativo* (fornecido com o Kaspersky Administration Kit) nos computadores da rede. Para saber mais sobre a instalação remota do Kaspersky Anti-Virus nos computadores da rede, consulte o Manual do Administrador para instalar o Kaspersky Administration Kit 6.0.

Observe as seguintes particularidades de uso do Kaspersky Anti-Virus por meio do Kaspersky Administration Kit:

Se os computadores da rede tiverem o Kaspersky Anti-Virus 5.0 instalado, execute as seguintes etapas antes de atualizar para a versão 6.0, pelo Kaspersky Administration Kit:

- Primeiro, interrompa a versão anterior do aplicativo (é possível fazê-lo remotamente pelo Kaspersky Administration Kit);
- Feche todos os outros aplicativos antes de iniciar a instalação;
- Reinicie o sistema operacional no computador remoto após a conclusão da instalação.

Depois de atualizar o plug-in de administração da Kaspersky Lab por meio do Kaspersky Administration Kit, feche o Console de Administração.

O *Console de Administração* (veja a Figura 106) permite administrar o aplicativo por meio do Kaspersky Administration Kit. Ele fornece uma **interface integrada ao MMC** padrão e permite que o administrador execute as seguintes funções:

- instalar remotamente o Kaspersky Anti-Virus 6.0 for Windows Workstations e o *Agente Administrativo* nos computadores da rede
- configurar remotamente o Kaspersky Anti-Virus nos computadores da rede
- atualizar as assinaturas de ameaças e módulos do Kaspersky Anti-Virus
- gerenciar licenças do aplicativo nos computadores da rede
- exibir informações sobre o funcionamento do programa nos computadores cliente

Ao administrar o programa centralmente pelo Kaspersky Administration Kit, o administrador determina as configurações de diretivas, tarefas e do aplicativo. A proteção é criada com essas configurações.

As **configurações do aplicativo** consistem em um conjunto de configurações gerais da operação do programa, incluindo configurações gerais de proteção, configurações de Backup, etc.

Uma **tarefa** é uma ação específica executada pelo aplicativo. As tarefas do Kaspersky Anti-Virus 6.0 são divididas por tipo (tarefas de instalação da chave de licença, tarefas de verificação por demanda, tarefas de reversão de atualizações do banco de dados de antivírus, tarefas de atualização do banco de dados de antivírus e dos módulos do aplicativo). Cada tarefa específica possui um conjunto de configurações do Kaspersky Anti-Virus quando executada (*configurações da tarefa*).

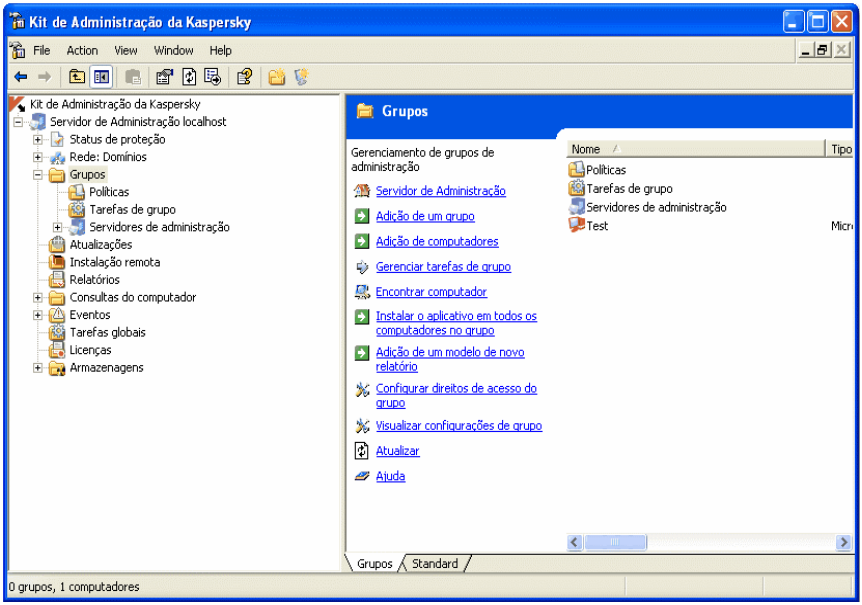


Figura 106. Console de Administração do Kaspersky Administration Kit

O principal recurso da administração centralizada é o agrupamento de computadores remotos e o gerenciamento de suas configurações através da criação e configuração de diretivas de grupo.

A **diretiva** se refere a uma coleção de configurações de operação do Kaspersky Anti-Virus em um grupo da rede. A diretiva também pode incluir restrições sobre a modificação das configurações atribuídas ao configurar o aplicativo ou a tarefa.

Uma diretiva permite que você gerencie toda a funcionalidade do aplicativo, pois ela contém as configurações do aplicativo e de todos os tipos de tarefas, exceto aquelas que devem ser configuradas diretamente quando uma tarefa é iniciada (por exemplo, programações de tarefas).

20.1. Administrando o aplicativo

O Kaspersky Administration Kit oferece a oportunidade de iniciar e pausar remotamente o Kaspersky Anti-Virus em computadores cliente individuais, além de definir as configurações gerais do aplicativo, como habilitar/desabilitar a proteção do computador, definir as configurações do Backup e da Quarentena e configurar a criação de relatórios.

Para gerenciar as configurações do aplicativo:

1. Selecione a pasta do grupo que contém o computador cliente na pasta **Grupos** (veja a Figura 106).
2. No painel de resultados, selecione o computador no qual deseja modificar as configurações do aplicativo. Selecione o comando **Aplicativos** no menu de contexto ou no menu **Ações**.
3. A guia **Aplicativos** na janela de propriedades do computador cliente (veja a Figura 107) exibe uma lista completa dos aplicativos da Kaspersky Lab instalados no computador cliente. Selecione **Kaspersky Anti-Virus 6.0 for Windows Workstations**.

Sob a lista, há botões que podem ser usados para:

- Exibir uma lista de eventos de funcionamento do aplicativo que ocorreram no servidor e que foram registrados no servidor de administração
- Exibir informações estatísticas sobre o funcionamento do aplicativo
- Configurar o aplicativo (consulte a 20.1.2 na p. 307)

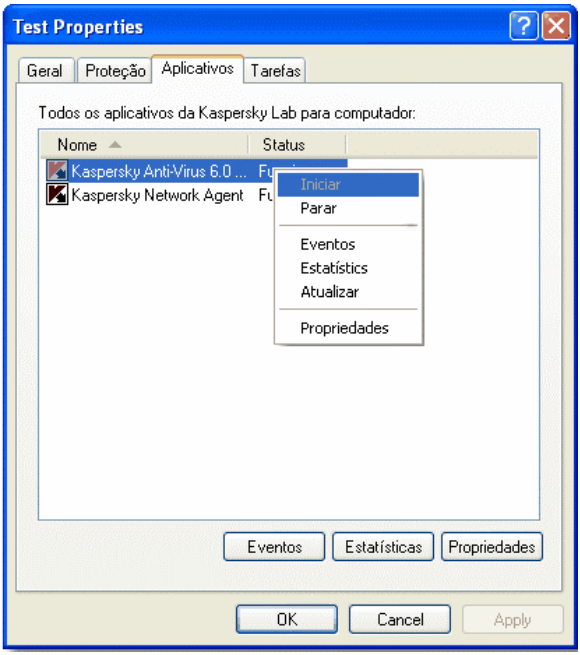


Figura 107. Lista de aplicativos da Kaspersky Lab

20.1.1. Iniciando/interrompendo o aplicativo

Você pode iniciar ou pausar o Kaspersky Anti-Virus em um computador remoto usando os comandos do menu de contexto na janela **Propriedades: nome do computador** (veja a Figura 107).

Também é possível fazê-lo usando os botões **Iniciar/Interromper** na janela de configurações na guia **Geral** (veja a Figura 108).

Na parte superior da janela, você encontrará o nome do aplicativo instalado, as informações de versão, a data de instalação, seu status (se o aplicativo está em execução ou pausado no computador local) e informações sobre o status do banco de dados de assinaturas de ameaças.

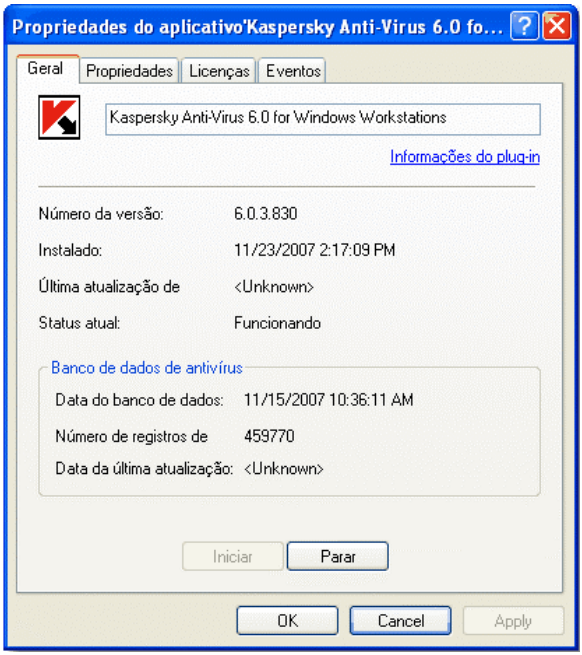


Figura 108. Configurando o Kaspersky Anti-Virus.
A guia **Geral**

20.1.2. Configurando o aplicativo

Para exibir ou modificar as configurações do aplicativo:

1. Abra a janela de propriedades do computador cliente na guia **Aplicativos** (veja a Figura 107).
2. Selecione **Kaspersky Anti-Virus 6.0 for Windows Workstations**. Clique no botão **Propriedades** para abrir a janela de configurações do aplicativo (veja a Figura 109).

Todas as guias, exceto a guia **Propriedades**, são padrão do Kaspersky Administration Kit. Para saber mais sobre as guias padrão, consulte o Manual do Administrador.

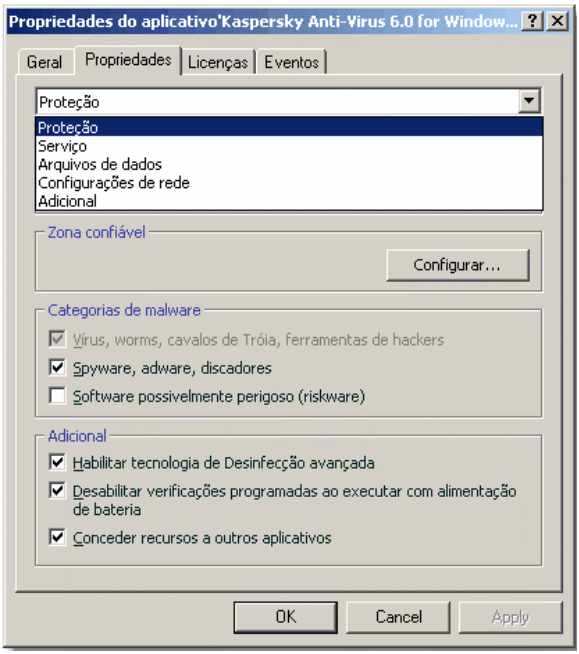


Figura 109. Configurando o Kaspersky Anti-Virus. A guia **Propriedades**

Se tiver sido criada uma diretiva para o aplicativo (consulte 20.3.1 na p. 316) que impede a redefinição de algumas configurações, elas não poderão ser editadas ao configurar o aplicativo.

Na guia **Propriedades**, você pode configurar a proteção geral, as ferramentas de proteção do aplicativo e a criação e o salvamento de estatísticas no relatório do aplicativo. Para fazê-lo, selecione o valor desejado no menu suspenso na parte superior da janela e defina as configurações.

Proteção
Na guia **Propriedades**, na seção **Proteção**, você pode: • habilitar/desabilitar a proteção em tempo real de um computador (consulte 6.1 na p. 71); • configurar a inicialização automática do aplicativo quando o computador é ligado (consulte 6.1.5 na p. 75); • criar uma zona confiável ou uma lista de exclusões (consulte 6.3 na p. 77); • selecionar os tipos de programas mal-intencionados que o aplicativo vai monitorar (consulte 6.2 na p. 76); • configurar a produtividade do aplicativo e as configurações de vários processadores (consulte 6.6 na p. 89).
Serviço
Na guia **Propriedades**, na seção **Serviço**, você pode: • Configurar notificações de eventos ocorridos (consulte a seção 17.11.1 na p. 271) • Gerenciar o recurso de autodefesa do aplicativo e das configurações da proteção do aplicativo por senha (consulte a seção 17.11.2 na p. 276) • Configurar a aparência do aplicativo (consulte a seção 20.1.3 na p. 309) • Configurar a compatibilidade do Kaspersky Anti-Virus com outros programas (consulte a seção 17.11.3 na p. 278)
Arquivos de dados
Nesta janela, você pode configurar a geração de estatísticas sobre o funcionamento do aplicativo (consulte a seção 17.3.1 na p. 242) e especificar por quanto tempo os arquivos serão armazenados no Backup (consulte a seção 17.1.2 na p. 236) e na Quarentena (consulte a seção 17.2.2 na p. 239).

Configurações de rede
Nesta janela, você pode editar a lista de portas usadas pelo Kaspersky Anti-Virus para a verificação (consulte a seção 17.7 na p. 261) e para habilitar/desabilitar a verificação de SSL (consulte a seção 17.8 na p. 263)

20.1.3. Definido configurações específicas

Ao administrar o Kaspersky Anti-Virus por meio do Kaspersky Administration Kit, você pode habilitar/desabilitar a interatividade e editar informações de Suporte Técnico. Para fazê-lo:

1. Abra a janela de propriedades do computador cliente na guia **Aplicativos** (veja a Figura 107). Selecione **Kaspersky Anti-Virus 6.0 for Windows Workstations** e clique no botão **Propriedades**. Como resultado, será aberta uma janela de configurações do aplicativo.
2. Vá para a guia **Configurações** (veja a Figura 108). Selecione **Serviço** no menu suspenso na parte superior da janela.

Na guia **Serviço** da janela **Aparência**, você pode habilitar/desabilitar a interatividade do Kaspersky Anti-Virus em um computador remoto: habilitando o ícone do Kaspersky Anti-Virus na bandeja do sistema, emitindo notificações sobre eventos que ocorrem com o aplicativo (por exemplo, a detecção de um objeto perigoso).

Se a opção ☑ **Habilitar interação da interface** estiver marcada, um usuário que trabalha em um computador remoto verá o ícone e as mensagens pop-up do antivírus e poderá decidir sobre o que fazer nas janelas de notificação dos eventos ocorridos. Para desabilitar a interatividade do aplicativo, desmarque a caixa de seleção.

Na guia **Informações sobre suporte personalizado** da janela que é aberta ao clicar no botão **Configurações**, você pode editar as informações sobre suporte técnico do usuário exibidas na seção **Serviço** do item **Suporte** no Kaspersky Anti-Virus (veja a Figura 97).

Para alterar as informações no campo superior, insira o texto atual sobre o suporte fornecido. No campo inferior, você pode editar os hiperlinks exibidos na caixa **Suporte técnico on-line** que é aberta ao selecionar **Suporte** na seção **Serviço**.

É possível editar a lista de fontes usando os botões **Adicionar**, **Editar** e **Excluir**. O Kaspersky Anti-Virus adicionará um novo link à parte superior da lista. Para alterar a ordem dos links na lista, use os botões **Para cima** e **Para baixo**.

Se a janela não contiver dados, as informações padrão sobre o suporte técnico não poderão ser editadas.

20.2. Gerenciando tarefas

Esta seção relaciona informações sobre o gerenciamento de tarefas do Kaspersky Anti-Virus 6.0 for Windows Workstations. Para obter mais detalhes sobre o conceito de gerenciamento de tarefas usando o Kaspersky Administration Kit 6.0, consulte o Manual do Administrador do programa.

Uma lista de tarefas do sistema é criada para cada computador ao instalar o aplicativo. Esta lista (veja a Figura 110) inclui tarefas de proteção em tempo real (Antivírus de Arquivos, Antivírus da Web, Antivírus de E-Mail, Defesa Proativa, Anti-Spy e Anti-Hacker), tarefas de verificação de vírus (Meu Computador, Objetos de inicialização, Áreas críticas) e tarefas de atualização (atualizações de assinaturas de ameaças e módulos do aplicativo e reversões de atualizações).

Você pode iniciar tarefas do sistema, definir suas configurações e programações, mas elas não podem ser excluídas.

Além disso, você pode criar suas próprias tarefas, como verificações de vírus, atualizações do aplicativo e reversões de atualizações, bem como tarefas de instalação da chave de licença (consulte a seção 20.2.2 na p. 312).

Para exibir uma lista das tarefas criadas para um computador cliente:

1. Selecione a pasta do grupo que contém o computador cliente na pasta **Grupos** (veja a Figura 106).
2. No painel de resultados, selecione o computador para o qual deseja exibir uma lista de tarefas locais. Use o comando **Tarefas** no menu de contexto ou no menu **Ações**. Em seguida, na janela principal será aberta uma janela exibindo as propriedades do computador cliente.
3. A guia **Tarefas** (veja a Figura 110) exibe uma lista completa de tarefas criadas para esse computador cliente.

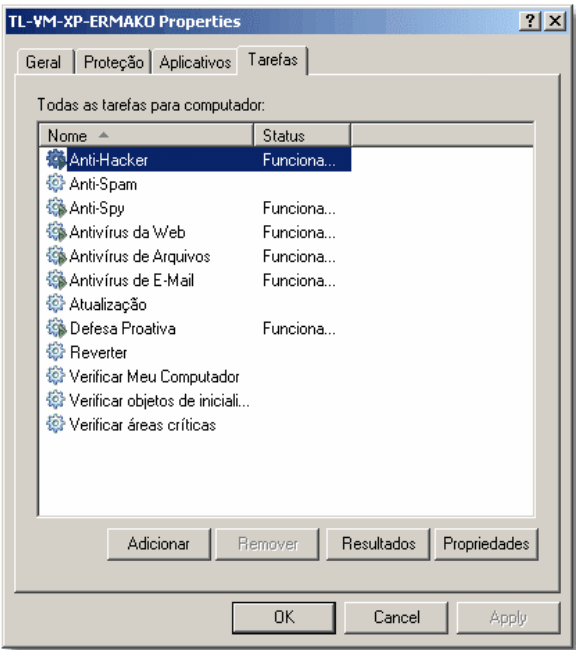


Figura 110. Lista de tarefas do aplicativo

20.2.1. Iniciando e interrompendo tarefas

As tarefas serão iniciadas no computador cliente somente se o aplicativo correspondente estiver em execução (consulte a 20.1.1 na p. 306). Se o aplicativo estiver parado, todas as tarefas serão encerradas.

As tarefas são iniciadas e pausadas automaticamente, de acordo com uma programação, ou manualmente, usando comandos do menu de contexto e da janela Exibir configurações de tarefas. Você também pode pausar e reiniciar tarefas.

Para iniciar/interromper/pausar/continuar uma tarefa manualmente:

Selecione a tarefa desejada (grupo ou global) no painel de resultados, abra o menu de contexto e selecione **Iniciar/Interromper/Pausar/Continuar** ou use os mesmos comandos no menu **Ação**.

Você pode iniciar as mesmas operações para todos os tipos de tarefa na janela de configurações da tarefa na guia **Geral** (veja a Figura 111) usando os botões correspondentes.

20.2.2. Criando tarefas

Ao trabalhar com o aplicativo por meio do Kaspersky Administration Kit, você pode criar:

- Tarefas locais, configuradas para computadores individuais
- Tarefas de grupos, configuradas para computadores unidos em um grupo de rede
- Tarefas globais, configuradas para qualquer conjunto de computadores de qualquer grupo de rede

Você pode modificar as configurações das tarefas, monitorar seu desempenho, copiar e mover tarefas de um grupo para outro e também excluí-las usando os comandos padrão **Copiar/Colar**, **Recortar/Colar** e **Excluir** no menu de contexto ou no menu **Ação**.

20.2.2.1. Criando tarefas locais

Para criar uma tarefa local, execute as seguintes etapas:

1. Abra a janela de propriedades do cliente local na guia **Tarefas** (veja a Figura 110).
2. Clique no botão **Adicionar** para adicionar uma nova tarefa. Será iniciado um assistente para criação de tarefas, que consiste em uma série de janelas ou etapas nas quais você pode navegar usando os botões **Voltar** e **Avançar**. Encerre o assistente pressionando **Concluir**. O botão **Cancelar** interromperá o Assistente a qualquer momento.

Etapa 1. Inserindo dados gerais na tarefa

A primeira janela-mestre é introdutória: nela, especifique o nome da tarefa (o campo **Nome**).

Etapa 2. Selecionando um aplicativo e um tipo de tarefa

Nesta etapa, você deve especificar o aplicativo para o qual a tarefa está sendo criada (Kaspersky Anti-Virus 6.0 for Windows Workstations). Também é

necessário selecionar o tipo de tarefa. As opções de tarefas para o Kaspersky Anti-Virus 6.0 são:

- *Verificação de vírus* – verifica vírus nas áreas especificadas pelo usuário
- *Atualização* – recupera e aplica os pacotes de atualização do programa
- *Reversão da atualização* – reverte para última atualização do programa
- *Instalação da chave de licença* – adiciona uma nova chave de licença para usar o aplicativo

Etapa 3. Configurando o tipo de tarefa selecionado

Dependendo do tipo de tarefa selecionado na etapa anterior, o conteúdo das janelas seguintes pode variar:

VERIFICAÇÃO DE VÍRUS

A janela de configuração da tarefa de verificação de vírus exige que você especifique a ação que o Kaspersky Anti-Virus deverá executar ao detectar um objeto perigoso (consulte a seção 14.4.4 na p. 208). Crie também uma lista de objetos a serem verificados (consulte a 14.2 na p. 200).

UPDATE

Para as tarefas de atualização das assinaturas de ameaças e módulos do aplicativo, é necessário especificar a fonte que será usada para baixar as atualizações (consulte a 16.4.1 na p. 222). A fonte de atualização padrão é o servidor de atualizações do Kaspersky Administration Kit.

REVERSÃO DA ATUALIZAÇÃO

Não há configurações específicas para reverter a atualização mais recente.

INSTALAÇÃO DA CHAVE DE LICENÇA

Para tarefas de instalação da chave de licença, especifique o caminho do arquivo da chave com o botão **Procurar**. Para fazer o backup de uma chave adicionada, marque **Adicionar como chave de backup**. A chave de licença de backup será ativada quando a chave de licença atual expirar.

Informações sobre a chave adicionada (número, tipo e data de validade da licença) são exibidas no campo a seguir.

Etapa 4. Selecionando um perfil de usuário

Nesta etapa, é solicitado que você configure tarefas para serem iniciadas em uma conta de usuário com privilégios suficientes para acessar o objeto que está

sendo verificado ou a fonte de atualização (para obter mais detalhes, consulte a seção 6.4 na p. 86).

Etapa 5. Configurando uma programação

Depois de configurar a tarefa, será solicitado que você configure uma programação automática de tarefas.

Para fazê-lo, selecione a freqüência de execução da tarefa no menu suspenso e ajuste as configurações da programação na parte inferior da janela.

Etapa 6. Concluindo a criação de uma tarefa

A última janela do assistente informará que você foi bem-sucedido na criação de uma tarefa.

20.2.2.2. Criando tarefas em grupo

Para criar uma tarefa em grupo, execute as seguintes etapas:

1. Selecione o grupo para o qual deseja criar uma tarefa na árvore do console.
2. Selecione a pasta **Tarefas** (veja a Figura 106), abra o menu de contexto e selecione o comando **Criar→Tarefa** ou use o mesmo comando no menu **Ação**. O assistente para criação de tarefas será iniciado, de maneira semelhante ao assistente para criação de tarefas locais (para saber mais, consulte 20.2.2.1 na p. 312). Siga suas instruções.

Quando o assistente for concluído, a tarefa será adicionada à pasta **Tarefas** desse grupo e todos os grupos sob ele, e estará visível no painel de resultados.

20.2.2.3. Criando tarefas globais

Para criar uma tarefa global, execute as seguintes etapas:

1. Selecione o nó **Tarefas globais** na árvore do console (veja a Figura 106), abra o menu de contexto e selecione o comando **Criar→Tarefa** ou use o mesmo comando no menu **Ação**.
2. O assistente para criação de tarefas será iniciado, de maneira semelhante ao assistente para criação de tarefas locais (para saber mais, consulte 20.2.2.1 na p. 312). A exceção é que existe um estágio para a criação de uma lista de computadores cliente da rede para os quais a tarefa global está sendo criada.

3. Selecione da rede os computadores que executarão a tarefa. Você pode selecionar computadores de várias pastas ou selecionar uma pasta inteira (para obter mais detalhes, consulte o Manual do Administrador do Kaspersky Administration Kit 6.0).

As tarefas globais são executadas apenas em um conjunto selecionado de computadores. Se novos computadores cliente forem adicionados a um grupo com computadores para os quais foi criada uma tarefa de instalação remota, essa tarefa não será executada para eles. Crie uma nova tarefa ou faça as alterações correspondentes às configurações da tarefa existente.

Quando o assistente for concluído, uma tarefa global será adicionada a nó **Tarefas globais** da árvore do console e estará visível no painel de resultados.

20.2.3. Configurando tarefas específicas

Para exibir e modificar as configurações de tarefas do computador cliente:

1. Abra a janela de propriedades do computador cliente na guia **Tarefas** (veja a Figura 110).
2. Selecione a tarefa na lista e clique no botão **Propriedades**. Como resultado, será aberta uma janela de configurações de tarefas (veja a Figura 111).

Todas as guias, exceto a guia **Configurações**, são padrão do Kaspersky Administration Kit 6.0. Elas são abordadas mais detalhadamente no Manual do Usuário do Administrador. A guia **Configurações** contém configurações específicas do Kaspersky Anti-Virus. O conteúdo dessa guia varia, dependendo do tipo de tarefa selecionado.

A configuração de tarefas do programa por meio da interface do Kaspersky Administration Kit é semelhante à configuração pela interface do Kaspersky Anti-Virus local, com exceção das configurações específicas de cada usuário, como as listas branca e negra do Anti-Spam. Consulte Capítulo 7 – Capítulo 16 nas pp. 92 – 218 desse Manual do Usuário para obter uma descrição mais detalhada da configuração de tarefas.

Se tiver sido criada uma diretiva para o aplicativo (consulte a seção 20.3 na p. 316) que bloqueia a redefinição de algumas configurações, elas não poderão ser editadas ao configurar as tarefas.

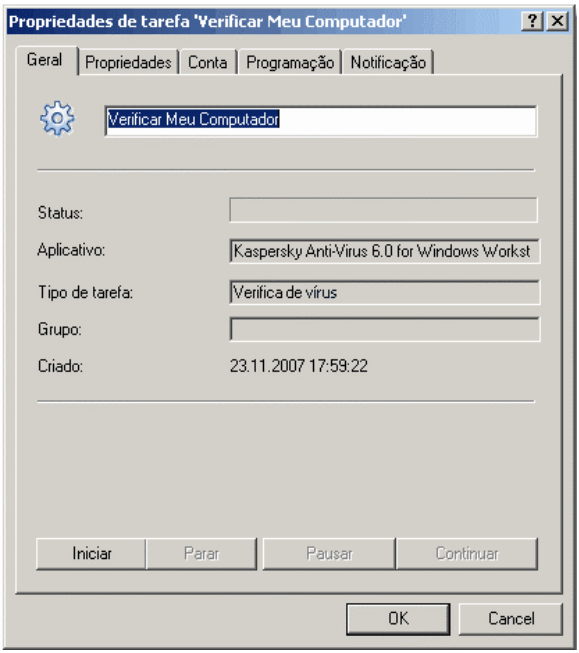


Figura 111. Configurando tarefas

20.3. Gerenciado diretivas

A configuração de diretivas permite aplicar configurações universais a aplicativos e tarefas nos computadores cliente que pertencem a um único grupo de rede.

Esta seção inclui informações sobre a criação e configuração de diretivas do Kaspersky Anti-Virus 6.0 for Windows Workstations. Para obter mais detalhes sobre o conceito de gerenciamento de tarefas usando o Kaspersky Administration Kit 6.0, consulte o Manual do Administrador do programa.

20.3.1. Criando diretivas

Para criar uma diretiva para o Kaspersky Anti-Virus, execute as seguintes etapas:

1. Na pasta **Grupos** (veja a Figura 106), selecione o grupo de computadores para os quais você deseja criar uma diretiva.

2. Selecione a pasta **Diretivas** que pertence ao grupo selecionado, abra o menu de contexto e use o comando **Criar→Diretiva**. Uma janela Criar nova diretiva aparecerá. As diretivas são criadas em um assistente que consiste em uma série de janelas ou etapas nas quais você pode navegar usando os botões **Voltar** e **Avançar**. Encerre o assistente pressionando **Concluir**. O botão **Cancelar** interromperá o Assistente a qualquer momento.

Durante cada etapa da criação de uma diretiva, as configurações inseridas podem ser bloqueadas com o botão . Se o cadeado no botão estiver fechado, no futuro os valores atribuídos pela diretiva criada serão usados ao usar a diretiva em computadores cliente.

Etapa 1. Inserindo dados gerais na diretiva

A primeira etapa do assistente é introdutória. Nela, especifique o nome da diretiva (o campo **Nome**). Na segunda janela, selecione **Kaspersky Anti-Virus 6.0 for Windows Workstations** no menu suspenso **Nome do aplicativo**. Se desejar que as configurações da diretiva entrem em vigor imediatamente após sua criação, marque **Tornar diretiva ativa**.

Etapa 2. Selecionando um status de diretiva

Esta janela solicitará que você especifique o status da diretiva. Para fazê-lo, mova o controle deslizante para a posição desejada: diretiva ativa ou diretiva inativa.

Várias diretivas podem ser criadas em um grupo para um aplicativo, mas apenas uma delas pode ser a diretiva (ativa) atual.

Etapa 3. Selecionando e configurando os componentes de proteção

Neste estágio, você pode habilitar, desabilitar e configurar os componentes de proteção que serão usados na diretiva.

Por padrão, todos os componentes de proteção estão habilitados. Para desabilitar um componente, desmarque a caixa de seleção ao lado do mesmo. Para fazer o ajuste fino das configurações de proteção ou para configurar o Antivírus de Arquivos, selecione-o na lista e clique no botão **Configurações**.

Etapa 4. Configurando a verificação de vírus

Nesta etapa, você pode definir as configurações que serão usadas pelas tarefas de verificação de vírus.

Na seção **Nível de segurança**, selecione uma das três opções de segurança predefinidas (consulte a seção 14.4.1 na p. 204). Clique no botão **Configurações** para fazer o ajuste fino do nível selecionado. Para restaurar as configurações do nível **Recomendado**, clique no botão **Padrão**.

Na seção **Ação**, especifique a ação que o Anti-Virus deverá executar quando um objeto perigoso for detectado (consulte a 14.4.4 na p. 208).

Etapa 5. Configurando a atualização

Nesta janela, configure o recurso de distribuição de atualizações do Kaspersky Anti-Virus.

Na seção **Configurações de atualização**, especifique o que deve ser atualizado (consulte a seção 16.4.2 na p. 225). Na janela que é aberta ao clicar no botão **Configurações**, atribua as configurações de rede local (consulte a 16.4.3 na p. 227) e especifique a fonte de atualização (consulte a 16.4.1 na p. 222).

Na seção **Ações após a atualização**, habilite/desabilite a verificação da Quarentena após receber um novo pacote de atualizações (consulte a 16.4.4 na p. 229).

Etapa 6. Impondo a diretiva

Nesta etapa, selecione um método para impor a diretiva nos computadores cliente do grupo (para obter mais detalhes, consulte o Manual do Administrador do Kaspersky Administration Kit 6.0).

Etapa 7. Concluindo a criação de uma diretiva

A última janela do assistente informa que você foi bem-sucedido na criação de uma diretiva.

Ao concluir o assistente, a diretiva do Kaspersky Anti-Virus será adicionada à pasta **Diretivas** (veja a Figura 106) do grupo correspondente e estará visível no painel de resultados.

Você pode editar as configurações da diretiva criada e definir restrições para a modificação de suas configurações usando o botão  para cada grupo de configurações. Um usuário no computador cliente não poderá alterar as configurações, se elas estiverem bloqueadas dessa forma. A diretiva será

aplicada aos computadores cliente na primeira vez que eles sincronizarem com o servidor.

Você pode copiar ou mover as diretivas de um grupo para outro e excluí-las usando os comandos padrão **Copiar**/**Colar**, **Recortar**/**Colar** e **Excluir** no menu de contexto ou no menu Ação.

20.3.2. Exibindo e editando configurações de diretivas

No estágio de edição, você pode modificar a diretiva e bloquear a modificação de configurações em diretivas de grupos aninhados e em configurações de aplicativos e tarefas.

Para exibir e editar as configurações de diretivas:

1. Selecione o grupo de computadores para os quais as configurações devem ser editadas na árvore do console, na pasta **Grupos**.
2. Selecione a pasta **Diretivas** que pertence a esse grupo (veja a Figura 106). Ao fazê-lo, o painel de resultados exibirá todas as diretivas criadas para o grupo.
3. Selecione a diretiva desejada na lista de diretivas do **Kaspersky Anti-Virus 6.0 for Windows Workstations** (o nome do aplicativo está especificado no campo **Aplicativo**).
4. Selecione o comando **Propriedades** no menu de contexto da diretiva selecionada. Uma janela de configurações da diretiva será aberta para o aplicativo, com várias guias (veja a Figura 112).

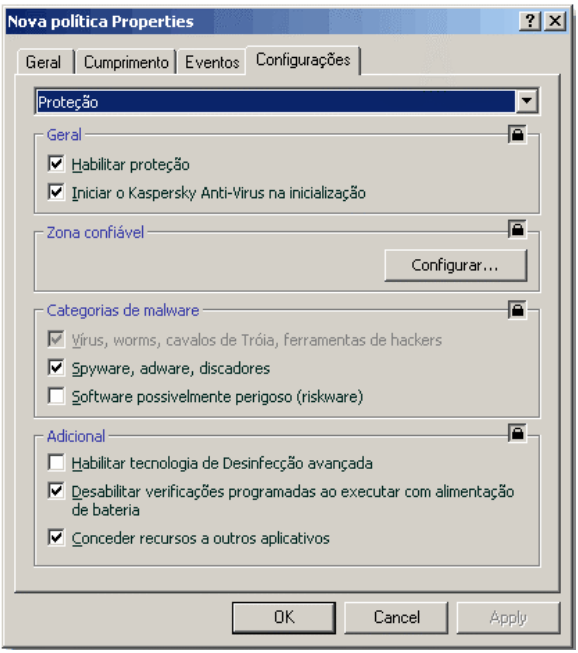


Figura 112. Configurando a diretiva

Todas as guias, exceto **Configurações**, são padrão do Kaspersky Administration Kit (para obter mais detalhes, consulte o Manual do Administrador do programa).

A guia **Configurações** contém as configurações de diretivas do Kaspersky Anti-Virus 6.0. As configurações de diretivas incluem configurações do programa (consulte a seção 20.1.2 na p. 307) e as configurações de tarefas (consulte a seção 20.1.3 na p. 309).

Para definir as configurações, selecione o valor desejado no menu suspenso.

CAPÍTULO 21. PERGUNTAS FREQÜENTES

Este capítulo é dedicado às perguntas mais freqüentes dos usuários com relação à instalação, configuração e ao funcionamento do Kaspersky Anti-Virus for Windows Workstations; aqui, tentaremos respondê-las detalhadamente.

Pergunta: É possível usar o Kaspersky Anti-Virus for Windows Workstations 6.0 com produtos antivírus de outros fornecedores?

Não. É recomendável desinstalar os produtos antivírus de outros fornecedores antes de instalar o Kaspersky Anti-Virus for Windows Workstations para evitar conflitos de software.

Pergunta: O Kaspersky Anti-Virus for Windows Workstations não verifica novamente os arquivos que já foram verificados. Por quê?

É verdade. O Kaspersky Anti-Virus for Windows Workstations não verifica novamente os arquivos que não foram alterados desde a última verificação.

Isso é possível devido às novas tecnologias iChecker e iStream. A tecnologia é implementada no programa usando um banco de dados e um armazenamento de somas de verificação de arquivos em fluxos NTFS alternados.

Pergunta: Por que é necessário um arquivo de chave de licença? O Kaspersky Anti-Virus for Windows Workstations funcionará sem ele?

O Kaspersky Anti-Virus for Windows Workstations será executado sem uma chave de licença, mas você não poderá acessar a Atualização e o Suporte Técnico.

Se ainda não tiver decidido adquirir o Kaspersky Anti-Virus for Windows Workstations, 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 for Windows Workstations, 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 for Windows Workstations 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 for Windows Workstations.
4. Use o link Configurações na janela principal e selecione a seção **Proteção** na janela de configurações do programa.
5. Desmarque **Iniciar o Kaspersky Anti-Virus 6.0 na inicialização** e clique em **OK**.

Reinicie o sistema operacional no modo normal.

Depois disso, entre em contato com o Serviço de Suporte Técnico através do site corporativo da Kaspersky Lab (**Serviços → Suporte Técnico**). Descreva o problema detalhadamente e as situações nas quais ele ocorre.

Verifique se você anexou um arquivo com um arquivo de despejo completo do sistema operacional Microsoft Windows à pergunta. Para criar este arquivo, faça o seguinte:

1. Clique com o botão direito do mouse em **Meu Computador** e selecione o item **Propriedades** no menu de atalho que será aberto.
2. Selecione a guia **Avançado** na janela **Propriedades do sistema** e pressione o botão **Configurações** na seção **Inicialização e recuperação**.
3. Selecione a opção **Despejo de memória completo** na lista suspensa da seção **Gravando informações de depuração**, na janela **Inicialização e recuperação**.
4. 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.
5. Reproduza o problema relacionado com o funcionamento do Kaspersky Anti-Virus for Windows Workstations.
6. 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 extensões usados nas configurações do Kaspersky Anti-Virus for Windows Workstations; também são fornecidas informações sobre as configurações no arquivo setup.ini, que é usado ao instalar o programa no modo oculto.

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

*dot** – um modelo de documento do Microsoft Word, como *dot* – um modelo de documento do Microsoft Word, *dotx* – um modelo de documento do Microsoft Word 2007, *dotm* – um modelo de documento do Microsoft 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* - extensão do Microsoft Office Excel, *xlc* - diagrama, *xlt* - modelos de documento. *xlsx* – uma pasta de trabalho do Microsoft Excel 2007, *xltm* – uma pasta de trabalho do Microsoft Excel 2007 com suporte de macro, *xlsb* – um Microsoft Excel 2007 em formato binário (não XML), *xltx* – um modelo do Microsoft Excel 2007, *xlsm* – um modelo do Microsoft Excel 2007 com suporte de macro, *xlam* – um plug-in do Microsoft Excel 2007 com suporte de macro.

*pp** – documentos e arquivos do Microsoft Office Excel, como: *xla* - extensão do Microsoft Office Excel, *xlc* - diagrama, *xlt* - modelos de documento. *xlsx* – uma pasta de trabalho do Microsoft Excel 2007, *xltm* – uma pasta de trabalho do Microsoft Excel 2007 com suporte de macro, *xlsb* – um Microsoft Excel 2007 em formato binário (não XML), *xltx* – um modelo do Microsoft Excel 2007, *xlsm* – um modelo do Microsoft Excel 2007 com suporte de macro, *xlam* – um plug-in do Microsoft Excel 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. Possíveis máscaras de exclusão de arquivos

Vamos examinar alguns exemplos de máscaras que podem ser usadas na criação de listas de exclusão de arquivos:

- 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*
- Máscaras com caminhos de arquivos absolutos:
  - **C:\dir*.***, **C:\dir*** ou **C:\dir** - todos os arquivos na pasta *C:\dir*
  - **C:\dir*.exe** – todos os arquivos da pasta *C:\dir* com extensão .exe
  - **C:\dir*.ex?** – todos os arquivos com extensão .ex? da pasta *C:\dir*, onde ? representa qualquer caractere
  - **C:\dir\teste** - somente o arquivo *C:\dir\teste*
  - Se não desejar que o programa verifique os arquivos nas subpastas dessa pasta, desmarque **Incluir subpastas** ao criar a máscara.
- 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 veredito 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 escolha de um veredito 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. Possíveis máscaras de exclusão de ameaças

Ao adicionar ameaças com um determinado veredito da classificação da Enciclopédia de Vírus como exclusões, você pode especificar:

- o nome completo da ameaça, como aparece na Enciclopédia de Vírus (em inglês), em http://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.

A.4. Visão geral das configurações em *setup.ini*

O arquivo *setup.ini*, localizado na pasta de instalação do Kaspersky Anti-Virus, é usado ao instalar o programa no modo não interativo do prompt de comando (consulte a seção 3.3 na p. 48) ou usando o Editor de Objeto de Diretiva de Grupo (consulte a seção 3.4 na p. 49). O arquivo contém as seguintes configurações:

[Setup] – configurações gerais de instalação do programa.

InstallDir=<caminho da pasta de instalação do programa>.

Reboot=yes|no – se o computador deve ser reiniciado depois da instalação do programa (não reinicia por padrão).

SelfProtection=yes|no – se o Kaspersky Anti-Virus deve habilitar a Autodefesa durante a instalação (habilitado por padrão).

[Components] – seleciona os componentes a serem instalados. Se nenhum componente estiver especificado, todos serão instalados. Se nenhum componente estiver especificado, aqueles que não estiverem listados não serão instalados.

FileMonitor=yes|no – instala o Antivírus de Arquivos

MailMonitor=yes|no – instala o Antivírus de E-Mail

WebMonitor=yes|no – instala o Antivírus da Web

ProactiveDefence=yes|no – instala a Defesa Proativa

AntiSpy=yes|no – instala o Anti-Spy

AntiHacker=yes|no – instala o Anti-Hacker

AntiSpam=yes|no – instala o Anti-Spam

[Tasks] – habilita as tarefas do Kaspersky Anti-Virus, caso nenhuma tarefa seja especificada; todas as tarefas serão executadas após a instalação. Se nenhuma tarefa for especificadas, todas as tarefas que não estão listadas serão desabilitadas.

ScanMyComputer=yes|no – tarefa de verificação completa do computador

ScanStartup=yes|no – tarefa de verificação dos objetos de inicialização

ScanCritical=yes|no – tarefa de verificação das áreas críticas

Updater=yes|no – tarefa de atualização das assinaturas de ameaças e módulos do programa

Em vez do valor **yes**, você pode usar os valores **1**, **on**, **enable** ou **enabled** e, em vez do valor **no**, pode usar **0**, **off**, **disable** ou **disabled** .

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 atual de vírus na bandeja do sistema
- 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 Anti-Virus® 7.0

O Kaspersky Anti-Virus 7.0 foi projetado para proteger PCs contra software mal-intencionado, combinando métodos convencionais de proteção antivírus e novas tecnologias proativas.

O programa oferece verificações antivírus complexas, incluindo:

- 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, bem como a desinfecção de bancos de dados de e-mail.
- Verificação antivírus em tempo real do tráfego da Internet transferido via HTTP.
- Verificação antivírus de arquivos, pastas ou unidades individuais. Além disso, uma tarefa de verificação predefinida pode ser usada para iniciar a análise de antivírus exclusivamente em áreas críticas do sistema operacional e em objetos de inicialização do Microsoft Windows.

A proteção proativa oferece os seguintes recursos:

- **Controle de alterações no sistema de arquivos**. O programa permite que os usuários criem uma lista de aplicativos que serão controlados por componente. Isso ajuda a proteger a integridade dos aplicativos contra a influência de software mal-intencionado.
- **Monitoramento de processos na memória RAM**. O Kaspersky Anti-Virus 7.0 notifica oportunamente os usuários sempre que detecta

processos perigosos, suspeitos ou ocultos, ou quando ocorrem alterações não autorizadas de processos ativos.

- **Monitoramento de alterações no Registro do sistema operacional** devido ao controle interno do Registro do sistema.
- **Monitoramento de processos ocultos** ajuda a proteger de códigos mal-intencionados escondidos no sistema operacional utilizando tecnologias de rootkit.
- **Analisador heurístico**. Ao verificar um programa, o analisador emula sua execução e registra toda a atividade suspeita, como a abertura ou gravação de um arquivo, a interrupção de interceptações de vetores etc. É tomada uma decisão com base neste procedimento com relação à possível infecção do programa por um vírus. A emulação ocorre em um ambiente virtual isolado que protege o computador contra infecções.
- **Restauração do sistema** depois de ataques de malware, registrando todas as alterações do Registro e do sistema de arquivos do computador e revertendo-os conforme o desejo do usuário.

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, como 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 módulo **Controle de Privacidade** mantém suas informações confidenciais protegidas do acesso e da transmissão não autorizados. O **Controle dos Pais é** um componente do Kaspersky Internet Security que monitora o acesso do usuário à Internet.

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 centralizadas;*
- *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 Work Space 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 centralizada;
- *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 todos os e-mails* no Microsoft Exchange Server quanto à presença de vírus, 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 do programa 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	WWW: http://www.kaspersky.com http://www.viruslist.com E-mail: info@kaspersky.com

APÊNDICE C. CONTRATO DE LICENÇA

Contrato de Licença do Usuário Final Padrão

AVISO A TODOS OS USUÁRIOS: LEIA CUIDADOSAMENTE O SEGUINTE CONTRATO LEGAL ("CONTRATO") RELATIVO À LICENÇA DO KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS WORKSTATIONS (“SOFTWARE”), PRODUZIDO PELA KASPERSKY LAB ("KASPERSKY LAB").

SE VOCÊ ADQUIRIU ESTE SOFTWARE PELA INTERNET, CLICANDO NO BOTÃO ACEITAR, VOCÊ (SEJA UM INDIVÍDUO OU UMA ENTIDADE ÚNICA) CONCORDA EM LIMITAR-SE E TORNAR-SE PARTE NESTE CONTRATO. SE NÃO CONCORDAR COM TODOS OS TERMOS DO PRESENTE CONTRATO, CLIQUE NO BOTÃO QUE INDICA QUE NÃO ACEITA OS TERMOS DO CONTRATO E NÃO INSTALE O SOFTWARE.

SE VOCÊ ADQUIRIU ESTE SOFTWARE EM UMA MÍDIA FÍSICA, AO QUEBRAR O LACRE DO CD, VOCÊ (SEJA UM INDIVÍDUO OU UMA ENTIDADE ÚNICA) CONCORDA EM LIMITAR-SE E TORNAR-SE PARTE NESTE CONTRATO. SE NÃO CONCORDA COM TODOS OS TERMOS DESTE CONTRATO, NÃO QUEBRE O LACRE DO CD, NÃO FAÇA DOWNLOAD, INSTALE OU USE ESTE SOFTWARE.

DE ACORDO COM A LEGISLAÇÃO RELATIVA AO SOFTWARE DA KASPERSKY DESTINADO A CONSUMIDORES INDIVIDUAIS E COMPRADOS NO SITE DA KASPERSKY LAB OU DE SEUS PARCEIROS, O CLIENTE DEVERÁ TER UM PERÍODO DO CATORZE (14) DIAS ÚTEIS A PARTIR DA ENTREGA DO PRODUTO PARA DEVOLVÊ-LO AO COMERCIANTE PARA TROCA OU REEMBOLSO, DESDE QUE O SOFTWARE ESTEJA SELADO.

COM RELAÇÃO AO SOFTWARE DA KASPERSKY DESTINADO A CONSUMIDORES INDIVIDUAIS NÃO ADQUIRIDO ON-LINE, PELA INTERNET, ESSE SOFTWARE NÃO PODERÁ SER DEVOLVIDO OU TROCADO, EXCETO POR PROVISÕES CONTRÁRIAS DO PARCEIRO QUE COMERCIALIZA O PRODUTO. NESTE CASO, A KASPERSKY LAB NÃO ESTARÁ SUJEITA ÀS CLÁUSULAS DO PARCEIRO.

O DIREITO DE DEVOLUÇÃO E REEMBOLSO SE ESTENDE APENAS AO COMPRADOR ORIGINAL.

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.

1.1 *Uso*. O número de computadores que o Usuário pode proteger com o Software é especificado no Arquivo da chave de licença e indicado na janela "Serviço". O Software não pode ser usado para proteger redes com um número de computadores maior que esse.

1.1.1 O Software está "em uso" em um computador quando está carregado na memória temporária (ou seja, a memória RAM) ou instalado na memória permanente (por exemplo, no disco rígido, no CD-ROM ou em outro dispositivo de armazenamento) desse computador. Esta licença o autoriza a fazer quantas cópias de backup do Software forem necessárias para sua utilização dentro dos termos da lei e unicamente para fins de backup, desde que todas essas cópias contenham todos os avisos sobre propriedade do Software. Você deverá manter registros do número e do local de todas as cópias do Software e da Documentação, e deverá adotar todas as precauções necessárias para proteger o Software de uso ou cópia não autorizados.

1.1.2 O Software protege computadores contra vírus e ataques de rede cujas assinaturas estão nos bancos de dados de assinaturas de ameaças e de ataques de redes disponíveis nos servidores de atualização da Kaspersky Lab.

1.1.3 Se você vender o computador no qual o Software está instalado, deverá verificar se todas as cópias do Software foram excluídas anteriormente.

1.1.4 Você não deverá descompilar, aplicar engenharia reversa, desmontar ou reduzir de qualquer outra forma qualquer parte deste Software a um formato legível, nem permitir que qualquer terceiro o faça. As informações de interface necessárias para obter a interoperabilidade do Software com programas de computador criados independentemente serão fornecidas pela Kaspersky Lab quando solicitado, mediante pagamento dos custos plausíveis e das despesas relativas à busca e ao fornecimento dessas informações. No caso de a Kaspersky Lab o notificar de que não pretende disponibilizar essas informações por qualquer motivo, incluindo custos (sem limitações), deverá ser permitido que você tome as medidas necessárias para conseguir a interoperabilidade, desde que seja feita a engenharia reversa ou descompilação do Software apenas até os limites permitidos pela lei.

1.1.5 Você não poderá fazer correções de erros ou de alguma outra forma modificar, adaptar ou converter o Software, nem criar trabalhos derivados do mesmo, nem permitir que terceiros o copiem (a menos que expressamente permitido pelo presente).

1.1.6 Você não poderá alugar, locar ou emprestar o Software a terceiros, nem transferir ou sublicenciar seus direitos de licença a qualquer outra pessoa.

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

1.1.8 Você não deverá usar este Software em ferramentas automáticas, semi-automáticas ou manuais projetadas para criar assinaturas de vírus, rotinas de detecção de vírus, qualquer outro código ou dados para detecção de código ou dados mal-intencionados.

1.1.9 Remoção de produtos potencialmente nocivos. Você aceita e concorda que, além de detectar software nocivo e mal-intencionado, o Produto também pode identificar, remover e/ou desabilitar produtos potencialmente nocivos, incluindo aqueles considerados ou classificados como Adware, Riskware, Pornware, etc.

2. *Suporte*.

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 compra, desde:

(a) o pagamento dos então atuais encargos relativos ao suporte e:

(b) 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.

(c) 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.

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.

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.

Por "Serviços de Suporte" entendem-se:

- Atualizações a cada hora do banco de dados de antivírus;
- Atualizações do banco de dados de ataques de rede;
- Atualizações do banco de dados de anti-spam;

Atualizações gratuitas de software, incluindo as atualizações de versão;

Suporte técnico pela Internet e pela linha direta de suporte fornecida pelo Fornecedor e/ou Revendedor;

Atualizações de detecção e desinfecção de vírus 24 horas por dia.

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 spams e vírus conhecidos, nem que ocasionalmente o Software não possa relatar erroneamente um vírus em um título não infectado por esse vírus.

(iv) A Kaspersky Lab não garante que este Software ofereça proteção após sua data de expiração (consulte a seção.2 (i))

(v) 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.

(vi) 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.

(vii) 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).