

Kaspersky Mobile Security 9

para SO Android

KASPERSKY **lab**

Guia do Usuário

VERSÃO DO PROGRAMA: 9.0

Prezado usuário,

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

Observação! Este documento é propriedade da Kaspersky Lab ZAO (também referida neste presente documento como Kaspersky Lab): todos os direitos desse documento são reservados pelas leis de direitos autorais da Federação Russa e por tratados internacionais. A reprodução e distribuição ilegal deste documento ou de partes dele, irá resultar em responsabilidade civil, administrativa ou criminal pelas leis aplicáveis.

A reprodução e distribuição de qualquer material em qualquer formato, incluindo sua tradução, só são permitidas com permissão escrita da Kaspersky Lab.

Este documento e as imagens gráficas relacionadas ao mesmo podem ser usados exclusivamente para fins de informação e uso não comercial ou pessoal.

A Kaspersky Lab se reserva o direito de emendar esse documento sem notificação adicional. A versão mais recente deste documento está disponível no site da Kaspersky Lab, em <http://www.kaspersky.com/docs>.

A Kaspersky Lab não será responsável pelo conteúdo, qualidade, relevância ou exatidão dos materiais usados neste documento, cujos direitos são mantidos por terceiros e por danos potenciais ou de fato associados ao uso desses materiais.

Nesse documento, são usadas marcas registradas e de serviço que são propriedade de seus respectivos proprietários.

Data de revisão: 20.01.2011

© 1997-2011 Kaspersky Lab ZAO. Todos os direitos reservados.

<http://brazil.kaspersky.com/>
<http://suporte.kasperskyamericas.com/>

CONTRATO DE LICENÇA DO USUÁRIO FINAL DA KASPERSKY LAB

IMPORTANTE CONVOCAÇÃO PARA TODOS OS USUÁRIOS: LEIA ATENTAMENTE O SEGUINTE CONTRATO ANTES DE COMEÇAR A USAR O SOFTWARE.

AO CLICAR NA TECLA “ACEITAR” NA JANELA DO CONTRATO DE LICENÇA OU ENTRAR NO (S) SÍMBOLO (S) CORRESPONDENTE (S), VOCÊ ACEITA ESTAR VINCULADO NOS TERMOS E CONDIÇÕES DESTE CONTRATO. **TAL ATO SIMBOLIZA A SUA ASSINATURA E VOCÊ ESTARÁ DE ACORDO VINCULADO COM AS OBRIGAÇÕES DESTE CONTRATO E TORNANDO-SE PARTE DO MESMO, CONCORDANDO SER ESTE CONTRATO EXECUTÁVEL DA MESMA FORMA QUE QUALQUER OUTRO CONTRATO POR ESCRITO NEGOCIADO E ASSINADO POR VOCÊ.** CASO NÃO ESTEJA DE ACORDO COM TODOS OS TERMOS E CONDIÇÕES DESTE CONTRATO, CANCELE A INSTALAÇÃO DO SOFTWARE E NÃO INSTALE O SOFTWARE.

APÓS CLICAR NA TECLA ACEITAR NA JANELA DO CONTRATO DE LICENÇA OU ENTRAR NO(S) SÍMBOLO(S) CORRESPONDENTE(S), VOCÊ TEM O DIREITO DE USAR O SOFTWARE DE ACORDO COM OS TERMOS E CONDIÇÕES DESTE CONTRATO.

1. Definições

- 1.1. **Programa** significa o programa de computador, incluindo quaisquer atualizações e materiais relacionados.
- 1.2. **Titular** (proprietário de todos os direitos, seja exclusivo ou não ao programa) significa a Kaspersky Lab ZAO, uma empresa constituída segundo as leis da Federação Russa.
- 1.3. **Computador(s)** significa o equipamento(s) físico, incluindo computadores pessoais, laptops, estações de trabalho, assistentes digitais pessoais, “telefones inteligentes”, aparelhos de mão, ou outros aparelhos eletrônicos para os quais o programa foi projetado e onde o programa será instalado e/ou utilizado.
- 1.4. **Usuário final (Você/Seu)** significa o(s) indivíduo(s) que instalar ou usar o programa em seu próprio nome ou que esteja legalmente usando uma cópia do programa; ou, se o programa está sendo baixado ou instalado em nome de uma organização, como um empregador, “Você” significa ainda a organização para a qual o programa é baixado ou instalado e é neste ato representado que tal organização autorizou a pessoa que aceita este contrato a fazê-lo em seu nome. Para fins deste contrato o termo “organização”, sem limitação, inclui qualquer parceria, sociedade de responsabilidade limitada, corporação, associação, sociedade por ações, custódia e administração de bens ou valores de terceiros, empreendimento conjunto, a organização do trabalho, organização sem personalidade jurídica, ou a autoridade governamental.
- 1.5. **Parceiro(s)** significa organizações ou indivíduo(s), que distribui o programa com base em um contrato e licença do Titular.
- 1.6. **Atualizações** significa todas as atualizações, revisões, correções, melhorias, reparos, modificações, cópias, acréscimos ou pacotes de manutenção, etc.
- 1.7. **Manual do usuário** significa manual do usuário, guia do administrador, livro de referência e materiais explicativos relacionados ou outros materiais.

2. Concessão de licença

- 2.1. O titular concede a você uma licença não-exclusiva para armazenar, carregar, instalar, executar e exibir (“usar”) o programa em um determinado número de computadores, a fim de ajudar a proteger o computador no qual o programa está instalado contra as ameaças descritas no Manual do usuário, de acordo com todos os requisitos técnicos descritos no Manual do usuário e de acordo com os termos e condições do presente Contrato (a “Licença”) e você aceita esta Licença:

Versão de teste. Se você tiver recebido, baixado e/ou instalado uma versão de teste do programa e lhe for concedida uma licença de avaliação para o programa, você poderá usar o programa somente para fins de avaliação e apenas durante o período único de avaliação aplicável, salvo indicação em contrário, a partir da data da instalação inicial. Qualquer uso do programa para outros fins ou para além do período de avaliação aplicável é estritamente proibido.

Programa para vários ambientes; programa para vários idiomas; programa com duas mídias; múltiplas cópias; pacotes. Se você usar diferentes versões do programa ou edições de idioma diferentes do programa, se você receber o programa em várias mídias, se você receber múltiplas cópias do programa ou tiver recebido o programa junto com outro programa, o número total permitido de computadores nos quais todas as versões do programa estão instaladas deve corresponder ao número de computadores especificados nas licenças obtidas pelo titular, a menos que os termos de licenciamento disponham em contrário, cada licença adquirida lhe dá o direito de instalar e usar o programa em um número tal de computadores, conforme especificado nas cláusulas 2.2 e 2.3.

- 2.2. Se o programa foi adquirido em uma mídia física, você tem o direito de usar o programa para a proteção de tal número de computadores, conforme especificado na embalagem do programa ou conforme especificado no contrato adicional.
- 2.3. Se o programa foi adquirido através da internet, você tem o direito de usar o programa para a proteção de tal número de computadores que foram especificados quando você adquiriu a licença do programa ou conforme especificado no contrato adicional.

- 2.4. Você tem o direito de fazer uma cópia do programa apenas para fins de cópia de segurança e apenas para substituir a cópia autorizada caso tal cópia seja perdida, destruída ou torna-se inutilizável. Essa cópia de segurança não pode ser usada para outros fins e deve ser destruída quando você perder o direito de utilizar o programa ou quando a sua licença expirar ou for finalizada por qualquer outro motivo, de acordo com a legislação em vigor no país de sua residência principal ou no país onde você estiver usando o programa.
- 2.5. A partir do momento da ativação do programa ou após a instalação da licença (com exceção de uma versão de teste do programa), você tem o direito de receber os seguintes serviços por um período definido no pacote de programa (se o programa foi adquirido em uma mídia física) ou especificados durante a aquisição (se o programa foi adquirido através da internet):
- Atualizações do programa através da internet quando e de acordo com a publicação do titular em seu website ou através de outros serviços online. Quaisquer atualizações que você possa receber se tornam parte do programa e os termos e condições do presente contrato se aplicam a elas;
 - Assistência técnica através da internet e da linha telefônica de suporte técnico.

3. Ativação e prazo

- 3.1. Se você modificar o computador ou fizer alterações no programa de outros fornecedores instalados nele, o titular pode solicitar que você repita a ativação do programa ou a instalação da licença. O titular reserva-se o direito de usar quaisquer meios e procedimentos de verificação para certificar-se da validade da licença e/ou legalidade de uma cópia do programa instalado e/ou utilizado no seu computador.
- 3.2. Se o programa foi adquirido em uma mídia física, o programa pode ser utilizado, mediante a sua aceitação do presente contrato, pelo período que está especificado na embalagem, com início a partir da aceitação do presente contrato ou conforme especificado no contrato adicional.
- 3.3. Se o programa foi adquirido através da internet, o programa pode ser utilizado, mediante a sua aceitação do presente contrato, pelo período especificado durante a aquisição ou conforme especificado no contrato adicional.
- 3.4. Você tem o direito de usar uma versão de teste do programa, tal como previsto na cláusula 2.1, sem qualquer custo pelo período único (7 dias) de avaliação aplicável a partir do momento da ativação do programa de acordo com este contrato, *desde que* a versão de teste não lhe dê o direito de suporte técnico e atualizações através da internet e linha telefônica de suporte técnico. Se o titular definir outra duração para o período único de avaliação aplicável, você será informado através de notificação.
- 3.5. Sua licença de uso desse programa estará limitada ao período de tempo especificado nas cláusulas 3.2 e 3.3 (caso pertinente) e o restante do período pode ser visto através dos meios descritos no Manual do usuário.
- 3.6. Se você tiver adquirido o programa que se destina a ser utilizado em mais de um computador, então a sua licença de uso do programa é limitada ao período de tempo a partir da data de ativação do programa ou de instalação da licença no primeiro computador.
- 3.7. Sem prejuízo de quaisquer outras medidas de direito ou de equidade que o titular possa ter, em caso de qualquer violação de qualquer dos termos e condições deste contrato, o titular tem, a qualquer momento, sem aviso prévio ao usuário, o direito de rescindir esta licença de uso do programa, sem o reembolso do preço de compra ou qualquer parte dele.
- 3.8. Você concorda que, ao utilizar o programa ou qualquer relatório ou informação obtida como resultado da utilização deste programa, irá cumprir com todas as leis e regulamentos internacionais, nacionais, estaduais, regionais e locais, incluindo, sem limitação, privacidade, direitos autorais, controle de exportação e obscenidade.
- 3.9. Exceto quando expressamente permitido neste contrato, você não pode transferir ou atribuir nenhum dos seus direitos concedidos ao abrigo do presente contrato ou qualquer das suas obrigações nos termos do presente regulamento.
- 3.10. Se você tiver adquirido o programa com o código de ativação válido para a localização de idioma do programa da região em que foi adquirido pelo titular ou seus parceiros, você não pode ativar o programa com a aplicação do código de ativação destinado à localização de outras línguas.
- 3.11. Se você adquiriu o programa destinado à operação com determinadas operadoras de telecomunicações, esse programa poderá ser utilizado apenas para operação da operadora especificada no momento da aquisição.
- 3.12. Em caso das restrições previstas nas cláusulas 3.10 e 3.11, a informação sobre estas restrições é indicada na embalagem e/ou no website do titular e/ou seus parceiros.

4. Suporte técnico

O suporte técnico descrito na cláusula 2.5 do presente contrato está previsto para você quando a versão mais recente do programa é instalada (com exceção de uma versão de teste do programa).

Serviço de suporte técnico: <http://support.kaspersky.com>

5. Limitações

- 5.1. Você não deve imitar, clonar, alugar, emprestar, arrendar, vender, modificar, descompilar, fazer engenharia reversa ou desmontar o programa, criar produtos derivados baseados no programa ou em qualquer parte dele com exceção exclusiva de um direito irrenunciável concedido a você pela legislação aplicável, e você, por outro lado, não poderá reduzir qualquer parte do programa a um formato legível ou transferir o programa licenciado, ou qualquer subconjunto do programa licenciado, nem permitir que terceiros o façam, salvo na medida em que a restrição acima é expressamente proibida pela legislação aplicável. Nem o código binário ou fonte do programa podem ser usados e engenharia reversa não pode ser feita para recriar o algoritmo do programa, que é proprietário. Todos os direitos não expressamente concedidos aqui são reservados pelo titular e/ou seus fornecedores, conforme aplicável. Qualquer uso não autorizado do programa deve resultar na rescisão imediata e automática do presente contrato e dessa licença concedida por este instrumento e pode resultar em processo criminal e/ou cível contra o usuário.
- 5.2. Você não poderá transferir os direitos de utilização do programa a terceiros, exceto conforme estabelecido no contrato adicional.
- 5.3. Você não poderá fornecer o código de ativação e/ou arquivo de chave de licença a terceiros ou permitir a terceiros o acesso ao código de ativação e/ou chave de licença que são considerados dados confidenciais do titular e você deve ter cuidado razoável em proteger o código de ativação e/ou chave de licença em sigilo, posto que você pode transferir o código de ativação e/ou chave de licença para terceiros, conforme estabelecido no contrato adicional.
- 5.4. Você não poderá alugar, arrendar ou emprestar o programa a terceiros.
- 5.5. Você não poderá usar o programa para a criação de dados ou programa utilizado para a detecção, bloqueio ou tratamento de ameaças descritos no manual do usuário.
- 5.6. O titular tem o direito de bloquear o arquivo de chave ou rescindir sua licença de uso do programa no caso de você violar qualquer dos termos e condições deste contrato, sem qualquer reembolso para você.
- 5.7. Se você estiver usando a versão de teste do programa, você não tem o direito de receber o suporte técnico especificado na cláusula 4 do presente contrato e você não tem o direito de transferir a licença ou o direito de uso do programa para terceiros.

6. Garantia limitada e exoneração

- 6.1. O titular garante que o programa será executado substancialmente de acordo com as especificações e as descrições estabelecidas no manual do usuário; *todavia*, tal garantia limitada não se aplica ao seguinte: (w) as deficiências e violação relacionada ao seu computador para as quais o titular expressamente se isenta de qualquer responsabilidade de garantia; (x) mau funcionamento, defeitos, ou avarias resultantes de má utilização; abuso; acidente; negligência; instalação incorreta; operação ou manutenção; roubo; vandalismo; atos fortuitos ou de força maior; atos de terrorismo; falhas de energia ou ondas; casualidades; alteração, modificação não-autorizada, ou reparos por qualquer outra parte que não o titular; ou quaisquer terceiros ou suas ações ou causas além do controle razoável da parte do titular; (y) qualquer defeito não mencionado por você ao titular logo que possível após o aparecimento do defeito pela primeira vez; e (z) incompatibilidade causada pelo hardware e/ou componentes de programas instalados em seu computador.
- 6.2. Você reconhece, aceita e concorda que nenhum programa está livre de erros e é recomendado o uso de cópia de segurança do computador com a frequência e a confiabilidade adequada para você.
- 6.3. Você reconhece, aceita e concorda que o titular do direito não é responsável por exclusão de dados autorizada por você. Os dados mencionados podem incluir qualquer informação pessoal ou confidencial.
- 6.4. O titular não oferece qualquer garantia de que o programa irá funcionar corretamente em caso de violação dos termos descritos no manual do usuário ou no presente contrato.
- 6.5. O titular não garante que o programa irá funcionar corretamente se você não baixar regularmente as atualizações especificadas na cláusula 2.5 do presente contrato.
- 6.6. O titular não garante a proteção contra as ameaças descritas no manual do usuário após a expiração do período especificado nas cláusulas 3.2 e 3.3 do presente contrato ou após a licença para uso do programa ter sido finalizada por qualquer motivo.
- 6.7. O PROGRAMA É FORNECIDO “COMO ESTÁ” E O TITULAR NÃO FAZ NENHUMA DECLARAÇÃO E NÃO DÁ NENHUMA GARANTIA QUANTO A SUA UTILIZAÇÃO OU DESEMPENHO. SALVO QUALQUER GARANTIA, CONDIÇÃO, DECLARAÇÃO OU TERMO, CUJA EXTENSÃO NÃO POSSA SER EXCLUÍDA OU LIMITADA PELA LEGISLAÇÃO APLICÁVEL, O TITULAR E SEUS PARCEIROS NÃO EMITEM QUALQUER GARANTIA, CONDIÇÃO, DECLARAÇÃO, OU TERMO (EXPRESSO OU IMPLICITAMENTE, SEJAM ELES ESTATUTÁRIOS, JUDICIÁRIOS, ALFANDEGÁRIOS, POR USO OU DE OUTRO TIPO) QUANTO A QUALQUER ASSUNTO, INCLUINDO, ENTRE OUTROS, A NÃO VIOLAÇÃO DE DIREITOS DE TERCEIROS, A CAPACIDADE DE COMERCIALIZAÇÃO, A QUALIDADE SATISFATÓRIA, A INTEGRAÇÃO, OU A APLICAÇÃO PARA UMA FINALIDADE PARTICULAR. VOCÊ ASSUME TODOS OS DEFEITOS E TODO O RISCO DE DESEMPENHO E RESPONSABILIDADE PELA ESCOLHA DO PROGRAMA PARA ATINGIR OS RESULTADOS PRETENDIDOS, BEM COMO PELA INSTALAÇÃO, PELO USO, E PELOS RESULTADOS OBTIDOS COM ESSE PROGRAMA. SEM LIMITAR AS DISPOSIÇÕES ANTERIORES, O TITULAR NÃO FAZ NENHUMA DECLARAÇÃO E NÃO DÁ NENHUMA GARANTIA DE QUE O PROGRAMA ESTARÁ LIVRE DE

ERROS OU DE INTERRUPTÕES OU OUTRAS FALHAS, OU QUE O PROGRAMA IRÁ SATISFAZER QUALQUER OU TODAS AS SUAS NECESSIDADES, DIVULGADAS OU NÃO AO TITULAR.

7. **Exclusão e limitação de responsabilidade**

AO MÁXIMO PERMITIDO PELA LEI APLICÁVEL, EM NENHUMA HIPÓTESE, O TITULAR OU SEUS PARCEIROS SERÃO RESPONSÁVEIS POR QUAISQUER DANOS ESPECIAIS, INCIDENTAIS, PUNITIVOS, INDIRETOS OU CONSEQUENTES (INCLUINDO, MAS NÃO SE LIMITANDO A, DANOS POR PERDA DE LUCROS OU DE INFORMAÇÕES CONFIDENCIAIS OU OUTRAS INFORMAÇÕES, POR INTERRUPTÃO DE NEGÓCIOS, PERDA DE PRIVACIDADE, POR CORRUPÇÃO, DANOS E PERDA DE DADOS OU PROGRAMAS, POR INCUMPRIMENTO DE QUALQUER OBRIGAÇÃO, (INCLUINDO QUALQUER OBRIGAÇÃO LEGAL, DEVER DE BOA-FÉ OU DEVER DE CUIDADO RAZOÁVEL, POR NEGLIGÊNCIA, POR PERDAS ECONÔMICAS, E POR QUALQUER OUTRA PERDA PECUNIÁRIA OU DE QUALQUER OUTRO TIPO) DECORRENTES OU DE QUALQUER FORMA RELACIONADA COM O USO DE OU INCAPACIDADE DE USAR O PROGRAMA, O FORNECIMENTO DE OU FALHA NO FORNECIMENTO DE ASSISTÊNCIA OU OUTROS SERVIÇOS, INFORMAÇÕES, PROGRAMA E CONTEÚDO RELACIONADO COM O PROGRAMA OU OUTRA FORMA RESULTANTES DO USO DO PROGRAMA, OU DE OUTRA FORMA SOB OU EM CONECÇÃO COM QUALQUER DISPOSIÇÃO DO PRESENTE CONTRATO, RESULTANTES DE QUALQUER VIOLAÇÃO DO CONTRATO OU UM ATO ILÍCITO (INCLUINDO NEGLIGÊNCIA, DECLARAÇÕES FALSAS, QUALQUER ESTRITA OBRIGAÇÃO DE RESPONSABILIDADE OU DIREITO), OU QUALQUER VIOLAÇÃO DE OBRIGAÇÃO LEGAL OU QUALQUER VIOLAÇÃO DE GARANTIA DO TITULAR OU QUALQUER DE SEUS PARCEIROS, MESMO QUE O TITULAR OU QUALQUER PARCEIRO TENHA SIDO AVISADO DA POSSIBILIDADE DE TAIS DANOS.

VOCÊ CONCORDA QUE, NA HIPÓTESE DO TITULAR E/OU SEUS PARCEIROS SEREM CONSIDERADOS RESPONÁVEIS, A RESPONSABILIDADE DO TITULAR E/OU SEUS PARCEIROS DEVE SER LIMITADA PELOS CUSTOS DO PROGRAMA. EM NENHUM CASO, A RESPONSABILIDADE DO TITULAR E/OU SEUS PARCEIROS, EXCEDERÁ AS TAXAS PAGAS PELO PROGRAMA AO TITULAR OU O PARCEIRO (COMO APLICÁVEL).

NADA NO PRESENTE CONTRATO EXCLUI OU LIMITA QUALQUER RECLAMAÇÃO DE MORTE E DANOS PESSOAIS. ALÉM DISSO, NA HIPÓTESE DE QUALQUER AVISO DE ISENÇÃO, EXCLUSÃO OU LIMITAÇÃO NESTE CONTRATO NÃO PUDER SER EXCLUÍDA OU LIMITADA DE ACORDO COM A LEI APLICÁVEL, ENTÃO APENAS TAL AVISO DE ISENÇÃO, EXCLUSÃO OU LIMITAÇÃO NÃO SE APLICARÁ A VOCÊ E VOCÊ CONTINUARÁ A SER VINCULADO POR TODOS OS AVISOS DE ISENÇÕES, EXCLUSÕES E LIMITAÇÕES RESTANTES.

8. **GNU e outras licenças de terceiros**

O programa pode incluir alguns outros programas que são licenciados (ou sublicenciados) para o usuário no âmbito da Licença Pública Geral do GNU ou outras licenças similares de programas livres que, entre outros direitos, permitem ao usuário copiar, modificar e redistribuir determinados programas ou partes dos mesmos, e ter acesso ao código fonte ("Software de Código Aberto"). Se essas licenças exigirem que para qualquer programa, distribuído em formato binário executável, o código-fonte também seja disponibilizado a esses usuários, então, o código-fonte deve ser disponibilizado através do envio do pedido ao e-mail source@kaspersky.com ou o código-fonte é fornecido com o programa. Se qualquer licença do software de código aberto exigir que o titular ofereça os direitos de usar, copiar ou modificar um programa de um software de código aberto, que são mais amplos do que os direitos concedidos neste contrato, tais direitos deverão prevalecer sobre os direitos e restrições aqui.

9. **Titularidade da propriedade intelectual**

9.1. Você concorda que o programa e a autoria, sistemas, ideias, métodos de operação, documentação e outras informações contidas no programa, são propriedade intelectual e/ou segredos comerciais valiosos do titular ou de seus parceiros e que o titular e seus parceiros, conforme o caso, são protegidos pela lei civil e penal, e pela lei de direitos autorais, segredos comerciais, marcas registradas e patente da Federação Russa, da União Europeia e dos Estados Unidos, assim como outros países e tratados internacionais. Este contrato não concede a você quaisquer direitos de propriedade intelectual, incluindo qualquer uma das marcas registradas ou marcas de serviço da titular e/ou seus parceiros ("marcas registradas"). Você pode usar as marcas registradas somente para identificar impressões produzidas pelo programa, de acordo com as práticas comerciais, incluindo a identificação do nome do proprietário da marca. Tal utilização de qualquer marca registrada não lhe dá nenhum direito de propriedade na referida marca registrada. O titular e/ou seus parceiros são proprietários e detêm todos os direitos, títulos e interesses relativos ao programa, incluindo, sem limitação, quaisquer correções de erros, melhorias, atualizações ou outras alterações ao programa, seja feita pelo titular ou por terceiros, e todos os direitos autorais, patentes, direitos de segredo comercial, marcas registradas e outros direitos de propriedade intelectual. A posse, instalação ou uso do programa não lhe transfere qualquer direito à propriedade intelectual do programa e você não adquirirá quaisquer direitos ao programa, exceto conforme expressamente estabelecido no presente contrato. Todas as cópias do programa original referidas neste documento devem conter os mesmos avisos de propriedade que aparecem no programa. Exceto conforme disposto neste documento, este contrato não concede a você quaisquer direitos de propriedade intelectual do programa, e você reconhece que a licença, definida a seguir, concedida ao abrigo do presente

contrato, somente lhe fornece um direito de utilização limitada, nos termos e condições do presente contrato. O titular se reserva todos os direitos não expressamente concedidos ao usuário neste contrato.

- 9.2. Você reconhece que o código fonte, código de ativação e/ou arquivo de chave de licença para o programa são propriedade do titular e constituem segredos comerciais do titular. Você concorda em não modificar, adaptar, traduzir, fazer engenharia reversa, descompilar, desmontar ou tentar descobrir o código-fonte do programa de qualquer maneira.
- 9.3. Você concorda em não modificar ou alterar o programa de qualquer maneira. Você não pode remover ou alterar qualquer aviso de direitos autorais ou outros avisos de propriedade em qualquer cópia do programa.

10. Legislação aplicável; arbitragem

Este contrato será regido e interpretado em conformidade com as leis da Federação Russa sem referência a conflitos de leis e princípios. O presente contrato não será regido pelas Nações Unidas sobre Contratos para a Venda Internacional de Mercadorias, cuja aplicação está expressamente excluída. Qualquer controvérsia decorrente da interpretação ou aplicação das cláusulas do presente contrato ou qualquer infração ao mesmo, salvo se resolvida por negociação direta, será resolvida pelo Tribunal Internacional de Arbitragem Comercial da Federação da Rússia na Câmara de Comércio e Indústria em Moscou, da Federação Russa. Qualquer sentença proferida pelo árbitro será final e vinculativa para as partes, e qualquer juízo sobre tal decisão arbitral pode ser executado em qualquer tribunal de jurisdição competente. Nada na presente seção 10 deve impedir uma parte de procurar ou obter a reparação justa de um tribunal de jurisdição competente, quer antes, durante ou depois do processo de arbitragem.

11. Prazo para interposição de recurso

Nenhum recurso, independentemente da forma, decorrente das operações no âmbito do presente contrato, pode ser interposto por qualquer das partes após mais de um (1) ano da causa da ação ter ocorrido, ou for descoberto de ter ocorrido, exceto se uma ação de violação dos direitos de propriedade intelectual for apresentada no prazo máximo legal aplicável.

12. Acordo integral; autonomia das cláusulas; nenhuma renúncia

Este contrato é o acordo completo entre você e o titular, substituindo qualquer outro acordo prévio, propostas, comunicações ou publicidade, oral ou escrita, com relação ao programa ou ao objeto do presente contrato. Você reconhece que leu este contrato, entendeu e aceitou ficar vinculado a esses termos. Se qualquer disposição deste contrato for considerada por um tribunal de jurisdição competente como inválida, nula ou inexecutável por qualquer motivo, no todo ou em parte, tal disposição será interpretada de forma mais restrita que se torna legal e aplicável, e todo o contrato não deixará de ter valor por conta do fato e o restante do contrato continuará em pleno vigor e efeito até o limite máximo permitido por lei ou equidade, preservando, na medida do possível, sua intenção original. Nenhuma renúncia de qualquer cláusula ou condição estabelecida neste documento será válida, salvo se, por escrito e assinado por você e por um representante autorizado do titular, sendo que nenhuma renúncia de qualquer violação de quaisquer disposições deste acordo constitui uma renúncia a qualquer violação prévia, concomitante ou subsequente. A falta do titular em exigir ou impor estrito cumprimento de qualquer disposição do presente contrato ou qualquer direito não deve ser interpretada como uma renúncia a qualquer disposição ou direito.

13. Informação de contato do titular

Se você tiver alguma dúvida sobre este contrato, ou se você desejar contatar o titular, por qualquer motivo, contate o nosso Departamento de serviço ao cliente em:

Kaspersky Lab ZAO, 10 build. 1, 1st Volokolamsky Proezd
 Moscow, 123060
 Russian Federation
 Tel.: +7-495-797-8700
 Fax: +7-495-645-7939
 E-mail: info@kaspersky.com
 Website: www.kaspersky.com

© 2004-2011 Kaspersky Lab ZAO. Todos os direitos reservados. O programa e a documentação que o acompanha são objeto de direitos autorais e protegidos pela legislação de direitos autorais e por tratados internacionais de direitos autorais, bem como por outros tratados e legislações sobre propriedade intelectual.

ÍNDICE

SOBRE ESTE GUIA	11
Neste documento	11
Convenções de documentos	14
FONTES DE DADOS ADICIONAIS	15
Fontes de informação para pesquisa adicional	15
Entrando em contato com o Departamento de Vendas	16
Discussão sobre aplicativos da Kaspersky Lab no fórum da web	16
Entrando em contato com o Grupo de Desenvolvimento de Documentação	16
KASPERSKY MOBILE SECURITY 9	17
Requisitos de hardware e software	18
Kit de distribuição	18
INSTALAÇÃO DO KASPERSKY MOBILE SECURITY 9	19
DESINSTALAÇÃO DO APLICATIVO	20
GUIA RÁPIDO	21
Ativação do aplicativo	21
Ativação da versão comercial	22
Ativação da assinatura do Kaspersky Mobile Security 9	23
Compra de um código de ativação online	23
Ativação da versão de teste	24
Definição do código secreto	24
Ativação da opção de recuperação do código secreto	25
Recuperação do código secreto	25
Inicialização do aplicativo	26
Visualização das informações sobre o aplicativo	26
GERENCIAMENTO DE LICENÇAS	27
Sobre o Contrato de Licença	27
Sobre as licenças do Kaspersky Mobile Security 9	27
Visualização das Informações da Licença	28
Renovação da licença	29
Renovação da licença com o código de ativação	29
Renovação da licença online	30
Renovação da licença através da ativação de uma assinatura	30
Cancelamento da assinatura	31
Renovação da assinatura	31
INTERFACE DO APLICATIVO	32
Janela de status de proteção	32
Widget da tela inicial	33
PROTEÇÃO DO SISTEMA DE ARQUIVOS	34
Sobre a Proteção	34
Ativação/Desativação da Proteção	34
Configuração da área de proteção	35
Seleção da ação a ser executada nos objetos detectados	36

VERIFICAÇÃO DO DISPOSITIVO.....	38
Sobre a verificação do dispositivo	38
Inicialização manual da verificação	38
Início de uma verificação agendada	39
Seleção do tipo de objeto a ser verificado	40
Configuração das verificações do arquivo	41
Seleção da ação a ser executada com os objetos detectados	41
FILTRAGEM DE CHAMADAS E SMS DE ENTRADA	43
Sobre o Filtro de Chamadas e SMS	43
Sobre os modos do Filtro de Chamadas e SMS.....	44
Alteração do modo do Filtro de Chamadas e SMS.....	44
Criação da Lista Negra.....	45
Adição de entradas na Lista Negra.....	45
Edição de entradas na Lista Negra.....	46
Exclusão de entradas da Lista Negra	47
Criação da Lista Branca	47
Adição de entradas na Lista Branca	48
Edição de entradas na Lista Branca	49
Exclusão de entradas da Lista Branca.....	50
Resposta às mensagens de SMS e às chamadas de contatos que não estão na agenda telefônica	50
Resposta às mensagens de SMS de algarismos não numéricos.....	51
Seleção da resposta ao SMS de entrada	52
Seleção da resposta às chamadas de entrada.....	53
Visualização dos registros de log	53
PROTEÇÃO DE DADOS NO CASO DE PERDA OU ROUBO DO DISPOSITIVO	55
Sobre o Anti-Roubo	55
Bloqueio do dispositivo	56
Exclusão dos dados pessoais	57
Criação de uma lista de pastas para excluir	59
Monitoramento da substituição de um cartão SIM no dispositivo	60
Determinação das coordenadas geográficas do dispositivo.....	61
Inicialização das funções do Anti-Roubo de forma remota.....	63
PROTEÇÃO DE PRIVACIDADE	64
Proteção de Privacidade.....	64
Modos de Proteção de Privacidade.....	64
Ativação/Desativação da Proteção de Privacidade	65
Ativação automática da Proteção de Privacidade	65
Ativação remota da Proteção de Privacidade.....	66
Seleção de dados para ocultar: Proteção de Privacidade	68
Criação de uma lista de números privados.....	69
Adição de um número à lista de números privados	69
Edição de um número na lista de números privados	70
Exclusão de um número da lista de números privados.....	70
ATUALIZAÇÃO DOS BANCOS DE DADOS DO APLICATIVO	72
Sobre a atualização dos bancos de dados do aplicativo	72
Início manual das atualizações.....	73
Início das atualizações agendadas.....	73

DEFINIÇÃO DAS CONFIGURAÇÕES ADICIONAIS	74
Alteração do código secreto	74
Exibição de avisos	74
Configuração das notificações sonoras	75
Mensagens na linha de status	75
ENTRANDO EM CONTATO COM O SERVIÇO DE SUPORTE TÉCNICO	77
GLOSSÁRIO	78
KASPERSKY LAB	80
INFORMAÇÕES SOBRE O CÓDIGO DE TERCEIROS	81
Código do programa distribuído	81
ADB	81
ADBWINAPI.DLL	81
ADBWINUSBAPI.DLL	81
Outras informações	83
ÍNDICE ALFABÉTICO	85

SOBRE ESTE GUIA

Este documento é o Guia para instalação, configuração e utilização do Kaspersky Mobile Security 9. O documento foi criado para um público abrangente.

Objetivos do documento:

- ajudar o usuário a instalar o aplicativo em um dispositivo móvel, ativá-lo e otimizar o aplicativo de acordo com suas necessidades;
- oferecer uma pesquisa rápida de informações sobre questões relacionadas ao aplicativo;
- dar informações sobre fontes alternativas de informação sobre o aplicativo e as possibilidades de recebimento de suporte técnico.

NESTA SEÇÃO

Neste documento	11
Convenções de documentos	14

NESTE DOCUMENTO

As seguintes seções estão incluídas no documento:

Fontes de dados adicionais

Esta seção uma descrição de fontes de informação adicionais sobre o aplicativo e os recursos da Internet onde você pode discutir sobre o programa, compartilhar ideias, fazer perguntas e receber respostas.

Kaspersky Mobile Security 9

Esta seção contém uma descrição das opções do aplicativo, assim como breves informações sobre seus componentes individuais e funções principais. A partir desta seção, você pode saber a função do pacote de instalação. A seção contém os requisitos do dispositivo e do programa que o dispositivo móvel deve atender para instalar o Kaspersky Mobile Security 9.

Instalação do Kaspersky Mobile Security 9

Esta seção contém instruções que lhe ajudarão a instalar o aplicativo em um dispositivo móvel.

Desinstalação do aplicativo

Esta seção contém instruções que lhe ajudarão a desinstalar o aplicativo de um dispositivo móvel.

Atualização do aplicativo

Esta seção contém instruções que lhe ajudarão a atualizar a versão anterior do aplicativo.

Guia rápido

Esta seção contém informações sobre como começar a trabalhar com o Kaspersky Mobile Security 9: ativá-lo, definir um código secreto para o aplicativo, ativar a função de recuperação do código secreto, recuperar o código secreto, iniciar o aplicativo, atualizar seus bancos de dados de antivírus e verificar o dispositivo quanto à presença de vírus.

Gerenciamento de licenças

Esta seção contém informações sobre os termos principais usados no contexto de licenciamento do aplicativo. Além disso, a seção apresenta informações sobre como encontrar informações sobre a licença do Kaspersky Mobile Security 9 e sobre a extensão do prazo da sua validade.

Interface do aplicativo

Esta seção inclui informações sobre os elementos principais da interface do Kaspersky Mobile Security 9.

Proteção do sistema de arquivos

Esta seção fornece informações sobre o componente de proteção que evita infecções do sistema de arquivos do seu dispositivo. A seção também descreve como ativar/parar a proteção e ajustar suas configurações de operação.

Verificação do dispositivo

Esta seção informa sobre a verificação do dispositivo por comando, que consegue detectar e remover as ameaças no seu dispositivo. A seção também descreve como iniciar uma verificação do dispositivo, configurar uma verificação automática agendada do sistema de arquivos, selecionar arquivos para verificação e definir a ação que será tomada no aplicativo quando for detectado um objeto malicioso.

Quarentena de objetos malware

Esta seção fornece informações sobre a *quarentena*, uma pasta especial onde são colocados os objetos maliciosos em potencial. Esta seção também descreve como visualizar, restaurar ou excluir os objetos maliciosos encontrados na pasta.

Filtragem de chamadas e SMS de entrada

Esta seção fornece informações sobre o Filtro de Chamadas e SMS que evita chamadas e SMSs indesejados de acordo com as Listas Negra e Branca criadas. A seção também descreve como selecionar o modo no qual o Filtro de Chamadas e SMS verifica as chamadas e SMSs de entrada, como definir as configurações de filtragem adicionais para chamadas e SMSs de entrada e também como criar as Listas Negra e Branca.

Restrição das chamadas e mensagens de SMS de saída. Controle de Pais

A seção apresenta informações sobre o componente Controle de Pais que permite a limitação das chamadas e mensagens de SMS de saída para números definidos. Além disso, a seção descreve como criar uma lista de números permitidos e proibidos e definir as configurações do Controle de Pais.

Proteção de dados no caso de perda ou roubo do dispositivo

Esta seção fornece informações sobre o Anti-Roubo que, no caso de roubo ou perda, bloqueia o acesso não autorizado aos dados salvos no seu dispositivo móvel e facilita encontrar o dispositivo.

Esta seção também especifica como ativar/desativar a função Anti-Roubo, configurar os parâmetros da sua operação e iniciar o Anti-Roubo a partir de outro dispositivo móvel de forma remota.

Proteção de Privacidade

A seção apresenta informações sobre a Proteção de Privacidade que pode ocultar as informações confidenciais do usuário.

Filtragem da atividade de rede. Firewall

Esta seção fornece informações sobre o Firewall que controla as conexões de rede no seu dispositivo. Esta seção descreve como ativar/desativar o Firewall e selecionar o modo requerido para ele.

Criptografia de dados pessoais

Esta seção fornece informações sobre Criptografia que pode criptografar pastas no seu dispositivo. Também descreve o processo de criptografia e descriptografia das pastas selecionadas.

Atualização dos bancos de dados do aplicativo

Esta seção fornece informações sobre atualização dos bancos de dados do aplicativo, que garante proteção atualizada do seu dispositivo. Além disso, esta seção descreve como visualizar as informações sobre os bancos de dados de antivírus instalados, executar a atualização manualmente e configurar a atualização automática dos bancos de dados de antivírus.

Logs do aplicativo

Esta seção apresenta informações sobre logs que registram a operação de todos os componentes e a execução de todas as tarefas (por exemplo, atualizações do banco de dados do aplicativo, verificações de vírus).

Definição das configurações adicionais

Esta seção fornece informações sobre as opções adicionais do Kaspersky Mobile Security 9: como administrar a notificação sonora do aplicativo e verificar a luz de fundo da tela e como ativar/desativar a exibição de dicas, ícone de proteção e janela de status de proteção.

Entrando em contato com o Serviço de Suporte Técnico

Esta seção contém recomendações para entrar em contato com a Kaspersky Lab a fim de obter ajuda a partir do escritório pessoal no website de suporte técnico ou por telefone.

Glossário

Esta seção contém uma lista de termos que são encontrados no documento e sua definição.

Kaspersky Lab

Esta seção fornece informações sobre a Kaspersky Lab ZAO.

Informações sobre o código de terceiros

Esta seção fornece informações sobre o código de terceiros usado no aplicativo.

Índice

Esta seção permite que você encontre rapidamente as informações necessárias no documento.

CONVENÇÕES DE DOCUMENTOS

As convenções do documento descritas na tabela a seguir são usadas neste Guia.

Table 1. Convenções de documentos

TEXTO DE AMOSTRA	DESCRIÇÃO DAS CONVENÇÕES DO DOCUMENTO
Observe o fato de que...	Os avisos estão destacados em vermelho e incluídos em quadros. Os avisos contêm informações importantes sobre, por exemplo, operações no computador onde a segurança é um fator crítico.
Recomenda-se o uso...	As observações estão incluídas em quadros. As observações contêm informações adicionais e de referência.
Exemplo: ...	Os exemplos são apresentados por seção, com um fundo amarelo, e sob o cabeçalho "Exemplo".
<i>Atualização</i> significa...	Os novos termos são marcados em itálico.
ALT+F4	Os nomes das teclas do teclado aparecem com uma fonte em negrito e com letras maiúsculas. Os nomes das teclas com um sinal "mais" indicam o uso de uma combinação de teclas.
Ativar	Os nomes dos elementos da interface, por exemplo, campos de entrada, comandos do menu, botões, etc., estão marcados em negrito.
➔ <i>Para configurar um agendamento de tarefa:</i>	As frases introdutórias da instrução estão marcadas em itálico.
ajuda	Os textos da linha de comando ou os textos das mensagens exibidas na tela utilizam uma fonte especial.
<Endereço IP do seu computador>	As variáveis estão incluídas entre sinais de maior e menor. Ao invés das variáveis, os valores correspondentes são posicionados em cada caso, e os sinais de maior e menor são omitidos.

FONTES DE DADOS ADICIONAIS

Se você tiver quaisquer dúvidas relacionadas à configuração ou utilização do Kaspersky Mobile Security 9, é possível encontrar as respostas usando várias fontes de informação. Você pode escolher a fonte mais adequada de acordo com a importância ou urgência da sua solicitação.

NESTA SEÇÃO

Fontes de informação para pesquisa adicional	15
Entrando em contato com o Departamento de Vendas	16
Discussão sobre aplicativos da Kaspersky Lab no fórum da web	16
Entrando em contato com o Grupo de Desenvolvimento de Documentação	16

FONTES DE INFORMAÇÃO PARA PESQUISA ADICIONAL

Você pode ver as seguintes fontes de informação sobre o aplicativo:

- website do aplicativo da Kaspersky Lab;
- a página da Base de Dados de Conhecimento do aplicativo no website do Serviço de Suporte Técnico;
- o sistema de Ajuda e dicas instalado;
- a documentação do aplicativo instalado.

Página no website da Kaspersky Lab

<http://brazil.kaspersky.com/produtos/produtos-para-usuarios-domesticos/mobile-security>

Essa página lhe fornecerá informações gerais sobre o Kaspersky Mobile Security 9 e os seus recursos e opções. Você também pode comprar o Kaspersky Mobile Security 9 na nossa E-Store.

Página do aplicativo no website do Serviço de Suporte Técnico (Base de dados de conhecimento)

<http://suporte.kasperskyamericas.com/>

Esta página contém artigos escritos por especialistas do Serviço de Suporte Técnico.

Esses artigos contêm informações úteis, recomendações e Respostas a Perguntas Frequentes (FAQs) relacionadas à compra, instalação e uso do Kaspersky Mobile Security 9. Estão organizados em tópicos, tais como "Atualizações de banco de dados" e "Solução de Problemas". Os artigos podem responder perguntas que estejam relacionadas não somente ao Kaspersky Mobile Security 9, mas também a outros produtos da Kaspersky Lab. Eles podem conter também notícias do Serviço de Suporte Técnico.

O sistema de Ajuda instalado

Se tiver quaisquer perguntas sobre as janelas ou guias específicas no Kaspersky Mobile Security 9, você pode ver a ajuda de contexto.

Para abrir a ajuda de contexto, abra a tela que lhe interessa e selecione **Ajuda**.

A documentação instalada

O Guia do Usuário contém informações detalhadas sobre as funções do aplicativo e como usar o Kaspersky Mobile Security 9, juntamente com conselhos e recomendações em relação à configuração do aplicativo.

Os documentos são fornecidos no formato PDF no pacote de distribuição do Kaspersky Mobile Security 9.

Também é possível fazer o download desses documentos em formato eletrônico do website da Kaspersky Lab.

ENTRANDO EM CONTATO COM O DEPARTAMENTO DE VENDAS

Se você tiver perguntas relacionadas à seleção ou compra do Kaspersky Mobile Security, ou sobre a extensão da sua licença, ligue para os especialistas do Departamento de Vendas na nossa Sede Central em Moscou, através dos números:

+7 (495) 797-87-00, +7 (495) 645-79-39, +7 (495) 956-70-00

O serviço é prestado em russo ou inglês.

Você também pode enviar suas perguntas para o Departamento de Vendas por e-mail, em sales@kaspersky.com.

DISCUSSÃO SOBRE APLICATIVOS DA KASPERSKY LAB NO FÓRUM DA WEB

Se a sua pergunta não precisar de uma resposta urgente, você poderá discuti-la com os especialistas da Kaspersky Lab e com outros usuários dos aplicativos de antivírus da Kaspersky Lab no nosso fórum em <http://forum.kaspersky.com>.

No fórum, você pode visualizar as discussões existentes, deixar seus comentários e criar tópicos novos ou usar o mecanismo de pesquisa para consultas específicas.

ENTRANDO EM CONTATO COM O GRUPO DE DESENVOLVIMENTO DE DOCUMENTAÇÃO

Se você tiver alguma questão sobre a documentação, ou se tiver encontrado algum erro na mesma, ou se quiser deixar um comentário, entre em contato com o nosso grupo de desenvolvimento de documentação do usuário. Para entrar em contato com o Grupo de Desenvolvimento de Documentação, envie um e-mail para docfeedback@kaspersky.com. Escreva no espaço de assunto: "Kaspersky Help Feedback: Kaspersky Mobile Security 9".

KASPERSKY MOBILE SECURITY 9

O Kaspersky Mobile Security 9 protege os dispositivos móveis (a seguir "dispositivos") em execução no sistema operacional Android OS. O aplicativo pode proteger as informações sobre o dispositivo de infecção por ameaças conhecidas, evitar chamadas e mensagens de SMS indesejadas, proteger informações sobre o dispositivo no caso de perda ou roubo e ocultar informações relacionadas aos contatos confidenciais. Todo o tipo de ameaça é processado em componentes separados do programa. Isso possibilita o ajuste das configurações do dispositivo dependendo das necessidades do usuário.

O Kaspersky Mobile Security 9 inclui os seguintes componentes de proteção:

- **Antivírus.** Protege o sistema de arquivo do dispositivo móvel de vírus e outros aplicativos maliciosos. O Antivírus pode detectar e neutralizar objetos maliciosos no seu dispositivo e atualizar os bancos de dados de antivírus do aplicativo.
- **Filtro de Chamadas e SMS.** Verificação de todas as chamadas e mensagens de SMS de entrada para existência de spam. O componente permite o bloqueio flexível de mensagens de texto e chamadas consideradas indesejadas.
- Pasta **Anti-Roubo.** Protege as informações contidas no dispositivo de acesso não autorizado quando for roubado ou perdido e também facilita sua localização. O Anti-Roubo permite que você bloqueie seu dispositivo de forma remota, exclua informações armazenadas nele e localize sua posição geográfica usando comandos SMS de outro dispositivo. Além disso, o Anti-Roubo permite que você bloqueie seu dispositivo se o cartão SIM for substituído ou se o dispositivo for ativado sem um cartão SIM.
- **Proteção de Privacidade.** Oculta informações relacionadas aos números confidenciais da lista de contatos. Para esses números, a Proteção de Privacidade oculta as entradas em Contatos, no histórico de chamadas e SMS, e em chamadas e SMS de entrada.

O Kaspersky Mobile Security 9 não se destina a backup e restauração.

NESTA SEÇÃO

Requisitos de hardware e software	18
Kit de distribuição	18

REQUISITOS DE HARDWARE E SOFTWARE

O Kaspersky Mobile Security 9 pode ser instalado em dispositivos móveis funcionando no sistema operacional Android OS 1.5, 1.6, 2.0, 2.1, 2.2.

KIT DE DISTRIBUIÇÃO

Você pode comprar o Kaspersky Mobile Security 9 online, quando o kit de distribuição e a documentação do aplicativo forem fornecidos no formato eletrônico. O Kaspersky Mobile Security 9 também pode ser comprado em todas as lojas a varejo de produtos tecnológicos e de telefonia. Para obter informações detalhadas sobre a compra do aplicativo e recebimento do kit de distribuição, entre em contato com o nosso departamento de vendas em sales@kaspersky.com.

INSTALAÇÃO DO KASPERSKY MOBILE SECURITY 9

O aplicativo é instalado em um dispositivo móvel em várias etapas.

➤ *Para instalar o Kaspersky Mobile Security 9:*

1. Faça uma cópia do pacote de distribuição do aplicativo para o seu dispositivo. Para fazer isso, realize uma das seguintes ações:
 - Ao comprar o aplicativo em CD, conecte o dispositivo móvel ao computador e inicie a instalação automática do Kaspersky Mobile Security 9 no disco comprado.
 - Ao obter o pacote de distribuição do aplicativo através da Internet, conecte o dispositivo móvel ao computador e faça uma cópia do pacote de distribuição.
 - Faça uma cópia do pacote de distribuição do aplicativo para o dispositivo móvel da loja online da Kaspersky Lab (<http://brazil.kaspersky.com/comprar/kaspersky-produtos-para-usuarios-domesticos>).

2. Execute a instalação do aplicativo. Para fazer isso, abra o arquivo ARK do pacote de distribuição no dispositivo móvel.

O assistente de instalação do aplicativo inicia. Quando o assistente finaliza, o aplicativo é instalado com os parâmetros recomendados pelos especialistas da Kaspersky Lab.

3. Abra o aplicativo. Para fazer isso, na janela principal mude para a janela do aplicativo, selecione **Kaspersky Mobile Security 9** e execute o aplicativo.
4. Leia o texto do Contrato de Licença que é celebrado entre você e a Kaspersky Lab. Se você concorda com todos os termos do contrato, pressione **Aceitar**. Em seguida, a janela **Ativação** abrirá. Se você não concorda com os termos do Contrato de Licença, pressione **Recusar**. O aplicativo fecha.
5. Execute o aplicativo (ver "Ativação do aplicativo" na página [21](#)).
6. Insira o novo código secreto do aplicativo. Para fazer isso, digite-o sucessivamente nos campos **Definir um novo código secreto** e **Inserir um novo código novamente** e clique em **Enter**.

DESINSTALAÇÃO DO APLICATIVO

O aplicativo só pode ser desinstalado do dispositivo se a opção de ocultar informações confidenciais estiver desativada. Antes de desinstalar o aplicativo, o usuário deverá garantir que esta condição é atendida.

➤ *Para desinstalar o Kaspersky Mobile Security 9:*

1. Desativar Proteção de Privacidade (página [64](#)).
2. Para fazer isso, na janela principal, mude para a janela do aplicativo e selecione **Configurações** → **Aplicativos** → **Gerenciamento de aplicativos**.
3. Selecione o Kaspersky Mobile Security 9 da lista.
A janela de **Detalhes do aplicativo** abre.
4. Clique em **Excluir**.
Uma janela para confirmar exclusão abre.
5. Confirme a exclusão do Kaspersky Mobile Security 9 pressionando o botão **OK**.
O aplicativo é excluído do dispositivo.
6. Após concluir a exclusão, clique **OK**.

GUIA RÁPIDO

Esta seção contém informações sobre como começar a usar o Kaspersky Mobile Security 9: ativá-lo, definir o código secreto do aplicativo, ativar a função de recuperação do código secreto, recuperar o código secreto e iniciar o aplicativo.

NESTA SEÇÃO

Ativação do aplicativo.....	21
Definição do código secreto	24
Ativação da opção de recuperação do código secreto.....	25
Recuperação de código secreto.....	25
Inicialização do aplicativo.....	26
Visualização das informações sobre o aplicativo	26

ATIVAÇÃO DO APLICATIVO

Antes de iniciar o uso do Kaspersky Mobile Security 9, é necessário ativá-lo.

O aplicativo pode ser ativado se uma conexão com a Internet for configurada no dispositivo, um cartão SIM operacional for inserido e o código PIN for digitado (se estiver definido). Se esses requisitos não forem atendidos, não será possível ativar o aplicativo.

Antes de ativar o aplicativo, certifique-se de que as configurações de data e hora do sistema do dispositivo estão corretas.

Você pode ativar o aplicativo como se segue:

- **Ative a licença de teste.** Ao ativar a versão de teste, o aplicativo recebe uma licença de teste gratuita. O período de validade da licença de teste é mostrado na tela após a conclusão da ativação. Uma vez que o período de validade da licença de teste expira, as funções do aplicativo serão limitadas. Somente os seguintes recursos estarão disponíveis:
 - Ativação do aplicativo;
 - gerenciamento da licença do aplicativo;
 - Sistema de Ajuda do Kaspersky Mobile Security 9;
 - desativação da Proteção de Privacidade.

É impossível reativar a versão de teste.

- **Ativação da licença de teste.** Para ativar a versão comercial, você deverá usar o código de ativação que recebeu ao comprar o aplicativo. Ao ativar a versão comercial, o aplicativo recebe uma licença comercial que lhe concede acesso a todas as funções do aplicativo. O período de validade da licença de teste é mostrado na tela do dispositivo. Uma vez que o período de validade da licença de teste expira, as funções do aplicativo serão limitadas e o mesmo não poderá ser atualizado.

Você pode obter um código de ativação das seguintes formas:

- online, indo através do aplicativo Kaspersky Mobile Security 9 para o website especial da Kaspersky Lab para dispositivos móveis;
- na eStore da Kaspersky Lab (<http://brazil.kaspersky.com/comprar/kaspersky-produtos-para-usuarios-domesticos>);
- através de distribuidores da Kaspersky Lab.
- **Ativação da assinatura.** Ao ativar a assinatura, o aplicativo recebe uma licença comercial com assinatura. O período de validade da licença comercial com assinatura é limitado por 30 dias. Quando a assinatura é ativada, o aplicativo renova a licença a cada 30 dias. Quando a licença é renovada, um pagamento fixo para o uso do aplicativo especificado na ativação da assinatura, é debitado da sua conta pessoal. Os valores são debitados enviando uma mensagem de SMS a pagar. Uma vez que os valores são debitados, o aplicativo recebe uma nova licença do servidor de ativação com uma assinatura que lhe concede acesso a todas as funções do aplicativo. Você pode cancelar a assinatura do Kaspersky Mobile Security 9. Nesse caso, quando a licença atual expira, a funcionalidade do aplicativo torna-se limitada e os bancos de dados do aplicativo não são mais atualizados.

NESTA SEÇÃO

Ativação da versão comercial	22
Ativação da assinatura do Kaspersky Mobile Security 9.....	23
Compra de um código de ativação online	23
Ativação da versão de teste	24

ATIVAÇÃO DA VERSÃO COMERCIAL

➤ *Para ativar a versão comercial do aplicativo com o código de ativação:*

1. Mude da janela principal para a janela do aplicativo.
2. Selecione **Kaspersky Mobile Security 9** e execute o aplicativo.
Isso abrirá a janela **Ativação**.
3. Selecione **Inserir código de ativação**.
Isso abrirá a janela **Inserir código de ativação**.
4. Em seguida, insira o código de ativação que você recebeu ao comprar o aplicativo e clique em **Ativar**.

O aplicativo enviará uma solicitação para o servidor de ativação da Kaspersky Lab e receberá uma licença. Quando a licença for recebida com sucesso, as informações sobre a mesma serão exibidas na tela.

Se o código de ativação inserido estiver inválido por alguma razão, uma mensagem é exibida na tela. Nesse caso, recomenda-se verificar se o código de ativação inserido está correto e entrar em contato com o vendedor de software que lhe vendeu a licença do Kaspersky Mobile Security 9.

Se ocorrer quaisquer erros ao fazer a conexão ao servidor e se não receber nenhuma licença, a ativação é cancelada. Neste caso, recomenda-se verificar os parâmetros de conexão com a Internet. Caso não seja possível corrigir os erros, entre em contato com o Suporte Técnico.

5. Defina o código secreto do aplicativo.

ATIVÇÃO DA ASSINATURA DO KASPERSKY MOBILE SECURITY 9

➤ *Para ativar a assinatura do Kaspersky Mobile Security 9:*

1. Mude da janela principal para a janela do aplicativo.
2. Selecione **Kaspersky Mobile Security 9** e execute o aplicativo.

Isso abrirá a janela **Ativação**.

3. Selecione **Compra com Um Clique**.
4. Leia as informações sobre a ativação da sua assinatura e clique em **Ativar**.

O aplicativo verificará se o serviço de assinatura está acessível ao provedor de serviço móvel que você usa. Se o serviço de assinatura estiver disponível, as informações sobre os termos de assinatura serão exibidas na tela.

Se o serviço de assinatura não puder ser fornecido, você receberá uma notificação do aplicativo sobre esse problema e voltará para a tela na qual é possível selecionar outra forma de ativação do aplicativo.

5. Leia os termos de assinatura e então confirme a ativação da assinatura do Kaspersky Mobile Security 9 pressionando **Ativar**.

O aplicativo enviará um SMS pago e então receberá uma licença do servidor de ativação da Kaspersky Lab. Quando a assinatura estiver ativada, você receberá uma notificação do Kaspersky Mobile Security 9.

Se sua conta não tiver saldo suficiente para enviar uma mensagem paga, a ativação da assinatura será cancelada.

Se ocorrer quaisquer erros ao fazer a conexão ao servidor e se não receber nenhuma licença, a ativação é cancelada. Neste caso, recomenda-se verificar os parâmetros de conexão com a Internet. Caso não seja possível corrigir os erros, entre em contato com o Suporte Técnico.

Se você não concorda com os termos de assinatura, volte para a janela **Ativação**. Nesse caso, o aplicativo cancela a ativação da assinatura e volta para a tela na qual é possível selecionar novamente a forma de ativação do aplicativo.

6. Defina o código secreto.

COMPRA DE UM CÓDIGO DE ATIVAÇÃO ONLINE

➤ *Para comprar um código de ativação para o aplicativo online, siga os seguintes passos:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Adicional**.

Isso abrirá a janela **Adicional**.

2. Selecione o item **Licença** → **Renovar a licença**.

Isso abrirá a janela **Ativação**.

Selecione **Comprar online**.

Isso abrirá a janela **Comprar online**.

3. Pressione **Abrir**.

Um website especial da Kaspersky Lab para dispositivos móveis abre, no qual será oferecido uma opção de renovar a licença.

4. Siga as instruções passo a passo.
5. Após concluir o procedimento de compra do código de ativação, mude para a ativação da versão comercial do aplicativo.

ATIVAÇÃO DA VERSÃO DE TESTE

➤ *Para ativar a versão de teste do Kaspersky Mobile Security 9:*

1. SMude da janela principal para a janela do aplicativo.
2. Selecione **Kaspersky Mobile Security 9** e execute o aplicativo.

Isso abrirá a janela **Ativação**.

3. Selecione **Versão de teste**.
4. Confirme a ativação da versão de teste clicando em **Ativar**.

O aplicativo enviará uma solicitação para o servidor de ativação da Kaspersky Lab e receberá uma licença. Em seguida, a janela **Sobre a licença** abre com as informações sobre a licença instalada do aplicativo.

Se ocorrer quaisquer erros ao fazer a conexão ao servidor e se não receber nenhuma licença, a ativação é cancelada. Neste caso, recomenda-se verificar os parâmetros de conexão com a Internet. Caso não seja possível corrigir os erros, entre em contato com o Suporte Técnico.

5. Defina o código secreto do aplicativo.

DEFINIÇÃO DO CÓDIGO SECRETO

Após a inicialização do aplicativo, será solicitado que você insira o código secreto do aplicativo. *O código secreto do aplicativo* evita qualquer acesso sem autorização aos parâmetros do aplicativo.

Posteriormente, é possível alterar o código secreto instalado.

O Kaspersky Mobile Security 9 solicita o código secreto nas seguintes circunstâncias:

- para acessar o aplicativo;
- ao enviar um comando SMS de outro dispositivo móvel para iniciar as seguintes funções de forma remota: Bloqueio, Limpeza de Dados, SIM Watch e Localização GPS e Proteção de Privacidade.

O código secreto é composto por números. O número mínimo de caracteres é quatro.

Se você esquecer o código secreto do aplicativo, é possível restaurá-lo (ver a seção "Recuperação de código secreto" na página [25](#)). Para esse fim, a opção de recuperação do código secreto deve ser ativada previamente (ver a seção "Recuperação do código secreto" na página [25](#)).

➤ *Para inserir o código secreto:*

1. Após a ativação do aplicativo, insira as imagens no campo **Inserir novo código**, que será seu código.

O código inserido é automaticamente verificado.

Se o código for considerado inválido de acordo com os resultados da verificação, uma mensagem de aviso é mostrada e o aplicativo solicitará confirmação. Para usar o código, pressione **Sim**. Para criar um novo código, pressione **Não**. Insira um novo código secreto do aplicativo.

2. Insira novamente o mesmo código no campo **Confirmar novo código**.

O código secreto é instalado.

ATIVAÇÃO DA OPÇÃO DE RECUPERAÇÃO DO CÓDIGO SECRETO

Após a primeira ativação do aplicativo, é possível ativar a opção de recuperação do código secreto do aplicativo. Então, futuramente, você poderá recuperar o código secreto caso seja esquecido.

Se você recusa ativar a função após a primeira ativação do aplicativo, você pode ativá-lo após a reinstalação do Kaspersky Mobile Security 9 no dispositivo.

Você pode somente recuperar o código secreto do aplicativo (ver a seção "Recuperação de código secreto" na página [25](#)) se a opção de recuperação estiver ativada. Se você esqueceu a sua senha e a função de recuperação do código secreto está desativada, é impossível usar as funções do Kaspersky Mobile Security 9.

➔ Para ativar a opção de recuperação do código secreto:

1. Após instalar o código secreto do aplicativo (ver a seção "Instalação do código secreto" na página [24](#)), insira seu endereço de e-mail na janela **Ativar opção de recuperação do código secreto**.
2. Confirme a ativação da função de recuperação do código secreto clicando em **Ativar**.

O endereço de e-mail fornecido será usado durante a recuperação do código secreto.

O aplicativo estabelecerá uma conexão com a Internet com o servidor de recuperação do código secreto, enviará as informações inseridas e ativará a opção de recuperação do código.

RECUPERAÇÃO DO CÓDIGO SECRETO

Você pode somente recuperar o código secreto ativando previamente a opção de recuperação de código secreto (ver "Ativação da opção de recuperação de código secreto" na página [25](#)).

➔ Para recuperar o código secreto do aplicativo:

1. Mude da janela principal para a janela do aplicativo.
2. Selecione **Kaspersky Mobile Security 9**.

A janela do **Kaspersky Mobile Security 9** abre.

3. Clique em **Menu** → **Recuperação de código secreto**.

Uma mensagem com as seguintes informações é exibida na janela:

- Website da Kaspersky Lab para recuperação do código secreto;
- código de identificação do dispositivo.

4. Pressione **Ir**.

Vá para o website <http://mobile.kaspersky.com/recover-code> para recuperar o código secreto.

5. Insira as seguintes informações nos campos apropriados:

- o endereço de e-mail designado anteriormente para recuperar o código secreto;
- código de identificação do dispositivo.

Como resultado, o código de recuperação será enviado para o e-mail indicado.

6. Mude para a janela do **Kaspersky Mobile Security 9**.
7. Clique em **Menu** → **Inserir código de recuperação** e insira o código de recuperação recebido.
8. Insira o novo código secreto do aplicativo. Para fazer isso, insira um novo código do aplicativo nos campos **Inserir novo código** e **Confirmar código secreto**.
9. Clique em **Enter**.

INICIALIZAÇÃO DO APLICATIVO

➔ *Para inicializar o Kaspersky Mobile Security 9:*

1. Mude da janela principal para a janela do aplicativo.
2. Selecione **Kaspersky Mobile Security 9**.
3. A janela do **Kaspersky Mobile Security 9** abre.
4. Insira o código secreto do aplicativo e pressione **OK**.

A janela principal do aplicativo abre.

VISUALIZAÇÃO DAS INFORMAÇÕES SOBRE O APLICATIVO

Você pode visualizar as informações gerais sobre o Kaspersky Mobile Security 9 e a sua versão.

➔ *Para visualizar as informações sobre o aplicativo:*

1. Na janela principal do Kaspersky Mobile Security 9, a caixa **Adicional** abre.
Isso abrirá a janela **Adicional**.
2. Na caixa **Informações**, selecione **Sobre**.

GERENCIAMENTO DE LICENÇAS

No contexto de licenças de aplicativos da Kaspersky Lab, é importante conhecer os termos a seguir:

- Contrato de Licença;
- licença.

Esses termos estão inseparavelmente ligados e constituem um padrão único de licenciamento. Vamos conhecer cada termo de forma mais detalhada.

Além disso, a seção apresenta informações sobre como encontrar informações sobre a licença do Kaspersky Mobile Security 9 e sobre a extensão do prazo da sua validade.

NESTA SEÇÃO

Sobre o Contrato de Licença.....	27
Sobre as licenças do Kaspersky Mobile Security 9.....	27
Visualização das Informações da Licença	28
Renovação da licença.....	29

SOBRE O CONTRATO DE LICENÇA

O *Contrato de Licença* é um acordo entre um indivíduo ou uma entidade legal que possui legalmente uma cópia do Kaspersky Mobile Security 9 e Kaspersky Lab. O contrato está incluído em todos os aplicativos da Kaspersky Lab. Indica as informações detalhadas sobre os direitos e limitações no uso do Kaspersky Mobile Security.

De acordo com o Contrato de Licença, ao comprar e instalar um aplicativo da Kaspersky Lab, você obtém direito ilimitado de propriedade da sua cópia.

A Kaspersky Lab também fornece serviços adicionais:

- suporte técnico;
- atualização dos bancos de dados de antivírus do Kaspersky Mobile Security 9;
- atualização dos módulos do programa do Kaspersky Mobile Security 9.

Para poder se beneficiar desses direitos, você deve comprar e ativar uma licença (ver a seção "Sobre as licenças do Kaspersky Mobile Security 9" na página [27](#)).

SOBRE AS LICENÇAS DO KASPERSKY MOBILE SECURITY 9

Uma *licença* é o direito de usar o Kaspersky Mobile Security 9 e seus serviços adicionais associados, tal como previsto pela Kaspersky Lab ou pelos seus parceiros.

Toda licença tem um tipo e período de validade.

Prazo da licença – período durante o qual os serviços adicionais são oferecidos:

- suporte técnico;
- atualização dos bancos de dados de antivírus do Kaspersky Mobile Security 9;
- atualização dos módulos de programa do Kaspersky Mobile Security 9.

O âmbito dos serviços fornecidos depende do tipo da licença.

Os seguintes tipos de licença estão disponíveis:

- *Teste*—licença gratuita com um período de validade limitado, por exemplo, 30 dias, oferecida para se familiarizar com o Kaspersky Mobile Security 9.

A licença de teste pode ser usada apenas uma vez.

Se você tiver uma licença de teste, poderá entrar em contato com o Serviço de Suporte Técnico se tiver dúvidas referentes à ativação do produto ou à compra de uma licença comercial. Assim que a licença de teste do Kaspersky Mobile Security 9 expira, todos os recursos são desativados. Para continuar com o aplicativo, você deve ativá-lo.

- *Comercial*—licença paga com um período de validade limitado (por exemplo, um ano), fornecida no ato da compra do Kaspersky Mobile Security 9.

Se uma licença comercial é ativada, todos os recursos do aplicativo e serviços adicionais estão disponíveis.

Ao término do período de validade da licença comercial, algumas funções do Kaspersky Mobile Security 9 ficam inacessíveis e os bancos de dados do aplicativo não serão atualizados. Uma semana antes da data de expiração da licença, você receberá uma notificação, assim poderá renovar a licença com antecedência.

- *Comercial com assinatura* – licença paga com uma opção de renová-la em modo automático ou manual. Uma licença com assinatura é distribuída pelos provedores de serviço.

A assinatura é válida por um período limitado (30 dias). Após a expiração da assinatura, é possível renová-la manual ou automaticamente. O método de renovação da assinatura depende da legislação e do provedor de serviço móvel. A assinatura é renovada automaticamente sujeita ao pré-pagamento pontual ao provedor.

Nesse caso, o valor fixo especificado nos termos da assinatura é debitado da sua conta pessoal. Os valores são debitados da sua conta pessoal após você enviar uma mensagem de SMS paga para o número do provedor de serviço.

Se a assinatura não for renovada, o Kaspersky Mobile Security 9 interrompe a atualização dos bancos de dados do aplicativo e a funcionalidade do mesmo passa a ser limitada.

Ao usar a assinatura, é possível ativar a licença comercial com um código de ativação. Nesse caso, a assinatura será cancelada automaticamente.

Ao usar a licença comercial, é possível ativar a assinatura. Se já tiver uma licença ativada com um prazo limitado no momento da ativação da assinatura, é substituída pela licença da assinatura.

VISUALIZAÇÃO DAS INFORMAÇÕES DA LICENÇA

Você pode visualizar as seguintes informações da licença: número da licença, tipo, data de ativação, data de expiração, quantidade de dias para expirar e número de série do dispositivo.

➔ *Para visualizar as informações da licença:*

1. Na janela principal do Kaspersky Mobile Security 9, a caixa **Adicional** abre.

Isso abrirá a janela **Adicional**.

2. Selecione **Licença** → **Sobre a licença**.

RENOVAÇÃO DA LICENÇA

O Kaspersky Mobile Security 9 permite que você renove a licença do aplicativo.

A licença pode ser prorrogada em uma das seguintes formas:

- Insira o código de ativação - ative o aplicativo com o código de ativação. Você pode comprar o código de ativação em <http://brazil.kaspersky.com/comprar/kaspersky-produtos-para-usuarios-domesticos>, ou de um distribuidor local da Kaspersky Lab.
- Compre o código de ativação online – vá para o website visitado a partir do seu dispositivo móvel e compre um código de ativação online.
- Assine o Kaspersky Mobile Security 9 – ative a assinatura para renovar a licença a cada 30 dias.

O aplicativo pode ser ativado se uma conexão com a Internet for configurada no dispositivo, um cartão SIM operacional for inserido e o código PIN for digitado (se estiver definido). Se esses requisitos não forem atendidos, não será possível ativar o aplicativo.

NESTA SEÇÃO

Renovação da licença com o código de ativação	29
Renovação da licença online	30
Renovação da licença através da ativação de uma assinatura.....	30
Cancelamento da assinatura.....	31
Renovação da assinatura.....	31

RENOVAÇÃO DA LICENÇA COM O CÓDIGO DE ATIVAÇÃO

➔ *Para renovar a licença com o código de ativação:*

1. Na janela principal do Kaspersky Mobile Security 9, a caixa **Adicional** abre.
Isso abrirá a janela **Adicional**.
2. Selecione o item **Licença** → **Prolongar licença**.
Isso abrirá a janela **Ativação**.
3. Selecione **Inserir código de ativação**.
Isso abrirá a janela **Inserir código de ativação**.
4. Em seguida, insira o código de ativação recebido e clique em **Ativar**.

O aplicativo enviará uma solicitação para o servidor de ativação da Kaspersky Lab e receberá uma licença. Quando a licença for recebida com sucesso, as informações sobre a mesma serão exibidas na tela.

Se o código de ativação inserido estiver inválido por alguma razão, uma mensagem é exibida na tela. Nesse caso, recomenda-se verificar se o código de ativação inserido está correto e entrar em contato com o vendedor de software que lhe vendeu a licença do Kaspersky Mobile Security 9.

Se ocorrer quaisquer erros ao fazer a conexão ao servidor e se não receber nenhuma licença, a ativação é cancelada. Neste caso, recomenda-se verificar os parâmetros de conexão com a Internet. Caso não seja possível corrigir os erros, entre em contato com o Suporte Técnico.

RENOVAÇÃO DA LICENÇA ONLINE

➤ *Para renovar sua licença online:*

1. Na janela principal do Kaspersky Mobile Security 9, a caixa **Adicional** abre.

Isso abrirá a janela **Adicional**.

2. Selecione o item **Licença** → **Prolongar licença**.

Isso abrirá a janela **Ativação**.

3. Selecione **Comprar online**.

Isso abrirá a janela **Comprar online**.

4. Pressione **Abrir**.

Um website especial da Kaspersky Lab para dispositivos móveis abre no qual você pode comprar um código de ativação online.

5. Siga as instruções passo a passo.

6. Quando o pedido de renovação da licença é processado, insira o código de ativação obtido (ver a seção "Renovação da licença com código de ativação" na página [29](#)).

RENOVAÇÃO DA LICENÇA ATRAVÉS DA ATIVAÇÃO DE UMA ASSINATURA

Você pode renovar os termos da licença ativando a assinatura (ver a seção "Sobre licenciamento do Kaspersky Mobile Security 9" na página [27](#)) em Kaspersky Mobile Security 9. Quando a assinatura é ativada, o Kaspersky Mobile Security 9 renova a licença a cada 30 dias. Sempre que a licença for renovada, o valor fixo especificado nos termos da assinatura é debitado da sua conta pessoal.

➤ *Para ativar a assinatura do Kaspersky Mobile Security 9:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Adicional**.

Isso abrirá a janela **Adicional**.

2. Selecione o item **Licença** → **Prolongar licença**.

Isso abrirá a janela **Ativação**.

Selecione **Compra com Um Clique**.

3. Leia as informações da assinatura e clique em **Ativar**.

O aplicativo verificará se o serviço de assinatura está acessível ao provedor de serviço móvel que você usa. Se o serviço de assinatura estiver disponível, as informações sobre os termos de assinatura serão exibidas na tela.

Se o serviço de assinatura não puder ser fornecido, você será informado sobre esse problema e voltará para a tela na qual é possível selecionar outro método de renovação da licença. A ativação da assinatura será cancelada.

4. Leia os termos de assinatura e então confirme a ativação da assinatura do Kaspersky Mobile Security 9 pressionando **Ativar**.

O aplicativo enviará um SMS pago e então receberá uma licença do servidor de ativação da Kaspersky Lab. Quando a assinatura estiver ativada, você receberá uma notificação do Kaspersky Mobile Security 9.

Se sua conta não tiver saldo suficiente para enviar uma mensagem paga, a ativação da assinatura será cancelada.

Se ocorrer quaisquer erros ao fazer a conexão ao servidor e se não receber nenhuma licença, a ativação é cancelada. Neste caso, recomenda-se verificar os parâmetros de conexão com a Internet. Caso não seja possível corrigir os erros, entre em contato com o Suporte Técnico.

Se você não concorda com os termos de assinatura, volte para a janela **Ativação**. O aplicativo cancelará a ativação da assinatura e voltará para a tela na qual é possível selecionar outro método de renovação da licença.

CANCELAMENTO DA ASSINATURA

Você pode cancelar a assinatura do Kaspersky Mobile Security 9. Nesse caso, o Kaspersky Mobile Security 9 não renovará a licença a cada 30 dias. Quando a licença atual expira, a funcionalidade do aplicativo torna-se limitada e os bancos de dados do aplicativo não são mais atualizados.

Se você cancelou sua assinatura, você pode retomá-la (ver a seção "Renovação da assinatura" na página [31](#)).

➔ *Para cancelar a assinatura do Kaspersky Mobile Security 9:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Adicional**.
2. Isso abrirá a janela **Adicional**.
3. Selecione **Cancelar assinatura**.
4. Confirme o cancelamento da assinatura pressionando **Sim**.

Você receberá uma notificação do Kaspersky Mobile Security 9 de cancelamento da assinatura.

RENOVAÇÃO DA ASSINATURA

Se você cancelou sua assinatura, você pode retomá-la.

Ao renovar a assinatura, os valores são somente debitados da sua conta pessoal se a licença atual expirar antes de três dias.

➔ *Para retomar a assinatura:*

1. Na janela principal do Kaspersky Mobile Security 9, a caixa **Adicional** abre.
Isso abrirá a janela **Adicional**.
2. Selecione o item **Licença** → **Prolongar licença**.
Isso abrirá a janela **Ativação**.
3. Selecione **Compra com Um Clique**.

Se o prazo de validade da licença tiver expirado, o Kaspersky Mobile Security 9 sugere a ativação da assinatura (ver a seção "Sobre as licenças do Kaspersky Mobile Security 9" na página [27](#)).

Se a licença atual ainda não tiver expirado, o Kaspersky Mobile Security 9 retoma a assinatura e renova a mesma a cada 30 dias após a expiração da licença atual.

INTERFACE DO APLICATIVO

Esta seção inclui informações sobre os elementos principais da interface do Kaspersky Mobile Security 9.

NESTA SEÇÃO

Janela de status de proteção	32
Widget da tela inicial	33

JANELA DE STATUS DE PROTEÇÃO

Após iniciar o programa, a janela principal do aplicativo abre (ver Figura abaixo).

Os módulos de expansão estão localizados na janela principal. Cada módulo permite alterar as configurações dos parâmetros de um dos componentes do aplicativo e realizar as tarefas de proteção.

A janela principal também mostra a condição de seus componentes principais.

Para cada módulo, as seguintes informações são exibidas abaixo de seu respectivo nome:

- **Antivírus** – status de proteção do dispositivo quanto a vírus e outros aplicativos maliciosos (ver seção "Proteção do sistema de arquivos" na página [34](#));
- **Proteção de Privacidade** – modo de ocultação de informações confidenciais.
- **Anti-Roubo** – status das funções do Anti-Roubo.
- **Filtro de Chamadas e SMS** – modo de filtragem de chamadas e SMS.
- **Adicional** – informações sobre os parâmetros adicionais agrupados neste módulo (ver seção "Atribuição de configurações adicionais" na página [74](#)).

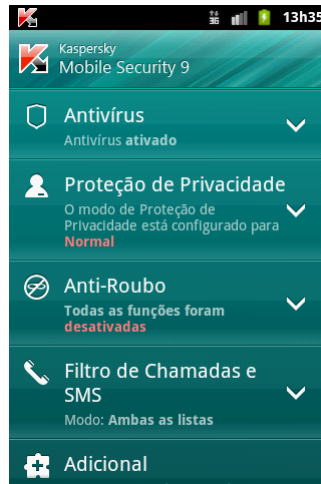


Figura 1. A janela principal do aplicativo

WIDGET DA TELA INICIAL

Ao usar o Kaspersky Mobile Security 9, o widget da tela inicial fica acessível. Após a instalação do aplicativo, o widget aparece automaticamente na janela principal do aplicativo (ver Figura abaixo).



Figura 2. Widget da tela inicial

O indicador colorido do widget na tela principal informa você sobre o status de proteção do seu dispositivo, do Proteção de Privacidade e da licença, e permite-lhe definir as configurações do aplicativo.

A indicação de cor a seguir é apresentada:

- se a proteção estiver verde, então está ativada;
- se a proteção estiver cinza, então está desativada;
- a cor verde do plano de fundo significa que as informações confidenciais estão ocultas;
- a cor cinza do plano de fundo significa que as informações confidenciais estão exibidas;
- um ponto de exclamação dentro de um triângulo amarelo significa que o prazo de validade da licença expirou ou que a licença não foi instalada.

PROTEÇÃO DO SISTEMA DE ARQUIVOS

Esta seção fornece informações sobre o componente de proteção que evita infecções do sistema de arquivos do seu dispositivo. A seção também descreve como ativar/parar a proteção e ajustar suas configurações de operação.

NESTA SEÇÃO

Sobre a Proteção	34
Ativação/Desativação da Proteção	34
Configuração da área de proteção.....	35
Seleção da ação a ser executada nos objetos detectados	36

SOBRE A PROTEÇÃO

A proteção inicia quando o sistema operacional é inicializado e quando é sempre encontrado na memória do dispositivo. A proteção verifica todos os arquivos abertos, salvos e inicializados (incluindo aqueles em cartões de memória), assim como os aplicativos instalados.

Os arquivos são verificados de acordo com o seguinte algoritmo:

1. A proteção verifica todos os arquivos quando são acessados pelo usuário.
2. A proteção analisa o arquivo quanto à presença de objetos maliciosos. Os objetos maliciosos são detectados comparando com os bancos de dados de antivírus do aplicativo. Os bancos de dados de antivírus contêm descrições de todos os objetos maliciosos atualmente conhecidos e os métodos para neutralizá-los.
3. De acordo com os resultados da análise, os seguintes tipos de Proteção são possíveis:
 - se um código malicioso for detectado no arquivo, a proteção realiza uma ação de acordo com as configurações definidas (ver seção "Seleção de ação em relação aos objetos detectados" na página [36](#));
 - Se nenhum código malicioso for descoberto no arquivo, ele será restaurado imediatamente.

A proteção verifica o aplicativo instalado para vírus quando é executada pela primeira vez. A proteção realiza uma verificação na base dos bancos de dados de antivírus. Se a proteção detecta um vírus durante a verificação do aplicativo, recomenda a exclusão do aplicativo.

ATIVAÇÃO/DESATIVAÇÃO DA PROTEÇÃO

Ao ativar a Proteção, todas as ações no sistema estão sob controle permanente.

Para garantir proteção contra vírus e outras ameaças, os recursos do dispositivo são usados. A fim de reduzir a carga no dispositivo ao executar várias tarefas, você pode parar temporariamente a Proteção.

Os especialistas da Kaspersky Lab recomendam enfaticamente que você não desative a Proteção, pois isso poderia levar a uma infecção do computador e à perda de dados.

Desativar a proteção não tem impacto no desempenho das tarefas de verificação de antivírus e na atualização dos bancos de dados de antivírus do aplicativo.

O status atual de proteção é exibido na janela principal do aplicativo no modelo de **Antivírus**.

➤ *Para ativar a Proteção:*

1. Na janela principal do Kaspersky Mobile Security 9, a caixa **Antivírus** abre.
2. Clique em **Adicional**.
A janela **Antivírus: Adicional** abre.
3. Marque a caixa **Ativar Proteção** (ver Figura abaixo).



Figura 3. Ativação da Proteção

➤ *Para desativar a Proteção:*

1. Na janela principal do Kaspersky Mobile Security 9, a caixa **Antivírus** abre.
2. Clique em **Adicional**.
A janela **Antivírus: Adicional** abre.
3. Desmarque a caixa **Ativar Proteção**.

CONFIGURAÇÃO DA ÁREA DE PROTEÇÃO

Por padrão, o Kaspersky Mobile Security 9 verifica todos os tipos de arquivos. Você pode selecionar arquivos para o Kaspersky Mobile Security 9 para verificar a presença de objetos maliciosos durante sua operação de Proteção.

Antes de configurar a proteção, primeiramente garanta que a proteção é ativada.

➤ *Para selecionar o tipo de arquivos a serem verificados:*

1. Na janela principal do Kaspersky Mobile Security 9, a caixa **Antivírus** abre.
2. Clique em **Adicional**.
A janela **Antivírus: Adicional** abre.
3. Selecione **Configurações de proteção** → **Tipo de arquivos para proteção**.

4. Selecione o valor para as configurações do **Tipo de arquivos para proteção** (ver figura abaixo):
- **Todos os arquivos** - verifica todos os tipos de arquivos.
 - **Somente executáveis** – verifica somente arquivos de aplicativo executáveis (por exemplo, arquivos nos formatos EXE, MDL, APP, DLL, SO, ELF).

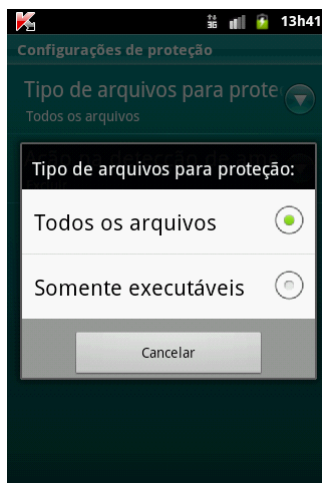


Figura 4. Seleção de objetos a verificar

SELEÇÃO DA AÇÃO A SER EXECUTADA NOS OBJETOS DETECTADOS

Por padrão, o Kaspersky Mobile Security 9 exclui a ameaça detectada. Você pode escolher a ação que o Kaspersky Mobile Security 9 realiza quando detecta um objeto malicioso.

➤ *Para configurar a resposta do aplicativo ao detectar uma ameaça, proceda da seguinte forma:*

1. Na janela principal do Kaspersky Mobile Security 9, a caixa **Antivírus** abre.
2. Clique em **Adicional**.
A janela **Antivírus: Adicional** abre.
3. Selecione **Configurações de proteção** → **Ação na detecção de ameaça**.
4. Defina uma ação a ser tomada pelo aplicativo quando encontrar um objeto malicioso. Para fazer isso, selecione o valor para as configurações da **Ação na detecção de ameaça** (ver Figura abaixo):
 - **Excluir** - exclui os objetos malware sem notificar o usuário.
 - **Ignorar** – ignora os objetos maliciosos. Bloqueia o objeto quando são feitas tentativas de usá-lo (por exemplo, copiar ou abrir).

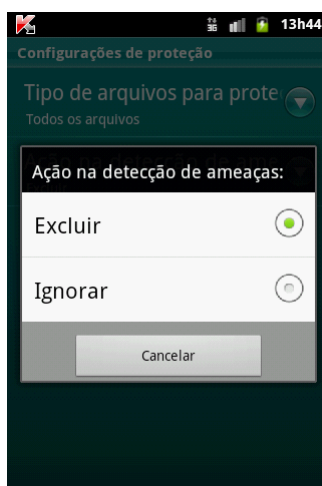


Figura 5. Seleção da ação na detecção de ameaça

VERIFICAÇÃO DO DISPOSITIVO

Esta seção informa sobre a verificação do dispositivo por comando, que consegue detectar e remover as ameaças no seu dispositivo. A seção também descreve como iniciar uma verificação do dispositivo, configurar uma verificação automática agendada do sistema de arquivos, selecionar arquivos para verificação e definir a ação que será tomada no aplicativo quando for detectado um objeto malicioso.

NESTA SEÇÃO

Sobre a verificação do dispositivo.....	38
Inicialização manual da verificação.....	38
Início de uma verificação agendada.....	39
Seleção do tipo de objeto a ser verificado.....	40
Configuração das verificações do arquivo.....	41
Seleção da ação a ser executada nos objetos detectados	41

SOBRE A VERIFICAÇÃO DO DISPOSITIVO

A verificação do dispositivo por comando ajuda a detectar e remover as ameaças no seu dispositivo. O Kaspersky Mobile Security 9 permite realizar uma verificação completa ou parcial do dispositivo incluído - isto é, verificar somente o conteúdo da memória integrada do dispositivo ou de uma pasta específica (incluindo aquela localizada no cartão de armazenamento).

O dispositivo é verificado como se segue:

1. O Kaspersky Mobile Security 9 verifica os tipos de arquivos definidos (ver a seção "Seleção dos tipos de objetos a serem verificados" na página [40](#)).
2. Durante a verificação, cada arquivo é analisado quanto à presença de objetos maliciosos (malware). Os objetos maliciosos são detectados comparando com os bancos de dados de antivírus do aplicativo. Os bancos de dados de antivírus contêm descrições de todos os objetos maliciosos conhecidos e os métodos para neutralizá-los.

Se a seguir à análise do arquivo, o aplicativo detecta um código malicioso, realiza-se uma ação selecionada de acordo com as configurações definidas (ver seção "Seleção de ação em relação aos objetos detectados" na página [41](#)).

A verificação inicia manual ou automaticamente de acordo com uma agenda (ver seção "Início de uma verificação agendada" na página [39](#)).

INICIALIZAÇÃO MANUAL DA VERIFICAÇÃO

Você pode iniciar manualmente uma verificação completa ou parcial como necessário.

➔ *Para iniciar uma verificação de antivírus manualmente:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo de **Antivírus**.
2. Selecione **Iniciar verificação**.

3. Selecione a área de verificação do dispositivo (ver Figura abaixo):

- **Verificação completa** – verifica todo o sistema de arquivos do dispositivo. Por padrão, o aplicativo verifica os arquivos salvos na memória interna e nos cartões de memória do dispositivo.
- **Verificação da pasta** - verifica um objeto separado no sistema de arquivos ou no cartão de memória do dispositivo. Quando a opção **Verificação da pasta** é selecionada, uma janela exibindo o **Sistema de arquivos** do dispositivo abrirá. Para inicializar uma pasta, selecione a pasta necessária e clique no ícone de verificação localizado à direita da pasta.
- **Verificação de memória** - verifica os processos inicializados na memória do sistema e nos seus arquivos correspondentes.

Após o início da verificação, uma janela de progresso da verificação abre mostrando o status atual da tarefa: o número de arquivos verificados, o caminho para o arquivo sendo verificado no momento e uma indicação dos resultados da verificação em porcentagem. Na janela de processo de verificação, você pode pausar a verificação clicando em **Suspender**, ou finalizar o processo de verificação clicando em **Cancelar**.

Se o Kaspersky Mobile Security 9 detecta um objeto malicioso, realiza uma ação de acordo com os parâmetros definidos de verificação (ver a seção "Seleção de uma ação a ser realizada em objetos" na página [41](#)).

Por padrão, se o Kaspersky Mobile Security 9 detecta uma ameaça, ele tenta eliminá-la. Se a desinfecção não é possível, o aplicativo exclui o objeto malicioso.

Quando a verificação for excluída, as estatísticas gerais são exibidas na tela com as seguintes informações:

- número de arquivos selecionados;
- número de vírus detectados e excluídos;
- número de arquivos aprovados (por exemplo, um arquivo é bloqueado pelo sistema operacional ou um arquivo não é executável, quando verifica somente arquivos de programa executáveis);
- tempo de verificação.



Figura 6. Seleção da área de verificação

INÍCIO DE UMA VERIFICAÇÃO AGENDADA

Você pode configurar a verificação do sistema do arquivo para iniciar automaticamente conforme agenda. Uma verificação agendada é realizada no modo de segundo plano. Quando um objeto malicioso é detectado, a ação selecionada nas configurações de verificação será realizada (ver a seção "Seleção de uma ação a ser realizada em objetos" na página [41](#)).

Por padrão, o início agendado da verificação de um arquivo é desativado.

➔ *Para configurar uma agenda de verificação:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo de **Antivírus**.
2. Clique em **Adicional**.
A janela **Antivírus: Adicional** abre.
3. Selecione **Configurações de verificação**.
A janela de **Configurações de verificação** abre.
4. Selecione o modo de início de verificação. Para fazer isso, defina um valor para as **Configurações de verificação agendada**:
 - **Semanalmente** – realiza a verificação uma vez por semana. Para fazer isso, configure o dia e a hora de início da verificação. Para fazer isso, selecione os valores para as configurações **Dia da verificação** e **Hora da verificação**.
 - **Diariamente** – realiza a verificação todos os dias. Para fazer isso, configure a hora de início da verificação. Defina um valor para a configuração da **Hora de verificação**.
 - **Desativado** – desativa as verificações agendadas.



Figura 7. Configure uma verificação automática

SELEÇÃO DO TIPO DE OBJETO A SER VERIFICADO

Por padrão, o Kaspersky Mobile Security 9 verifica todos os arquivos salvos no dispositivo e no cartão de armazenamento. Para encurtar o tempo de verificação, você pode selecionar o tipo de objeto a ser verificado, isto é, determina que formatos de arquivo o aplicativo deverá verificar para ver o código malicioso.

➔ *Para selecionar objetos a serem verificados:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo de **Antivírus**.
2. Clique em **Adicional**.
A janela **Antivírus: Adicional** abre.
3. Selecione **Configurações de verificação** → **Área de verificação**.

A janela **Área de verificação** abre.

4. Defina um valor para configuração **Tipos de arquivos** (ver Figura abaixo):
 - **Todos os arquivos** - verifica todos os tipos de arquivos.
 - **Somente executáveis** – verifica somente arquivos de aplicativo executáveis nos seguintes formatos EXE, DLL, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS, SO, ELF.



Figura 8. Seleção dos tipos de arquivos para verificar

CONFIGURAÇÃO DAS VERIFICAÇÕES DO ARQUIVO

Vírus normalmente ocultados em arquivos. O programa verifica os seguintes formatos de arquivos: ZIP, JAR, JAD, SIS, SISX, CAB e APK. Os arquivos são descompactados durante a verificação que pode reduzir significativamente a velocidade da Verificação por Comando.

Você pode ativar / desativar a verificação de arquivo para código malicioso durante a Verificação por Comando.

➔ *Para ativar a verificação de arquivos:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo de **Antivírus**.
2. Clique em **Adicional**.
A janela **Antivírus: Adicional** abre.
3. Selecione **Configurações de verificação** → **Área de verificação**.
A janela **Área de verificação** abre.
4. Selecione a caixa de seleção **Verificar arquivos**.

SELEÇÃO DA AÇÃO A SER EXECUTADA COM OS OBJETOS DETECTADOS

Por padrão, o Kaspersky Mobile Security 9 tenta retificar uma ameaça na detecção, se a mesma falhar, exclui a ameaça. Você pode configurar as ações do aplicativo quando uma ameaça for detectada.

➔ Para alterar a forma como o aplicativo age no objeto malicioso detectado:

1. Na janela principal do Kaspersky Mobile Security 9, abra a pasta **Antivírus**.

2. Clique em **Adicional**.

A janela **Antivírus: Adicional** abre.

3. Selecione **Configurações de proteção** → **Ação na detecção de ameaça**.

A janela **Ação na detecção de ameaça** abre.

4. Defina a primeira ação a respeito de uma ameaça detectada. Marque a caixa de seleção **Desinfectar** para que o aplicativo tente primeiro desinfectar a ameaça detectada. Desmarque a caixa de seleção **Desinfectar** para que o aplicativo não tente desinfectar a ameaça detectada.

5. Defina a segunda ação do aplicativo se uma ameaça detectada não puder ser desinfectada. Para fazer isso, selecione o valor para a configuração **Se não for possível a desinfecção** (ver Figura abaixo):

- **Perguntar ao usuário** - pergunta ao usuário por ações quando um objeto malicioso é detectado.
- **Excluir** - exclui os objetos malware sem notificar o usuário.
- **Ignorar** – não processa os objetos malware e registra as informações sobre sua detecção no log do aplicativo. Bloqueia o objeto quando são feitas tentativas de usá-lo (por exemplo, copiar ou abrir).

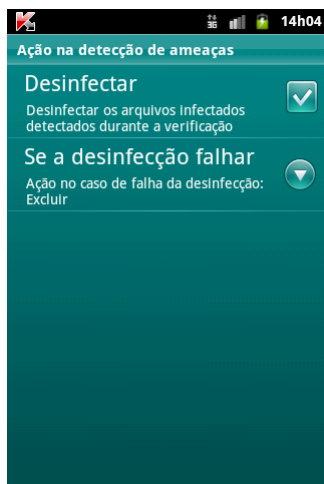


Figura 9. Seleção de uma ação com objetos maliciosos, se não puderem ser desinfectados

FILTRAGEM DE CHAMADAS E SMS DE ENTRADA

Esta seção fornece informações sobre o Filtro de Chamadas e SMS que evita chamadas e SMSs indesejados de acordo com as Listas Negra e Branca criadas. A seção também descreve como selecionar o modo no qual o Filtro de Chamadas e SMS verifica as chamadas e SMSs de entrada, como definir as configurações de filtragem adicionais para chamadas e SMSs de entrada e também como criar as Listas Negra e Branca.

NESTA SEÇÃO

Sobre o Filtro de Chamadas e SMS.....	43
Sobre os modos do Filtro de Chamadas e SMS	44
Alteração do modo do Filtro de Chamadas e SMS	44
Criação da Lista Negra.....	44
Criação da Lista Branca	47
Resposta às mensagens de SMS e às chamadas de contatos que não estão na agenda telefônica.....	50
Resposta às mensagens de SMS de algarismos não numéricos	51
Seleção da resposta ao SMS de entrada.....	52
Seleção da resposta às chamadas de entrada	53
Visualização dos registros de log.....	53

SOBRE O FILTRO DE CHAMADAS E SMS

O Filtro de Chamadas/SMS evita chamadas e SMSs não desejados a serem entregues com base na Lista Negra e Lista Branca que você compilou.

As listas consistem de entradas. Uma entrada em ambas as listas contém as seguintes informações:

- O número de telefone, da qual o Filtro de Chamadas e SMS bloqueia qualquer informação se o número estiver na Lista Negra e fornece qualquer informação se o número estiver na Lista Branca.
- O tipo de caso que o Filtro de Chamadas e SMS bloqueia se o número estiver na Lista Negra e fornece se estiver na Lista Branca. Os seguintes tipos de comunicações estão disponíveis: chamadas e SMS, somente chamadas e somente SMS.
- A frase chave usada pelo Filtro de Chamadas e SMS para identificar o SMS desejado e o não desejado. Para a Lista Negra, o Filtro de Chamadas e SMS bloqueia o SMS que contém esta frase, enquanto fornece aqueles que não a contém. Para a Lista Branca, o Filtro de Chamadas e SMS fornece o SMS que contém essa frase, enquanto bloqueia aqueles que não a contém.

As chamadas e mensagens dos filtros Anti-Spam como prescritos pelo modo selecionado (ver a seção "Sobre os modos do Filtro de Chamadas e SMS" na página [44](#)). De acordo com o modo, o Filtro de Chamadas e SMS verifica todas as chamadas e SMSs e então determina se são desejados ou indesejados (spam). Assim que o Filtro de Chamadas e SMS determina o status desejado ou indesejado a uma chamada ou SMS, a verificação é concluída.

As informações sobre chamadas e SMSs bloqueados estão registradas no log de filtro de chamadas e SMS (ver seção "Visualizações das entradas no log" na página [53](#)).

SOBRE OS MODOS DO FILTRO DE CHAMADAS E SMS

O modo define as regras segundo as quais o Filtro de Chamadas e SMS filtra as chamadas e SMSs de entrada.

Os seguintes modos de Filtro de Chamadas e SMS estão disponíveis:

- **Desligado** – todas as chamadas e SMSs são permitidos.
- **Lista Negra** – todas as chamadas e SMSs são permitidos, exceto aqueles originados dos números da Lista Negra.
- **Lista Branca** – somente chamadas e SMSs originados dos números da Lista Branca são permitidos.
- **Ambas as listas** – chamadas e SMSs de entrada dos números da Lista Branca são permitidos enquanto aqueles números da Lista Negra são bloqueados. Após uma conversa ou a leitura de um SMS de um número em nenhuma das listas, o Filtro de Chamadas e SMS pedirá que você insira o número em uma das listas.

Você pode alterar o modo do Filtro de Chamadas e SMS (ver a seção "Alteração do modo do Filtro de Chamadas e SMS" na página [44](#)). O modo atual do Filtro de Chamadas e SMS é exibido na guia **Filtro de Chamadas e SMS** próxima do item do menu **Modo**.

ALTERAÇÃO DO MODO DO FILTRO DE CHAMADAS E SMS

➔ Para alterar o modo do Filtro de Chamadas e SMS, proceda da seguinte forma:

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Filtro de Chamadas e SMS**.
2. Selecione **Modo: <modo atual do componente>**.
A janela do **Filtro de Chamadas e SMS** abre.
3. Selecione o valor para a configuração do **modo do Filtro de Chamadas e SMS** (ver Figura abaixo).

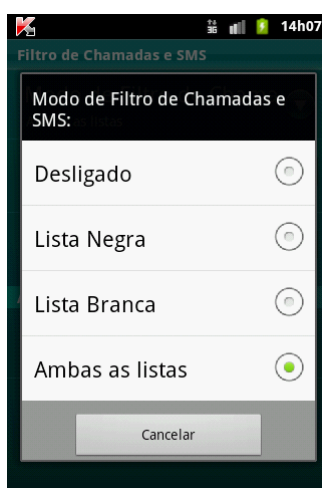


Figura 10. Alteração do modo do Filtro de Chamadas e SMS

CRIAÇÃO DA LISTA NEGRA

A Lista Negra contém entradas de números proibidos, isto é, os números dos quais o Filtro de Chamadas e SMS bloqueia as chamadas e SMSs. Cada entrada contém as seguintes informações:

- Número de telefone do qual o Filtro de Chamadas e SMS bloqueia as chamadas e / ou SMSs.
- Tipos de eventos que o Filtro de Chamadas e SMS bloqueia deste número. Os seguintes tipos de eventos estão disponíveis: chamadas e SMS, somente chamadas e somente SMS.
- Frase chave que o Filtro de Chamadas e SMS usa para classificar um SMS como não solicitado (spam). O Filtro de Chamadas e SMS bloqueia somente o SMS contendo a frase chave, enquanto fornece todos os outros SMSs.

O Filtro de Chamadas e SMS bloqueia chamadas e SMSs que cumprem com todos os critérios para a entrada na Lista Negra. Chamadas e SMS que falham em cumprir com pelo menos um dos critérios para uma entrada na Lista Negra serão permitidos pelo Filtro de Chamadas e SMS.

Você não pode adicionar um número de telefone com o mesmo critério de filtragem tanto para a Lista Negra como para a Lista Branca.

As informações sobre chamadas e SMSs bloqueados estão registradas no log de filtro de chamadas e SMS (ver seção "Visualizações das entradas no log" na página [53](#)).

NESTA SEÇÃO

Adição de entradas na Lista Negra	45
Edição de entradas na Lista Negra	46
Exclusão de entradas da Lista Negra	47

ADIÇÃO DE ENTRADAS NA LISTA NEGRA

Tenha em mente que o mesmo número com critérios de filtragem semelhantes não podem ser incluídos nas Listas Branca e Negra dos números do Filtro de Chamadas e SMS ao mesmo tempo. Se um número com esse critério de filtragem já está salvo em uma das listas, você receberá uma notificação do Kaspersky Mobile Security 9 sobre esse evento e a mensagem relevante aparecerá na tela.

➔ Para adicionar uma entrada na Lista Negra do Filtro de Chamadas e SMS:

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Filtro de Chamadas e SMS**.
2. Selecione **Lista Negra**.
Isso abrirá a janela **Lista Negra**.
3. Clique em **Adicionar**.
4. Defina os valores para as seguintes configurações:
 - **Bloquear entrada** – tipo de evento do número de telefone que o Filtro de Chamadas e SMS bloqueia para os números da Lista Negra:
 - **SMS**: bloqueia somente as mensagens de SMS de entrada.

- **Chamadas:** bloqueia somente as chamadas de entrada.
- **Chamadas e SMS:** bloqueia as mensagens de SMS e chamadas de entrada.
- **Número de telefone bloqueado** – número de telefone para o qual o Filtro de Chamadas e SMS bloqueia as informações de entrada. O número de telefone deve conter somente caracteres alfanuméricos, podendo começar com um dígito, uma letra ou ser precedido pelo símbolo "+". Como um número, também é possível usar as máscaras "*" ou "?" (onde "*" é qualquer quantidade de símbolos e "?" qualquer símbolo). Por exemplo, *1234? na Lista Negra. O Filtro de Chamadas e SMS bloqueia as chamadas e SMSs de um número no qual um símbolo segue a figura 1234.
- **Texto bloqueado** – frase chave indicando que a mensagem de SMS recebida é indesejada (spam). O Filtro de Chamadas e SMS bloqueia somente o SMS contendo a frase chave, enquanto fornece todos os outros SMSs.

Configuração acessível para eventos de **SMS**.

Se você deseja que todos os SMSs de entrada de um número específico na Lista Negra sejam bloqueados, deixe este campo de entrada **Texto bloqueado** em branco.

5. Pressione **Salvar**:

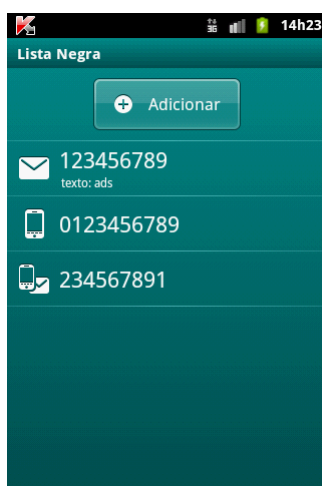


Figura 11. Adição de entradas na Lista Negra

EDIÇÃO DE ENTRADAS NA LISTA NEGRA

Você pode alterar os valores de todas as configurações para as entradas da Lista Negra.

➔ Para editar uma entrada na Lista Negra do Filtro de Chamadas e SMS:

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Filtro de Chamadas e SMS**.
2. Selecione **Lista Negra**.
Isso abrirá a janela **Lista Negra**.
3. Selecione uma entrada da lista que você deseja alterar e selecione **Alterar** no menu de contexto para a entrada.
4. Altere as configurações necessárias:

- **Número de telefone bloqueado** – número de telefone para o qual o Filtro de Chamadas e SMS bloqueia as informações de entrada. O número de telefone deve conter somente caracteres alfanuméricos, podendo

começar com um dígito, uma letra ou ser precedido pelo símbolo "+". Como um número, também é possível usar as máscaras "*" ou "?" (onde "*" é qualquer quantidade de símbolos e "?" qualquer símbolo). Por exemplo, *1234? na Lista Negra. O Filtro de Chamadas e SMS bloqueia as chamadas e SMSs de um número no qual um símbolo segue a figura 1234.

- **Texto bloqueado** – frase chave indicando que a mensagem de SMS recebida é indesejada (spam). O Filtro de Chamadas e SMS bloqueia somente o SMS contendo a frase chave, enquanto fornece todos os outros SMSs.

Configuração acessível para eventos de **SMS**.

Se você deseja que todos os SMSs de entrada de um número específico na Lista Negra sejam bloqueados, deixe este campo de entrada **Texto bloqueado** em branco.

5. Pressione **Salvar**:

EXCLUSÃO DE ENTRADAS DA LISTA NEGRA

Você pode excluir um número da Lista Negra. Além disso, você pode limpar a Lista Negra do Filtro de Chamadas e SMS removendo todas as entradas dela.

➔ *Para excluir uma entrada da Lista Negra do Filtro de Chamadas e SMS:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Filtro de Chamadas e SMS**.
2. Selecione **Lista Negra**.
Isso abrirá a janela **Lista Negra**.
3. Selecione uma entrada da lista que você deseja excluir e selecione **Excluir** para a entrada no menu de contexto.

➔ *Para limpar a Lista Negra do Filtro de Chamadas e SMS:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Filtro de Chamadas e SMS**.
2. Selecione **Lista Negra**.
Isso abrirá a janela **Lista Negra**.
3. Selecione **Excluir todos** no menu de contexto.
A janela de confirmação abre.
4. Confirme a desinstalação pressionando o botão **Sim**.

A lista está vazia.

CRIAÇÃO DA LISTA BRANCA

A Lista Branca contém entradas de números permitidos, isto é, números dos quais o Filtro de Chamadas e SMS fornece as chamadas e SMSs ao usuário. Cada entrada contém as seguintes informações:

- Número de telefone do qual o Filtro de Chamadas e SMS fornece as chamadas e / ou SMSs.
- Tipos de eventos que o Filtro de Chamadas e SMS fornece deste número. Os seguintes tipos de eventos estão disponíveis: chamadas e SMS, somente chamadas e somente SMS.

- Frase chave usada pelo Filtro de Chamadas e SMS para classificar um SMS como solicitado (não é spam). O Filtro de Chamadas e SMS fornece somente o SMS contendo a frase chave, enquanto bloqueia todos os outros SMSs.

O Filtro de Chamadas e SMS permite chamadas e SMS que cumprem com todos os critérios para uma entrada na Lista Branca. Chamadas e SMS que falham em cumprir com pelo menos um dos critérios para uma entrada na Lista Branca serão bloqueados pelo Filtro de Chamadas e SMS.

NESTA SEÇÃO

Adição de entradas na Lista Branca	48
Edição de entradas na Lista Branca	49
Exclusão de entradas da Lista Branca	50

ADIÇÃO DE ENTRADAS NA LISTA BRANCA

Tenha em mente que o mesmo número com critérios de filtragem semelhantes não podem ser incluídos nas Listas Branca e Negra dos números do Filtro de Chamadas e SMS ao mesmo tempo. Se um número com esse critério de filtragem já está salvo em uma das listas, você receberá uma notificação do Kaspersky Mobile Security 9 sobre esse evento e a mensagem relevante aparecerá na tela.

➔ Para adicionar uma entrada na Lista Branca do Filtro de Chamadas e SMS:

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Filtro de Chamadas e SMS**.
2. Selecione **Lista Branca**.
Isso abrirá a janela **Lista Branca**.
3. Pressione **Adicionar** (ver Figura abaixo).
4. Aplique as seguintes configurações para a nova entrada:

- **Permitir entrada** – tipo de evento do número de telefone que o Filtro de Chamadas e SMS permite para os números da Lista Branca:
 - **SMS:** permite somente as mensagens de SMS de entrada.
 - **Chamadas:** permite somente as chamadas de entrada.
 - **Chamadas e SMS:** permite as mensagens de SMS e chamadas de entrada.
- **Número de telefone permitido:** frase chave indicando que a mensagem de SMS recebida é desejada. O número de telefone deve conter somente caracteres alfanuméricos, podendo começar com um dígito, uma letra ou ser precedido pelo símbolo "+". Como um número, também é possível usar as máscaras "*" ou "?" (onde "*" é qualquer quantidade de símbolos e "?" qualquer símbolo). Por exemplo, *1234? na Lista Branca. O Filtro de Chamadas e SMS fornece as chamadas ou SMSs de um número no qual um símbolo segue a figura 1234.
- **Texto permitido** – frase chave indicando que a mensagem de SMS recebida é desejada. Para os números na Lista Branca, o Filtro de Chamadas e SMS fornece somente as mensagens de SMS contendo a frase chave e bloqueia todas as outras.

Configuração acessível para eventos de **SMS**.

Se você deseja que todos os SMSs de entrada de um número específico na Lista Branca sejam fornecidos, deixe este campo de entrada **Texto permitido** em branco.

5. Pressione **Salvar**:

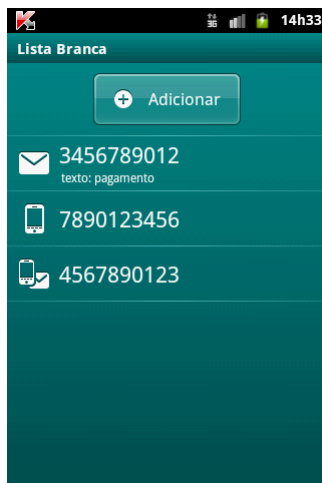


Figura 12. Adição de uma entrada na Lista Branca

EDIÇÃO DE ENTRADAS NA LISTA BRANCA

Para uma entrada da Lista Branca de números permitidos, você pode alterar os valores de todas as configurações.

➔ Para editar uma entrada na Lista Branca do Filtro de Chamadas e SMS:

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Filtro de Chamadas e SMS**.
2. Selecione **Lista Branca**.
Isso abrirá a janela **Lista Branca**.
3. Selecione uma entrada da lista que você deseja excluir e selecione **Alterar** para a entrada no menu de contexto.
4. Altere as configurações necessárias:

- **Número de telefone permitido**– número de telefone para o qual o Filtro de Chamadas e SMS bloqueia as informações de entrada. O número de telefone deve conter somente caracteres alfanuméricos, podendo começar com um dígito, uma letra ou ser precedido pelo símbolo "+". Como um número, também é possível usar as máscaras "*" ou "?" (onde "*" é qualquer quantidade de símbolos e "?" qualquer símbolo). Por exemplo, *1234? na Lista Branca. O Filtro de Chamadas e SMS fornece as chamadas ou SMSs de um número no qual um símbolo segue a figura 1234.
- **Texto permitido** – frase chave indicando que a mensagem de SMS recebida é desejada. Para os números na Lista Branca, o Filtro de Chamadas e SMS fornece somente as mensagens de SMS contendo a frase chave e bloqueia todas as outras.

Configuração acessível para eventos de **SMS**.

Se você deseja que todos os SMSs de entrada de um número específico na Lista Branca sejam fornecidos, deixe este campo de entrada **Texto permitido** em branco.

5. Pressione **Salvar**:

EXCLUSÃO DE ENTRADAS DA LISTA BRANCA

Você pode excluir uma entrada da Lista Branca, assim como limpá-la completamente.

➤ *Para excluir uma entrada da Lista Branca do Filtro de Chamadas e SMS:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Filtro de Chamadas e SMS**.
2. Selecione **Lista Branca**.
Isso abrirá a janela **Lista Branca**.
3. Selecione uma entrada da lista que você deseja excluir e selecione **Excluir** para a entrada no menu de contexto.

➤ *Para limpar a Lista Branca do Filtro de Chamadas e SMS:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Filtro de Chamadas e SMS**.
2. Selecione **Lista Branca**.
Isso abrirá a janela **Lista Branca**.
3. Selecione **Excluir todos** no menu de contexto.
A janela de confirmação abre.
4. Confirme a desinstalação pressionando o botão **Sim**.

A Lista Branca está vazia.

RESPOSTA ÀS MENSAGENS DE SMS E ÀS CHAMADAS DE CONTATOS QUE NÃO ESTÃO NA AGENDA TELEFÔNICA

Se os modos do Filtro de Chamadas e SMS **Ambas as listas** ou **Lista Branca** forem selecionados, você pode configurar adicionalmente uma resposta para o Filtro de Chamadas e SMS para as chamadas e SMSs dos assinantes, cujos números não estão contidos em Contatos. Além disso, o Filtro de Chamadas e SMS permite a expansão da Lista Branca adicionando números da lista de contatos para ela.

➤ *Para selecionar a resposta do Filtro de Chamadas e SMS a um número não incluído na agenda telefônica:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Filtro de Chamadas e SMS**.
2. Selecione **Modo: <modo atual do componente>**.
A janela do **Filtro de Chamadas e SMS** abre.
3. Selecione o valor para a configuração de **Permitir Contatos** (ver Figura abaixo):
 - para Anti-Spam contar os números de Contatos como Lista Branca adicional e bloquear as mensagens de SMS e chamadas de assinantes que não estão em Contatos, marque a caixa **Permitir Contatos**;
 - para o Filtro de Chamadas e SMS filtrar as mensagens de SMS e chamadas baseadas no modo definido do Filtro de Chamadas e SMS, marque a caixa de seleção **Permitir contatos**.

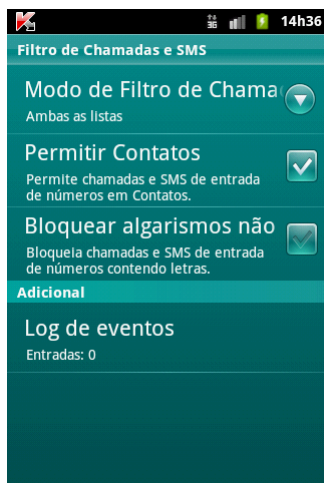


Figura 13. Reação do Filtro de Chamadas e SMS aos números que não estão em Contatos

RESPOSTA ÀS MENSAGENS DE SMS DE ALGARISMOS NÃO NUMÉRICOS

Para o modo do Filtro de Chamadas e SMS **Ambas as listas** ou **Lista Branca**, você pode expandir a Lista Negra incluindo todos os algarismos não numéricos (contendo letras). Nesse caso, o Filtro de Chamadas e SMS processa os SMSs e algarismos não numéricos como números da Lista Negra.

➔ Para configurar a resposta do Filtro de Chamadas e SMS ao receber mensagens de algarismos não numéricos:

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Filtro de Chamadas e SMS**.
2. Selecione **Modo: <modo atual do componente>**.

A janela do **Filtro de Chamadas e SMS** abre.

3. Selecione o valor para a configuração **Bloquear algarismos não numéricos** (ver a Figura abaixo):
 - para o Filtro de Chamadas e SMS bloquear os algarismos não numéricos, marque a caixa de seleção **Bloquear algarismos não numéricos**;
 - para o Filtro de Chamadas e SMS filtrar SMS de algarismos não numéricos na base do modo Filtro de Chamadas e SMS definido, desmarque a caixa de seleção **Bloquear algarismos não numéricos**.

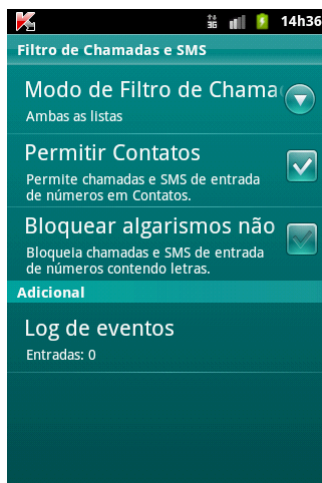


Figura 14. Seleção de uma ação para o Filtro de Chamadas e SMS realizar ao receber um SMS do algarismo não numérico

SELEÇÃO DA RESPOSTA AO SMS DE ENTRADA

O Filtro de Chamadas e SMS verifica as mensagens de chegada em relação às listas Branca e Negra no modo **Ambas as listas**.

Após receber uma mensagem de SMS de um número que não está incluído em nenhuma das listas, o Filtro de Chamadas e SMS pedirá que você insira o número em uma das listas (ver Figura abaixo).

Você pode selecionar uma das seguintes ações a ser realizada em respeito ao SMS:

- Para bloquear o SMS e adicionar o número de telefone à Lista Negra, clique **Bloquear**.
- Para fornecer o SMS e adicionar o número de telefone do remetente à Lista Branca, clique **Permitir**.
- Para fornecer a mensagem de SMS sem adicionar o número de telefone do remetente à nenhuma lista, pressione **Ignorar**.

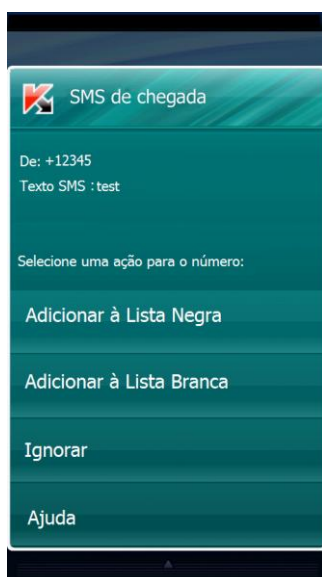


Figura 15. Notificação do Filtro de Chamadas e SMS sobre um SMS aceito

As informações sobre chamadas e SMSs bloqueados estão registradas no log de filtro de chamadas e SMS (ver seção "Visualizações das entradas no log" na página [53](#)).

SELEÇÃO DA RESPOSTA ÀS CHAMADAS DE ENTRADA

O Filtro de Chamadas e SMS verifica as mensagens de entrada em relação às listas Branca e Negra no modo **Ambas as listas**. Após receber uma chamada de um número que não está incluído em nenhuma das listas, o Filtro de Chamadas e SMS pedirá que você insira o número em uma das listas (ver Figura abaixo).

Você pode selecionar uma das seguintes ações para o número do qual a chamada foi realizada:

- Para adicionar o número de telefone do autor da chamada à Lista Negra, clique **Bloquear**.
- Para adicionar o número de telefone do autor da chamada à Lista Branca, clique **Permitir**.
- Se você não quiser adicionar o número do autor da chamada a nenhuma lista, pressione **Ignorar**.

As informações sobre chamadas e SMSs bloqueados estão registradas no log de filtro de chamadas e SMS (ver seção "Visualizações das entradas no log" na página [53](#)).

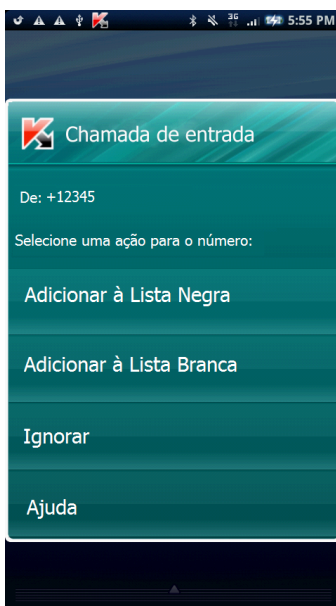


Figura 16. Notificação do Filtro de Chamadas e SMS sobre uma chamada recebida aceita

VISUALIZAÇÃO DOS REGISTROS DE LOG

Você pode visualizar as informações sobre chamadas e SMSs bloqueados no log do Filtro de Chamadas e SMS. As entradas no log são organizadas em ordem cronológica reversa.

As informações a seguir são fornecidas para todas as entradas:

- número de telefone, do qual o evento foi bloqueado pelo Filtro de Chamadas e SMS;
- data de bloqueio;
- hora de bloqueio.

➡ Para visualizar as informações sobre as chamadas e SMSs bloqueadas, proceda da seguinte forma:

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo do **Filtro de Chamadas e SMS**.

2. Selecione **Modo: <modo atual do componente>**.

A janela do **Filtro de Chamadas e SMS** abre.

3. Clique no módulo **Adicional Log de eventos**.

A janela do **Log do Filtro de Chamadas e SMS** abre.

- ◆ *Para visualizar as informações detalhadas sobre o evento bloqueado,*
selecione a entrada relevante no log

PROTEÇÃO DE DADOS NO CASO DE PERDA OU ROUBO DO DISPOSITIVO

Esta seção fornece informações sobre o Anti-Roubo que, no caso de roubo ou perda, bloqueia o acesso não autorizado aos dados salvos no seu dispositivo móvel e facilita encontrar o dispositivo.

Esta seção também especifica como ativar/desativar a função Anti-Roubo, configurar os parâmetros da sua operação e iniciar o Anti-Roubo a partir de outro dispositivo móvel de forma remota.

NESTA SEÇÃO

Sobre o Anti-Roubo.....	55
Bloqueio do dispositivo.....	56
Exclusão dos dados pessoais.....	57
Criação de uma lista de pastas para excluir.....	59
Monitoramento da substituição de um cartão SIM no dispositivo.....	60
Determinação das coordenadas geográficas do dispositivo.....	61
Inicialização das funções do Anti-Roubo de forma remota.....	63

SOBRE O ANTI-ROUBO

O Anti-Roubo protege as informações armazenadas no seu dispositivo móvel do acesso não autorizado.

O Anti-Roubo inclui as seguintes funções:

- **Bloqueio** – permite o bloqueio do dispositivo de forma remota e dá o texto a ser exibido na tela do dispositivo bloqueado.
- **Limpeza de Dados** – permite que você exclua a seguinte informação pessoal do dispositivo de forma remota: Entradas de cartão SIM e Contatos, SMS, log de chamadas, calendário, configurações de conexão com a Internet, contas do usuário (exceto as contas do Google), assim também como arquivos da lista de pastas a serem excluídas.

O Kaspersky Mobile Security 9 exclui somente contatos no cartão SIM em dispositivos com versão 2.0 ou mais recente do sistema operacional Android.

- **SIM Watch** permite obter o número de telefone atual no caso de substituição do cartão SIM, assim como bloquear o dispositivo se o cartão SIM for bloqueado ou se o dispositivo estiver ativado sem um cartão SIM. As informações sobre um novo número de telefone são enviadas como uma mensagem para o telefone e / ou e-mail que você especificou.
- A funcionalidade **Localização GPS** permite que você localize um dispositivo. As coordenadas geográficas do dispositivo são enviadas como uma mensagem para o número de telefone do qual foi enviado um comando SMS especial e para um endereço de e-mail.

Após a instalação do Kaspersky Mobile Security 9, todas as funções do Anti-Roubo são desativadas.

O Kaspersky Mobile Security 9 pode remotamente iniciar o Anti-Roubo com envio de comandos SMS de outro dispositivo móvel (ver "Início remoto das funções do Anti-Roubo" na página [63](#)).

Para iniciar de forma remota as funções do Anti-Roubo, você deve conhecer o código secreto do aplicativo que foi definido na primeira inicialização do Kaspersky Mobile Security 9 do dispositivo, para o qual o comando SMS foi enviado.

O status atual de todas as funções é exibido na tela **Anti-Roubo** próxima do nome da função.

BLOQUEIO DO DISPOSITIVO

Após o recebimento do comando SMS especial, a função de Bloqueio permite que você bloqueie de forma remota o acesso ao dispositivo e às informações armazenadas nele. O dispositivo pode ser somente desbloqueado inserindo o código secreto.

Esta função não bloqueia o dispositivo, mas simplesmente ativa a opção de bloqueio remoto.

➤ *Para ativar a função de Bloqueio:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Anti-Roubo**.
2. Clique **Bloquear: <status atual da função>**.
Isso abrirá a janela **Bloquear**.
3. Marque a caixa **Ativar Bloqueio**.
4. Insira a mensagem que será exibida na tela do dispositivo no modo bloqueado no campo **Texto quando bloqueado**. Por padrão, o texto padrão no qual você pode adicionar o telefone do proprietário é usado para a mensagem.

Se a função de Bloqueio está ativada em outro dispositivo, você pode bloqueá-la usando qualquer dos métodos a seguir:

- Use um aplicativo móvel da Kaspersky Lab, como o Kaspersky Mobile Security 9, em outro dispositivo móvel para criar e enviar um comando SMS para o seu dispositivo. Para criar um comando SMS especial, use a função **Enviar comando**. Como resultado, seu dispositivo receberá um SMS secreto e o dispositivo será bloqueado.
- Em outro dispositivo móvel, crie e envie um SMS com o texto especial e o código secreto anteriormente definido para o recebimento do dispositivo. Como resultado, seu dispositivo receberá um SMS secreto e o dispositivo será bloqueado.

As mensagens de SMS de saída serão cobradas com as taxas definidas pelo provedor de serviço móvel do outro dispositivo móvel.

Para bloquear de forma remota o dispositivo, recomenda-se o uso de um método seguro com a função de **Enviar comando**. O código secreto do aplicativo é então enviado em forma criptografada.

➤ *Para enviar um comando SMS para outro dispositivo usando a função **Enviar comando**:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Adicional**.
Isso abrirá a janela **Adicional**.
2. Selecione **Envio de um comando SMS**.

3. Para a configuração de **Comando SMS**, selecione **Bloquear**.
4. No campo **Número de telefone recebendo o comando SMS**, insira o número de telefone do dispositivo que recebe o comando SMS.
5. No campo **Código secreto do número de telefone recebendo o comando SMS**, insira o código secreto do aplicativo declarado no dispositivo que recebe o comando SMS.
6. Pressione **Enviar**.

➔ *Para criar um SMS com as funções padrão de criação de SMS do telefone,*

envie um SMS padrão para outro dispositivo; deve conter o texto `block:<código>`, onde `<código>` é o código secreto do aplicativo definido em outro dispositivo. A mensagem não é um caso sensível e os espaços antes e depois dos dois pontos serão ignorados.

EXCLUSÃO DOS DADOS PESSOAIS

Após o recebimento do comando SMS especial, a função de Limpeza de Dados permite que você exclua as seguintes informações armazenadas no dispositivo:

- detalhes pessoais do usuário (entradas em Contatos no cartão SIM, SMS, log de chamadas, calendário, configurações de conexão com a Internet, entradas de login com exceção da entrada de login do Google;
- arquivos da lista de objetos para exclusão (ver a seção "Criação de uma lista de pastas para excluir" na página [59](#)).

Esta função não exclui os dados salvos no dispositivo, mas inclui a opção para excluí-los.

➔ *Para ativar a função de Limpeza de Dados:*

1. Na janela principal do Kaspersky Mobile Security 9, abra a pasta **Anti-Roubo**.
2. Clique **Limpeza de Dados: <status atual da função>**.
Isso abrirá a janela **Limpeza de Dados**.
3. Marque a caixa **Ativar Limpeza de Dados**.
4. Selecione as informações que você deseja excluir. Para fazer isso, marque as caixas próximas das configurações desejadas no bloco **Informações a serem excluídas** (ver Figura abaixo):
 - para excluir os dados pessoais, marque a caixa **Dados pessoais**;
 - para excluir arquivos da lista de pastas a serem excluídas, defina a caixa de seleção **Pastas** e vá para criação de lista para exclusão (ver seção "Criação de lista de pastas a serem excluídas" na página [59](#)).

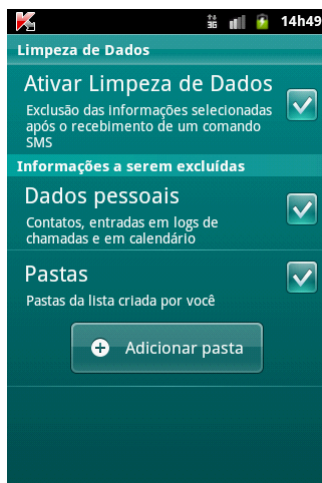


Figura 17. Configurações da função de Limpeza de Dados

Você pode excluir os dados pessoais do dispositivo com a função ativada usando os seguintes métodos:

- Use um aplicativo móvel da Kaspersky Lab, como o Kaspersky Mobile Security 9, em outro dispositivo móvel para criar e enviar um comando SMS para o seu dispositivo. Como resultado, seu dispositivo recebe uma mensagem de SMS secreta que depois a informação será excluída. Para criar um comando SMS especial, use a função **Enviar comando**.
- Em outro dispositivo móvel, crie e envie um SMS com o texto especial e o código secreto anteriormente definido para o recebimento do dispositivo. Como resultado, seu dispositivo recebe uma mensagem de SMS secreta que depois a informação será excluída.

As mensagens de SMS de saída serão cobradas com as taxas definidas pelo provedor de serviço móvel do outro dispositivo móvel.

Para excluir as informações de forma remota do dispositivo, recomenda-se o uso de um método seguro com a função de **Enviar comando**. O código secreto do aplicativo é então enviado em forma criptografada.

➔ Para enviar um comando SMS para outro dispositivo usando a função **Enviar comando**:

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Adicional**.
Isso abrirá a janela **Adicional**.
2. Selecione **Enviar comando**.
3. Para a configuração de **Comando SMS**, selecione **Limpeza de Dados**.
4. No campo **Número de telefone recebendo o comando SMS**, insira o número de telefone do dispositivo que recebe o comando SMS.
5. No campo **Código secreto do número de telefone recebendo o comando SMS**, insira o código secreto do aplicativo declarado no dispositivo que recebe o comando SMS.
6. Pressione **Enviar**.

➔ Para criar um SMS com as funções padrão de criação de SMS do telefone:

envie um SMS padrão para outro dispositivo; deve conter o texto `wipe:<código>` onde `<código>` é o código secreto do aplicativo definido em outro dispositivo. A mensagem não é um caso sensível e os espaços antes e depois dos dois pontos serão ignorados.

CRIAÇÃO DE UMA LISTA DE PASTAS PARA EXCLUIR

A função de Limpeza de Dados permite que você crie uma lista de pastas a serem excluídas após o recebimento de um comando SMS especial.

Para ativar Anti-Roubo para excluir todas as pastas da lista após o recebimento de uma mensagem SMS especial, certifique-se de que a caixa **Pastas** está selecionada nas configurações de Limpeza de Dados.

➤ *Para adicionar à lista de pastas a serem excluídas:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o Pasta **Anti-Roubo**.
2. Clique **Limpeza de Dados**.

Isso abrirá a janela **Limpeza de Dados**.

3. Clique **Adicionar** (ver Figura abaixo).

A janela **Seleção de pasta** abre.

4. Selecione a pasta necessária clicando no ícone à direita do nome da pasta.

A pasta é adicionada à lista de pastas para exclusão localizada abaixo das configurações **Pasta**

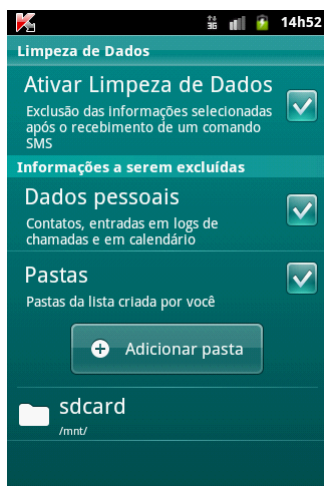


Figura 18. Adição de uma pasta

➤ *Para remover a pasta da lista:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Anti-Roubo**.
2. Clique **Limpeza de Dados**.

Isso abrirá a janela **Limpeza de Dados**.

3. Vá para a lista de objetos para exclusão.
4. Selecione uma pasta da lista e clique **Excluir pasta** no menu de contexto.

A pasta é excluída da lista de pastas para exclusão.

MONITORAMENTO DA SUBSTITUIÇÃO DE UM CARTÃO SIM NO DISPOSITIVO

Se o cartão SIM é substituído, o SIM Watch permite que você envie uma mensagem com o novo número para seu telefone e / ou e-mail ou que você bloqueie o dispositivo.

➤ *Para ativar a função SIM Watch e monitorar a substituição do cartão SIM:*

1. Na janela principal do Kaspersky Mobile Security 9, o módulo **Anti-Roubo** abre.
2. Clique em **SIM Watch: <status atual do componente>**.

Isso abrirá a janela **SIM Watch**.

3. Marque a caixa **Ativar SIM Watch**.
4. Para verificar a substituição do cartão SIM no dispositivo, faça as seguintes configurações:

- Para receber automaticamente um SMS usando o número do seu telefone, insira um número de telefone para o qual o SMS será enviado no módulo **Enviar novo número** para a configuração do **Número de telefone**.

O número de telefone pode começar com um dígito ou com "+" e deve conter somente dígitos.

- Para receber um e-mail com o número de telefone, no módulo **Enviar novo número** insira um endereço de e-mail para a configuração **Endereço de e-mail**.
- Para bloquear o dispositivo se o cartão SIM for substituído ou se o dispositivo estiver ligado com o cartão SIM removido, marque a caixa **Bloquear dispositivo** no bloco **Adicional**. Somente é possível desbloquear o dispositivo se for inserido o código secreto do aplicativo.
- Para exibir a mensagem na tela no status bloqueado, insira o texto da mensagem no módulo **Adicional** para a configuração **Texto quando bloqueado**.

Por padrão, o texto padrão no qual você pode adicionar o número do proprietário é usado para a mensagem.

A configuração é acessível se a caixa de seleção **Bloquear** estiver selecionada.



Figura 19. Configurações da função SIMWatch

DETERMINAÇÃO DAS COORDENADAS GEOGRÁFICAS DO DISPOSITIVO

Após o recebimento de um comando SMS especial, a Localização GPS permite que você detecte as coordenadas geográficas do dispositivo e as envie por SMS e e-mail para o dispositivo solicitado e para o e-mail.

As mensagens de SMS de saída serão cobradas com a taxa do seu provedor de serviço móvel.

Se o receptor GPS for instalado no dispositivo, é ativado automaticamente após o dispositivo receber um comando SMS especial. Se a função Localização GPS não puder obter as coordenadas do dispositivo com o uso do GPS, ela determina as coordenadas aproximadas do dispositivo com base nas estações de base.

➤ Para ativar a função de Localização GPS:

1. Na janela principal do Kaspersky Mobile Security 9, abra o Pasta **Anti-Roubo**.
2. Clique em **Localização GPS: <status atual do componente>**.
Isso abrirá a janela **Localização GPS**.
3. Marque a caixa **Ativar Localização GPS**.

Após o recebimento de um comando SMS especial, o Kaspersky Mobile Security 9 envia automaticamente as coordenadas do dispositivo por um SMS de resposta para o número do qual o comando SMS foi enviado.

4. Para receber também as coordenadas do dispositivo por e-mail, insira um endereço de e-mail no módulo **Enviar coordenadas do dispositivo** para as configurações **Endereço de e-mail** (ver Figura abaixo).

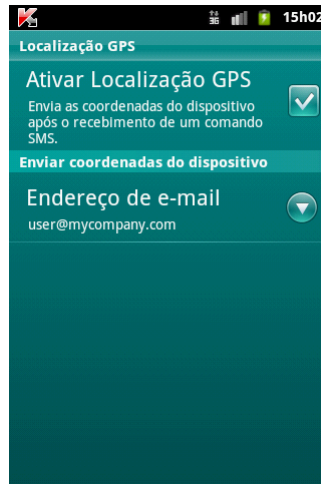


Figura 20. Configurações da função de Localização GPS

Você pode solicitar as coordenadas de um dispositivo no qual a Localização GPS está ativada, usando os seguintes métodos:

- Use um aplicativo móvel da Kaspersky Lab, como o Kaspersky Mobile Security 9, em outro dispositivo móvel para criar e enviar um comando SMS para o seu dispositivo. Como resultado, seu dispositivo receberá um SMS secreto e o aplicativo enviará as coordenadas do dispositivo. Para criar um comando SMS especial, use a função Enviar comando.
- Em outro dispositivo móvel, crie e envie um SMS com o texto especial e o código secreto anteriormente definido para o recebimento do dispositivo. Como resultado, seu dispositivo receberá um SMS secreto e o aplicativo enviará as coordenadas do dispositivo.

As mensagens de SMS de saída serão cobradas com as taxas definidas pelo provedor de serviço móvel do outro dispositivo móvel.

Para receber a localização do dispositivo, recomenda-se o uso de um método seguro com a função de Enviar comando. O código secreto do aplicativo é então enviado em modo criptografado.

➔ Para enviar um comando para outro dispositivo usando a função Enviar comando:

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Adicional**.
Isso abrirá a janela **Adicional**.
2. Clique em **Enviar comando**.
3. Selecione o valor em **Localização GPS** para a configuração **Selecionar comando SMS**.
4. No campo **Número de telefone recebendo o comando SMS**, insira o número de telefone do dispositivo que recebe o comando SMS.
5. No campo **Código secreto do número de telefone recebendo o comando SMS**, insira o código secreto do aplicativo declarado no dispositivo que recebe o comando SMS.
6. Pressione **Enviar**.

➔ Para criar um SMS com as funções padrão de criação de SMS do telefone:

envie um SMS para outro dispositivo; a mensagem deve conter o texto `find:<código> onde <código>` é o código secreto do aplicativo definido em outro dispositivo. A mensagem não é um caso sensível e os espaços antes e depois dos dois pontos serão ignorados.

Uma mensagem de SMS com as coordenadas do dispositivo será enviada para o número de telefone do qual o comando SMS foi enviado e para um e-mail se você tiver especificado um nas opções de Localização GPS.

INICIALIZAÇÃO DAS FUNÇÕES DO ANTI-ROUBO DE FORMA REMOTA

O aplicativo permite o envio de um comando SMS especial para executar as funções do Anti-Roubo de forma remota em outro dispositivo com o Kaspersky Mobile Security instalado. Um comando SMS é enviado como um SMS criptografado e contém o código secreto definido no outro dispositivo. A recepção do comando SMS não será observada.

O SMS será cobrado com a taxa atual do seu provedor de serviço móvel.

➤ Para enviar um comando SMS para outro dispositivo:

1. Na janela principal do Kaspersky Mobile Security 9, amplie o módulo **Adicional**.
2. Selecione a função para inicializar remotamente em outro dispositivo móvel. Para fazer isso, selecione um dos seguintes valores propostos para a configuração **Selecionar comando SMS** (ver Figura abaixo):
 - **Bloquear;**
 - **Limpeza de Dados;**
 - **Localização GPS.**
 - **Proteção de Privacidade.**
3. No campo **Número de telefone recebendo o comando SMS**, insira o número de telefone do dispositivo que recebe o comando SMS.
4. No campo **Código secreto do número de telefone recebendo o comando SMS**, insira o código secreto do aplicativo declarado no dispositivo que recebe o comando SMS.
5. Pressione **Enviar**.

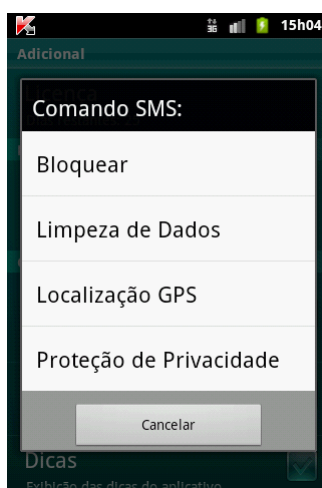


Figura 21. Inicialização remota das funções de Anti-Roubo e Proteção de Privacidade

PROTEÇÃO DE PRIVACIDADE

A seção apresenta informações sobre a Proteção de Privacidade que pode ocultar as informações confidenciais do usuário.

NESTA SEÇÃO

Proteção de Privacidade	64
Modos de Proteção de Privacidade	64
Ativação/Desativação da Proteção de Privacidade	65
Ativação automática da Proteção de Privacidade	65
Ativação remota da Proteção de Privacidade	66
Seleção de dados para ocultar: Proteção de Privacidade	68
Criação de uma lista de números privados	68

PROTEÇÃO DE PRIVACIDADE

A Proteção de Privacidade oculta os dados privados com base na sua Lista de Contatos que lista os números privados. Para os números confidenciais, a Proteção de Privacidade oculta as entradas de Contatos, de entrada, rascunhos e envia SMS assim como as entradas do histórico de chamadas. A Proteção de Privacidade omite o novo sinal de SMS e oculta as mensagens na caixa de entrada. A Proteção de Privacidade bloqueia as chamadas de entrada de números privados e não mostra na tela as informações da chamada de entrada. Como resultado, o autor da chamada recebe um sinal de ocupado. Para visualizar as chamadas e SMSs de entrada para o período em que a Proteção de Privacidade estava ativada, desative Proteção de Privacidade. Ao repetir a ativação da Proteção de Privacidade, as informações não serão exibidas.

Você pode ativar a Proteção de Privacidade do Kaspersky Mobile Security 9 ou de forma remota de outro dispositivo móvel. No entanto, a Proteção de Privacidade pode somente ser desativada do aplicativo.

MODOS DE PROTEÇÃO DE PRIVACIDADE

Você pode administrar o modo de operação da Proteção de Privacidade. O modo define se a Proteção de Privacidade está ativada ou desativada.

Por padrão, a Proteção de Privacidade está desativada.

Os seguintes modos de Proteção de Privacidade estão disponíveis:

- **O modo de Proteção de Privacidade configurado para Normal** – a ocultação de informações confidenciais está desativada. As configurações de Proteção de Privacidade são acessíveis para modificação.
- **O modo de Proteção de Privacidade configurado para Privado** – a ocultação de informações confidenciais está ativada. As configurações de Proteção de Privacidade não podem ser modificadas.

Você pode configurar a Proteção de Privacidade para iniciar automaticamente (ver seção "Ativação automática da Proteção de Privacidade" na página [65](#)) ou iniciar de forma remota de outro dispositivo (ver seção "Ativação remota da Proteção de Privacidade" na página [66](#)).

O status atual de ocultação das informações confidenciais é exibido na janela principal do aplicativo no módulo **Proteção de Privacidade**

ATIVAÇÃO/DESATIVAÇÃO DA PROTEÇÃO DE PRIVACIDADE

➤ *Para alterar o modo de Proteção de Privacidade:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Proteção de Privacidade**.
2. Clique **Ocultar informações** (ver Figura abaixo).

O nome do item altera dependendo do modo de Proteção de Privacidade. Se o **O modo de Proteção de Privacidade configurado para Normal** é selecionado, o item é chamado de **Ocultar informações**. Se o modo **Informações confidenciais estão ocultadas** é selecionado, o item é chamado de **Exibir informações**.

A alteração do modo de Proteção de Privacidade pode levar algum tempo.

O modo atual de ocultação de Proteção de Privacidade é exibido no módulo **Proteção de Privacidade**.

O ícone de troca para à direita do item **Ocultar informações / Exibir informações** é alterado dependendo do modo selecionado.



Figura 22. Alteração do modo de Proteção de Privacidade

ATIVAÇÃO AUTOMÁTICA DA PROTEÇÃO DE PRIVACIDADE

Você pode configurar o modo automático ativando a ocultação de informações confidenciais após um intervalo de tempo especificado. A função fica ativada após a troca do dispositivo para o modo de economia de energia.

Desativação da Proteção de Privacidade antes de editar as configurações da Proteção de Privacidade.

➤ *Para ativar a Proteção de Privacidade de forma automática após um intervalo de tempo especificado decorrido:*

1. Na janela principal do Kaspersky Mobile Security 9, o módulo **Proteção de Privacidade** é ampliado.
2. Clique em **Configurações**.

A janela de **Configurações de Proteção de Privacidade** abre.

3. Selecione um valor para a configuração **Ocultação automática** dependendo das seguintes tarefas (ver a Figura abaixo):
 - Para desativar a ativação automática da ocultação das informações confidenciais, selecione **Desativar**.
 - Para iniciar a ocultação das informações confidenciais dentro de um período de tempo definido após a troca do dispositivo para o modo de economia de energia, selecione um dos seguintes valores:
 - **Sem atraso.**
 - **Após 1 minuto.**
 - **Após 5 minutos.**
 - **Após 15 minutos.**
 - **Após 1 hora.**

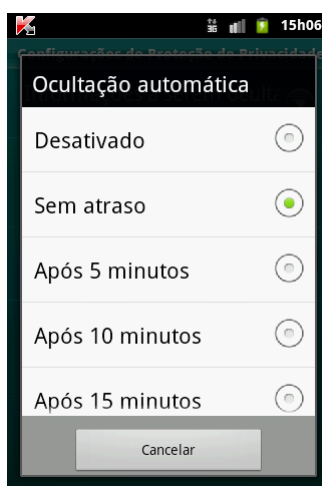


Figura 23. Início automático da Proteção de Privacidade

ATIVAÇÃO REMOTA DA PROTEÇÃO DE PRIVACIDADE

O Kaspersky Mobile Security 9 permite que você ative a Proteção de Privacidade de forma remota a partir de outro dispositivo móvel. Para isso, primeiro ative a opção Ocultar no comando SMS no seu dispositivo.

➤ *Para permitir a ativação remota da Proteção de Privacidade:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Proteção de Privacidade**.
2. Clique em **Configurações**.
A janela de **Configurações de Proteção de Privacidade** abre.
3. Marque a caixa **Ocultar no comando SMS** (ver Figura abaixo).

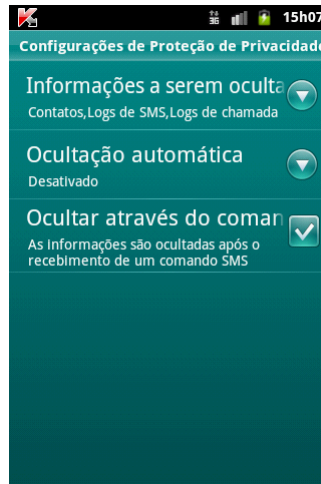


Figura 24. Configurações de ativação remota da Proteção de Privacidade

Você pode ativar a Proteção de Privacidade de forma remota usando qualquer um dos seguintes métodos:

- Use um aplicativo móvel da Kaspersky Lab, como o Kaspersky Mobile Security 9, em outro dispositivo móvel para criar e enviar um comando SMS para o seu dispositivo. Como resultado, seu dispositivo recebe um SMS de forma imperceptível e as informações confidenciais são ocultadas. Para criar um comando SMS especial, use a função **Enviar comando**.
- Em outro dispositivo móvel, crie e envie um SMS com um texto especial e o código secreto do aplicativo especificado no seu dispositivo. Como resultado, seu dispositivo recebe um SMS e as informações confidenciais são ocultadas.

Os SMSs de saída serão cobrados com as taxas definidas pelo provedor móvel para o telefone onde o comando SMS se origina.

➔ *Para iniciar a ocultação remota das informações confidenciais a partir de outro dispositivo móvel com o comando SMS especial:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Adicional**.
2. Isso abrirá a janela **Adicional**.
3. Selecione **Enviar comando**.
4. Para o **Comando SMS**, configure o valor de **Proteção de Privacidade**.
5. No campo **Número de telefone recebendo o comando SMS**, insira o número de telefone do dispositivo que recebe o comando SMS.
6. No campo **Código secreto do número de telefone recebendo o comando SMS**, insira o código secreto do aplicativo declarado no dispositivo que recebe o comando SMS.
7. Pressione **Enviar**.

Quando um comando SMS é recebido no dispositivo, o Kaspersky Mobile Security 9 ativa a ocultação das informações confidenciais e as informações no dispositivo são ocultadas.

➔ *Para ativar a Proteção de Privacidade de forma remota usando as ferramentas padrão do telefone para criar um SMS:*

envie um SMS para outro dispositivo; a mensagem deve conter o texto `hide:<código>` onde `<código>` é o código secreto do aplicativo definido em outro dispositivo. A mensagem não é um caso sensível e os espaços antes e depois dos dois pontos serão ignorados.

SELEÇÃO DE DADOS PARA OCULTAR: PROTEÇÃO DE PRIVACIDADE

A Proteção de Privacidade pode ocultar as seguintes informações para números na Lista de Contatos: contatos, correspondência de SMS, entradas no log de chamadas e mensagens de SMS. Você pode selecionar as informações e eventos que a Proteção de Privacidade deve ocultar para os números privados.

Desativação da Proteção de Privacidade antes de editar as configurações da Proteção de Privacidade.

➔ Para selecionar as informações e eventos que devem ser ocultados para os números privados:

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Proteção de Privacidade**.
2. Clique em **Configurações**.

A janela de **Configurações de Proteção de Privacidade** abre (ver Figura abaixo).

3. Selecione as informações e eventos que estão ocultados para números confidenciais. Para fazer isso, configure **Informações a serem ocultadas** e selecione a caixa de seleção próxima das configurações necessárias. As configurações a seguir estão disponíveis:
 - **Contatos** – oculta todas as informações sobre os números confidenciais em Contatos.
 - **Logs de SMS** — oculta as mensagens de SMS nas pastas **De entrada**, **De saída** e **Enviadas** para números confidenciais.
 - **SMS de chegada** – oculta SMS de entrada de números privados.
 - **Logs de chamadas** – aceita as chamadas de números confidenciais, mas não mostra o número do autor da chamada e nem as informações sobre os números confidenciais na lista de chamadas (de entrada, de saída e perdidas).
 - **Chamadas de entrada** – bloqueia as chamadas de números privados (neste caso, o autor da chamada escutará um sinal de ocupado). As informações sobre as chamadas recebidas serão exibidas quando a Proteção de Privacidade estiver desativada.

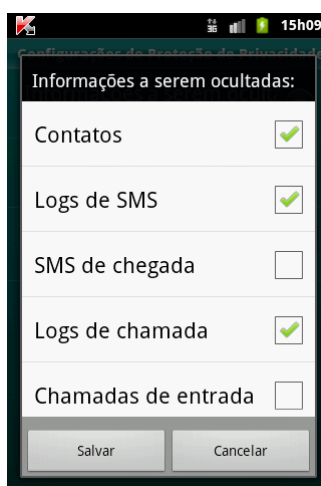


Figura 25. Seleção de informações e eventos ocultados

CRIAÇÃO DE UMA LISTA DE NÚMEROS PRIVADOS

A Lista de Contatos contém os números privados para o qual a Proteção de Privacidade oculta as informações e eventos. Você pode ampliar a lista adicionando manualmente um número ou importando um de Contatos ou do cartão SIM.

Antes de fazer a Lista de Contatos, desative a ocultação de informações confidenciais.

NESTA SEÇÃO

Adição de um número à lista de números privados	69
Edição de um número na lista de números privados	70
Exclusão de um número da lista de números privados.....	70

ADIÇÃO DE UM NÚMERO À LISTA DE NÚMEROS PRIVADOS

Você pode adicionar manualmente números de telefones à Lista de contatos ou importá-los de Contatos.

Antes de fazer a Lista de Contatos, desative a ocultação de informações confidenciais.

➔ Para adicionar um número de telefone à Lista de contatos:

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Proteção de Privacidade**.
2. Clique em **Lista de contatos**.

A janela da **Lista de Contatos** abrirá.

3. Realize uma das seguintes ações (ver Figura abaixo):

- Para adicionar um número de Contatos, selecione **Adicionar** → **Contatos**. Selecione a entrada requerida na janela Lista de Contatos que será aberta.
- Para adicionar um número, selecione **Adicionar** → **Número**, preencha o campo **Número de telefone** e pressione **Salvar**.

O número será adicionada na Lista de Contatos

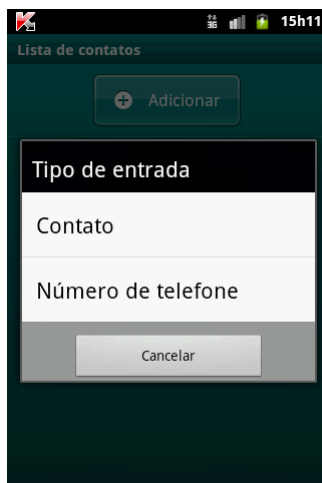


Figura 26. Adição de entradas na lista de contatos protegidos

EDIÇÃO DE UM NÚMERO NA LISTA DE NÚMEROS PRIVADOS

Desativação da Proteção de Privacidade antes de editar as configurações da Proteção de Privacidade.

Os números de telefone adicionados manualmente estão somente disponíveis para edição na Lista de Contatos. Não é possível editar números que foram selecionados a partir de Contatos.

➤ *Para editar um número de telefone na Lista de Contatos:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Proteção de Privacidade**.
2. Clique em **Lista de contatos**.
A janela da **Lista de Contatos** abrirá.
3. Selecione da Lista de contatos um número para edição e selecione **Editar** no menu de contexto.
A janela **Edição de uma entrada** abre.
4. Altere os dados.
5. Ao concluir a edição, pressione **Salvar**.

O número está alterado.

EXCLUSÃO DE UM NÚMERO DA LISTA DE NÚMEROS PRIVADOS

Você pode excluir um número ou apagar a Lista de contatos completamente.

Desativação da Proteção de Privacidade antes de editar as configurações da Proteção de Privacidade.

➤ *Para remover um número da Lista de Contatos:*

1. Na janela principal do Kaspersky Mobile Security 9, o módulo **Proteção de Privacidade** é ampliado.
2. Clique em **Lista de contatos**.
A janela da **Lista de Contatos** abrirá.

3. Selecione o número a ser excluído e selecione **Excluir** no menu de contexto.

➤ *Para apagar a Lista de Contatos:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Proteção de Privacidade**.

2. Clique em **Lista de contatos**.

A janela da **Lista de Contatos** abrirá.

3. Selecione **Excluir todos** no menu de contexto.

A janela de confirmação abre.

4. Confirme a exclusão. Para fazer isso, pressione **Sim**.

A Lista de Contatos fica vazia.

ATUALIZAÇÃO DOS BANCOS DE DADOS DO APLICATIVO

Esta seção fornece informações sobre atualização dos bancos de dados do aplicativo, que garante proteção atualizada do seu dispositivo. Além disso, esta seção descreve como visualizar as informações sobre os bancos de dados de antivírus instalados, executar a atualização manualmente e configurar a atualização automática dos bancos de dados de antivírus.

NESTA SEÇÃO

Sobre a atualização dos bancos de dados do aplicativo.....	72
Início manual das atualizações	73
Início das atualizações agendadas	73

SOBRE A ATUALIZAÇÃO DOS BANCOS DE DADOS DO APLICATIVO

O aplicativo verifica o dispositivo para programas malware usando o banco de dados de antivírus do aplicativo, que contém descrições de todos os programas indesejados e malwares atualmente conhecidos, e os métodos para seu tratamento. É extremamente importante manter seus bancos de dados de antivírus atualizados.

Recomenda-se atualizar regularmente os bancos de dados do aplicativo. Se já passaram mais de 15 dias desde a última atualização, os bancos de dados são considerados desatualizados. A proteção será menos confiável.

O Kaspersky Mobile Security 9 realiza atualizações do banco de dados do aplicativo a partir dos servidores de atualização da Kaspersky Lab. São sites especiais da Internet que contêm atualizações para os bancos de dados de todos os produtos da Kaspersky Lab.

Para atualizar os bancos de dados de antivírus do aplicativo, você deve configurar uma conexão com a Internet no seu dispositivo móvel.

Os bancos de dados de antivírus do aplicativo são atualizados de acordo com os seguintes algoritmos:

1. Os bancos de dados do aplicativo instalados no seu dispositivo móvel são comparados com aqueles localizados no servidor de atualização especial da Kaspersky Lab.
2. O Kaspersky Mobile Security 9 executa uma das seguintes ações:
 - Se você possui instalado os bancos de dados de antivírus mais recentes, uma mensagem é mostrada na tela.
 - Se os bancos de dados de antivírus instalados são diferentes, um novo pacote de atualização será baixado e instalado.

Quando o processo de atualização tiver concluído, a conexão é automaticamente fechada. Se a conexão foi estabelecida antes do início da atualização, permanecerá aberta para maior uso.

Você pode iniciar a tarefa de atualização manualmente a qualquer momento quando o dispositivo não estiver ocupado com outras tarefas ou agendar as atualizações automáticas.

Ao fazer o roaming, é possível desativar a atualização do banco de dados de antivírus do Kaspersky Mobile Security 9 para evitar custos desnecessários.

As informações detalhadas sobre os bancos de dados de antivírus usados estão acessíveis em **Antivírus** → **Adicional** em **Iniciar atualização**.

INÍCIO MANUAL DAS ATUALIZAÇÕES

Você pode iniciar manualmente a atualização dos bancos de dados de antivírus do aplicativo.

➤ *Para iniciar manualmente o processo de atualização do banco de dados de antivírus do aplicativo:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Antivírus**.
2. Clique em **Adicional**.
A janela **Antivírus: Adicional** abre.
3. Clique em **Iniciar atualização**.

O aplicativo inicia o processo de atualização dos bancos de dados do servidor da Kaspersky Lab. As informações sobre o processo de atualização são mostradas na tela.

INÍCIO DAS ATUALIZAÇÕES AGENDADAS

As atualizações regulares são pré-requisitos de proteção eficaz do seu dispositivo em relação à infecção por objetos malware. Para sua conveniência, você pode configurar atualizações de banco de dados automáticas e criar uma agenda de atualização.

Para executar uma atualização, o dispositivo deverá permanecer ligado por todo tempo de verificação.

Além disso, você pode configurar a atualização automática quando estiver em roaming.

➤ *Para configurar um início de atualização agendada:*

1. Na janela principal do Kaspersky Mobile Security 9, amplie o módulo **Antivírus**.
2. Clique em **Adicional**.
A janela **Antivírus: Adicional** abre.
3. Selecione **Atualizar configurações**.
A janela **Atualizar configurações** abre.
4. Defina um dos seguintes valores para as configurações de **Atualização agendada**:
 - **Semanalmente**: atualiza os bancos de dados do aplicativo uma vez por semana. Selecione os valores para o **Dia de início** e a **Hora de início**.
 - **Diariamente**: atualiza os bancos de dados do aplicativo todos os dias. Insira um valor para a **Hora da atualização**.
 - **Desativado** – não atualiza os bancos de dados do aplicativo na agenda.

DEFINIÇÃO DAS CONFIGURAÇÕES ADICIONAIS

Esta seção fornece informações sobre as opções adicionais do Kaspersky Mobile Security 9: como ativar/desativar as mensagens emergentes na linha de status na operação do aplicativo, notificação sonora, exibição de avisos antes de ajustar as configurações de todos os componentes, como configurar o widget da tela inicial e como alterar o código secreto do aplicativo.

NESTA SEÇÃO

Alteração do código secreto	74
Exibição de avisos	74
Configuração das notificações sonoras	75
Mensagens na linha de status.....	75

ALTERAÇÃO DO CÓDIGO SECRETO

Você pode alterar o código secreto definido após a primeira inicialização do aplicativo.

➤ *Para alterar o código secreto:*

1. Na janela principal do Kaspersky Mobile Security 9, amplie o módulo **Adicional**.
Isso abrirá a janela **Adicional**.
2. Selecione **Alterar código secreto**.
3. Insira o código secreto atual do aplicativo no campo de entrada **Inserir código secreto** e pressione **Seguinte**.
4. Insira o novo código secreto do aplicativo no campo **Definir novo código secreto** e pressione **Seguinte**.

O código inserido é automaticamente verificado.

Se o código for considerado inválido de acordo com os resultados da verificação, uma mensagem de aviso é mostrada e o aplicativo solicitará confirmação. Para usar o código, pressione **Sim**. Para criar um novo código, pressione **Não**. Insira um novo código secreto do aplicativo.

5. Insira este código novamente no campo **Inserir repetidamente o novo código**.

O código secreto é alterado.

EXIBIÇÃO DE AVISOS

Quando definir as configurações dos componentes, por padrão, o Kaspersky Mobile Security 9 exibe um aviso com uma descrição breve da função selecionada. Você pode configurar a exibição das dicas do Kaspersky Mobile Security 9.

➤ *Para configurar a exibição de dicas, execute as seguintes ações:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo da guia **Adicional**.

Isso abrirá a janela **Adicional**.

2. Realize ações dependendo das seguintes tarefas:
 - Para ativar a exibição de avisos, marque a caixa de seleção **Dicas**.
 - Para desativar a exibição de avisos, desmarque a caixa de seleção **Dicas**.

CONFIGURAÇÃO DAS NOTIFICAÇÕES SONORAS

Como resultado da operação do aplicativo, surgem eventos, por exemplo, um arquivo infectado é detectado, o prazo de validade da licença expirou. Para o aplicativo informá-lo sobre todos os eventos, você pode ativar a notificação sonora da ocorrência do evento.

O Kaspersky Mobile Security 9 inclui notificação sonora somente de acordo com o modo definido do dispositivo.

➤ *Para administrar a notificação sonora do aplicativo, realize os seguintes passos:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo da guia **Adicional**.
Isso abrirá a janela **Adicional**.
2. Realize ações dependendo das seguintes tarefas:
 - Para ativar a notificação sonora, marque a caixa de seleção **Som**.
 - Para desativar a notificação sonora, desmarque a caixa de seleção **Som**.

MENSAGENS NA LINHA DE STATUS

O Kaspersky Mobile Security 9 permite receber notificações emergentes na linha de status sobre os eventos do aplicativo, por exemplo, sobre a inicialização do aplicativo, a data de expiração da validade da licença ou a desativação da proteção. Você pode ativar / desativar o recebimento de notificações sobre os eventos do aplicativo na linha de status.

➤ *Para administrar as notificações emergentes na operação do aplicativo, proceda da seguinte forma:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo da guia **Adicional**.
Isso abrirá a janela **Adicional**.
2. Realize ações dependendo das seguintes tarefas:
 - Para ativar notificações emergentes na operação do aplicativo, marque a caixa de seleção **Notificações**.
 - Para desativar notificações emergentes, desmarque a caixa de seleção **Notificações**.

Ao usar o Kaspersky Mobile Security 9, o widget da tela inicial fica acessível (ver página [33](#)). O widget da tela inicial serve para indicar o status de proteção do seu dispositivo, para ocultar as informações confidenciais e para a licença do aplicativo.

Após a instalação do aplicativo, o widget aparece automaticamente na janela principal do aplicativo. Você pode adicionar um widget à janela principal ou excluí-lo e também configurar a indicação de ocultação das informações confidenciais no Widget da tela inicial (ver a seção "Ocultação das informações confidenciais" na página [64](#)).

➤ *Para administrar a exibição do widget na janela principal, proceda da seguinte forma:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o **Adicional**.

Isso abrirá a janela **Adicional**.

2. Selecione **Widget**.

A janela do **Widget da tela inicial** abre.

3. Realize ações dependendo das seguintes tarefas:

- Para exibir uma alteração no modo de ocultação das informações confidenciais no widget da tela inicial, marque a caixa de seleção **Ativar widget**.
- Para excluir o widget do Widget da tela inicial, desmarque a caixa de seleção **Ativar widget**.

➔ *Para configurar a indicação do status das informações confidenciais no Widget da tela inicial, proceda da seguinte forma:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Adicional**.

Isso abrirá a janela **Adicional**.

2. Selecione **Widget**.

A janela do **Widget da tela inicial** abre.

3. Realize ações dependendo das seguintes tarefas:

- Para exibir uma alteração no modo de ocultação das informações confidenciais no widget da tela inicial, marque a caixa de seleção **Mostrar status da Proteção de Privacidade**
- Para ocultar uma alteração no modo de ocultação das informações confidenciais no widget da tela inicial, desmarque a caixa de seleção **Mostrar status da Proteção de Privacidade**.

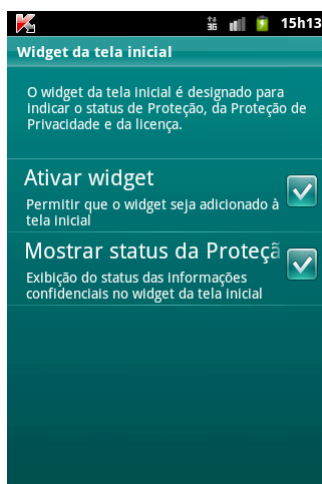


Figura 27. Configurações do widget da tela inicial

ENTRANDO EM CONTATO COM O SERVIÇO DE SUPORTE TÉCNICO

Se já comprou o Kaspersky Internet Security, você pode obter informações sobre o aplicativo provenientes do Serviço de Suporte Técnico por telefone ou pela Internet.

Os especialistas em Serviço de Suporte Técnico responderão suas perguntas sobre instalação e uso do aplicativo. Se o seu computador foi afetado, eles também irão lhe ajudar a eliminar as consequências da atividade de malware.

Antes de entrar em contato com o Serviço de Suporte Técnico, leia as Regras de suporte para os produtos da Kaspersky Lab (<http://support.kaspersky.com/support/rules>).

Envio de e-mail ao Serviço de Suporte Técnico

Você pode enviar sua pergunta para os especialistas do Serviço de Suporte Técnico preenchendo um formulário online no Helpdesk em (<http://support.kaspersky.com/helpdesk.html>).

Você pode enviar sua consulta em russo, inglês, alemão, francês ou espanhol.

Para enviar um e-mail com a sua pergunta, você deve incluir o **ID de Cliente** e a **senha** que recebeu ao se registrar no website do Serviço de Suporte Técnico.

Se você ainda não é um usuário registrado dos aplicativos da Kaspersky Lab, poderá preencher um formulário de registro (<https://support.kaspersky.com/personalcabinet/registration/form/>). Durante o registro, insira o *código de ativação* do seu aplicativo ou o *nome do arquivo chave*.

O Serviço de Suporte Técnico responderá à sua solicitação no seu Gabinete Pessoal (<https://support.kaspersky.com/PersonalCabinet>) e no endereço de e-mail que especificou em sua solicitação.

Na sua consulta, descreva o problema que encontrou. Especifique o seguinte nos campos obrigatórios:

- **Tipo de solicitação.** Selecione um tópico que mais corresponde ao problema decorrente, por exemplo "Instalação do Produto/Problema de Remoção" ou "Verificação de antivírus/Problema de remoção de antivírus". Se você não encontrar um tópico apropriado, selecione "Pergunta geral".
- **Nome de aplicativo e número da versão.**
- **Texto da solicitação.** Descreva o problema que encontrou, fornecendo o máximo possível de detalhes relevantes.
- **ID de Cliente e senha.** Insira o ID de cliente e a senha que recebeu durante o registro no website do Serviço de Suporte Técnico.
- **Endereço de e-mail.** O Serviço de Suporte Técnico responderá à sua pergunta neste endereço de e-mail.

Suporte técnico por telefone

Se tiver um problema urgente, você pode ligar para o Serviço de Suporte Técnico. Antes de entrar em contato com seu Serviço de Suporte Técnico local (<http://suporte.kasperskyamericas.com/>) ou internacional (<http://support.kaspersky.com/support/international>), colete todas as informações necessárias (<http://support.kaspersky.com/support/details>) sobre o seu dispositivo e o aplicativo de antivírus instalado. Isso permitirá que nossos especialistas o ajudem mais rapidamente.

GLOSSÁRIO

A

ALGARISMOS NÃO NUMÉRICOS

Um número de telefone que inclui letras ou é formado somente por letras.

ARQUIVO

Arquivo "contendo" um ou vários outros objetos que também podem ser arquivos.

ATIVACÃO DO APLICATIVO

Conversão do aplicativo em modo de função completa. O usuário precisa usar uma licença para ativar o aplicativo.

B

BANCOS DE DADOS ANTIVÍRUS

Bancos de dados criados pelos especialistas da Kaspersky Lab, que contêm descrições detalhadas de todas as ameaças à segurança de computadores existentes atualmente, além dos métodos usados para sua detecção e desinfecção. Esses bancos de dados são atualizados pela Kaspersky Lab constantemente conforme surgem novas ameaças.

C

CÓDIGO SECRETO DO APLICATIVO

O código secreto do aplicativo evita o acesso sem autorização às configurações do aplicativo e às informações bloqueadas no dispositivo. O usuário define-o na primeira inicialização do aplicativo e consistem de, no mínimo, quatro caracteres. O código secreto é solicitado nas seguintes instâncias:

para acessar as configurações do aplicativo;

ao enviar um comando SMS de outro dispositivo móvel para iniciar as seguintes funções de forma remota: Bloqueio, Limpeza de Dados, SIM Watch e Localização GPS e Proteção de Privacidade.

D

DESINFECÇÃO DE OBJETOS

Um método usado para o processamento de objetos infectados, que resulta na recuperação de dados parcial ou completa ou na decisão de que os objetos não podem ser desinfetados. A desinfecção de objetos é executada com base no banco de dados do aplicativo. Parte dos dados legítimos do arquivo pode ser perdida durante o processo de desinfecção.

E

EXCLUSÃO DAS MENSAGENS DE SMS

Método de processar uma mensagem de SMS contendo recursos SPAM, excluindo-os. Recomenda-se usar este método com mensagens de SMS que certamente contêm spam.

EXCLUSÃO DE UM OBJETO

Método de processamento de objetos que os exclui fisicamente de seu local original. Recomenda-se aplicar este método de processamento para quaisquer objetos maliciosos que não puderam ser desinfetados.

L**LISTA BRANCA**

As entradas nesta lista contêm as seguintes informações:

Número de telefone do qual o Filtro de Chamadas e SMS fornece as chamadas e / ou SMSs.

Tipos de eventos que o Filtro de Chamadas e SMS fornece deste número. Os seguintes tipos de eventos estão disponíveis: chamadas e SMS, somente chamadas e somente SMS.

Frase chave usada pelo Filtro de Chamadas e SMS para classificar um SMS como solicitado (não é spam). O Filtro de Chamadas e SMS fornece somente o SMS contendo a frase chave, enquanto bloqueia todos os outros SMSs.

LISTA NEGRA

As entradas nesta lista contêm as seguintes informações:

Número de telefone do qual o Filtro de Chamadas e SMS bloqueia as chamadas e / ou SMSs.

Tipos de eventos que o Filtro de Chamadas e SMS bloqueia deste número. Os seguintes tipos de eventos estão disponíveis: chamadas e SMS, somente chamadas e somente SMS.

Frase chave que o Filtro de Chamadas e SMS usa para classificar um SMS como não solicitado (spam). O Filtro de Chamadas e SMS bloqueia somente o SMS contendo a frase chave, enquanto fornece todos os outros SMSs.

M**MÁSCARA DO NÚMERO DE TELEFONE**

Colocar um número de telefone na Lista Branca ou Negra usando caracteres curinga. Os dois caracteres curinga básicos usados nas máscaras de arquivos são "*" e "?" (em que "*" representa qualquer número de qualquer caractere e "?" é usado para qualquer caractere único). Por exemplo, *1234? na Lista Negra. O Filtro de Chamadas e SMS fornece as chamadas e SMSs de um número no qual um símbolo segue a figura 1234.

O**OBJETO INFECTADO**

Objeto contendo código malicioso. O aplicativo detecta objetos infectados verificando seu código binário e descobrindo que a seção do código do objeto é idêntica à seção do código de uma ameaça conhecida. Os especialistas da Kaspersky Lab não recomendam usar esses objetos, pois eles podem propiciar a infecção do seu dispositivo.

KASPERSKY LAB

A Kaspersky Lab foi fundada em 1997. Hoje é um desenvolvedor líder de uma ampla gama de produtos de software de segurança de informações de alto desempenho, incluindo sistemas antivírus, anti-spam e anti-hacking.

A Kaspersky Lab é uma empresa internacional. Com sede na Federação Russa, a empresa possui escritórios no Reino Unido, França, Alemanha, Japão, países da Benelux, China, Polônia, Romênia e EUA (Califórnia). Um novo escritório da empresa, o Centro de Pesquisas Antivírus Europeia, foi recentemente inaugurado na França. A rede de parceiros da Kaspersky Lab possui mais de 500 empresas em todo o mundo.

Hoje, a Kaspersky Lab emprega mais de mil especialistas altamente qualificados, incluindo 10 detentores de MBA e 16 PhD. Todos os especialistas antivírus sêniores da Kaspersky Lab são membros da Organização de Pesquisadores Antivírus de Computador (CARO).

A Kaspersky Lab oferece as melhores soluções de segurança do mercado, com base na sua experiência e conhecimento únicos e obtidos em mais de 14 anos de combate a vírus de computador. Uma análise criteriosa das atividades de vírus de computador capacita os especialistas da empresa a prever tendências no desenvolvimento de malware e fornecer aos nossos usuários proteção oportuna contra novos tipos de ataques. Essa vantagem é a base dos produtos e serviços da Kaspersky Lab. Em todo momento, os produtos da empresa estão pelo menos um passo adiante de muitos outros fornecedores para oferecer ampla cobertura antivírus para usuários domésticos e clientes corporativos por igual.

Anos de trabalho árduo tornaram a empresa um dos principais desenvolvedores de software antivírus. A Kaspersky Lab foi a primeira a desenvolver muitos dos padrões modernos de software antivírus. O produto mais importante da empresa, o Kaspersky Anti-Virus, protege confiavelmente todos os tipos de sistemas de computador contra ataques de vírus, incluindo estações de trabalho, servidores de arquivo, sistemas de correio, firewalls, gateways da Internet e computadores portáteis. Os clientes da Kaspersky Lab beneficiam-se de vários serviços adicionais que asseguram o funcionamento estável dos produtos da empresa e a conformidade com seus requisitos empresariais específicos. Muitos fabricantes conhecidos utilizam o núcleo do Kaspersky Anti-Virus® em seus produtos, incluindo a Nokia ICG (EUA), Aladdin (Israel), Sybari (EUA), G Data (Alemanha), Deerfield (EUA), Alt-N (EUA), Microworld (Índia) e BorderWare (Canadá).

Os clientes da Kaspersky Lab dispõem de vários serviços adicionais que asseguram o funcionamento estável dos produtos da empresa e a conformidade total com seus requisitos empresariais específicos. Nós planejamos, instalamos e suportamos pacotes de antivírus corporativos. O banco de dados de antivírus da Kaspersky Lab é atualizado de hora em hora. A empresa fornece aos seus clientes serviço de Suporte Técnico 24 horas em vários idiomas.

Caso tenha perguntas, comentários ou sugestões, você pode nos contatar através de nossos distribuidores, ou na Kaspersky Lab diretamente. Consultas detalhadas são fornecidas por telefone ou e-mail. Você receberá respostas completas para todas as suas perguntas.

Website da Kaspersky Lab

<http://www.kaspersky.com>

Enciclopédia de Vírus:

<http://www.securelist.com/>

Laboratório antivírus:

newvirus@kaspersky.com

(somente para o envio de objetos suspeitos em arquivos comprimidos)

<http://support.kaspersky.com/virlab/helpdesk.html>

(para o envio de solicitações aos analistas de vírus)

Fórum da web da Kaspersky Lab:

<http://forum.kaspersky.com>

INFORMAÇÕES SOBRE O CÓDIGO DE TERCEIROS

O código de terceiro é usado para criar o aplicativo.

NESTA SEÇÃO

Código do programa distribuído	81
Outras informações	81

CÓDIGO DO PROGRAMA DISTRIBUÍDO

O código independente do programa de fabricantes externos é distribuído juntamente com o programa em sua forma original ou binária sem alterações.

NESTA SEÇÃO

ADB.....	81
ADBWINAPI.DLL	81
ADBWINUSBAPI.DLL	81

ADB

ADB

Copyright (C) 2005-2008, The Android Open Source Project

Distributed under the terms of the Apache License, version 2.0 of the License

ADBWINAPI.DLL

ADBWINAPI.DLL

Copyright (C) 2005-2008, The Android Open Source Project

Distributed under the terms of the Apache License, version 2.0 of the License

ADBWINUSBAPI.DLL

ADBWINUSBAPI.DLL

Copyright (C) 2005-2008, The Android Open Source Project

 Apache License

Version 2.0, January 2004

<http://www.apache.org/licenses/>

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution

incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

OUTRAS INFORMAÇÕES

Informações adicionais sobre o código de terceiros.

Para criar e verificar assinaturas digitais, o Kaspersky Internet Security utiliza a biblioteca de software de segurança de dados Crypto C da CryptoEx LLC.

Website corporativo da CryptoEx LLC: <http://www.cryptoex.ru>

ÍNDICE ALFABÉTICO

A

Adição	
Lista Branca do Filtro de Chamadas e SMS	48
lista de números confidenciais da Proteção de Privacidade	69
Lista Negra do Filtro de Chamadas e SMS	45
Agenda	
Atualização	73
Verificações por comando	39
Anti-Roubo	55
Bloqueio	56
Limpeza de Dados	57
Localização GPS	61
SIM Watch	60
Arquivos	
Verificações por comando	41
Ativação	
Filtro de Chamadas e SMS	44
Proteção de Privacidade	65
Ativação do aplicativo	21
licença	27
Atualização	
início agendado	73

B

Bloqueio	
chamadas de entrada	45
dispositivo	56
SMS de entrada	45

C

Código	
código de ativação	22, 23
código secreto do aplicativo	24
Código secreto do aplicativo	24, 25

D

Dados	
exclusão remota	57
DADOS	
INFORMAÇÕES CONFIDENCIAIS	64
Desativação	
Filtro de Chamadas e SMS	44
Proteção de Privacidade	65
DESINSTALANDO O APLICATIVO	20
Determinação da localização do dispositivo	61

E

Edição	
Lista Branca do Filtro de Chamadas e SMS	49
lista de contatos confidenciais da Proteção de Privacidade	70
Lista Negra do Filtro de Chamadas e SMS	46
Entrada	
Lista Branca do Filtro de Chamadas e SMS	48
Lista Negra do Filtro de Chamadas e SMS	45

Envio de um comando SMS	63
Exclusão	
Lista Branca do Filtro de Chamadas e SMS	50
lista de contatos confidenciais da Proteção de Privacidade	70
Lista Negra do Filtro de Chamadas e SMS	47
F	
FILTRAGEM	
CHAMADAS DE ENTRADA	43
SMS DE ENTRADA	43
Filtro de Chamadas e SMS	43
ação em relação a uma chamada	53
ação em relação ao SMS	52
algarismos não numéricos	51
Lista Branca	47
Lista Negra	45
modos	44
números que não estão em Contatos	50
I	
Inicialização	
aplicativo	26
INSTALANDO O APLICATIVO	19
L	
Licença	
ativação do aplicativo	21
Contrato de Licença	27
informações	28
renovação	29
Limpeza	
informações salvas no dispositivo	57
Lista Branca	
Filtro de Chamadas e SMS	47
Lista Negra	
Filtro de Chamadas e SMS	45
M	
Modos	
Filtro de Chamadas e SMS	44
Proteção de Privacidade	64, 65
P	
Permissão	
Chamadas de entrada	48
SMS de entrada	48
Proteção de Privacidade	64
início automático	65
início remoto	66
lista de contatos confidenciais	69
modos	64
seleção de informações e eventos a serem ocultados	68
R	
Renovação da licença	29
S	
Som	75

V

Verificações por comando	
Ações a serem realizadas em objetos.....	41
arquivos.....	41
início agendado	39