

Kaspersky Mobile Security 9

para Android OS

KASPERSKY **lab**

Manual do Utilizador

VERSÃO DO PROGRAMA: 9.0

Caro utilizador,

Obrigado por escolher o nosso produto. Esperamos que esta documentação o ajude no seu trabalho e lhe proporcione todas as respostas necessárias relativamente a este produto de software.

Nota! Este documento é propriedade do Kaspersky Lab ZAO (doravante referido como Kaspersky Lab): todos os direitos a este documento são reservados pelas leis de copyright da Federação Russa, e por tratados internacionais. A reprodução e distribuição ilegais deste documento ou de partes do mesmo resultará em responsabilidade civil, administrativa ou criminal, de acordo com as leis aplicáveis.

A reprodução ou distribuição de quaisquer materiais sob qualquer formato, incluindo traduções, apenas é permitida com autorização por escrito da Kaspersky Lab.

Este documento, bem como as imagens gráficas relacionadas com o mesmo, podem ser utilizadas para fins exclusivamente informativos, não comerciais e pessoais.

A Kaspersky Lab reserva-se o direito de alterar este documento sem aviso prévio. Pode encontrar a versão mais recente deste documento no sítio de internet da Kaspersky Lab, em <http://www.kaspersky.com/docs>.

A Kaspersky Lab não será responsável pelo conteúdo nem pela qualidade, relevância ou exactidão de quaisquer materiais utilizados neste documento cujos direitos sejam detidos por terceiros, bem como por quaisquer perdas potenciais ou reais associadas à utilização destes materiais.

Neste documento, são utilizadas marcas registadas e marcas comerciais de serviços que são propriedade dos detentores dos direitos correspondentes.

Data de revisão: 20.01.2011

© 1997-2011 Kaspersky Lab ZAO. Todos os Direitos Reservados.

<http://www.kaspersky.pt/>
<http://support.kaspersky.com/pt/>

CONTRATO DE LICENÇA DE UTILIZADOR FINAL DO KASPERSKY LAB

AVISO LEGAL IMPORTANTE A TODOS OS UTILIZADORES: LEIA COM ATENÇÃO O SEGUINTE ACORDO LEGAL ANTES DE COMEÇAR A UTILIZAR O SOFTWARE.

AO CLICAR NO BOTÃO ACEITAR NA JANELA DO CONTRATO DE LICENÇA OU AO INTRODUIR SÍMBOLO(S) CORRESPONDENTE(S) CONCORDA EM ESTAR VINCULADO PELOS TERMOS E CONDIÇÕES DESTE CONTRATO. **ESSA ACÇÃO SIMBOLIZA A SUA ASSINATURA E ESTÁ A CONCORDAR ESTAR VINCULADO AO CONTRATO, CONSTITUINDO UMA PARTE DO MESMO, E CONCORDA QUE ESTE CONTRATO É EXECUTÓRIO COMO QUALQUER OUTRO CONTRATO NEGOCIADO POR ESCRITO E ASSINADO POR SI. SE NÃO CONCORDAR COM TODOS OS TERMOS E CONDIÇÕES DESTE CONTRATO, CANCELE A INSTALAÇÃO DO SOFTWARE E NÃO O INSTALE.**

DEPOIS DE CLICAR NO BOTÃO ACEITAR NA JANELA DO CONTRATO DE LICENÇA OU APÓS TER INTRODUIZIDO O(S) SÍMBOLO(S) CORRESPONDENTE(S), TEM O DIREITO DE UTILIZAR O SOFTWARE DE ACORDO COM OS TERMOS E CONDIÇÕES DESTE CONTRATO.

1. Definições

- 1.1. **Software** refere-se ao software, incluindo quaisquer Actualizações e materiais relacionados.
- 1.2. **Detentor dos Direitos** (proprietário de todos os direitos, quer exclusivos ou relativos ao Software) refere-se à Kaspersky Lab ZAO, uma empresa incorporada de acordo com as leis da Federação Russa.
- 1.3. **Computador(es)** refere-se ao(s) hardware(s), incluindo os computadores pessoais, portáteis, estações de trabalho, assistentes digitais pessoais, 'smart phones', dispositivos manuais ou outros dispositivos electrónicos para os quais o Software foi concebido e onde o Software será instalado e/ou usado.
- 1.4. **Utilizador Final** refere-se ao(s) indivíduo(s) que instalam ou utilizam o Software a seu favor ou que utilizam legalmente uma cópia do Software; ou, se o Software for transferido ou instalado em nome de uma organização, quando se refere a um funcionário, "*Utilizador Final*" refere-se ainda à organização para a qual o Software foi transferido ou instalado ficando por este meio claramente definido que essa organização autorizou a pessoa que aceitou este contrato a fazê-lo em seu nome. Para fins deste contrato, o termo "*organização*", sem limitações, inclui quaisquer parcerias, empresas de responsabilidade limitada, corporações, associações, empresas de capitais mistos, empresas de crédito, "joint ventures", sindicatos de trabalho, empresas não constituídas em sociedade ou autoridades governamentais.
- 1.5. **Parceiro(s)** refere-se a organizações ou indivíduo(s), que distribuem o Software com base num contrato e numa licença do Detentor dos Direitos.
- 1.6. **Actualização(ões)** refere-se a todas as actualizações, revisões, correcções ("patches"), melhorias, "fixes", modificações, cópias, adições ou pacotes de manutenção, etc.
- 1.7. **Manual do Utilizador** refere-se ao manual do utilizador, guia do administrador, livro de referências e material explicativo ou de outro tipo relacionado.

2. Concessão de licença

- 2.1. O Detentor de Direitos concede, por este meio, uma licença de não exclusividade ao Utilizador Final que lhe permite armazenar, carregar, instalar, executar e visualizar (para "utilizar") o Software num número específico de Computadores, tendo como finalidade ajudar a proteger o Computador do Utilizador Final no qual o Software está instalado, contra as ameaças descritas no Manual do Utilizador, de acordo com todos os requisitos técnicos descritos no Manual do Utilizador e com os termos e condições deste Contrato (a "Licença") e o utilizador final aceita esta Licença:

Versão experimental. Se recebeu, transferiu e/ou instalou uma versão experimental do Software sendo-lhe por este meio concedida uma licença de avaliação para o Software, só pode utilizar o Software para fins de avaliação e apenas durante o período de avaliação único aplicável, a não ser se indicado o contrário, a contar da data da instalação inicial. A utilização do Software para outros fins ou para além do período de avaliação aplicável é estritamente proibida.

Software de vários ambientes; Software de vários idiomas; Software de dualidade de multimédia; várias cópias; pacotes. Se utilizar versões diferentes do Software ou edições do Software em idiomas diferentes, se receber o Software em vários suportes, se receber várias cópias do Software ou se receber o Software num pacote junto com outro software, o número total permitido de Computadores em que as versões do Software estão instaladas devem corresponder ao número de computadores especificados em licenças obtidas junto do Detentor dos Direitos e, a não ser que os termos da licença indiquem o contrário, cada licença adquirida dá-lhe o direito de instalar e utilizar o Software nessa quantidade de Computador(es), como especificado nas Cláusulas 2.2 e 2.3.

- 2.2. Se o Software foi adquirido num meio físico, o Utilizador Final tem o direito de utilizar o Software para protecção na quantidade de Computador(es) especificada na embalagem do Software ou como especificado no contrato adicional.

- 2.3. Se o Software foi adquirido através da Internet, o Utilizador Final tem o direito de utilizar o Software para protecção na quantidade de Computador(es) especificada na Licença do Software quando adquirido ou como especificado no contrato adicional.
- 2.4. Tem o direito de fazer uma cópia do Software apenas para fins de cópia de segurança e apenas para substituir a cópia legal caso essa cópia se perca, seja destruída ou fique inutilizada. Esta cópia de segurança não pode ser utilizada para outros fins e tem de ser destruída se perder o direito de utilização do Software ou quando a licença de Utilizador Final expirar ou for rescindida por qualquer outra razão, de acordo com a legislação em vigor no país de residência principal do Utilizador Final ou no país onde o mesmo está a utilizar o Software.
- 2.5. A partir do momento em que o Software foi activado ou que o ficheiro da chave de licença foi instalado (à excepção de uma versão experimental do Software), tem o direito de receber os seguintes serviços pelo período definido especificado na embalagem de Software (se o Software foi adquirido num meio físico) ou especificado durante a compra (se o Software foi adquirido através da Internet):
 - Actualizações do Software através da Internet quando e como o Detentor dos Direitos os publicar no seu próprio website ou através de outros serviços online. Quaisquer Actualizações que possa receber passam a fazer parte do Software e os termos e condições deste Contrato aplicam-se às mesmas;
 - Assistência técnica através da Internet e assistência técnica através de uma linha telefónica grátis.

3. Activação e Termo

- 3.1. Se o Utilizador Final modificar o seu Computador ou fizer alterações ao software de outros fabricantes instalado nesse mesmo Computador, o Detentor dos Direitos poderá exigir que repita a activação do Software ou a instalação do ficheiro da chave de licença. O Detentor dos Direitos reserva-se o direito de utilizar quaisquer meios ou procedimentos de verificação para confirmar a validade da Licença e/ou a legalidade de uma cópia instalada do Software e/ou utilizada no Computador do Utilizador Final.
- 3.2. Se o Software foi adquirido num meio físico, o Software pode ser utilizado, mediante a sua aceitação deste Contrato, pelo período especificado na embalagem. Esse período terá início a partir do momento de aceitação deste Contrato ou como especificado no contrato adicional.
- 3.3. Se o Software foi adquirido através da Internet, o Software pode ser utilizado, mediante a sua aceitação deste Contrato, pelo período especificado durante a aquisição ou como especificado no contrato adicional.
- 3.4. Tem o direito de utilizar uma versão experimental do Software, como disposto na Cláusula 2.1 sem que tenha de pagar nada durante o período de avaliação (7 dias) desde o momento em que o Software é activado, de acordo com este Contrato, desde que a versão experimental não de ao Utilizador Final acesso a Actualizações e a assistência técnica através da Internet e da linha telefónica. Se o Detentor dos Direitos definir outra duração para o período de aplicação único Você será informado através de notificação.
- 3.5. A Licença para Utilização do Software está limitada ao período de tempo especificado nas Cláusulas 3.2 ou 3.3 (como aplicável) e o restante período pode ser visto através dos meios descritos no Manual do Utilizador.
- 3.6. Se tiver adquirido o Software que se destina a ser usado em mais do que um Computador, a sua Licença para Usar o Software estará limitada ao período de tempo que tem início com a data de activação do Software ou da instalação do ficheiro da chave de licença no primeiro Computador.
- 3.7. Sem prejuízo de quaisquer recursos legais ou de justiça natural que o Detentor dos Direitos possa ter, caso haja alguma violação de qualquer parte dos termos e condições deste Contrato por parte do Utilizador Final, o Detentor dos Direitos pode, em qualquer altura e sem qualquer aviso prévio ao Utilizador Final, rescindir esta Licença de utilização do Software sem reembolsar o preço de compra ou qualquer outra parte do mesmo.
- 3.8. Concorde que, ao utilizar o Software e qualquer relatório ou informações derivadas resultantes da utilização deste Software, irá cumprir todas as leis e regulamentos internacionais, nacionais, estatais, regionais e locais aplicáveis, incluindo, mas não se limitando às leis da privacidade, direitos de autor, controlo de exportação e obscenidade.
- 3.9. Excepto quando especificamente indicado neste documento, não pode transferir nem atribuir a terceiros nenhum dos direitos a si concedidos, ao abrigo deste Contrato, nem nenhuma das suas obrigações em conformidade com o presente.
- 3.10. Se o Utilizador tiver adquirido o Software com um código de activação válido para a localização de idioma do Software da região onde o mesmo foi adquirido ao Titular do Direito ou aos seus Parceiros, o Utilizador não poderá activar o Software aplicando o código de activação destinado a outra localização de idioma.
- 3.11. Se o Utilizador tiver adquirido Software destinado a ser utilizado com determinadas operadoras de telecomunicações, tal Software apenas poderá ser utilizado exclusivamente com a operadora especificada durante a aquisição.
- 3.12. No caso das limitações especificadas nas Cláusulas 3.10 e 3.11, a informação sobre estas limitações encontra-se indicada na embalagem e/ou website do Titular do Direito e/ou dos seus Parceiros.

4. Assistência técnica

A assistência técnica descrita na Cláusula 2.5 deste Contrato é fornecida ao Utilizador Final depois de ter sido instalada a mais recente Actualização do Software (excepto quando se trata de uma versão experimental do Software).

Serviço de assistência técnica: <http://support.kaspersky.com/pt/>

5. Limitações

- 5.1 Não deve emular, clonar, alugar, emprestar, arrendar, vender, modificar, descompilar ou inverter a engenharia do Software, nem desmontar ou criar trabalhos dele derivados e baseados no Software ou em qualquer parte do mesmo, sendo que a única excepção é a existência de um direito sem limitações concedido ao Utilizador Final pela legislação aplicável, bem como não pode reduzir qualquer parte do Software a uma forma legível, nem transferir o Software licenciado, ou qualquer outro subconjunto do Software licenciado, nem permitir que terceiros o façam, excepto até ao ponto em que as restrições indicadas sejam expressamente proibidas pela lei aplicável. Não se pode utilizar o código de binários nem a fonte do Software, nem inverter a engenharia, para recriar o algoritmo do programa, que é registado. Todos os direitos que não são aqui expressamente concedidos são reservados pelo Detentor dos Direitos e/ou pelos seus fornecedores, como aplicável. Qualquer utilização não autorizada do Software resultará na rescisão imediata e automática deste Contrato e da Licença concedida pelo mesmo e pode resultar em processos criminais e/ou civis contra o Utilizador Final.
- 5.2 Não pode transferir os direitos de utilização do Software para terceiros, excepto conforme disposto neste contrato adicional.
- 5.3 Não pode fornecer o código de activação e/ou a chave da licença a terceiros nem permitir que terceiros acessem ao código de activação e/ou chave da licença que são considerados dados confidenciais do Detentor dos Direitos e terá todo o cuidado em proteger o código de activação e/ou chave da licença contando que pode transferir o código de activação e/ou a chave de licença a terceiros como definido no contrato adicional.
- 5.4 Não pode alugar, arrendar ou emprestar o Software a terceiros.
- 5.5 Não pode utilizar o Software para criação de dados ou de software utilizado para a detecção, bloqueio ou tratamento das ameaças descritas no Manual do Utilizador.
- 5.6 O Detentor dos Direitos tem o direito de bloquear o ficheiro da chave ou rescindir a Licença de utilização do Software caso haja alguma violação de qualquer parte dos termos e condições deste Contrato por parte do Utilizador Final sem qualquer reembolso.
- 5.7 Se o Utilizador Final está a utilizar a versão experimental do Software, não tem o direito de receber a Assistência Técnica especificada na Cláusula 4 deste Contrato e o Utilizador Final não tem o direito de transferir a licença ou os direitos de utilização do Software a terceiros.

6. Garantia limitada e Renúncias

- 6.1 O Detentor dos Direitos garante que o Software irá cumprir substancialmente o que lhe é devido, de acordo com as especificações e descrições indicadas no Manual do Utilizador *desde que, no entanto*, essa garantia limitada não se aplique ao seguinte: (w) As deficiências e violações relacionadas do computador para as quais o Detentor dos Direitos renuncia expressamente todas as responsabilidades da garantia; (x) avarias, defeitos ou falhas resultantes de má utilização; abuso; acidente; negligência; instalação imprópria, operação ou manutenção; roubo; vandalismo; casos fortuitos; actos de terrorismo; falhas de energia ou picos de potência; acidentes; alterações, modificações não permitidas ou reparações por qualquer parte além do Detentor de Direitos; ou as acções do Utilizador Final ou causas que estejam para além do controlo razoável do Detentor dos Direitos; (y) qualquer defeito que o Utilizador Final não tenha dado a conhecer ao Detentor de Direitos logo que possível depois de o defeito aparecer pela primeira vez; e (z) incompatibilidade provocada pelos componentes de hardware e/ou software instalados no Computador do Utilizador Final.
- 6.2 O Utilizador Final reconhece, aceita e concorda que não existe nenhum software isento de erros e o Utilizador Final é aconselhado a fazer cópias de segurança do Computador, com a frequência e a fiabilidade adequada para o Utilizador Final.
- 6.3 Você reconhece, aceita e concorda que o Detentor dos Direitos não é responsável pela eliminação de dados autorizada por Si. Esses dados podem incluir dados pessoais ou informação de carácter confidencial.
- 6.4 O Detentor dos Direitos não oferece qualquer garantia de que o Software irá funcionar correctamente em caso de violações dos termos descritos no Manual do Utilizador ou neste Contrato.
- 6.5 O Detentor dos Direitos não garante que o Software irá funcionar correctamente se o Utilizador Final não fizer regularmente transferências das Actualizações especificadas na Cláusula 2.5 deste Contrato.
- 6.6 O Detentor dos Direitos não garante protecção das ameaças descritas no Manual do Utilizador após a expiração do período especificado nas Cláusulas 3.2 ou 3.3 deste Contrato ou após a rescisão da Licença de utilização do Software, caso ela seja rescindida por qualquer razão.
- 6.7 O SOFTWARE É ENTREGUE "TAL COMO ESTÁ" E O DETENTOR DOS DIREITOS NÃO FAZ QUALQUER REPRESENTAÇÃO NEM DÁ QUAISQUER GARANTIAS DA SUA UTILIZAÇÃO OU DESEMPENHO. EXCEPTO NO QUE SE REFERE A QUALQUER GARANTIA, CONDIÇÃO, REPRESENTAÇÃO OU TERMO NA MEDIDA EM QUE NÃO POSSA SER EXCLUÍDA OU LIMITADA PELA LEI APLICÁVEL, O DETENTOR DOS DIREITOS E OS SEUS PARCEIROS NÃO CONCEDEM QUALQUER GARANTIA, CONDIÇÃO, REPRESENTAÇÃO OU TERMO (EXPRESSO OU IMPLÍCITO, QUER SEJA POR ESTATUTO, LEI COMUM, PERSONALIZAÇÃO, UTILIZAÇÃO OU QUALQUER OUTRO) QUE, SEM OUTRO ASSUNTO INCLUINDO, MAS NÃO SE LIMITANDO, A NÃO INFRAÇÃO DOS DIREITOS DE TERCEIROS, COMERCIALIZAÇÃO, QUALIDADE SATISFATÓRIA, INTEGRAÇÃO OU APLICABILIDADE A UM FIM ESPECÍFICO. O UTILIZADOR FINAL ASSUME TODAS AS AVARIAS E TODO O RISCO DE DESEMPENHO E RESPONSABILIDADE POR SELECIONAR O SOFTWARE DE MODO A CONSEGUIR OS RESULTADOS PRETENDIDOS, E PELA INSTALAÇÃO, UTILIZAÇÃO E RESULTADOS OBTIDOS DO SOFTWARE. SEM LIMITAR AS DISPOSIÇÕES ANTERIORES, O DETENTOR DOS DIREITOS NÃO CONCEDE QUALQUER REPRESENTAÇÃO E NÃO DÁ GARANTIAS DE QUE O SOFTWARE NÃO CONTÉM ERROS OU NÃO ESTÁ LIVRE DE INTERRUPTÕES

OU OUTRAS FALHAS OU QUE O SOFTWARE VAI AO ENCONTRO DE TODOS E QUAISQUER REQUISITOS DO UTILIZADOR FINAL TENHAM OU NÃO SIDO DIVULGADOS AO DETENTOR DOS DIREITOS.

7. Exclusão e limitação da responsabilidade

NA MEDIDA MÁXIMA PERMITIDA PELA LEI APLICÁVEL, EM CASO ALGUM O DETENTOR DOS DIREITOS OU OS SEUS PARCEIROS SÃO RESPONSÁVEIS POR QUAISQUER DANOS ESPECIAIS, ACIDENTAIS, PUNITIVOS, INDIRECTOS OU CONSEQUENCIAIS, SEJAM ELES QUAIS FOREM, (INCLUINDO, MAS NÃO SE LIMITANDO A DANOS POR PERDA DE LUCROS OU DE INFORMAÇÕES CONFIDENCIAIS, OU OUTRAS, POR INTERRUPTÃO DO NEGÓCIO, POR PERDA DE PRIVACIDADE, POR CORRUPÇÃO, DANOS E PERDAS DE DADOS OU PROGRAMAS, POR FALHA DE PAGAMENTO DE QUAISQUER DIREITOS INCLUINDO QUAISQUER DIREITOS LEGAIS, DIREITOS DE LEALDADE OU DIREITOS DE CUIDADOS RAZOÁVEIS, POR NEGLIGÊNCIA, POR PERDA ECONÓMICA, E POR QUALQUER PERDA PECUNIÁRIA OU OUTRA, SEJA ELA QUAL FOR) QUE SURJA DE UMA QUALQUER FORMA RELACIONADA COM A UTILIZAÇÃO OU INCAPACIDADE DE UTILIZAÇÃO DO SOFTWARE, A DISPOSIÇÃO OU FALHA DE FORNECIMENTO DE ASSISTÊNCIA OU OUTROS SERVIÇOS, INFORMAÇÕES, SOFTWARE E CONTEÚDOS RELACIONADOS ATRAVÉS DO SOFTWARE OU QUE, POR OUTRO LADO, SURJA DA UTILIZAÇÃO DO SOFTWARE, OU, AO CONTRÁRIO, MEDIANTE OU EM LIGAÇÃO A QUALQUER DISPOSIÇÃO DESTE CONTRATO, OU QUE SURJA DE QUALQUER VIOLAÇÃO DO CONTRATO OU QUALQUER DELITO (INCLUINDO NEGLIGÊNCIA, MÁ REPRESENTAÇÃO OU QUALQUER OBRIGAÇÃO OU DEVER DE RESPONSABILIDADE LIMITADA), OU QUALQUER VIOLAÇÃO DOS DEVERES LEGAIS, OU QUALQUER VIOLAÇÃO DA GARANTIA DO DETENTOR DOS DIREITOS OU QUALQUER UM DOS SEUS PARCEIROS, MESMO QUE O DETENTOR DOS DIREITOS OU QUALQUER PARCEIRO TENHA SIDO AVISADO DA POSSIBILIDADE DESSES DANOS.

O UTILIZADOR FINAL CONCORDA QUE, CASO O DETENTOR DOS DIREITOS E/OU OS SEUS PARCEIROS SEJAM TIDOS COMO RESPONSÁVEIS, A RESPONSABILIDADE DO DETENTOR DOS DIREITOS E/OU DOS SEUS PARCEIROS DEVE SER LIMITADA PELOS CUSTOS DO SOFTWARE. EM CASO ALGUM DEVE A RESPONSABILIDADE DO DETENTOR DOS DIREITOS E/OU DOS SEUS PARCEIROS EXCEDER AS TAXAS PAGAS PELO SOFTWARE AO DETENTOR DOS DIREITOS OU AO PARCEIRO (COMO SE APLICAR).

NADA NESTE ACORDO EXCLUI OU LIMITA QUAISQUER REIVINDICAÇÕES DE MORTE E FERIMENTOS PESSOAIS. ALÉM DISSO, NO CASO DE ALGUMA RESPONSABILIDADE, EXCLUSÃO OU LIMITAÇÃO NESTE CONTRATO NÃO POSSAM SER EXCLUÍDAS OU LIMITADAS DE ACORDO COM A LEI APLICÁVEL, ENTÃO APENAS ESSA RESPONSABILIDADE, EXCLUSÃO OU LIMITAÇÃO NÃO SE DEVEM APLICAR AO UTILIZADOR FINAL E CONTINUA A FICAR VINCULADO POR TODAS AS RESTANTES RESPONSABILIDADES, EXCLUSÕES E LIMITAÇÃO.

8. GNU e outras licenças de terceiros

O Software pode incluir alguns programas de software licenciados (ou sublicenciados) ao utilizador no âmbito da Licença Pública Geral GNU (General Public License, GPL) ou outras licenças semelhantes de software grátis que, entre outros direitos, permite ao utilizador copiar, modificar e redistribuir determinados programas, ou partes do mesmo, e ter acesso ao código fonte ("Software de Código Aberto"). Se essas licenças necessitarem que, para qualquer software que é distribuído às pessoas num formato de binário executável, que o código fonte também seja tornado disponível a esses utilizadores, então o código fonte deve ser tornado disponível enviando o pedido para source@kaspersky.com ou é fornecido com o Software. Se quaisquer licenças de Software de Código Aberto precisarem que o Detentor dos Direitos forneça direitos de utilização, cópia ou modificação de um programa de Software de Código Aberto, mais vastos do que os direitos concedidos neste Contrato, então esses direitos devem ter precedência sobre os direitos e restrições aqui indicados.

9. Posse dos direitos de propriedade

9.1 Concorda que o Software e a respectiva autoria, os sistemas, ideias, métodos de funcionamento, documentação e outras informações contidas no Software, são propriedade intelectual registada e/ou segredo comercial, de grande valor, do Detentor dos Direitos ou dos seus parceiros e que o Detentor dos Direitos e os seus parceiros, conforme aplicável, estão protegidos pela lei civil e criminal e pelas leis de direitos de autor, segredos comerciais, marcas registadas e patentes da Federação Russa, União Europeia e Estados Unidos e de outros países, bem como pelos tratados internacionais. Este Contrato não concede ao Utilizador Final quaisquer direitos no que se refere à propriedade intelectual, incluindo as marcas comerciais ou as marcas dos serviços do Detentor dos Direitos e/ou dos seus parceiros ("Marcas Comerciais"). Pode utilizar as Marcas Comerciais apenas e até ao ponto de identificar resultados impressos produzidos pelo Software de acordo com a prática das marcas comerciais aceites, incluindo a identificação do nome do proprietário da Marca Comercial. A utilização de qualquer Marca Comercial não dá ao Utilizador Final quaisquer direitos de propriedade sobre essa Marca Comercial. O Detentor dos Direitos e/ou os seus parceiros são proprietários e retêm todos os direitos, títulos e interesse no Software e em relação ao mesmo, incluindo, sem limitações, quaisquer correcções de erros, melhoramentos, Actualizações ou outras modificações ao Software, quer sejam feitas pelo

Detentor dos Direitos ou por quaisquer terceiros, e todos os direitos sobre direitos de autor, patentes, segredos comerciais, marcas comerciais e outras propriedades intelectuais contidas neste documento. A posse, instalação ou utilização do Software não lhe transfere qualquer título para a propriedade intelectual no Software e não adquire quaisquer direitos ao Software excepto quando expressamente estipulado neste Contrato. Todas as cópias do Software realizadas nos termos do presente Contrato têm de conter os mesmos avisos de propriedade que aparecem no Software. Excepto como aqui indicado, este Contrato não concede ao Utilizador Final quaisquer direitos de propriedade intelectual sobre o Software e o Utilizador Final reconhece que a Licença, tal como está definida aqui, concedida nos termos deste Contrato, concede apenas o direito de utilização limitada mediante os termos e as condições deste Contrato. O Detentor dos Direitos reserva-se todos os direitos não expressamente concedidos ao Utilizador Final neste Contrato.

- 9.2 O Utilizador Final reconhece que o código fonte, o código de activação e/ou o ficheiro da chave da licença do Software são propriedade do Detentor dos Direitos e constituem segredos comerciais do Detentor dos Direitos. Concorde em não modificar, adaptar, traduzir, inverter a engenharia, descompilar, desmontar ou tentar, de qualquer outro modo, descobrir o código fonte do Software seja de que forma for.
- 9.3 Concorde em não modificar nem alterar o Software seja de que forma for. Não pode remover nem alterar quaisquer avisos de direitos de autor ou outros avisos de propriedade em nenhuma cópia do Software.

10. Lei vigente; arbitragem

Este Contrato é regido, e será interpretado, de acordo com as leis da Federação Russa sem referência a conflitos de regras e princípios legais. Este Contrato não será regido pela Convenção das Nações Unidas referente a Contratos para a Venda Internacional de Bens, a aplicação da qual é expressamente excluída. Qualquer litígio que surja no seguimento da interpretação ou aplicação dos termos deste Contrato ou qualquer infracção ao mesmo, a não ser que se resolva por negociação directa, deverá ser resolvido no Tribunal de Arbitragem Comercial Internacional na Câmara do Comércio e Indústria da Federação Russa em Moscovo, na Federação Russa. Qualquer decisão apresentada pelo árbitro deve ser final e obrigatória para as partes e qualquer julgamento sobre essa decisão de arbitragem pode ser feita cumprir em qualquer tribunal da jurisdição competente. Nada nesta Secção 10 deve impedir que uma Parte procure e obtenha qualquer reparação equitativa de um tribunal da jurisdição competente, quer seja antes, durante ou depois dos processos de arbitragem.

11. Período para interpor acções.

Nenhuma acção, independentemente da forma, que surja das transacções nos termos deste Contrato, pode ser trazida aqui por qualquer uma das partes mais de um (1) ano depois da causa da acção ter ocorrido, ou de ter sido descoberta a ocorrência, excepto que uma acção por violação dos direitos de propriedade intelectual seja trazida dentro do período legal máximo aplicável.

12. Contrato completo; redução; sem renúncia.

Este Contrato constitui todo o contrato entre o Utilizador Final e o Detentor dos Direitos e substitui quaisquer outros acordos prévios, propostas, comunicações ou publicidade, oral ou escrita, referente ao Software ou ao assunto deste Contrato. O Utilizador Final reconhece que leu este Contrato, compreendeu-o e concorda em estar vinculado pelos seus termos. Se qualquer disposição deste Contrato for indicada por um tribunal de jurisdição competente como sendo inválida, nula ou inexecutável por qualquer razão, no todo ou em parte, essa disposição será ainda mais restritamente interpretada de tal forma que será legal e executória, e todo o Contrato não falhará por conta do mesmo e o saldo do Contrato continuará válido e com efeitos até ao máximo permitido por lei ou equidade ao mesmo tempo que preserva, até ao máximo possível, a sua intenção original. Nenhuma renúncia de nenhuma disposição ou condição aqui indicadas será válida a não ser por escrito e assinada pelo Utilizador Final e um representante autorizado do Detentor dos Direitos desde que nenhuma renúncia de nenhuma infracção de nenhuma disposição deste Contrato constitua uma renúncia de qualquer infracção anterior, concorrente ou subsequente. A não insistência por parte do Detentor dos Direitos no que se refere a fazer valer o desempenho rigoroso de todas as disposições deste Contrato ou nenhum direito deve ser interpretado como sendo uma renúncia de qualquer uma dessas disposições ou direitos.

13. Informações de contacto do Detentor dos Direitos.

Se tiver quaisquer dúvidas referentes a este Contrato ou se, por qualquer razão, pretender contactar o Detentor dos Direitos, contacte o nosso Departamento de Apoio ao Cliente em:

Kaspersky Lab ZAO, 10 build. 1 1st Volokolamsky Proezd
 Moscovo, 123060
 Federação Russa
 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 Software e toda a documentação que o acompanha têm direitos de autor e estão protegidos pelas leis de direitos de autor e por tratados internacionais de direitos de autor, bem como por outras leis e tratados de propriedade intelectual.

ÍNDICE

SOBRE ESTE MANUAL	12
Neste documento	12
Convenções de documentos	14
FONTES DE DADOS ADICIONAIS	16
Fontes de informação para pesquisa mais aprofundada	16
Contactar o Departamento de Vendas	17
Discussão das aplicações da Kaspersky Lab no fórum da Web	17
Contactar o Grupo de Desenvolvimento de Documentação	17
KASPERSKY MOBILE SECURITY 9	18
Requisitos de hardware e software	19
Kit de distribuição	19
INSTALAR O KASPERSKY MOBILE SECURITY 9	20
DESINSTALAR A APLICAÇÃO	21
INICIAÇÃO	22
Activar a aplicação	22
Activar a versão comercial	23
Activar a subscrição do Kaspersky Mobile Security 9	24
Adquirir um código de activação online	24
Activar a versão de avaliação	25
Configurar o código secreto	25
Activar a opção para recuperar o código secreto	26
Recuperar o código secreto	26
Iniciar a aplicação	27
Ver informações sobre a aplicação	27
GERIR A LICENÇA	28
Sobre o Contrato de Licença	28
Sobre as licenças do Kaspersky Mobile Security 9	28
Ver informações da Licença	29
Renovar a licença	30
Renovar a licença com o código de activação	30
Renovar a licença online	31
Renovar a licença ao activar a subscrição	31
Retirar a subscrição	32
Renovar a subscrição	32
INTERFACE DA APLICAÇÃO	33
Janela de estado da protecção	33
Widget do ecrã inicial	34
PROTECÇÃO DO SISTEMA DE FICHEIROS	35
Sobre a Protecção	35
Activa/Desactiva a Protecção	35
Configurar a área de protecção	36
Seleccionar a acção a efectuar em objectos detectados	37

VERIFICAR O DISPOSITIVO	39
Sobre a verificação do dispositivo	39
Iniciar uma verificação manualmente	39
Iniciar uma verificação agendada	41
Seleção do tipo de objecto a verificar	42
Configurar verificações activas.....	42
Seleccionar a acção a efectuar em objectos detectados.....	43
FILTRAGEM DE CHAMADAS E MENSAGENS SMS DE ENTRADA	45
Sobre o Filtro de Chamadas e SMS	45
Sobre os modos do Filtro de Chamadas e SMS.....	46
Mudar o modo do Filtro de Chamadas e SMS.....	46
Criar a Lista Negra	47
Adicionar registos à Lista Negra	47
Editar registos na Lista Negra.....	48
Apagar registos da Lista Negra.....	49
Criar uma Lista Branca.....	49
Adicionar registos à Lista Branca.....	50
Editar entradas na Lista Branca.....	51
Apagar registos da Lista Branca	52
Responder a mensagens SMS e chamadas de contactos não incluídos na lista de números	52
Responder a mensagens SMS de números não numéricos.....	53
Seleccionar uma resposta para SMS de entrada	54
Seleccionar uma resposta para chamadas de entrada	55
Ver registos do Log	55
PROTECÇÃO DE DADOS EM CASO DE PERDA OU ROUBO DO DISPOSITIVO	57
Sobre o Anti-Roubo	57
Bloquear dispositivo	58
Apagar dados pessoais	59
Criar uma lista de pastas a eliminar.	61
Monitorizar a substituição de um cartão SIM no dispositivo	62
Determinar as coordenadas geográficas do dispositivo	63
Iniciar as funções Anti-Roubo remotamente.....	65
PROTECÇÃO DE PRIVACIDADE	67
Protecção de Privacidade.....	67
Modos de Protecção de Privacidade	67
Activar/desactivar a Protecção de Privacidade.....	68
Activar automaticamente a Protecção de Privacidade	68
Activar remotamente a Protecção de Privacidade.....	69
Seleccionar dados a ocultar: Protecção de Privacidade.....	71
Criar uma lista de números privados.	72
Adicionar um número à lista de números privados	72
Editar um número na lista de números privados.....	73
Apagar um número da lista de números privados.....	73
ACTUALIZAR AS BASES DE DADOS DA APLICAÇÃO	75
Sobre a actualização das bases de dados da aplicação	75
Iniciar actualizações manualmente.....	76
Iniciar actualizações agendadas.....	76

CONFIGURAR DEFINIÇÕES ADICIONAIS.....	77
Alterar o código secreto.....	77
Apresentar sugestões.....	77
Configurar notificações com som	78
Mensagens na linha de estado.....	78
CONTACTAR O SERVIÇO DE ASSISTÊNCIA TÉCNICA.....	80
GLOSSÁRIO	81
KASPERSKY LAB.....	83
INFORMAÇÃO SOBRE CÓDIGO DE TERCEIROS	84
Código de programa distribuído	84
Outras informações	84
ÍNDICE	85

SOBRE ESTE MANUAL

Este documento é o Manual de instalação, configuração e utilização do Kaspersky Mobile Security 9. O documento foi concebido para um público amplo.

Objectivos do documento:

- ajuda o utilizador a configurar de modo independente a aplicação num dispositivo móvel, activá-la e optimizá-la para as suas necessidades;
- disponibilizar informações imediatas sobre questões relacionadas com a aplicação;
- proporcionar informações sobre fontes alternativas de informação sobre a aplicação e sobre a possibilidade de receber suporte técnico.

NESTA SECÇÃO

Neste documento	12
Convenções de documentos	14

NESTE DOCUMENTO

As seguintes secções são incluídas no documento:

Fontes de dados adicionais

Esta secção contém uma descrição das fontes adicionais de informação sobre a aplicação e dos recursos na Internet nos quais pode debater o programa, partilhar ideias, colocar questões e receber respostas às mesmas.

Kaspersky Mobile Security 9

Esta secção contém uma descrição das opções da aplicação assim como breves informações sobre os componentes individuais e as suas funções principais. A partir desta secção pode aprender sobre a função do pacote de instalação. A secção contém os requisitos do dispositivo e do programa que o dispositivo deve cumprir para instalar o Kaspersky Mobile Security 9.

Instalar o Kaspersky Mobile Security 9

Esta secção contém instruções que o irão ajudar a instalar a aplicação num dispositivo móvel.

Desinstalar a aplicação

Esta secção contém instruções que o irão ajudar a desinstalar a aplicação num dispositivo móvel.

Actualizar a aplicação

Esta secção contém instruções que o irão ajudar a actualizar a versão anterior da aplicação.

Iniciação

Esta secção contém informações sobre como começar a trabalhar com o Kaspersky Mobile Security 9: activá-lo, configurar o código secreto da aplicação, activar a função de recuperação do código secreto, recuperar o código secreto, iniciar a aplicação, actualizar as suas bases de dados antivírus e verificar o dispositivo quanto a vírus.

Gerir a licença

Esta secção contém informações sobre os termos principais utilizados no contexto do licenciamento da aplicação. Além disso, a secção apresenta informações sobre como encontrar informações sobre a licença do Kaspersky Mobile Security 9 e alargar o prazo de validade da mesma.

Interface da aplicação

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

Protecção do sistema de ficheiros

Esta secção fornece informações sobre o componente de Protecção que permite impedir infecções no sistema de ficheiros do dispositivo. A secção igualmente especifica a forma de activar/parar a Protecção e regular as suas configurações de funcionamento.

Verificar o dispositivo

Esta secção fornece informações sobre a verificação do dispositivo a pedido, que pode detectar e remover ameaças no seu dispositivo. A secção também descreve como executar uma verificação do dispositivo, configurar uma verificação agendada automática do sistema de ficheiros, seleccionar ficheiros para a verificação e definir a acção que a aplicação irá tomar quando for detectado um objecto malicioso.

Colocar objectos de software maligno na quarentena

Esta secção fornece informações sobre a *quarentena*, uma pasta especial em que são colocados objectos potencialmente maliciosos. Esta secção também descreve como visualizar, restaurar ou eliminar objectos maliciosos encontrados na pasta.

Filtragem de chamadas e mensagens SMS de entrada

Esta secção disponibiliza informações sobre o Filtro de Chamadas e SMS que bloqueia chamadas e SMS indesejadas de acordo com as Listas Branca e Negra que criar. A secção também descreve como seleccionar o modo no qual o Filtro de Chamadas e SMS verifica chamadas e SMS, sobre como configurar definições de filtragem adicionais para SMS e chamadas de entrada e também sobre como criar Listas Negras e Brancas.

Limitar chamadas e mensagens SMS de saída. Controlo Parental

A secção proporciona informações sobre o componente Controlo Parental, que permite limitar as chamadas e mensagens SMS de saída para números especificados. Além disso, a secção descreve a forma de criar uma lista de números permitidos e bloqueados e definir as configurações do Controlo Parental.

Protecção de dados em caso de perda ou roubo do dispositivo

Esta secção fornece informações sobre o Anti-Roubo, que no caso de roubo ou perda bloqueia o acesso não autorizado aos dados guardados no seu dispositivo móvel e tornam mais fácil encontrar o dispositivo.

Esta secção também especifica como activar/desactivar a função Anti-Roubo, definir os parâmetros de funcionamento e como iniciar o Anti-Roubo de modo remoto a partir de outro dispositivo.

Protecção de Privacidade

A secção apresenta informações sobre a Protecção de Privacidade, que pode ocultar as informações confidenciais do utilizador.

Encriptar dados pessoais

Esta secção fornece informações sobre a Encriptação, que pode encriptar pastas no seu dispositivo. Também descreve como encriptar e desencriptar as pastas seleccionadas.

Actualizar as bases de dados da aplicação

Esta secção fornece informações sobre a actualização das bases de dados da aplicação, o que assegura a protecção actualizada do seu dispositivo. Adicionalmente esta secção descreve como ver informações nas bases de dados de antivírus instaladas, executar a actualização manualmente e configurar a actualização automática das bases de dados antivírus.

Logs da aplicação

A secção apresenta informações sobre logs que registam o funcionamento de cada componente e a execução de cada tarefa (por exemplo, actualizações de bases de dados da aplicação, verificações de vírus).

Configurar definições adicionais

Esta secção fornece informações sobre opções adicionais do Kaspersky Mobile Security 9: como gerir a notificação com som da aplicação a luz de fundo do ecrã, bem como activar/desactivar a apresentação das sugestões, o ícone de protecção e a janela de estado da protecção.

Contactar o Serviço de Assistência Técnica

Esta secção contém recomendações sobre como contactar a Kaspersky Lab relativamente a suporte do escritório pessoal no site de suporte técnico e por telefone.

Glossário

Esta secção contém uma lista de termos encontrados no documento e a sua definição.

Kaspersky Lab

A secção fornece informações sobre a Kaspersky Lab ZAO.

Informação sobre código de terceiros

Esta secção fornece informações sobre códigos de terceiros utilizados na aplicação.

Índice

Esta secção permite que rapidamente encontre as informações necessárias no documento.

CONVENÇÕES DE DOCUMENTOS

As convenções de documentos descritas na tabela abaixo são utilizadas neste Manual.

Table 1. Convenções de documentos

TEXTO DE AMOSTRA	DESCRIÇÃO DAS CONVENÇÕES DE DOCUMENTOS
Saiba que...	Os avisos são destacados a vermelho dentro de um rectângulo. Os avisos contêm informações importantes, por exemplo, sobre operações do computador críticas para a segurança.
Recomenda-se que utilize...	As notas aparecem dentro de um rectângulo. As notas contêm informações adicionais e de referência.
Exemplo: ...	Os exemplos são apresentados por secções, com um fundo amarelo e por baixo do título "Exemplo".
Actualização significa...	Os novos termos aparecem a itálico.
ALT+F4	Os nomes das teclas do teclado aparecem a negrito e em letras maiúsculas. Os nomes das teclas seguidos de um sinal "mais" indicam a utilização de uma combinação de teclas.
Activar	Os nomes dos elementos da interface, por exemplo, campos de registo, comandos de menu, botões, etc., são assinalados a negrito.
➡ <i>Para configurar um agendamento de tarefas:</i>	As frases de introdução das instruções são marcadas em itálico.
ajuda	Os textos na linha de comandos ou os textos das mensagens apresentadas no ecrã são destacados com um tipo de letra especial.
<endereço IP do seu computador>	As variáveis aparecem entre parênteses angulares. Em vez das variáveis, os seus respectivos valores são colocados em cada caso e os parênteses são omitidos.

FONTES DE DADOS ADICIONAIS

Se tiver quaisquer questões sobre configurar ou utilizar o Kaspersky Mobile Security 9, poderá obter respostas delas, utilizando várias fontes de informação. Pode escolher a fonte mais adequada de acordo com quão importante ou urgente seja o seu pedido.

NESTA SECÇÃO

Fontes de informação para pesquisa mais aprofundada	16
Contactar o Departamento de Vendas	17
Discussão das aplicações da Kaspersky Lab no fórum da Web	17
Contactar o Grupo de Desenvolvimento de Documentação	17

FONTES DE INFORMAÇÃO PARA PESQUISA MAIS APROFUNDADA

Pode consultar as seguintes fontes de informação sobre a aplicação:

- o Web site de aplicações da Kaspersky Lab;
- a página da Base de Dados de Conhecimento no Web site do Serviço de Apoio Técnico;
- o sistema de ajuda e sugestões instalados;
- a documentação da aplicação instalada.

Página no Web site da Kaspersky Lab

<http://www.kaspersky.com/pt/kaspersky-mobile-security>

Esta página irá disponibilizar informações gerais sobre o Kaspersky Mobile Security 9 e as suas funcionalidades e opções. Pode adquirir o Kaspersky Mobile Security 9 na nossa loja online.

A página da aplicação no Web site do Serviço de Apoio Técnico (Base de Conhecimento)

<http://support.kaspersky.com/pt/>

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

Estes artigos contêm informações úteis, recomendações e Perguntas Frequentes (FAQs) relativas à compra, instalação e utilização do Kaspersky Mobile Security 9. Estas estão dispostas em tópicos, tais como "Actualizações da base de dados" e "Resolução de problemas". Os artigos poderão responder a questões não só sobre o Kaspersky Mobile Security 9, mas também sobre outros produtos Kaspersky Lab. Além disso, poderão também conter novidades do Serviço de Assistência Técnica.

O sistema de ajuda instalado

Se tiver quaisquer questões sobre janelas ou separadores específicos no Kaspersky Mobile Security 9, poderá visualizar o contexto da ajuda .

De modo a abrir o contexto da ajuda, abra a janela na qual está interessado e seleccione o item **Ajuda**.

A Documentação instalada

O Manual do Utilizador contém informações detalhadas sobre as funções da aplicação e como utilizar o Kaspersky Mobile Security 9, bem como conselhos e recomendações sobre a configuração da aplicação.

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

Também pode transferir estes documentos, em formato electrónico, a partir do Web site da Kaspersky Lab.

CONTACTAR O DEPARTAMENTO DE VENDAS

Se tiver dúvidas sobre como seleccionar ou adquirir o Kaspersky Mobile Security, ou expandir a sua licença, contacte os especialistas do Departamento de Vendas na nossa sede em Moscovo, através do número:

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

O serviço é fornecido em russo ou em inglês.

Pode também enviar as suas dúvidas para o Departamento de Vendas por e-mail, através do endereço sales@kaspersky.com.

DISCUSSÃO DAS APLICAÇÕES DA KASPERSKY LAB NO FÓRUM DA WEB

Se as suas dúvidas não necessitarem de resposta urgente, pode discuti-las com especialistas da Kaspersky Lab e outros utilizadores de aplicações antivírus da Kaspersky Lab no nosso fórum, no endereço <http://forum.kaspersky.com>.

No fórum, pode ver as discussões existentes, deixar comentários e criar novos tópicos ou utilizar o motor de pesquisa para consultas específicas.

CONTACTAR O GRUPO DE DESENVOLVIMENTO DE DOCUMENTAÇÃO

Se possuir quaisquer questões sobre a documentação, ou se tiver encontrado algum erro nela, ou gostaria de deixar um comentário, contacte o nosso grupo de desenvolvimento de documentação para o utilizador. Para contactar o grupo de desenvolvimento de documentação envie um e-mail para docfeedback@kaspersky.com. Utilize a linha de assunto: "Comentário sobre a Ajuda da Kaspersky: Kaspersky Mobile Security 9".

KASPERSKY MOBILE SECURITY 9

Kaspersky Mobile Security 9 protege dispositivos móveis (daqui em diante "dispositivos") a executar o sistema operativo Android. A aplicação pode proteger informações no dispositivo da infecção por parte de ameaças conhecidas, impedir mensagens SMS e chamadas indesejadas, proteger informações no dispositivo em caso de roubo ou perda e ocultar informações relacionadas com contactos confidenciais. Cada tipo de ameaça é processado em componentes diferentes do programa. Esta característica permite ajustar as configurações do programa consoante as necessidades do utilizador.

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

- **Antivírus.** Protege o sistema de ficheiros do dispositivo móvel de vírus e outras aplicações maliciosas. O Antivírus pode detectar e neutralizar objectos maliciosos no seu dispositivo e actualizar as bases de dados antivírus da aplicação.
- **Filtro de Chamadas e SMS.** Verifica a presença de spam em todas as mensagens SMS e chamadas de entrada. O componente permite o bloqueio flexível de mensagens de texto e chamadas consideradas indesejáveis.
- **Pasta Anti-Roubo.** Esta protege informações no dispositivo do acesso não autorizado quando este for perdido ou roubado e também faz com que seja mais fácil de encontrar. O Anti-Roubo permite que bloqueie o seu dispositivo remotamente, apague quaisquer informações armazenadas nele e obtenha as coordenadas geográficas utilizando comandos SMS de outro dispositivo. Para além disso, o Anti-Roubo permite-lhe bloquear o seu dispositivo se o cartão SIM for substituído ou se o dispositivo for activado sem um cartão SIM.
- **Protecção de Privacidade.** Oculta informações relacionadas com números confidenciais da lista de contactos. Para estes números, a Protecção de Privacidade oculta as entradas nos Contactos, o histórico de chamadas e SMS, chamadas e SMS de entrada.

O Kaspersky Mobile Security 9 não se destina a fins de cópia de segurança e restauro.

NESTA SECÇÃO

Requisitos de hardware e software	19
Kit de distribuição	19

REQUISITOS DE HARDWARE E SOFTWARE

Kaspersky Mobile Security 9 pode ser instalado em dispositivos móveis a trabalhar num sistema operativo Android 1,5, 1,6, 2,0, 2,1, 2,2.

KIT DE DISTRIBUIÇÃO

Pode adquirir o Kaspersky Mobile Security 9 online e, neste caso, o kit de distribuição e a documentação da aplicação são fornecidos em formato electrónico. O Kaspersky Mobile Security 9 também pode ser adquirido em todas as boas lojas de telemóveis e tecnologia. Para obter informações detalhadas sobre a aquisição da aplicação e receber o kit de distribuição, contacte o nosso departamento de vendas através do endereço sales@kaspersky.com.

INSTALAR O KASPERSKY MOBILE SECURITY 9

A aplicação é instalada num dispositivo móvel em vários passos.

➤ *Para instalar o Kaspersky Mobile Security 9:*

1. Copie o pacote de distribuição da aplicação para o seu dispositivo, para fazer isto desempenhe uma das seguintes acções:
 - Ao adquirir a aplicação em CD, ligue o dispositivo móvel ao computador e inicie a instalação automática do Kaspersky Mobile Security 9 no disco adquirido.
 - Quando obtiver o pacote de distribuição da aplicação através da Internet, ligue o dispositivo móvel ao computador e copie o pacote de distribuição da aplicação para ele.
 - Copie o pacote de distribuição da aplicação para o dispositivo móvel a partir da loja online Kaspersky Lab (<http://www.kasperskystore.com.pt>).

2. Execute a instalação da aplicação. Para fazer isto, abra o arquivo ARK do pacote de distribuição no dispositivo móvel.

O assistente de instalação da aplicação inicia. Quando o assistente chegar ao fim, a aplicação é instalada com os parâmetros recomendados pelos especialistas Kaspersky Lab.

3. Abra a aplicação. Para fazer isto, na janela principal mude para a janela da aplicação, seleccione **Kaspersky Mobile Security 9** e execute a aplicação.
4. Leia o texto do Contrato de Licença estabelecido entre o utilizador e a Kaspersky Lab. Se concordar com todos os termos do contrato, prima **Aceitar**. Em seguida irá abrir a janela **Ativação**. Se não concordar com os termos do Contrato de Licença, prima **Declinar**. A aplicação encerra.
5. Execute a aplicação (consulte "Activar a aplicação" na página [22](#)).
6. Introduza o novo código secreto da aplicação. Para fazer isto, preencha sucessivamente os campos **Definir um novo código secreto** e **Volte a introduzir um código novo** e clique na tecla **Enter**.

DESINSTALAR A APLICAÇÃO

A aplicação apenas pode ser desinstalada do dispositivo se a ocultação de informações confidenciais estiver desactivada. Antes de desinstalar a aplicação o utilizador deve assegurar que esta condição é cumprida.

► *Para desinstalar o Kaspersky Mobile Security 9:*

1. Desactivar Protecção da Privacidade (página [67](#)).
2. Na janela principal, mude para a janela da aplicação e seleccione **Definições** → **Aplicações** → **Gestão das aplicações**.
3. Seleccione Kaspersky Mobile Security 9 a partir da lista.
A janela **Detalhes da aplicação** abre.
4. Clique em **Apagar**.
Irá abrir uma janela de confirmação da eliminação.
5. Confirme a eliminação do Kaspersky Mobile Security 9, clicando em **OK**.
A aplicação é apagada do dispositivo.
6. Após concluir a eliminação, clique em **OK**.

INICIAÇÃO

Esta secção contém informações sobre como começar a utilizar o Kaspersky Mobile Security 9: activá-lo, definir o código secreto da aplicação, activar a função de recuperação do código secreto, recuperar o código secreto e iniciar a aplicação.

NESTA SECÇÃO

Activar a aplicação	22
Configurar o código secreto	25
Activar a opção para recuperar o código secreto	26
Recuperar o código secreto	26
Iniciar a aplicação	27
Ver informações sobre a aplicação	27

ACTIVAR A APLICAÇÃO

Antes de começar a utilizar o Kaspersky Mobile Security 9, este precisa de ser activado.

A aplicação pode ser activada se for configurada uma ligação à Internet no dispositivo, for inserido um cartão SIM e introduzido o código PIN (se um tiver sido definido). Se esses requisitos não forem cumpridos, não será possível activar a aplicação.

Antes de activar a aplicação, certifique-se de que as configurações de data do sistema do dispositivo estão correctas.

É possível activar a aplicação da seguinte forma:

- **Activar a licença de avaliação.** Quando activa a versão de avaliação, a aplicação recebe uma licença de avaliação gratuita. O período de validade da licença de avaliação é apresentado no ecrã depois da activação estar concluída. Uma vez expirado o prazo de validade da licença de avaliação, as funções da aplicação ficarão limitadas. Apenas estarão disponíveis as seguintes funcionalidades:
 - Activar a aplicação;
 - gerir a licença da aplicação;
 - Sistema de ajuda do Kaspersky Mobile Security 9;
 - desactivar a Protecção de Privacidade.

É impossível reactivar uma versão de avaliação.

- **Activar a licença comercial.** Para activar a versão comercial, deve utilizar o código de activação que recebeu ao adquirir a aplicação. Ao activar a versão comercial, a aplicação recebe uma licença comercial, que lhe dá acesso a todas as funções da aplicação. O período de validade da licença é apresentado no ecrã do dispositivo. Quando o período de validade da licença expirar, as funções da aplicação serão limitadas e esta não poderá ser actualizada.

É possível obter um código de activação da seguinte forma:

- online, deslocando-se da aplicação Kaspersky Mobile Security 9 até ao website Kaspersky Lab especial para dispositivos móveis;
 - na eLoja da Kaspersky Lab (<http://www.kasperskystore.com.pt>);
 - junto dos distribuidores da Kaspersky Lab.
- **Activar subscrição.** Ao activar a subscrição, a aplicação recebem uma licença comercial com a subscrição. O período de validade da licença comercial com subscrição é limitado a 30 dias. Quando a subscrição é activada, a aplicação renova a licença a cada 30 dias. Quando a licença é renovada, na sua conta pessoal é deduzida uma quantia fixa para utilização da aplicação, especificada durante a activação da subscrição. A quantia é debitada ao enviar uma mensagem SMS paga. Quando os fundos tiverem sido debitados, a aplicação recebe uma nova licença do servidor de activação com uma subscrição que concede um acesso a todas as funções da aplicação. Pode cancelar a subscrição para o Kaspersky Mobile Security 9. Neste caso, quando a licença actual expirar a funcionalidade da aplicação tornar-se-á limitada, e as bases de dados da aplicação deixarão de ser actualizadas.

NESTA SECÇÃO

Activar a versão comercial	23
Activar a subscrição do Kaspersky Mobile Security 9	24
Adquirir um código de activação online.....	24
Activar a versão de avaliação	25

ACTIVAR A VERSÃO COMERCIAL

➔ *Para activar a versão comercial da aplicação com o código de activação:*

1. Mudar da janela principal para a janela da aplicação.
2. Seleccione **Kaspersky Mobile Security 9** e execute a aplicação.
Este procedimento irá abrir a janela **Activação**.
3. Seleccionar **Inserir código de activação**.
Este procedimento irá abrir a janela **Inserir código de activação**.
4. Subsequentemente insira o código de activação recebido ao adquirir a aplicação e clique em **Activar**.

A aplicação irá enviar um pedido ao servidor de activação do Kaspersky Lab e irá receber uma licença. Quando a licença tiver sido recebida com sucesso, irão ser apresentadas no ecrã informações relativas à licença.

Se o código de activação que tiver introduzido for inválido por qualquer motivo, é apresentada uma mensagem informativa no ecrã. Neste caso, recomenda-se que verifique se o código de activação que introduziu está correcto e que contacte o distribuidor de software junto do qual adquiriu o Kaspersky Mobile Security 9.

Se tiverem ocorrido quaisquer erros na ligação ao servidor e não tiver sido recebida nenhuma licença, a activação é cancelada. Neste caso, recomenda-se que verifique os parâmetros da ligação à Internet. Se não for possível rectificar os erros, contacte o Apoio Técnico.

5. Desloque-se até à configuração do código secreto da aplicação.

ACTIVAR A SUBSCRIÇÃO DO KASPERSKY MOBILE SECURITY 9

➤ *Para activar a subscrição do Kaspersky Mobile Security 9:*

1. Mudar da janela principal para a janela da aplicação.
2. Seleccione **Kaspersky Mobile Security 9** e execute a aplicação.

Este procedimento irá abrir a janela **Activação**.

3. Seleccionar **Comprar com um clique**.
4. Leia as informações sobre como activar a sua subscrição e clique em **Activar**.

A aplicação irá verificar se o serviço de subscrição está acessível para o prestador de serviço móvel que está a utilizar. Se o serviço de subscrição estiver disponível, serão apresentadas no ecrã informações sobre os termos da subscrição.

Se os serviços de subscrição não puderem ser fornecidos, a aplicação irá notificá-lo disto e voltar ao ecrã no qual pode seleccionar outro modo de activar a aplicação.

5. Leia os termos da subscrição e em seguida confirme a activação da subscrição do Kaspersky Mobile Security 9 premindo **Activar**.

A aplicação irá enviar uma mensagem SMS a pagar e em seguida irá receber uma licença do servidor de activação do Kaspersky Lab. Quando a subscrição ficar activa, o Kaspersky Mobile Security 9 irá notificá-lo do sucedido.

Se o seu saldo não possuir fundos suficientes para enviar uma mensagem SMS a pagar, a activação da subscrição será cancelada.

Se tiverem ocorrido quaisquer erros na ligação ao servidor e não tiver sido recebida nenhuma licença, a activação é cancelada. Neste caso, recomenda-se que verifique os parâmetros da ligação à Internet. Se não for possível rectificar os erros, contacte o Apoio Técnico.

Se não concordar com os termos da subscrição, regresse à janela de **Activação**. Neste caso, a aplicação cancela a activação da subscrição e volta para o ecrã no qual pode voltar a seleccionar o modo de activar a aplicação.

6. Desloque-se até à configuração do código secreto.

ADQUIRIR UM CÓDIGO DE ACTIVAÇÃO ONLINE

➤ *Para adquirir um código de activação para a aplicação online, execute os seguintes passos:*

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

Este procedimento irá abrir a janela **Adicional**.

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

Este procedimento irá abrir a janela **Activação**.

Seleccione **Comprar online**.

Este procedimento irá abrir a janela **Comprar online**.

3. Prima **Abrir**.

Abre um website especial para dispositivos móveis do Kaspersky Lab, no qual poderá adquirir a renovação da licença.

4. Siga as instruções passo a passo.
5. Após concluir a compra do código de activação, passe à activação da versão comercial da aplicação.

ACTIVAR A VERSÃO DE AVALIAÇÃO

➤ *Para activar a versão de avaliação do Kaspersky Mobile Security 9:*

1. Mudar da janela principal para a janela da aplicação.
2. Seleccione **Kaspersky Mobile Security 9** e execute a aplicação.

Este procedimento irá abrir a janela **Activação**.

3. Seleccione **Versão de avaliação**.
4. Confirme a activação da versão de avaliação clicando em **Activar**.

A aplicação irá enviar um pedido ao servidor de activação do Kaspersky Lab e irá receber uma licença. Subsequentemente, a janela **Sobre a licença** abre com informações sobre a licença da aplicação instalada.

Se tiverem ocorrido quaisquer erros na ligação ao servidor e não tiver sido recebida nenhuma licença, a activação é cancelada. Neste caso, recomenda-se que verifique os parâmetros da ligação à Internet. Se não for possível rectificar os erros, contacte o Apoio Técnico.

5. Desloque-se até à configuração do código secreto da aplicação.

CONFIGURAR O CÓDIGO SECRETO

Após iniciar a aplicação ser-lhe-á pedido que introduza o código secreto da aplicação. *O código secreto da aplicação impede o acesso não autorizado aos parâmetros da aplicação.*

Pode alterar o código secreto instalado mais tarde.

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

- para acesso à aplicação;
- ao enviar um comando SMS a partir de outro dispositivo móvel para iniciar remotamente as seguintes funções: Bloqueio, Limpeza de Dados, Prot. Cartão SIM, Localização por GPS, Protecção de Privacidade.

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

Se se esquecer do código secreto da aplicação, pode restaurá-la (consulte a secção "Recuperar o código secreto" na página [26](#)). Para isso, a opção de recuperação do código secreto tem de ser activada com antecedência (consulte a secção "Recuperar o código secreto" na página [26](#)).

➤ *Para introduzir o código secreto:*

1. Depois de activar a aplicação, introduza no campo **Introduzir novo código** os valores que irão constituir o seu código.

O código introduzido é verificado automaticamente.

Se o código for considerado inválido de acordo com os resultados da verificação, é apresentada uma mensagem de aviso e a aplicação pede a confirmação. Para utilizar o código, prima **Sim**. Para criar um novo código, prima **Não**. Introduza um novo código secreto da aplicação.

2. Reintroduza o mesmo código no campo **Confirmar novo código**.

O código secreto é instalado.

ACTIVAR A OPÇÃO PARA RECUPERAR O CÓDIGO SECRETO

Após a primeira activação da aplicação poderá activar a opção para recuperar o código secreto da aplicação. Desse modo, no futuro poderá recuperar o código secreto se o esquecer.

Se declinar a activação da função após a primeira activação da aplicação, pode activá-la após reinstalar o Kaspersky Mobile Security 9 no dispositivo.

Apenas pode recuperar o código secreto da aplicação (consulte a secção "Recuperar o código secreto" na página 26) se a recuperação do código secreto for activada. Se tiver esquecido a sua palavra-passe e a função de recuperação do código secreto estiver desactivada, será impossível utilizar as funções do Kaspersky Mobile Security 9.

➔ *Para activar a opção de recuperação do código secreto:*

1. Após instalar o código secreto da aplicação (consulte a secção "Instalar o código secreto" na página 25) introduza o seu endereço de e-mail na janela **Activar opção para recuperar código secreto**.
2. Confirme a activação da função de recuperação do código secreto clicando em **Activar**.

O endereço de e-mail que fornecer será utilizado durante a recuperação do código secreto.

A aplicação estabelecerá uma ligação à Internet com o servidor de recuperação do código secreto, enviará a informação introduzida e activará a opção de recuperação do código secreto.

RECUPERAR O CÓDIGO SECRETO

Só pode recuperar o código secreto se activar previamente a opção de recuperação do código secreto (consulte "Activar a opção para recuperar o código secreto" na página 26).

➔ *Para recuperar o código secreto da aplicação:*

1. Mudar da janela principal para a janela da aplicação.
2. Instalar o **Kaspersky Mobile Security 9**.

É apresentada a janela do **Kaspersky Mobile Security 9**.

3. Clicar em **Menu** → **Recuperar código secreto**.

É apresentada na janela uma mensagem com as seguintes informações:

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

4. Premir **Ir**.

Desloque-se até ao website <http://mobile.kaspersky.com/recover-code> para recuperar o código secreto.

5. Introduza as informações seguintes nos campos apropriados:

- o endereço de e-mail que designou previamente para recuperação do código secreto;
- código de identificação do dispositivo.

Como resultado, o código de recuperação será enviado para o endereço de e-mail que indicou.

6. Mude para a janela do **Kaspersky Mobile Security 9**.

7. Clique em **Menu** → **Introduzir código de recuperação** e introduza o código de recuperação recebido.

8. Introduza o novo código secreto da aplicação. Para o fazer, introduza um novo código secreto da aplicação nos campos **Introduzir novo código** e **Confirmar código secreto**.

9. Clique em **Enter**.

INICIAR A APLICAÇÃO

➤ *Para iniciar o Kaspersky Mobile Security 9:*

1. Mudar da janela principal para a janela da aplicação.
2. Instalar o **Kaspersky Mobile Security 9**.
3. É apresentada a janela do **Kaspersky Mobile Security 9**.
4. Introduza o código secreto da aplicação e prima **OK**.

A janela principal da aplicação abre.

VER INFORMAÇÕES SOBRE A APLICAÇÃO

Pode visualizar a informação geral sobre o Kaspersky Mobile Security 9 e a respectiva versão.

➤ *Para ver informações sobre a aplicação:*

1. Na janela principal do Kaspersky Mobile Security 9, a caixa **Adicional** abre.
Este procedimento irá abrir a janela **Adicional**.
2. Na caixa **Informação**, seleccione **Sobre**.

GERIR A LICENÇA

No contexto de licenciamento de aplicações da Kaspersky Lab, é importante conhecer os seguintes termos:

- Contrato de Licença;
- licença.

Estes termos estão intrinsecamente interligados e constituem um único padrão de licenciamento. Segue-se uma análise mais aprofundada de cada um dos termos.

Além disso, a secção apresenta informações sobre como encontrar informações sobre a licença do Kaspersky Mobile Security 9 e alargar o prazo de validade da mesma.

NESTA SECÇÃO

Sobre o Contrato de Licença.....	28
Sobre as licenças do Kaspersky Mobile Security 9.....	28
Ver informações da Licença.....	29
Renovar a licença	30

SOBRE O CONTRATO DE LICENÇA

O *Contrato de Licença* é um contrato celebrado entre um indivíduo privado ou uma entidade legal, a qual é proprietária legal de uma cópia do Kaspersky Mobile Security 9, e a Kaspersky Lab. O contrato está incluído em todas as aplicações da Kaspersky Lab. Este contrato apresenta informações detalhadas sobre os direitos e limitações relacionados com a utilização do Kaspersky Mobile Security.

De acordo com o Contrato de Licença, ao adquirir e instalar uma aplicação da Kaspersky Lab, o utilizador obtém o direito ilimitado de propriedade da respectiva cópia.

Kaspersky Lab também disponibiliza serviços adicionais:

- suporte técnico;
- actualização das bases de dados antivírus do Kaspersky Mobile Security 9;
- actualização dos módulos de programa do Kaspersky Mobile Security 9.

Para beneficiar destes serviços, tem de adquirir e activar uma licença (consulte a secção “Sobre as Licenças do Kaspersky Mobile Security 9” na página [28](#)).

SOBRE AS LICENÇAS DO KASPERSKY MOBILE SECURITY 9

Uma *licença* é o direito de utilização do Kaspersky Mobile Security 9 e dos serviços adicionais associados com este conforme disponibilizados pela Kaspersky Lab ou seus parceiros.

Cada licença tem um prazo de validade e um tipo.

Termo de licença – um período durante o qual são oferecidos os serviços adicionais.

- suporte técnico;
- actualização das bases de dados antivírus do Kaspersky Mobile Security 9;
- actualização dos módulos de programa do Kaspersky Mobile Security 9.

O âmbito dos serviços fornecidos depende do tipo de licença.

Estão disponíveis os seguintes tipos de licença:

- *Demonstração*– licença gratuita com um período de validade limitado, por exemplo, de 30 dias, oferecido de modo a se familiarizar com o Kaspersky Internet Security 9.

A licença de demonstração pode ser apenas utilizada uma vez.

Se possuir uma licença de demonstração, poderá apenas contactar o Serviço de Assistência Técnica se a sua questão estiver relacionada com a activação do produto ou sobre como adquirir uma licença comercial. Quando a licença de demonstração do Kaspersky Mobile Security 9 expirar, todas as funcionalidades ficam desactivadas. Para continuar com a aplicação deve activá-la.

- *Comercial*– licença paga com um período de validade limitado (por exemplo, um ano), fornecida aquando da compra do Kaspersky Internet Security 9.

Se for activada uma licença comercial, todas as características da aplicação e serviços adicionais estarão disponíveis.

Ao terminar o período de validade da licença comercial, algumas funções do Kaspersky Mobile Security 9 ficam inacessíveis, e as bases de dados da aplicação não serão actualizadas. Uma semana antes da data de expiração da licença, a aplicação irá notificá-lo desta ocorrência de modo a que possa renovar a licença antecipadamente.

- *Comercial com subscrição* – licença paga com uma opção de renovação em modo automático ou manual. Uma licença com subscrição é distribuída por prestadores de serviços

A subscrição é válida por um período limitado (30 dias). Após a subscrição expirar ela pode ser renovada manualmente ou automaticamente. O método de renovação da subscrição depende da legislação e do prestador de serviços móveis. A subscrição é renovada automaticamente sujeita a um pagamento prévio atempado ao prestador.

Neste caso a quantia fixa especificada nos termos da subscrição é debitada da sua conta pessoal. Os fundos são debitados da sua conta pessoal após ter enviado uma mensagem SMS a pagar para o número do prestador de serviços.

Se a subscrição não for renovada, o Kaspersky Mobile Security 9 pára de actualizar as bases de dados da aplicação, a funcionalidade da aplicação torna-se limitada.

Ao utilizar a subscrição pode activar a licença comercial com um código de activação. Neste caso, a subscrição será cancelada automaticamente.

Ao utilizar a licença comercial pode activar a subscrição. Se já tiver uma licença activa com um termo limitado no momento de activação da subscrição, é substituído pela licença de subscrição.

VER INFORMAÇÕES DA LICENÇA

Pode ver as seguintes informações da licença: número da licença, tipo, data de activação, data de expiração, número de dias até à expiração e número de série do dispositivo.

➤ *Para ver informações sobre a licença:*

1. Na janela principal do Kaspersky Mobile Security 9, a caixa **Adicional** abre.
Este procedimento irá abrir a janela **Adicional**.
2. Seleccione **Licença** → **Sobre a licença**.

RENOVAR A LICENÇA

Kaspersky Mobile Security 9 permite que renove a licença da aplicação.

A licença pode ser expandida de uma das seguintes formas:

- Inserir código de activação – activar a aplicação com o código de activação. Pode adquirir o código de activação em <http://www.kasperskystore.com.pt/> ou junto do distribuidor da Kaspersky Lab da sua área.
- Compre o código de activação online – desloque-se até ao website visitado no seu dispositivo móvel e adquira um código de activação online.
- Subscreva o Kaspersky Mobile Security 9 – active a subscrição de modo a renovar a licença cada 30 dias.

A aplicação pode ser activada se for configurada uma ligação à Internet no dispositivo, for inserido um cartão SIM e introduzido o código PIN (se um tiver sido definido). Se esses requisitos não forem cumpridos, não será possível activar a aplicação.

NESTA SECÇÃO

Renovar a licença com o código de activação	30
Renovar a licença online	31
Renovar a licença ao activar a subscrição	31
Retirar a subscrição	32
Renovar a subscrição.....	32

RENOVAR A LICENÇA COM O CÓDIGO DE ACTIVAÇÃO

➤ *Para renovar a licença com o código de activação:*

1. Na janela principal do Kaspersky Mobile Security 9, a caixa **Adicional** abre.
Este procedimento irá abrir a janela **Adicional**.
2. Seleccione o item **Licença** → **Prolongar licença**.
Este procedimento irá abrir a janela **Activação**.
3. Seleccione **Inserir código de activação**.
Este procedimento irá abrir a janela **Inserir código de activação**.
4. Subsequentemente introduza o código de activação recebido e clique em **Activar**.

A aplicação irá enviar um pedido ao servidor de activação do Kaspersky Lab e irá receber uma licença. Quando a licença tiver sido recebida com sucesso, irão ser apresentadas no ecrã informações relativas à licença.

Se o código de activação que tiver introduzido for inválido por qualquer motivo, é apresentada uma mensagem informativa no ecrã. Neste caso, recomenda-se que verifique se o código de activação que introduziu está correcto e que contacte o distribuidor de software junto do qual adquiriu o Kaspersky Mobile Security 9.

Se tiverem ocorrido quaisquer erros na ligação ao servidor e não tiver sido recebida nenhuma licença, a activação é cancelada. Neste caso, recomenda-se que verifique os parâmetros da ligação à Internet. Se não for possível rectificar os erros, contacte o Apoio Técnico.

RENOVAR A LICENÇA ONLINE

➤ *Para renovar a licença online:*

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

Este procedimento irá abrir a janela **Adicional**.

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

Este procedimento irá abrir a janela **Activação**.

3. Seleccione **Comprar online**.

Este procedimento irá abrir a janela **Comprar online**.

4. Prima **Abrir**.

Abre um website especial para dispositivos móveis do Kaspersky Lab no qual pode adquirir um código de activação online.

5. Siga as instruções passo a passo.

6. Uma vez processada a encomenda para renovação da licença, introduza o código de activação obtido (consulte a secção "Renovar a licença com o código de activação" na página [30](#)).

RENOVAR A LICENÇA AO ACTIVAR A SUBSCRIÇÃO

Pode renovar o termo da licença activando a subscrição (consulte a secção "Sobre o licenciamento do Kaspersky Mobile Security 9" na página [28](#)) no Kaspersky Mobile Security 9. Quando a subscrição for activada, o Kaspersky Mobile Security 9 renova a licença cada 30 dias. Cada vez que a licença for renovada, a quantia fixa especificada nos termos da subscrição é debitada da sua conta pessoal.

➤ *Para activar a subscrição do Kaspersky Mobile Security 9:*

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

Este procedimento irá abrir a janela **Adicional**.

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

Este procedimento irá abrir a janela **Activação**.

Seleccione **Comprar com um clique**.

3. Leia as informações da subscrição e clique em **Activar**.

A aplicação irá verificar se o serviço de subscrição está acessível para o prestador de serviço móvel que está a utilizar. Se o serviço de subscrição estiver disponível, serão apresentadas no ecrã informações sobre os termos da subscrição.

Se os serviços de subscrição não puderem ser fornecidos, a aplicação irá notificá-lo disto e voltar ao ecrã no qual pode seleccionar outro modo de renovar a aplicação. A activação da subscrição será cancelada.

4. Leia os termos da subscrição e em seguida confirme a activação da subscrição do Kaspersky Mobile Security 9 premindo **Activar**.

A aplicação irá enviar uma mensagem SMS a pagar e em seguida irá receber uma licença do servidor de activação do Kaspersky Lab. Quando a subscrição ficar activa, o Kaspersky Mobile Security 9 irá notificá-lo do sucedido.

Se o seu saldo não possuir fundos suficientes para enviar uma mensagem SMS a pagar, a activação da subscrição será cancelada.

Se tiverem ocorrido quaisquer erros na ligação ao servidor e não tiver sido recebida nenhuma licença, a activação é cancelada. Neste caso, recomenda-se que verifique os parâmetros da ligação à Internet. Se não for possível rectificar os erros, contacte o Apoio Técnico.

Se não concordar com os termos da subscrição, regresse à janela de **Activação**. A aplicação irá cancelar a activação da subscrição e voltar para o ecrã no qual pode seleccionar outro método para renovar a licença.

RETIRAR A SUBSCRIÇÃO

Pode cancelar a subscrição para o Kaspersky Mobile Security 9. Neste caso, o Kaspersky Mobile Security 9 não irá renovar a licença cada 30 dias. Neste caso, quando a licença actual expirar a funcionalidade da aplicação tornar-se-á limitada, e as bases de dados da aplicação deixarão de ser actualizadas.

Se tiver cancelado a sua licença, pode retomá-la (consulte a secção "Renovar a subscrição" na página [32](#)).

➤ *Para cancelar uma subscrição do Kaspersky Mobile Security 9:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Adicional**.
2. Este procedimento irá abrir a janela **Adicional**.
3. Seleccione **Retirar a subscrição**.
4. Confirme o cancelamento da subscrição premindo em **Sim**.

O Kaspersky Mobile Security 9 irá notificá-lo do cancelamento da subscrição.

RENOVAR A SUBSCRIÇÃO

Se tiver cancelado a subscrição pode retomá-la.

Ao retomar a subscrição, os fundos são apenas debitados da sua conta pessoal se a licença actual expirar em menos de três anos.

➤ *Para retomar a subscrição:*

1. Na janela principal do Kaspersky Mobile Security 9, a caixa **Adicional** abre.
Este procedimento irá abrir a janela **Adicional**.
2. Seleccione o item **Licença** → **Prolongar licença**.

Este procedimento irá abrir a janela **Activação**.

3. Seleccionar **Comprar com um clique**.

Se o termo de validade da licença actual tiver expirado, o Kaspersky Mobile Security 9 sugere activar a subscrição (consulte a secção "Sobre as licenças Kaspersky Mobile Security 9" na página [28](#)).

Se a licença actual ainda não tiver expirado, o Kaspersky Mobile Security 9 retoma a subscrição e renova-a cada 30 dias após a expiração da licença actual.

INTERFACE DA APLICAÇÃO

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

NESTA SECÇÃO

Janela de estado da protecção	33
Widget do ecrã inicial	34

JANELA DE ESTADO DA PROTECÇÃO

Após iniciar o programa, abre a janela principal da aplicação (consulte a Figura abaixo).

Os módulos de expansão estão localizados na janela principal. Cada módulo permite mudar as definições dos parâmetros de um dos componentes da aplicação e efectuar tarefas de protecção.

A janela principal também apresenta a condição dos seus componentes principais.

Para cada módulo são apresentadas as seguintes informações abaixo do seu nome:

- **Antivírus** – estado da protecção do dispositivo de vírus e outras aplicações maliciosas (consulte a secção "Protecção do sistema de ficheiros" na página [35](#));
- **Protecção de Privacidade** – modo de ocultação de informações confidenciais.
- **Anti-Roubo** – Estados das funções Anti-Roubo.
- **Filtro de Chamadas e SMS** – modo de filtragem para chamadas e SMS.
- **Adicional** – informações sobre parâmetros adicionais neste módulo (consulte a secção "Efectuar definições adicionais" na página [77](#)).

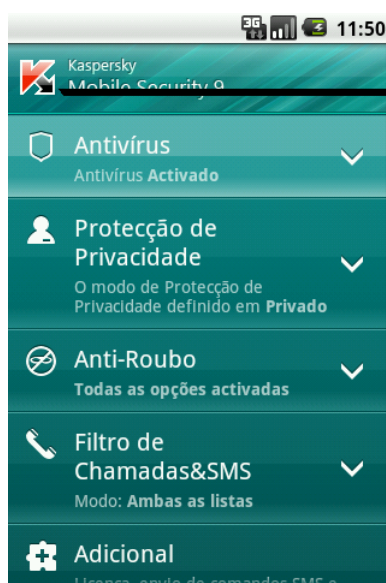


Figura 1. A janela principal da aplicação

WIDGET DO ECRÃ INICIAL

Ao utilizar o Kaspersky Mobile Security 9, o widget do ecrã inicial fica acessível. Após instalar a aplicação, o widget automaticamente surge na janela principal do dispositivo (consulte a Figura abaixo).

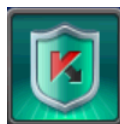


Figura 2. Widget do ecrã inicial

O indicador de cor do widget no ecrã principal informa-o sobre o estado de protecção do seu dispositivo, a Protecção de Privacidade e a licença, e permite que configure as definições da aplicação.

Está presente a seguinte indicação a cores:

- se a protecção for verde, a protecção está activada;
- se a protecção for cinzenta, a protecção é desactivada;
- uma cor de fundo verde significa que as informações confidenciais estão ocultas;
- uma cor de fundo cinzenta significa que as informações confidenciais estão apresentadas;
- um ponto de exclamação num triângulo amarelo significa que os termos de validade da licença expiraram ou que a licença não foi instalada.

PROTECÇÃO DO SISTEMA DE FICHEIROS

Esta secção fornece informações sobre o componente de Protecção que permite impedir infecções no sistema de ficheiros do dispositivo. A secção igualmente especifica a forma de activar/parar a Protecção e regular as suas configurações de funcionamento.

NESTA SECÇÃO

Sobre a Protecção	35
Activa/Desactiva a Protecção.....	35
Configurar a área de protecção.....	36
Seleccionar a acção a efectuar em objectos detectados	37

SOBRE A PROTECÇÃO

A Protecção inicia-se quando o sistema operativo arranca e encontra-se sempre na memória do dispositivo. A protecção verifica todos os ficheiros abertos, guardados e iniciados (incluindo aqueles em cartões de memória), assim como as aplicações instaladas.

Os ficheiros são verificados de acordo com o seguinte algoritmo:

1. A protecção verifica cada ficheiro quando o utilizador lhe acede.
2. A protecção analisa o ficheiro quanto à presença de objectos maliciosos. Os objectos maliciosos são detectados em comparação com as bases de dados de antivírus da aplicação. As bases de dados antivírus contêm descrições de todos os objectos maliciosos conhecidos actualmente e dos métodos para neutralizá-los.
3. De acordo com os resultados da análise, são possíveis os seguintes tipos de Protecção:
 - Se for detectado um código malicioso no ficheiro, a protecção desempenha uma acção de acordo com as definições efectuadas (consulte a secção "Seleção de acção relativamente aos objectos detectados" na página [37](#));
 - Se não tiver sido detectado código malicioso no ficheiro, este será imediatamente restaurado.

A protecção verifica a aplicação instalada quanto a vírus quando esta for executada pela primeira vez. A protecção desempenha uma verificação relativamente às bases de dados antivírus. Se a protecção detectar um vírus durante a verificação de uma aplicação, esta sugere eliminar a aplicação.

ACTIVA/DESACTIVA A PROTECÇÃO

Ao activar a Protecção, todas as acções no sistema ficam sob controlo permanente.

Para assegurar a protecção de vírus e outras ameaças são utilizados os recursos do dispositivo. Para reduzir a carga no dispositivo ao executar diversas tarefas, pode parar temporariamente a Protecção.

Os especialistas da Kaspersky Lab recomendam que não desactive a Protecção, uma vez que este procedimento pode provocar a infecção do seu computador e a perda de dados.

Desactivar a protecção não tem qualquer impacto no desempenho de tarefas de verificação antivírus e na actualização das bases de dados antivírus da aplicação.

O estado actual da protecção é apresentado na janela principal da aplicação no modelo **Antivírus**.

➔ *Para activar a Protecção:*

1. Na janela principal do Kaspersky Mobile Security 9, a caixa **Antivírus** abre.
2. Clique **Adicional**.
A janela **Antivírus: Adicional** abre.
3. Seleccione a caixa **Activar Protecção** (consulte a Figura abaixo).

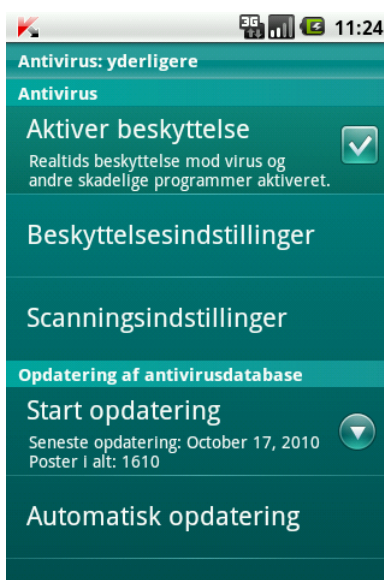


Figura 3. Activar a Protecção

➔ *Para desactivar a Protecção:*

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

CONFIGURAR A ÁREA DE PROTECÇÃO

Por defeito, o Kaspersky Mobile Security 9 verifica todos os tipos de ficheiro. Pode seleccionar ficheiros para o Kaspersky Mobile Security 9 verificar quanto à presença de objectos maliciosos durante a operação da Protecção.

Antes de configurar a protecção assegure-se primeiro de que a protecção está activada.

➤ *Para seleccionar o tipo de ficheiros a verificar:*

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

A janela **Antivírus: Adicional** abre.

3. Seleccionar **Definições de protecção** → **Tipo de ficheiros para protecção**.
4. Seleccionar o valor para as definições do **Tipo de ficheiros para protecção** (consulte a Figura abaixo):

- **Todos os ficheiros** — verificar todos os tipos de ficheiro.
- **Apenas executáveis** – verificar apenas ficheiros de aplicação executáveis (por exemplo, ficheiros dos formatos EXE, MDL, APP, DLL, SO, ELF).

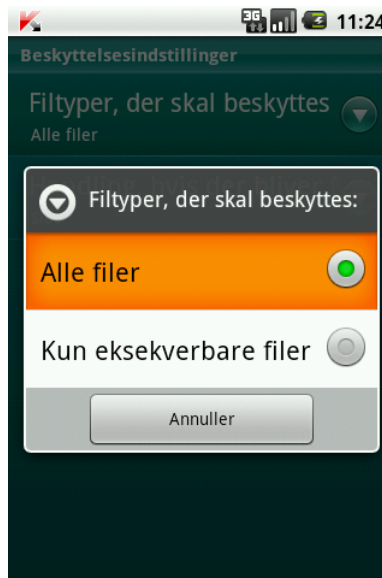


Figura 4. Seleccionar os objectos a verificar

SELECIONAR A ACÇÃO A EFECTUAR EM OBJECTOS DETECTADOS

Por predefinição, o Kaspersky Mobile Security 9 elimina a ameaça detectada. Pode escolher a acção que o Kaspersky Mobile Security 9 executa após a detecção de um objecto malicioso.

➤ *Para definir a resposta da aplicação ao detectar uma ameaça, proceda do modo seguinte:*

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

A janela **Antivírus: Adicional** abre.

3. Seleccionar **Definições de Protecção** → **Acção a tomar ao detectar ameaça**.
4. Configure uma acção que a aplicação irá executar se encontrar um objecto malicioso. Para fazer isto, seleccione um valor para as definições da **Acção a tomar ao detectar ameaça** (consulte a Figura abaixo):

- **Apagar** — apagar os objectos de software malicioso sem notificar o utilizador.
- **Ignorar** – ignorar objectos maliciosos. Bloquear o objecto quando forem efectuadas tentativas de utilizá-lo (por exemplo, copiar ou abrir).

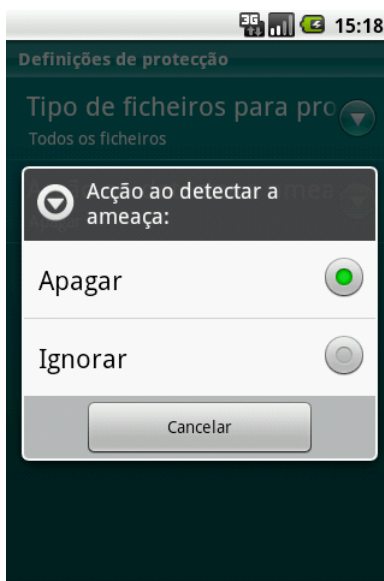


Figura 5. Seleccionar a acção a tomar ao detectar a ameaça

VERIFICAR O DISPOSITIVO

Esta secção fornece informações sobre a verificação do dispositivo a pedido, que pode detectar e remover ameaças no seu dispositivo. A secção também descreve como executar uma verificação do dispositivo, configurar uma verificação agendada automática do sistema de ficheiros, seleccionar ficheiros para a verificação e definir a acção que a aplicação irá tomar quando for detectado um objecto malicioso.

NESTA SECÇÃO

Sobre a verificação do dispositivo	39
Iniciar uma verificação manualmente	39
Iniciar uma verificação agendada	40
Seleção do tipo de objecto a verificar	41
Configurar verificações activas	42
Seleccionar a acção a efectuar em objectos detectados	43

SOBRE A VERIFICAÇÃO DO DISPOSITIVO

A verificação do dispositivo a pedido ajuda a detectar e remover ameaças no seu dispositivo. O Kaspersky Mobile Security 9 permite uma verificação integral ou parcial do dispositivo incluído, isto é, verifica apenas o conteúdo da memória incorporada do dispositivo ou de uma pasta específica (incluindo uma pasta localizada no cartão de memória).

O dispositivo é verificado da seguinte forma:

1. O Kaspersky Mobile Security 9 verifica os tipos de ficheiro definidos (consulte a secção "Seleccionar os tipos de objecto a verificar" na página [41](#)).
2. Durante a verificação cada ficheiro é analisado quanto à presença de objectos maliciosos (software malicioso). Os objectos maliciosos são detectados em comparação com as bases de dados de antivírus da aplicação. As bases de dados antivírus contêm descrições de todos os objectos maliciosos conhecidos e dos métodos para neutralizá-los.

Se na sequência de uma análise do ficheiro a aplicação detectar um código malicioso, esta desempenha a acção seleccionada em conformidade com as definições efectuadas (consulte a secção "Seleção da acção a tomar relativamente aos objectos detectados" consulte a página [43](#)).

A verificação inicia manual ou automaticamente de acordo com uma agenda (consulte "Iniciar uma verificação agendada" na página [40](#)).

INICIAR UMA VERIFICAÇÃO MANUALMENTE

Pode iniciar manualmente uma verificação integral ou parcial conforme requerido.

➤ *Para iniciar uma verificação antivírus manualmente:*

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

3. Seleccione a área de verificação do dispositivo (seleccione a Figura abaixo):

- **Verificação completa:** verificar todo o sistema de ficheiros do dispositivo. Por defeito, a aplicação verifica os ficheiros guardados na memória incorporada do dispositivo e nos cartões de memória.
- **Verificação de pasta** - verificar um objecto individual no sistema de ficheiros do dispositivo ou no cartão de memória. Quando for seleccionado **Verificação de pasta**, será apresentada uma janela que mostra o **Sistema de ficheiros** do dispositivo. Para começar a verificar uma pasta seleccione a pasta requerida e clique no ícone da verificação localizado à direita da pasta.
- **Verificação da memória** - verificar os processos iniciados na memória do sistema e os ficheiros correspondentes.

Após a verificação iniciar, abre uma janela de progresso da verificação que apresenta o estado da tarefa actual: o número de ficheiros verificados, o caminho para o ficheiro a ser actualmente verificado e uma indicação dos resultados da verificação em percentagem. Na janela do progresso da verificação, pode pausar a verificação clicando em **Suspender**, ou concluir o processo de verificação clicando em **Cancelar**.

Se o Kaspersky Mobile Security 9 detectar um objecto malicioso, efectua uma acção de acordo com os parâmetros configurados para a verificação (consulte a secção “Seleccionar uma acção a executar em objectos⁴³” na página).

Por defeito, se detectar uma ameaça, o Kaspersky Mobile Security 9. tenta eliminá-la. Se a desinfecção falhar ou for impossível, a aplicação elimina o objecto malicioso.

Uma vez concluída a verificação, as estatísticas globais são apresentadas no ecrã com as seguintes informações:

- número de ficheiros verificados;
- número de vírus detectados e eliminados;
- número de ficheiros aceites (por exemplo, um ficheiro é bloqueado pelo sistema operativo ou não é executável, ao verificar apenas ficheiros de programa executáveis);
- hora da verificação.

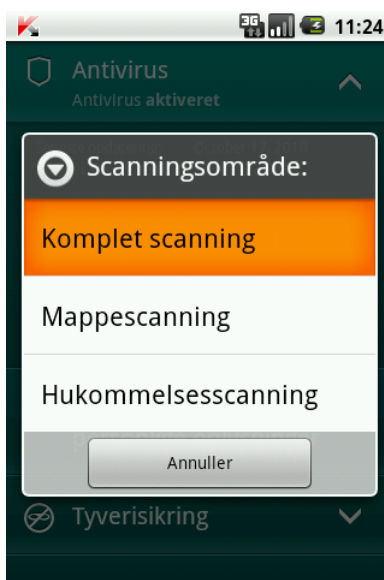


Figura 6. Selecciona a área de verificação

INICIAR UMA VERIFICAÇÃO AGENDADA

Pode configurar a verificação do sistema de ficheiros para iniciar automaticamente conforme programado. Uma verificação agendada é desempenhada em modo de fundo. Quando é detectado um objecto infectado, a acção seleccionada nas configurações de verificação será executada no mesmo (consulte a secção “Seleccionar uma acção a executar em objectos” na página [43](#)).

Por defeito, o início de uma verificação agendada do sistema de ficheiros está desactivado.

➤ *Para definir um agendamento de verificação:*

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

A janela **Antivírus: Adicional** abre.

3. Seleccionar as **Definições de verificação**.

A janela das **Definições de verificação** abre.

4. Seleccionar o modo de início da verificação. Para fazer isto, defina o valor para as **Definições da verificação agendada**:
 - **Semanalmente** — executa a verificação uma vez por semana. Para fazer isto defina o dia e hora de início da verificação. Para fazer isto seleccione valores para as definições **Dia da verificação** e **Hora da verificação**.
 - **Diariamente** — executa a verificação todos os dias. Para fazer isto defina a hora de início da verificação. Defina o valor para a definição da **Hora da verificação**.
 - **Desactivada** – desactivar verificações agendadas.



Figura 7. Configurar verificação automática

SELECÇÃO DO TIPO DE OBJECTO A VERIFICAR

Por defeito, o Kaspersky Mobile Security 9 verifica todos os ficheiros guardados no dispositivo e no cartão de memória. Para reduzir o tempo de verificação, pode seleccionar o tipo de objecto a verificar, isto é, determinar quais os formatos de ficheiro que a aplicação deve verificar relativamente à presença de código malicioso.

➔ *Para seleccionar objectos a verificar:*

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

2. Clique **Adicional**.

A janela **Antivírus: Adicional** abre.

3. Selecciona **Definições de verificação** → **Área de verificação**.

A janela da **Área de verificação** abre.

4. Defina o valor para a definição **Tipo de ficheiros** (consulte a Figura abaixo):

- **Todos os ficheiros** — verificar todos os tipos de ficheiro.
- **Apenas executável** – apenas verifica ficheiros da aplicação executáveis nos seguintes formatos: EXE, DLL, MDL, APP, RDL, PRT, PXT, LDD, PDD, CLASS, SO, ELF.



Figura 8. Seleccionar tipo de ficheiros a verificar

CONFIGURAR VERIFICAÇÕES ACTIVAS

Os vírus ficam frequentemente ocultos em arquivos. O programa verifica os seguintes formatos de arquivos: ZIP, JAR, JAD, SIS, SISX, CAB e APK. Os arquivos são descomprimidos durante a verificação, o que pode reduzir significativamente a velocidade da Verificação a pedido.

Pode activar / desactivar a verificação de arquivos quanto a códigos maliciosos durante a Verificação a pedido.

➔ *Para activar a verificação de arquivos:*

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

2. Clique **Adicional**.

A janela **Antivírus: Adicional** abre.

3. Seleccione **Definições de verificação** → **Área de verificação**.

A janela da **Área de verificação** abre.

4. Seleccionar a caixa de verificação **Arquivos de verificação**.

SELECIONAR A ACÇÃO A EFECTUAR EM OBJECTOS DETECTADOS

Por predefinição, o Kaspersky Mobile Security 9 tenta rectificar uma ameaça ao detectá-la, se a desinfecção falhar apaga-a. Pode definir as acções da aplicação ao detectar uma ameaça.

► *Para alterar o modo como a aplicação age perante o objecto malicioso detectado:*

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

2. Clique **Adicional**.

A janela **Antivírus: Adicional** abre.

3. Seleccione **Definições de Protecção** → **Acção a tomar ao detectar ameaça**.

A janela **Acção a tomar ao detectar ameaça** abre.

4. Defina a primeira acção a tomar relativamente à ameaça detectada. Seleccione a caixa de verificação **Desinfectar**, de modo a que a aplicação tente primeiro desinfectar a ameaça detectada. Retire a selecção da caixa de verificação **Desinfectar**, de modo a que a aplicação não tente primeiro desinfectar a ameaça detectada.

5. Defina a segunda acção da aplicação se a ameaça detectada não puder ser desinfectada. Para fazer isto, seleccione o valor para a definição **Se não for possível desinfectar** (consulte a Figura abaixo):

- **Perguntar ao Utilizador** — solicitar acções ao utilizador quando for detectado um objecto malicioso.
- **Apagar** — apagar os objectos de software malicioso sem notificar o utilizador.
- **Ignorar** : não processar objectos de software malicioso e registar informações sobre a respectiva detecção no log da aplicação. Bloquear o objecto quando forem efectuadas tentativas de utilizá-lo (por exemplo, copiar ou abrir).

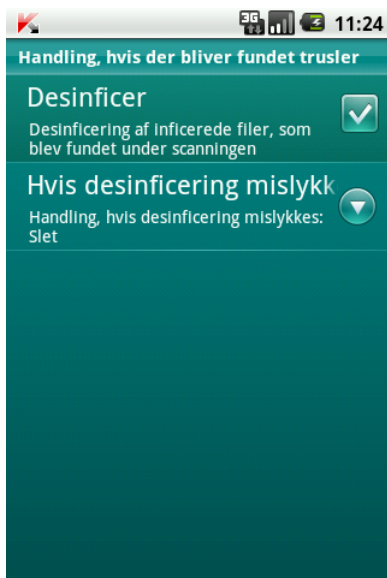


Figura 9. Seleccionar uma acção perante objectos maliciosos, se eles não puderem ser desinfectados

FILTRAGEM DE CHAMADAS E MENSAGENS SMS DE ENTRADA

Esta secção disponibiliza informações sobre o Filtro de Chamadas e SMS que bloqueia chamadas e SMS indesejadas de acordo com as Listas Branca e Negra que criar. A secção também descreve como seleccionar o modo no qual o Filtro de Chamadas e SMS verifica chamadas e SMS, sobre como configurar definições de filtragem adicionais para SMS e chamadas de entrada e também sobre como criar Listas Negras e Brancas.

NESTA SECÇÃO

Sobre o Filtro de Chamadas e SMS.....	45
Sobre os modos do Filtro de Chamadas e SMS	46
Alterar o modo do Filtro de Chamadas e SMS	46
Criar a Lista Negra	46
Criar uma Lista Branca.....	49
Responder a mensagens SMS e chamadas de contactos não incluídos na lista de números.....	52
Responder a mensagens SMS de números não numéricos	53
Seleccionar uma resposta para SMS de entrada.....	54
Seleccionar uma resposta para chamadas de entrada	55
Ver registos do Log	55

SOBRE O FILTRO DE CHAMADAS E SMS

O Filtro de Chamadas e SMS evita que as chamadas e SMS indesejadas sejam entregues, com base na Lista Negra e na Lista Branca que compilou.

A lista é constituída por registos. Uma entrada em uma das listas contém as seguintes informações:

- O número de telefone do qual o Filtro de Chamadas e SMS bloqueia informações caso este esteja na Lista Negra e entrega informações caso o número esteja na Lista Branca.
- O tipo de evento que o Filtro de Chamadas e SMS bloqueia se estiver na Lista Negra e entrega se estiver na Lista Branca. Estão disponíveis os seguintes tipos de comunicações: chamadas e SMS, apenas chamadas e apenas SMS.
- A expressão-chave utilizada pelo Filtro de Chamadas e SMS para identificar SMS desejadas e indesejadas. Para a Lista Negra, o Filtro de Chamadas e SMS bloqueia SMS que contenham esta frase, entregando aquelas que não a contenham. Para a Lista Branca, o Filtro de Chamadas e SMS entrega SMS que contenham esta frase, bloqueando aquelas que não a contenham.

O Anti-Spam filtra as chamadas e mensagens conforme prescrito pelo modo seleccionado (consulte a secção "Sobre os modos do Filtro de Chamadas e SMS" na página [46](#)). De acordo com o modo, o Filtro de Chamadas e SMS verifica cada mensagem SMS ou chamada de entrada e, em seguida, determina se esta mensagem ou chamadas é desejada ou indesejada (spam). Assim que o Filtro de Chamadas e SMS atribuir o estado desejado ou indesejado a uma mensagem SMS ou chamada, a verificação está concluída.

As informações em SMS e chamadas bloqueadas são registadas no Log do Filtro de Chamadas e SMS (consulte a secção "Ver entradas no log" na página [55](#)).

SOBRE OS MODOS DO FILTRO DE CHAMADAS E SMS

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

Encontram-se disponíveis os seguintes modos do Filtro de Chamadas e SMS:

- **Off** – todas as chamadas e SMS de entrada são permitidas.
- **Lista Negra** – todas as chamadas e SMS são permitidas excepto aquelas que tenham origem em números na Lista Negra.
- **Lista Branca** – apenas são permitidas chamadas e SMS que tenham origem na Lista Branca.
- **Ambas listas** – a entrada de chamadas e SMS de números na Lista Branca é permitida enquanto aquelas da Lista Negra são bloqueadas. Na sequência de uma conversa ou da leitura de uma SMS proveniente de um número que não se encontre em nenhuma das listas, o Filtro de Chamadas e SMS irá pedir-lhe que introduza o número em uma das listas.

Pode alterar o modo do Filtro de Chamadas e SMS (consulte a secção "Alterar o modo do Filtro de Chamadas e SMS" na página [46](#)). O modo actual do Filtro de Chamadas e SMS é apresentado no separador **Filtro de Chamadas e SMS** junto do item do menu **Modo**.

MUDAR O MODO DO FILTRO DE CHAMADAS E SMS

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

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

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

3. Selecciono o valor para a definição **Modo do Filtro de Chamadas e SMS** (consulte a Figura abaixo).



Figura 10. Alterar o modo do Filtro de Chamadas e SMS

CRIAR A LISTA NEGRA

A Lista Negra contém entradas de número banidos, isto é, os números cujas chamadas e SMS o Filtro de Chamadas e SMS bloqueia. Cada entrada contém as seguintes informações:

- Número de telefone do qual o Filtro de Chamadas e SMS bloqueia as chamadas e / ou SMS.
- Tipos de eventos que o Filtro de Chamadas e SMS bloqueia deste número. Estão disponíveis os seguintes tipos de eventos: chamadas e SMS, apenas chamadas e apenas SMS.
- Expressão-chave que o Filtro de Chamadas e SMS utiliza para classificar uma SMS como não solicitada (spam). O Filtro de Chamadas e SMS apenas bloqueia SMS que contenham a expressão-chave, sendo que entrega todas as outras SMS.

O Filtro de Chamadas e SMS bloqueia chamadas e SMS que cumpram todos os critérios de uma entrada na Lista Negra. As chamadas e SMS que não cumpram nem que seja um dos critérios das entradas na Lista Negra serão permitidas pelo Filtro de Chamadas e SMS.

Não pode adicionar um número de telefone com critérios de filtragem idênticos tanto à Lista Negra como à Lista Branca.

As informações em SMS e chamadas bloqueadas são registadas no Log do Filtro de Chamadas e SMS (consulte a secção "Ver entradas no log" na página [55](#)).

NESTA SECÇÃO

Adicionar registos à Lista Negra	47
Editar registos na Lista Negra	48
Apagar registos da Lista Negra	49

ADICIONAR REGISTOS À LISTA NEGRA

Lembre-se de que o mesmo número com critérios de filtragem idênticos não pode ser incluído simultaneamente nas listas Branca e Negra do Filtro de Chamadas e SMS. Se um número com tais critérios de filtragem já tiver sido incluído numa das listas, o Kaspersky Mobile Security 9 irá notificá-lo da ocorrência, e irá surgir no ecrã uma mensagem relevante.

➤ Para adicionar um registo à Lista Negra do Filtro de Chamadas e SMS:

1. Na janela principal do Kaspersky Mobile Security 9, abra o Módulo do **Filtro de Chamadas e SMS**.
2. Seleccionar **Lista Negra**.

Este procedimento irá abrir a janela **Lista Negra**.

3. Clicar **Adicionar**.
4. Configure os valores com as seguintes definições:
 - **Entrada bloqueada** – tipo de evento de um número de telefone que o Filtro de Chamadas e SMS bloqueia para números da Lista Negra:
 - **SMS**: bloquear apenas mensagens SMS de entrada.
 - **Chamadas**: bloquear apenas chamadas de entrada.

- **Chamadas e SMS:** bloquear chamadas e mensagens SMS de entrada.
- **Número de telefone bloqueado** – número de telefone para o qual o Filtro de Chamadas e SMS bloqueia a entrada de informações. Este número deve conter apenas caracteres alfanuméricos; pode começar com um dígito, uma letra ou com o símbolo “+”. Como número, também é possível utilizar as máscaras “*” ou “?” (em que “*” corresponde a qualquer quantidade de símbolos e “?” a qualquer símbolo único). Por exemplo, *1234? na Lista Negra. O Filtro de Chamadas e SMS bloqueia chamadas ou SMS de um número no qual quaisquer símbolos sigam a figura 1234.
- **Texto bloqueado** – expressão-chave que indica que a SMS recebida é indesejada (spam). O Filtro de Chamadas e SMS apenas bloqueia SMS que contenham a expressão-chave, sendo que entrega todas as outras SMS.

Definição acessível para eventos de **SMS** .

Se desejar que todas as SMS de entrada de um número específico da Lista Negra sejam bloqueadas, deixe o campo **Texto bloqueado** desta entrada em branco.

5. Prima **Guardar**:

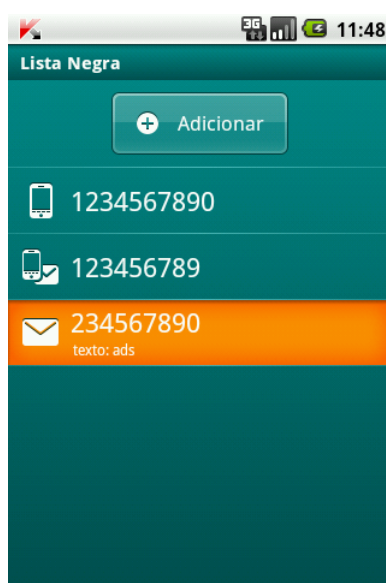


Figura 11. Adicionar registos à Lista Negra

EDITAR REGISTOS NA LISTA NEGRA

Pode alterar os valores de todas as configurações relativas a registos 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 do **Filtro de Chamadas e SMS**.
2. Seleccione **Lista Negra**.

Este procedimento irá abrir a janela **Lista Negra**.

3. Seleccione uma entrada da lista que deseje alterar e seleccione **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 a entrada de informações. Este número deve conter apenas caracteres alfanuméricos; pode começar com um dígito, uma letra ou com o símbolo "+". Como número, também é possível utilizar as máscaras "*" ou "?" (em que "*" corresponde a qualquer quantidade de símbolos e "?" a qualquer símbolo único). Por exemplo, *1234? na Lista Negra. O Filtro de Chamadas e SMS bloqueia chamadas ou SMS de um número no qual quaisquer símbolos sigam a figura 1234.
- **Texto bloqueado** – expressão-chave que indica que a SMS recebida é indesejada (spam). O Filtro de Chamadas e SMS apenas bloqueia SMS que contenham a expressão-chave, sendo que entrega todas as outras SMS.

Definição acessível para eventos de **SMS** .

Se desejar que todas as SMS de entrada de um número específico da Lista Negra sejam bloqueadas, deixe o campo **Texto bloqueado** desta entrada em branco.

5. Prima **Guardar**:

APAGAR REGISTOS DA LISTA NEGRA

Pode apagar um número da Lista Negra. Além disso, pode limpar a Lista Negra do Filtro de Chamadas e SMS removendo todos os registos da mesma.

➤ *Para apagar um registo da Lista Negra do Filtro de Chamadas e SMS:*

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

Este procedimento irá abrir a janela **Lista Negra**.

3. Seleccione uma entrada na lista que deva ser eliminada e seleccione **Apagar** 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 do **Filtro de Chamadas e SMS**.
2. Seleccionar **Lista Negra**.

Este procedimento irá abrir a janela **Lista Negra**.

3. Seleccione **Apagar todos** no menu de contexto.

A janela de confirmação abre.

4. Confirme a desinstalação da aplicação premindo o botão **Sim**.

A lista é esvaziada.

CRIAR UMA LISTA BRANCA

A Lista Branca contém entradas de números permitidos, ou seja, números dos quais o Filtro de Chamadas e SMS entrega as chamadas e SMS ao utilizador. Cada entrada contém as seguintes informações:

- Número de telefone do qual o Filtro de Chamadas e SMS entrega as chamadas e / ou SMS.

- Tipos de eventos que o Filtro de Chamadas e SMS entrega deste número. Estão disponíveis os seguintes tipos de eventos: chamadas e SMS, apenas chamadas e apenas SMS.
- Expressão-chave que o Filtro de Chamadas e SMS utiliza para classificar uma SMS como solicitada (não spam). O Filtro de Chamadas e SMS apenas entrega SMS que contenham a expressão-chave, sendo que bloqueia todas as outras SMS.

O Filtro de Chamadas e SMS permite apenas as chamadas e SMS que cumprem todos os critérios das entradas na Lista Branca. As chamadas e SMS que não cumpram nem que seja um dos critérios das entradas na Lista Branca serão bloqueadas pelo Filtro de Chamadas e SMS.

NESTA SECÇÃO

Adicionar registos à Lista Branca	50
Editar registos na Lista Branca	51
Apagar registos da Lista Branca	52

ADICIONAR REGISTOS À LISTA BRANCA

Lembre-se de que o mesmo número com critérios de filtragem idênticos não pode ser incluído simultaneamente nas listas Branca e Negra do Filtro de Chamadas e SMS. Se um número com tais critérios de filtragem já tiver sido incluído numa das listas, o Kaspersky Mobile Security 9 irá notificá-lo da ocorrência, e irá surgir no ecrã uma mensagem relevante.

➤ Para adicionar um registo à Lista Branca do Filtro de Chamadas e SMS:

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

Este procedimento irá abrir a janela **Lista Branca**.

3. Prima **Adicionar** (consulte a Figura abaixo).
4. Aplique as seguintes definições para a nova entrada:
 - **Entrada permitida** – tipo de evento de um número de telefone do qual o Filtro de Chamadas e SMS permite para números da Lista Negra:
 - **SMS**: permitir apenas mensagens SMS de entrada.
 - **Chamadas**: permitir apenas chamadas de entrada.
 - **Chamadas e SMS**: permitir chamadas e mensagens SMS de entrada.
 - **Número de telefone permitido**: expressão-chave que indica que a mensagem de SMS é desejada. Este número deve conter apenas caracteres alfanuméricos; pode começar com um dígito, uma letra ou com o símbolo "+". Como número, também é possível utilizar as máscaras "*" ou "?" (em que "*" corresponde a qualquer quantidade de símbolos e "?" a qualquer símbolo único). Por exemplo, *1234? na Lista Branca. O Filtro de Chamadas e SMS entrega chamadas ou SMS de um número no qual quaisquer símbolos sigam a figura 1234.
 - **Texto permitido** : expressão-chave que indica que a mensagem de SMS recebida é desejada. Para números na Lista Branca, o Filtro de Chamadas e SMS apenas entrega mensagens SMS que contenham a expressão-chave e bloqueiam todas as outras.

Definição acessível para eventos de **SMS** .

Se desejar que todas as SMS de entrada de um número específico da Lista Branca sejam bloqueadas, deixe o campo **Texto permitido** desta entrada em branco.

5. Prima **Guardar**:

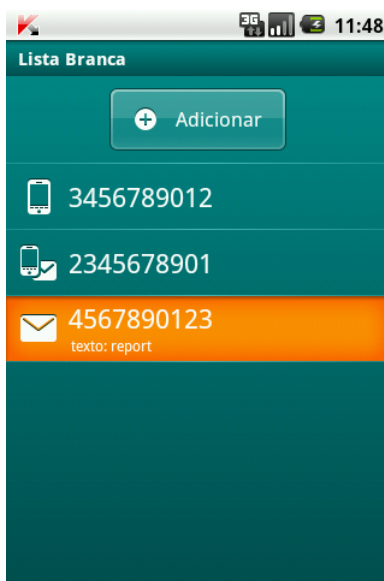


Figura 12. Adicionar uma nova entrada à Lista Branca

EDITAR ENTRADAS NA LISTA BRANCA

Relativamente a um registo da Lista Branca de números permitidos, 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 do **Filtro de Chamadas e SMS**.
2. Seleccionar **Lista Branca**.

Este procedimento irá abrir a janela **Lista Branca**.

3. Selecciona uma entrada na lista que deva ser eliminada e selecciona **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 a recepção de informações. Este número deve conter apenas caracteres alfanuméricos; pode começar com um dígito, uma letra ou com o símbolo "+". Como número, também é possível utilizar as máscaras "*" ou "?" (em que "*" corresponde a qualquer quantidade de símbolos e "?" a qualquer símbolo único). Por exemplo, *1234? na Lista Branca. O Filtro de Chamadas e SMS entrega chamadas ou SMS de um número no qual quaisquer símbolos sigam a figura 1234.
- **Texto permitido** : expressão-chave que indica que a mensagem de SMS recebida é desejada. Para números na Lista Branca, o Filtro de Chamadas e SMS apenas entrega mensagens SMS que contenham a expressão-chave e bloqueiam todas as outras.

Definição acessível para eventos de **SMS** .

Se desejar que todas as SMS de entrada de um número específico da Lista Branca sejam bloqueadas, deixe o campo **Texto permitido** desta entrada em branco.

5. Prima **Guardar**:

APAGAR REGISTOS DA LISTA BRANCA

Pode apagar uma entrada da Lista Branca, assim como limpá-la por completo.

➤ *Para apagar uma entrada na Lista Branca do Filtro de Chamadas e SMS:*

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

Este procedimento irá abrir a janela **Lista Branca**.

3. Seleccione uma entrada na lista que deva ser eliminada e seleccione **Apagar** 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 do **Filtro de Chamadas e SMS**.
2. Seleccione **Lista Branca**.

Este procedimento irá abrir a janela **Lista Branca**.

3. Seleccione **Apagar todos** no menu de contexto.

A janela de confirmação abre.

4. Confirme a desinstalação da aplicação premindo o botão **Sim**.

A Lista Branca é esvaziada.

RESPONDER A MENSAGENS SMS E CHAMADAS DE CONTACTOS NÃO INCLUÍDOS NA LISTA DE NÚMEROS

Se estiverem seleccionados os modos **Ambas listas** ou **Lista Branca** do Filtro de Chamadas e SMS, pode também definir uma resposta do Filtro de Chamadas e SMS para as mensagens e chamadas de subscritores cujos números não estejam nos Contactos. Adicionalmente, o Filtro de Chamadas e SMS permite a expansão da Lista Branca através da adição de números da lista de contactos à mesma.

➤ *Para seleccionar a resposta do Filtro de Chamadas e SMS a um número não incluído na lista de números:*

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

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

3. Seleccione o valor para a definição **Permitir Contactos** (consulte a Figura abaixo):

- para que o Anti-Spam conte números dos Contactos como Lista Branca adicional e bloqueie mensagens SMS e chamadas de subscritores que não estejam nos Contactos, seleccione a caixa **Permitir Contactos**;

- de modo a que o Filtro de Chamadas e SMS filtre mensagens SMS e chamadas com base no modo do Filtro de Chamadas e SMS definido, seleccione a caixa de verificação **Permitir Contactos**.

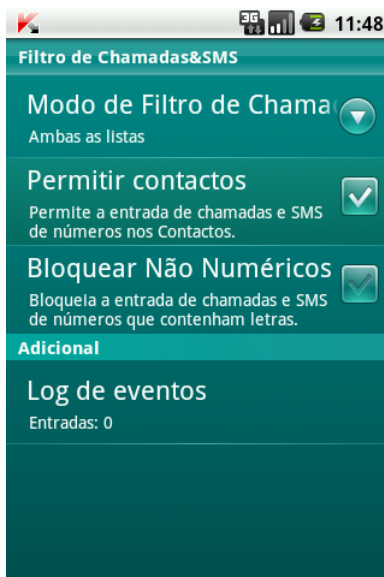


Figura 13. Reacção do Filtro de Chamadas e SMS perante números não presentes nos Contactos

RESPONDER A MENSAGENS SMS DE NÚMEROS NÃO NUMÉRICOS

Para o modo **Ambas listas** ou **Lista Branca** do Filtro de Chamadas e SMS, pode também expandir a Lista Negra incluindo nela números não numéricos (que contenham letras). Neste evento, o Filtro de Chamadas e SMS processa SMS e números não numéricos tais como números da Lista Negra.

➤ *Para configurar a resposta do Filtro de Chamadas e SMS ao receber mensagens de números não numéricos:*

- Na janela principal do Kaspersky Mobile Security 9, abra o Módulo do **Filtro de Chamadas e SMS**.
- Seleccionar **Modo: <modo do componente actual>**.

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

- Seleccione o valor para a definição **Bloquear números não numéricos** (consulte a Figura abaixo):
 - para que o Filtro de Chamadas e SMS bloqueie números não numéricos, seleccione a caixa de verificação **Bloquear números não numéricos**;
 - para que o Filtro de Chamadas e SMS filtre SMS de números não numéricos com base no modo do Filtro de Chamadas e SMS definido, retire a selecção da caixa de verificação **Bloquear números não numéricos**.

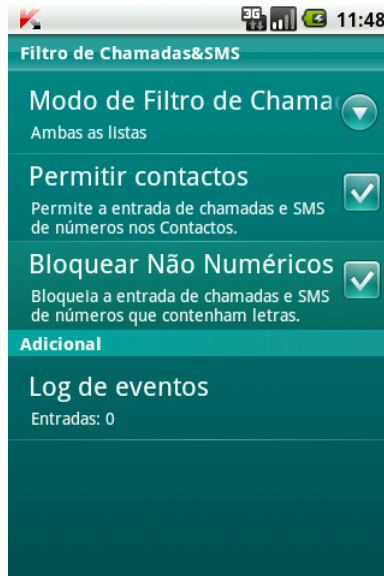


Figura 14. Seleccione uma acção para o Filtro de Chamadas e SMS desempenhar ao receber uma SMS de um número não numérico.

SELECIONAR UMA RESPOSTA PARA SMS DE ENTRADA

O Filtro de Chamadas e SMS verifica a entrada de SMS relativamente às listas Negra e Branca no modo **Ambas listas**.

Após receber uma mensagem SMS de um número que não esteja incluído em nenhuma lista, o Filtro de Chamadas e SMS irá pedir-lhe para introduzir o número numa das listas (consulte a Figura abaixo).

Pode seleccionar uma das seguintes acções a executar relativamente à SMS:

- Para bloquear uma SMS e adicionar um número de telefone à Lista Negra, clique **Bloquear**.
- Para entregar SMS e adicionar o número de telefone do remetente à Lista Branca, clique **Permitir**.
- Para entregar a mensagem SMS sem adicionar o número de telefone a nenhuma das listas, prima **Ignorar**.

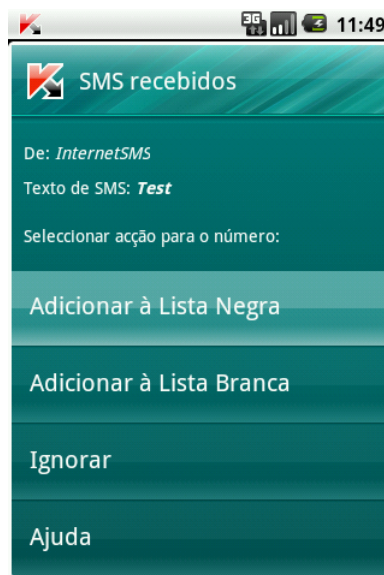


Figura 15. Notificação do Filtro de Chamadas e SMS sobre uma SMS aceite

As informações em SMS e chamadas bloqueadas são registadas no Log do Filtro de Chamadas e SMS (consulte a secção "Ver entradas no log" na página [55](#)).

SELECIONAR UMA RESPOSTA PARA CHAMADAS DE ENTRADA

O Filtro de Chamadas e SMS verifica a entrada de SMS relativamente às listas Negra e Branca no modo **Ambas listas**. Após receber uma chamada de um número que não se encontra em nenhuma das listas, o Filtro de Chamadas e SMS irá pedir-lhe que introduza o número em uma das listas (consulte a Figura abaixo).

Pode seleccionar uma das seguintes acções para o número de origem da chamada:

- Para adicionar o número de telefone do chamador à Lista Negra, clique em **Bloquear**.
- Para adicionar o número de telefone do chamador à Lista Branca, clique em **Permitir**.
- Se não desejar adicionar o número do chamador a nenhuma das listas, prima em **Ignorar**.

As informações em SMS e chamadas bloqueadas são registadas no Log do Filtro de Chamadas e SMS (consulte a secção "Ver entradas no log" na página [55](#)).

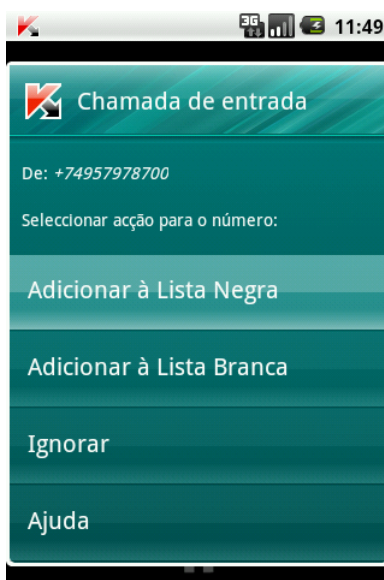


Figura 16. Notificação do Filtro de Chamadas e SMS sobre uma chamada aceite recebida

VER REGISTOS DO LOG

Pode ver informações sobre chamadas e SMS bloqueados no log do Filtro de Chamadas e SMS. As entradas no log são ordenadas pela ordem cronológica inversa.

As seguintes informações são fornecidas para cada entrada:

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

➤ *Para ver informações sobre as chamadas e SMS bloqueados, proceda do modo seguinte:*

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

2. Seleccione **Modo: <modo do componente actual>**.

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

3. Clique no **Log de evento** do módulo **Adicional**.

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

➤ *Para ver informações detalhadas sobre o evento bloqueado,*

selecione a entrada relevante no log

PROTECÇÃO DE DADOS EM CASO DE PERDA OU ROUBO DO DISPOSITIVO

Esta secção fornece informações sobre o Anti-Roubo, que no caso de roubo ou perda bloqueia o acesso não autorizado aos dados guardados no seu dispositivo móvel e tornam mais fácil encontrar o dispositivo.

Esta secção também especifica como activar/desactivar a função Anti-Roubo, definir os parâmetros de funcionamento e como iniciar o Anti-Roubo de modo remoto a partir de outro dispositivo.

NESTA SECÇÃO

Sobre o Anti-Roubo.....	57
Bloquear dispositivo	58
Apagar dados pessoais.....	59
Criar uma lista de pastas a eliminar.....	61
Monitorizar a substituição de um cartão SIM no dispositivo.....	62
Determinar as coordenadas geográficas do dispositivo	63
Iniciar as funções Anti-Roubo remotamente	65

SOBRE O ANTI-ROUBO

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

O Anti-Roubo inclui as seguintes funções:

- **Bloquear** – permite o bloqueio do dispositivo remotamente e apresenta o texto a ser mostrado no ecrã do dispositivo bloqueado.
- **Limpeza de Dados** – a função de Limpeza de Dados permite que apague os seguintes dados pessoais do dispositivo remotamente: Contactos e entradas do cartão SIM, SMS, log de chamadas, calendário, definições de ligação à Internet, contas de utilizador (excepto contas Google), assim como ficheiros da lista de pastas a serem apagadas.

O Kaspersky Mobile Security 9 apenas apaga contactos no cartão SIM em dispositivos com a versão 2,0 ou acima do sistema operativo Android.

- **Prot. Cartão SIM** permite obter o número de telefone actual caso o cartão SIM seja substituído, bloqueando também o dispositivo caso o cartão SIM seja substituído ou o dispositivo activado sem um cartão SIM. Informações sobre um novo número de telefone são enviadas como mensagem para um número de telefone e / ou e-mail que tiver especificado.
- A funcionalidade de **Localização por GPS** permite que localize o dispositivo. As coordenadas geográficas do dispositivo são enviadas como mensagem para o número de telefone a partir do qual um comando de SMS especial foi enviado, e para um endereço de e-mail.

Uma vez instalado o Kaspersky Mobile Security 9, todas as funções de Anti-Roubo ficam desactivadas.

O Kaspersky Mobile Security 9 pode iniciar remotamente o Anti-Roubo ao enviar comandos SMS de outro dispositivo móvel (consulte "Início remoto das funções Anti-Roubo" na página [65](#)).

Para iniciar remotamente as funções Anti-Roubo, deve conhecer o código secreto da aplicação definido no primeiro arranque do Kaspersky Mobile Security 9 do dispositivo, para o qual o comando SMS é enviado.

O estado actual de cada função é apresentado no ecrã **Anti-Roubo**, junto do nome da função.

BLOQUEAR DISPOSITIVO

Depois de ser recebido um comando de SMS especial, a função de Bloqueio permite-lhe bloquear, remotamente, o acesso ao dispositivo e aos dados armazenados no mesmo. O dispositivo só pode ser desbloqueado inserindo o código secreto.

Esta função não bloqueia o dispositivo, apenas activa a opção de bloqueio remoto.

➔ *Para activar a função Bloquear:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Anti-Roubo**.
2. Clique **Bloquear: <estado da função actual>**.
Este procedimento irá abrir a janela **Bloquear**.
3. Seleccione a caixa **Activar Bloqueio**.
4. Introduza a mensagem que é apresentada no ecrã do dispositivo em modo bloqueado no campo **Testar quando bloqueado**. Por defeito, é utilizado para a mensagem o texto padrão em que é possível adicionar o telefone do proprietário.

Se a função de Bloqueio for activada em outro dispositivo, pode bloqueá-lo utilizando qualquer um dos métodos seguintes:

- Use uma aplicação móvel da Kaspersky Lab como, por exemplo, o Kaspersky Mobile Security 9 noutro dispositivo móvel para criar e enviar um comando de SMS para o seu dispositivo. Para criar um comando SMS especial, utilize a função **Enviar um comando**. Como resultado o seu dispositivo irá receber uma mensagem SMS secreta e o dispositivo será bloqueado.
- Em outro dispositivo móvel, crie e envie uma mensagem SMS com o texto especial e o código secreto definido previamente para o dispositivo receptor. Como resultado o seu dispositivo irá receber uma mensagem SMS secreta e o dispositivo será bloqueado.

As mensagens SMS enviadas serão cobradas às taxas definidas pelo prestador de serviços móveis do outro dispositivo móvel.

Para bloquear o dispositivo remotamente é aconselhável utilizar o método seguro com a função de **Enviar um comando**. O código secreto da aplicação é então enviado de modo encriptado.

➔ *Para enviar um comando de SMS a outro dispositivo utilizando a função de Envio de um comando:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Adicional**.
Este procedimento irá abrir a janela **Adicional**.
2. Seleccione **Enviar comando SMS**.

3. Para a definição de **Comando SMS**, seleccione **Bloquear**.
4. No campo **Número de telefone a receber o comando SMS**, introduza o número de telefone do dispositivo que irá receber o comando SMS.
5. No campo **Código secreto do dispositivo a receber o comando SMS**, introduza o código secreto da aplicação expresso no dispositivo a receber o comando SMS.
6. Prima **Enviar**.

➤ *Para criar uma mensagem SMS com as funções de criação padrão de SMS do telefone,*

envie uma mensagem SMS padrão a outro dispositivo; deve conter o texto `bloquear:<código>`, onde `<código>` seja o código secreto da aplicação definido em outro dispositivo. A mensagem não é sensível a maiúsculas e minúsculas e os espaços antes ou depois dos dois pontos são ignorados.

APAGAR DADOS PESSOAIS

Após o comando especial SMS ter sido recebido, a função de Limpeza de Dados permite eliminar as informações seguintes armazenadas no dispositivo.

- detalhes pessoais do utilizador (entradas nos Contactos e no cartão SIM, SMS, log de chamadas, calendário, definições de ligação à Internet, registos de início de sessão com a excepção do registo de início de sessão no Google);
- ficheiros da lista de objectos a serem eliminados (consulte a secção "Criar uma lista de pastas a serem apagadas" na página [61](#)).

Esta função não apaga os dados guardados no dispositivo mas inclui a opção de apagá-los.

➤ *Para activar a função Limpeza de Dados:*

1. Na janela principal do Kaspersky Mobile Security 9, abra a pasta **Anti-Roubo**.
2. Clique **Limpeza de Dados: <estado da função actual>**.

Este procedimento irá abrir o ecrã **Limpeza de Dados**.

3. Seleccione a caixa **Activar Limpeza de Dados**.
4. Seleccione as informações que deseja eliminar. Para fazer isto, seleccione as caixas junto das definições desejadas no bloco **Informações a serem apagadas** (consulte a Figura abaixo):
 - para apagar dados pessoais, seleccione a caixa **Dados pessoais**;
 - para eliminar ficheiros da lista de pasta para eliminação, seleccione a caixa de verificação **Pastas** e desloque-se até à criação de lista para eliminação (consulte a secção "Criação de lista de pastas a serem eliminadas" na página [61](#)).

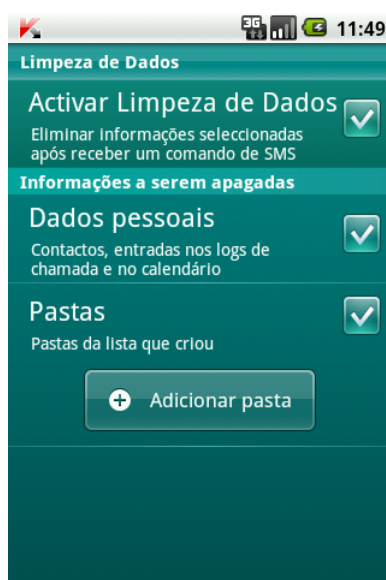


Figura 17. Definições da função de Limpeza de Dados

Pode apagar dados pessoais do dispositivo com a função activada utilizando os seguintes métodos:

- Use uma aplicação móvel da Kaspersky Lab como, por exemplo, o Kaspersky Mobile Security 9 noutro dispositivo móvel para criar e enviar um comando de SMS para o seu dispositivo. Como resultado o seu dispositivo recebe uma mensagem SMS secreta após a qual a informação é eliminada. Para criar um comando SMS especial, utilize a função Enviar um comando.
- Em outro dispositivo móvel, crie e envie uma mensagem SMS com o texto especial e o código secreto definido previamente para o dispositivo receptor. Como resultado o seu dispositivo recebe uma mensagem SMS secreta após a qual a informação é eliminada.

As mensagens SMS enviadas serão cobradas às taxas definidas pelo prestador de serviços móveis do outro dispositivo móvel.

Para eliminar informações remotamente do dispositivo, é aconselhável que utilize o método seguro com a função do comando Enviar. O código secreto da aplicação é então enviado de modo encriptado.

➔ Para enviar um comando de SMS a outro dispositivo utilizando a função de Envio de um comando:

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Adicional**.
Este procedimento irá abrir a janela **Adicional**.
2. Seleccione **Enviar comando**.
3. Para a definição do **Comando SMS**, seleccione **Limpeza de Dados**.
4. No campo **Número de telefone a receber o comando SMS**, introduza o número de telefone do dispositivo que irá receber o comando SMS.
5. No campo **Código secreto do dispositivo a receber o comando SMS**, introduza o código secreto da aplicação expresso no dispositivo a receber o comando SMS.
6. Prima **Enviar**.

- Para criar uma mensagem SMS com as funções de criação padrão de SMS do telefone:

enviar uma SMS padrão a outro dispositivo; ela deve conter o texto `eliminar:<código>` onde `<código>` seja o código secreto da aplicação definido em outro dispositivo. A mensagem não é sensível a maiúsculas e minúsculas e os espaços antes ou depois dos dois pontos são ignorados.

CRIAR UMA LISTA DE PASTAS A ELIMINAR.

A função de Eliminação de Dados permite a criação de uma lista de pastas a serem eliminadas após a recepção de um comando de SMS especial.

Para permitir que o Anti-Roubo elimine todas as pastas da lista após a recepção de uma SMS especial, certifique-se de que a caixa **Pastas** está assinalada nas definições de Limpeza de Dados.

- Para adicionar uma pasta à lista de pastas a apagar:

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

Este procedimento irá abrir o ecrã **Limpeza de Dados**.

3. Clique **Adicionar** (consulte a Figura abaixo).

A janela de **Seleção de pasta** abre.

4. Seleccione a pasta requerida clicando no ícone à direita do nome da pasta.

A pasta é adicionada à lista de pastas a serem eliminadas localizada abaixo das definições de **Pasta**

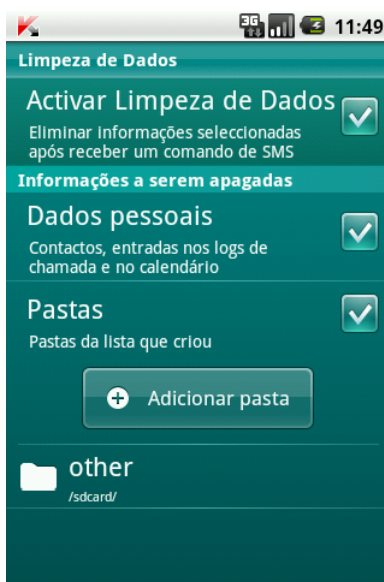


Figura 18. Adicionar uma pasta

- Para remover uma pasta da lista:

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

Este procedimento irá abrir o ecrã **Limpeza de Dados**.

3. Desloque-se até à lista de objectos para eliminação.
4. Seleccione uma pasta da lista e clique em **Apagar pasta** no menu de contexto.

A pasta é apagada da lista de pastas para eliminação.

MONITORIZAR A SUBSTITUIÇÃO DE UM CARTÃO SIM NO DISPOSITIVO

Se o cartão SIM for substituído, a Prot. Cartão SIM permite que envie uma mensagem com o número novo para o seu número de telefone / e-mail, ou que bloqueie o dispositivo.

➤ *Para activar a função Prot. Cartão SIM e monitorizar a substituição do cartão SIM:*

1. Na janela principal do Kaspersky Mobile Security 9, o módulo **Anti-Roubo** abre.
2. Clicar **Prot. Cartão SIM: <estado do componente actual>**.

Este procedimento irá abrir a janela **Prot. Cartão SIM**.

3. Seleccione a caixa **Activar Prot. Cartão SIM**.
4. Para verificar a substituição do cartão SIM no dispositivo, estabeleça as seguintes configurações:
 - Para receber automaticamente SMS utilizando o número do seu telefone, introduza um número de telefone para o qual a SMS deva ser enviada no módulo **Enviar número novo** para a definição do **Número de telefone**.

Este número de telefone pode começar com um dígito ou com um “+” e tem de conter apenas dígitos.

 - Para receber um e-mail com o número de telefone novo, no módulo **Enviar número novo** introduza um endereço de e-mail para a definição de **Endereço de e-mail**.
 - Para bloquear o dispositivo se o cartão SIM for substituído, ou se o dispositivo for ligado com o cartão SIM removido, marque a caixa **Bloquear dispositivo** no bloco **Adicional**. Você pode desbloquear o dispositivo inserindo o código secreto da aplicação.
 - Para apresentar a mensagem no ecrã no estado bloqueado, introduza o texto da mensagem no módulo **Adicional** para a definição **Texto quando bloqueado**.

Por defeito, é utilizado para a mensagem o texto padrão em que é possível adicionar o número do proprietário.

A definição está disponível se a caixa de verificação **Bloqueio** estiver seleccionada.

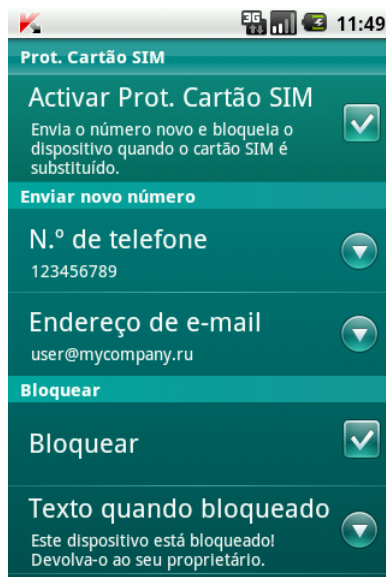


Figura 19. Definições da função de Prot. Cartão SIM

DETERMINAR AS COORDENADAS GEOGRÁFICAS DO DISPOSITIVO

Após a recepção de um comando de SMS especial, a Localização por GPS permite a detecção da localização do dispositivo, enviando as coordenadas geográficas por SMS e e-mail ao dispositivo que o pede e um endereço de e-mail.

As mensagens SMS enviadas são cobradas na taxa actual do seu operador de serviço móvel.

Se um receptor GPS estiver instalado no dispositivo, este irá activar automaticamente após o dispositivo receber um comando de SMS especial. Se a função de Localização por GPS não conseguir obter as coordenadas do dispositivo utilizando o GPS, ela determina as coordenadas aproximadas do dispositivo com base nas estações base.

➤ *Para activar a função Localização por GPS:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o Pasta **Anti-Roubo**.
2. Clicar **Localização por GPS: <estado do componente actual>**.

Este procedimento irá abrir a janela **Localização por GPS**.

3. Seleccione a caixa **Activar Localização por GPS**.

Ao receber um comando especial SMS, o Kaspersky Mobile Security 9 automaticamente envia as coordenadas do dispositivo numa SMS de resposta ao número a partir do qual o comando SMS foi enviado.

4. Para também receber as coordenadas do dispositivo por e-mail, introduza um endereço de e-mail no módulo **Enviar coordenadas do dispositivo** para as definições de **Endereço de E-mail** (consulte a Figura abaixo).



Figura 20. Definições da função de Localização por GPS

Pode pedir as coordenadas de um dispositivo em que a Localização por GPS esteja activada, utilizando os seguintes métodos:

- Use uma aplicação móvel da Kaspersky Lab como, por exemplo, o Kaspersky Mobile Security 9 noutro dispositivo móvel para criar e enviar um comando de SMS para o seu dispositivo. Como resultado o seu dispositivo irá receber uma mensagem SMS secreta, e a aplicação irá enviar as coordenadas do dispositivo. Para criar um comando SMS especial, utilize a função Enviar um comando.
- Em outro dispositivo móvel, crie e envie uma mensagem SMS com o texto especial e o código secreto definido previamente para o dispositivo receptor. Como resultado o seu dispositivo irá receber uma mensagem SMS secreta, e a aplicação irá enviar as coordenadas do dispositivo.

As mensagens SMS enviadas serão cobradas às taxas definidas pelo prestador de serviços móveis do outro dispositivo móvel.

Para receber a localização do dispositivo, é aconselhável que utilize o método seguro com a função do comando Enviar. O código secreto da aplicação é então enviado de modo encriptado.

➔ Para enviar um comando a outro dispositivo utilizando a função de Envio de um comando:

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo **Adicional**.
Este procedimento irá abrir a janela **Adicional**.
2. Clicar em **Enviar comando**.
3. Seleccionar o valor da **Localização por GPS** para a definição **Seleccionar comando SMS**.
4. No campo **Número de telefone a receber o comando SMS**, introduza o número de telefone do dispositivo que irá receber o comando SMS.
5. No campo **Código secreto do dispositivo a receber o comando SMS**, introduza o código secreto da aplicação expresso no dispositivo a receber o comando SMS.
6. Prima **Enviar**.

➔ *Para criar uma mensagem SMS com as funções de criação padrão de SMS do telefone:*

envie uma SMS a outro dispositivo; a mensagem deve conter o texto `ocultar:<código> onde <código>` seja o código secreto da aplicação definido em outro dispositivo. A mensagem não é sensível a maiúsculas e minúsculas e os espaços antes ou depois dos dois pontos são ignorados.

Será enviada uma mensagem SMS com as coordenadas do dispositivo para o número de telefone a partir do qual o comando de SMS foi enviado e para o endereço de e-mail se tiver especificado um nas opções da Localização por GPS.

INICIAR AS FUNÇÕES ANTI-ROUBO REMOTAMENTE

A aplicação permite o envio de um comando de SMS especial para executar as funções Anti-Roubo de modo remoto em outro dispositivo com o Kaspersky Mobile Security instalado. É enviado um comando de SMS como SMS encriptado e contém o código secreto da aplicação definido em outro dispositivo. A recepção do comando de SMS não será notada.

A SMS será cobrada à taxa actual do seu prestador de serviços móveis.

➔ *Para enviar um comando SMS para outro dispositivo:*

1. Na janela principal do Kaspersky Mobile Security 9, expanda o módulo **Adicional**.
2. Seleccione a função para a execução remota a partir de outro dispositivo móvel. Para fazer isto seleccione um dos valores propostos para a definição **Seleccionar comando SMS** (consulte a Figura abaixo):
 - **Bloqueio;**
 - **Limpeza de Dados;**
 - **Localiz. GPS.**
 - **Protecção de Privacidade.**
3. No campo **Número de telefone a receber o comando SMS**, introduza o número de telefone do dispositivo que irá receber o comando SMS.
4. No campo **Código secreto do dispositivo a receber o comando SMS**, introduza o código secreto da aplicação expresso no dispositivo a receber o comando SMS.
5. Prima **Enviar**.

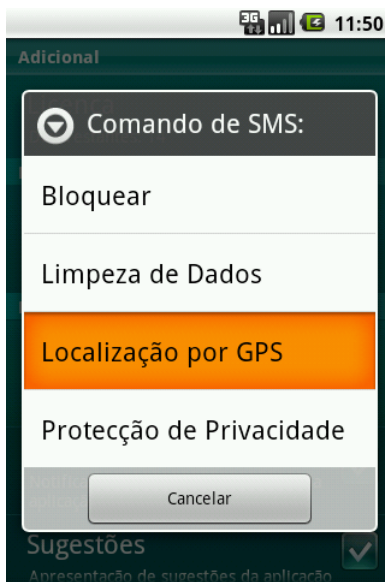


Figura 21. Início remoto das funções Anti-Roubo e de Protecção de Privacidade

PROTECÇÃO DE PRIVACIDADE

A secção apresenta informações sobre a Protecção de Privacidade, que pode ocultar as informações confidenciais do utilizador.

NESTA SECÇÃO

Protecção de Privacidade	67
Modos de Protecção de Privacidade.....	67
Activar/desactivar a Protecção de Privacidade	68
Activar automaticamente a Protecção de Privacidade	68
Activar remotamente a Protecção de Privacidade	69
Seleccionar dados a ocultar: Protecção de Privacidade	71
Criar uma lista de números privados.....	72

PROTECÇÃO DE PRIVACIDADE

A Protecção de Privacidade oculta dados privados com base na sua Lista de Contactos, que lista números privados. Para números confidenciais, a Protecção de Privacidade oculta entradas dos Contactos, rascunhos, SMS de entrada e saída, assim como entradas do histórico de chamadas. A Protecção de Privacidade suprime o novo sinal de SMS e oculta a própria mensagem na caixa de entrada. A Protecção de Privacidade bloqueia a entrada de chamadas de números privados e não apresenta as informações das chamadas de entrada no ecrã. Como resultado, o autor da chamada recebe um sinal de ocupado. Para ver chamadas de entrada e SMS do período de tempo no qual a Protecção de Privacidade foi activada, desactive a Protecção de Privacidade. Ao repetir a activação da Protecção de Privacidade, as informações não são apresentadas.

Pode activar a Protecção de Privacidade no Kaspersky Mobile Security 9 ou remotamente a partir de outro dispositivo móvel. No entanto, a Protecção de Privacidade apenas pode ser desactivada na aplicação.

MODOS DE PROTECÇÃO DE PRIVACIDADE

Pode gerir o modo de operação da Protecção de Privacidade. O modo define se a Protecção de Privacidade é activada ou desactivada.

Por defeito, a Protecção de Privacidade está desactivada.

Encontram-se disponíveis os modos seguintes de Protecção de Privacidade.

- **Modo de Protecção de Privacidade definido em Normal** – a ocultação de informações confidenciais está desactivada. As configurações de Protecção de Privacidade estão acessíveis para modificação.
- **Modo de Protecção de Privacidade definido em Privado** – a ocultação de informações confidenciais está activada. Não é possível alterar as configurações de Protecção de Privacidade.

Pode definir a Protecção de Privacidade para iniciar automaticamente (consulte a secção "Activar automaticamente a Protecção de Privacidade" na página [68](#)) ou iniciar remotamente a partir de outro dispositivo (consulte a secção "Activar remotamente a Protecção de Privacidade" na página [69](#)).

O modo actual de ocultação de informações confidenciais é apresentado na janela principal da aplicação no módulo de **Protecção de Privacidade**

ACTIVAR/DESACTIVAR A PROTECÇÃO DE PRIVACIDADE

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

1. Na janela principal do Kaspersky Mobile Security 9, abra o **Protecção de Privacidade**.
2. Clique em **Ocultar informações** (consulte a Figura abaixo).

O nome do item muda consoante o modo de Protecção de Privacidade. Se estiver definido o modo de **Protecção de Privacidade definido em Normal**, o item é chamado **Ocultar informações**. Se estiver definido o modo **Informações confidenciais são ocultadas**, o item é chamado **Apresentar informações**.

A alteração do modo de Protecção de Privacidade pode demorar algum tempo.

O modo actual de Protecção de Privacidade é apresentado no módulo de **Protecção de Privacidade**.

O ícone de interruptor à direita do item **Ocultar informações** / **Apresentar informações** é alterado consoante o modo seleccionado.



Figura 22. Alterar o modo de Protecção de Privacidade

ACTIVAR AUTOMATICAMENTE A PROTECÇÃO DE PRIVACIDADE

Pode configurar a activação automática da ocultação de informações após ter passado um intervalo temporal especificado. A função fica activa após o dispositivo mudar para o modo de poupança de energia.

Desactive a Protecção de Privacidade antes de editar as definições de Protecção de Privacidade.

➤ Para activar automaticamente a Protecção de Privacidade após ter passado um intervalo temporal especificado:

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

É apresentada a janela **Definições da Protecção de Privacidade**.

3. Seleccione um valor para a definição de **Ocultação automática** consoante as seguintes tarefas (consulte a Figura abaixo):

- Para desactivar a activação automática da ocultação de informações confidenciais, seleccione **Desactivado**.
- Para iniciar a ocultação de informações confidenciais num período temporal definido após o dispositivo mudar para o modo de poupança de energia, seleccione um dos seguintes valores:
 - **Sem espera.**
 - **Após 1 minuto.**
 - **Após 5 minutos.**
 - **Após 15 minutos.**
 - **Após 1 hora.**



Figura 23. Início automático da Protecção de Privacidade

ACTIVAR REMOTAMENTE A PROTECÇÃO DE PRIVACIDADE

O Kaspersky Mobile Security 9 permite que active a Protecção de Privacidade remotamente a partir de outro dispositivo móvel. Para conseguir isto primeiro active a opção de Ocultar após comando SMS no seu dispositivo.

➤ Para permitir o início remoto da Protecção de Privacidade:

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

É apresentada a janela **Definições da Protecção de Privacidade**.

3. Seleccione a caixa **Ocultar após comando SMS** (consulte a figura abaixo).

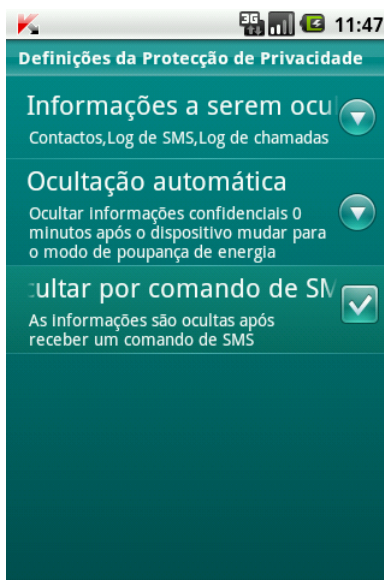


Figura 24. Definições de activação remota da Protecção de Privacidade

Pode activar a Protecção de Privacidade remotamente utilizando qualquer um dos métodos seguintes:

- Use uma aplicação móvel da Kaspersky Lab como, por exemplo, o Kaspersky Mobile Security 9 noutro dispositivo móvel para criar e enviar um comando de SMS para o seu dispositivo. Como resultado, o dispositivo imperceptivelmente recebe uma SMS e as informações confidenciais são ocultadas. Para criar um comando SMS especial, utilize a função Enviar um comando.
- Em outro dispositivo móvel, crie e envie uma mensagem SMS com um texto especial e o código secreto da aplicação especificada no seu dispositivo. Como resultado, o dispositivo recebe uma SMS e as informações confidenciais são ocultadas.

As SMS enviadas serão cobradas às taxas definidas pelo prestador de serviços móveis para o telefone do qual o comando SMS originar.

➔ Para começar a ocultação de informações confidenciais de outro dispositivo móvel com o comando especial de SMS.

1. Na janela principal do Kaspersky Mobile Security 9, abra o Módulo **Adicional**.
2. Este procedimento irá abrir a janela **Adicional**.
3. Seleccionar **Enviar comando**.
4. Para o **Comando SMS** defina o valor da **Protecção de Privacidade**.
5. No campo **Número de telefone a receber o comando SMS**, introduza o número de telefone do dispositivo que irá receber o comando SMS.
6. No campo **Código secreto do dispositivo a receber o comando SMS**, introduza o código secreto da aplicação expresso no dispositivo a receber o comando SMS.
7. Prima **Enviar**.

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

- *Para activar a Protecção de Privacidade remotamente utilizando as ferramentas padrão do telefone para criação de SMS:*

envie uma SMS a outro dispositivo; a mensagem deve conter o texto `ocultar:<código>`, onde `<código>` seja o código secreto da aplicação definido em outro dispositivo. A mensagem não é sensível a maiúsculas e minúsculas e os espaços antes ou depois dos dois pontos são ignorados.

SELECIONAR DADOS A OCULTAR: PROTECÇÃO DE PRIVACIDADE

A Protecção de Privacidade pode ocultar as seguintes informações para números na Lista de Contactos: contactos, correspondência por SMS, entradas no log de chamadas, chamadas e SMS de entrada. Pode seleccionar informações e eventos que a Protecção de Privacidade deve ocultar para números privados.

Desactive a Protecção de Privacidade antes de editar as definições de Protecção de Privacidade.

- *Para seleccionar informações e eventos que devem ser ocultos para números privados:*

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

A janela das **Definições da Protecção de Privacidade** abre (consulte a Figura abaixo).

3. Selecciona informações e eventos que são ocultos para números confidenciais. Para fazer isto, defina as **Informações a serem ocultas** e coloque a caixa de verificação junto das definições requeridas. Estão disponíveis as seguintes configurações:
 - **Contactos** – oculta todas as informações sobre números confidenciais nos Contactos.
 - **Logs de SMS** — ocultar mensagens SMS nas pastas **Entrada**, **Saída** e **Enviadas** para números confidenciais.
 - **SMS de entrada** – ocultar a entrada de SMS de números privados.
 - **Logs de chamadas** – aceitar chamadas de números confidenciais mas não apresentar o número do chamador e não apresentar informações sobre números confidenciais na lista de chamadas (entrada, saída, e perdidas).
 - **Chamadas de entrada** — bloqueia chamadas de números privados (neste caso, o autor da chamada irá ouvir o tom de ocupado). Informações relativas a uma chamada recebida serão apresentadas quando a Protecção de Privacidade for desactivada.

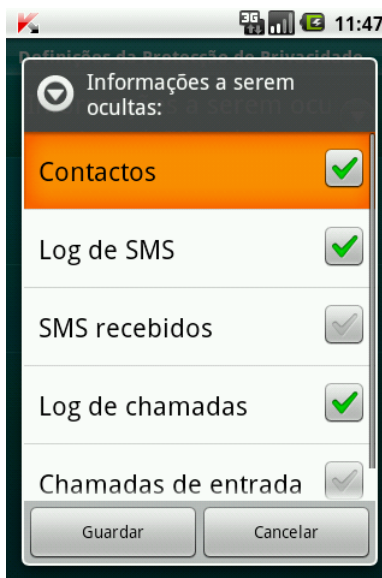


Figura 25. Seleccionar informações e eventos ocultos

CRIAR UMA LISTA DE NÚMEROS PRIVADOS.

A Lista de Contactos contém números privados relativamente aos quais a Protecção de Privacidade oculta informações e eventos. Pode prolongar a lista adicionando um número manualmente ou importando um dos Contactos no cartão SIM.

Antes de criar a Lista de Contactos, desactive a ocultação de informações confidenciais.

NESTA SECÇÃO

Adicionar um número à lista de números privados	72
Editar um número na lista de números privados	73
Apagar um número da lista de números privados	73

ADICIONAR UM NÚMERO À LISTA DE NÚMEROS PRIVADOS

Pode adicionar números de telefone à lista de Contactos manualmente ou importá-los dos Contactos.

Antes de criar a Lista de Contactos, desactive a ocultação de informações confidenciais.

➤ Para adicionar um número de telefone na Lista de Contactos:

1. Na janela principal do Kaspersky Mobile Security 9, abra o **Protecção de Privacidade**.
2. Clique na **Lista de Contactos**.
Será apresentada a janela **Lista de contactos**.
3. Efectue uma das seguintes acções (consulte a Figura abaixo):

- Para adicionar um número dos Contactos, seleccione **Adicionar** → **Contactos**. Seleccione a entrada requerida da Lista de Contactos na janela que abre.
- Para adicionar um número, seleccione **Adicionar** → **Número**, preencha o campo **Número de telefone** e prima **Guardar**.

O número irá ser adicionado à lista de Contactos



Figura 26. Adicionar registos à lista de contactos protegidos

EDITAR UM NÚMERO NA LISTA DE NÚMEROS PRIVADOS

Desactive a Protecção de Privacidade antes de editar as definições de Protecção de Privacidade.

Os números de telefone introduzidos manualmente apenas estão disponíveis para editar na Lista de Contactos. Não é possível editar números que tenham sido seleccionados dos Contactos.

➤ *Para editar um número de telefone na Lista de Contactos*

1. Na janela principal do Kaspersky Mobile Security 9, abra o módulo da **Protecção de Privacidade**.
2. Clique na **Lista de Contactos**.
Será apresentada a janela **Lista de contactos**.
3. Seleccione um número da Lista de Contactos para editar e seleccione **Editar** no menu de contexto.
A janela **Editar uma entrada** é apresentada.
4. Altere os dados.
5. Uma vez concluída a edição, prima **Guardar**.

O número é alterado.

APAGAR UM NÚMERO DA LISTA DE NÚMEROS PRIVADOS

Pode eliminar um número ou limpar na totalidade a Lista de Contactos.

Desative a Protecção de Privacidade antes de editar as definições de Protecção de Privacidade.

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

1. Na janela principal do Kaspersky Mobile Security 9, O módulo da **Protecção de Privacidade** é expandido.
2. Clique na **Lista de Contactos**.
Será apresentada a janela **Lista de contactos**.
3. Seleccione o número a ser apagado e seleccione **Apagar** no menu de contexto.

➤ *Para limpar a Lista de Contactos:*

1. Na janela principal do Kaspersky Mobile Security 9, abra o Módulo de **Protecção de Privacidade**.
2. Clique na **Lista de Contactos**.
Será apresentada a janela **Lista de contactos**.
3. Seleccione **Apagar todos** no menu de contexto.
A janela de confirmação abre.
4. Confirme a eliminação. Para tal, prima **Sim**.

A Lista de Contactos fica vazia.

ACTUALIZAR AS BASES DE DADOS DA APLICAÇÃO

Esta secção fornece informações sobre a actualização das bases de dados da aplicação, o que assegura a protecção actualizada do seu dispositivo. Adicionalmente esta secção descreve como ver informações nas bases de dados de antivírus instaladas, executar a actualização manualmente e configurar a actualização automática das bases de dados antivírus.

NESTA SECÇÃO

Sobre a actualização das bases de dados da aplicação.....	75
Iniciar actualizações manualmente	76
Iniciar actualizações agendadas	76

SOBRE A ACTUALIZAÇÃO DAS BASES DE DADOS DA APLICAÇÃO

A aplicação verifica o dispositivo a fim de detectar a presença de programas de software maligno que utilizem a base de dados da aplicação, que contém descrições de todos os programas de software maligno actualmente conhecidos e outros programas indesejados, bem como métodos para o tratamento dos mesmos. É extremamente importante manter as suas bases de dados antivírus actualizadas.

Recomenda-se que actualize regularmente as bases de dados da aplicação. Se tiverem passado mais de 15 dias desde a última actualização as bases de dados serão consideradas desactualizadas. A protecção será então menos fiável.

O Kaspersky Mobile Security 9 desempenha actualizações da base de dados da aplicação a partir dos servidores de actualização Kaspersky Lab. Tratam-se de sites da Internet especiais que contém actualizações para bases de dados de todos os produtos da Kaspersky Lab.

Para actualizar as bases de dados antivírus da aplicação, é necessário ter uma ligação à Internet configurada no dispositivo móvel.

As bases de dados antivírus da aplicação são actualizadas de acordo com o seguinte algoritmo:

1. As bases de dados da aplicação instaladas no seu dispositivo móvel são comparadas com as localizadas no servidor de actualizações especial da Kaspersky Lab.
2. O Kaspersky Mobile Security 9 efectua uma das seguintes acções:
 - Se tiver as bases de dados antivírus mais recentes da aplicação instaladas, é apresentada uma mensagem informativa no ecrã.
 - Se as bases de dados antivírus instaladas forem diferentes, é transferido e instalado um novo pacote de actualização.

Uma vez concluído o processo de actualização, a ligação é automaticamente fechada. Se a ligação tiver sido estabelecida antes do início da actualização, permanecerá aberta para utilização adicional.

Pode iniciar a tarefa de actualização manualmente, em qualquer altura em que o dispositivo não esteja ocupado com outras tarefas, ou agendar actualizações automáticas.

Em roaming, é possível desactivar a actualização das bases de dados antivírus do Kaspersky Mobile Security 9 para evitar custos desnecessários.

Informações detalhadas sobre as bases de dados antivírus utilizadas estão acessíveis no módulo **Antivírus** → **Adicional** em **Iniciar actualização**.

INICIAR ACTUALIZAÇÕES MANUALMENTE

Pode iniciar a actualização das bases de dados antivírus da aplicação manualmente.

➤ *Para iniciar o processo de actualização das bases de dados antivírus manualmente:*

1. Na janela principal do Kaspersky Mobile Security 9, abra a pasta do módulo **Antivírus**.
2. Clique **Adicional**.
A janela **Antivírus: Adicional** abre.
3. Clique **Iniciar actualização**.

A aplicação inicia o processo de actualização das bases de dados a partir do servidor da Kaspersky Lab. No ecrã, são apresentadas informações sobre o processo de actualização.

INICIAR ACTUALIZAÇÕES AGENDADAS

As actualizações regulares são um pré-requisito para a protecção eficaz do dispositivo contra infecção por objecto de software maligno. Para sua conveniência, pode configurar as actualizações automáticas da base de dados e criar uma agenda de actualizações.

Para executar uma actualização, o dispositivo deve permanecer ligado pela totalidade do período da verificação.

Adicionalmente, pode definir a actualização automática quando estiver a fazer roaming.

➤ *Para configurar um início da actualização agendada:*

1. Na janela principal do Kaspersky Mobile Security 9, expanda o módulo **Antivírus**.
2. Clique **Adicional**.
A janela **Antivírus: Adicional** abre.
3. Seleccione **Configuração das Actualizações**.
A janela **Configuração das Actualizações** abre.
4. Defina um dos seguintes valores para as definições da **Actualização agendada**:
 - **Semana**: actualizar as bases de dados da aplicação uma vez por semana. Seleccione os valores para o **Dia de início** e **Hora de início**.
 - **Diariamente**: actualizar as bases de dados da aplicação todos os dias. Introduzir o valor para a **Hora de actualização**.
 - **Desactivado** – não actualizar as bases de dados conforme a agenda.

CONFIGURAR DEFINIÇÕES ADICIONAIS

A secção fornece informações sobre as opções adicionais do Kaspersky Mobile Security 9: como activar / desactivar as mensagens emergentes na linha de estado da operação da aplicação, notificações áudio, apresentação de comandos antes de ajustar as definições de cada componente, como definir o widget do ecrã inicial e como alterar o código secreto da aplicação.

NESTA SECÇÃO

Alterar o código secreto	77
Apresentar sugestões	77
Configurar notificações com som	78
Mensagens na linha de estado	78

ALTERAR O CÓDIGO SECRETO

Pode alterar o código secreto definido após o primeiro arranque da aplicação.

➤ *Para alterar o código secreto:*

1. Na janela principal do Kaspersky Mobile Security 9, expanda o Módulo **Adicional**.
Este procedimento irá abrir a janela **Adicional**.
2. Seleccionar **Alterar código secreto**.
3. Introduza o código secreto actual da aplicação no campo de entrada **Introduzir código secreto** e prima **Seguinte**.
4. Introduza o novo código secreto da aplicação no campo **Definir novo código secreto** e prima **Seguinte**.

O código introduzido é verificado automaticamente.

Se o código for considerado inválido de acordo com os resultados da verificação, é apresentada uma mensagem de aviso e a aplicação pede a confirmação. Para utilizar o código, prima **Sim**. Para criar um novo código, prima **Não**. Introduza um novo código secreto da aplicação.

5. Introduza este código de novo no campo **Repetir introdução do novo código**.

O código secreto é alterado.

APRESENTAR SUGESTÕES

Ao estabelecer as configurações dos componentes, o Kaspersky Mobile Security 9 apresenta, por defeito, um pedido de informação com uma breve descrição da função seleccionada. Pode configurar a apresentação de sugestões do Kaspersky Mobile Security 9.

➤ *Para configurar a apresentação de sugestões desempenhe os passos seguintes:*

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

Este procedimento irá abrir a janela **Adicional**.

2. Desempenha acções dependendo das tarefas seguintes:
 - Para activar a apresentação de solicitações, seleccione a caixa de verificação **Sugestões**.
 - Para desactivar a apresentação de solicitações, retire a selecção da caixa de verificação **Sugestões**.

CONFIGURAR NOTIFICAÇÕES COM SOM

Como resultado da operação da aplicação, surgem eventos por exemplo quando um ficheiro infectado é detectado, quando o termo de validade da licença tiver expirado. Para que a aplicação o informe sobre cada evento similar, pode activar a notificação sonora do evento que ocorre.

Por defeito, o Kaspersky Mobile Security 9 inclui notificação com som apenas de acordo com o modo configurado para o dispositivo.

➤ *Para gerir a notificação com som da aplicação, efectue os seguintes passos:*

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

Este procedimento irá abrir a janela **Adicional**.

2. Desempenha acções dependendo das tarefas seguintes:
 - Para activar a notificação áudio, marque a caixa de verificação **Som**.
 - Para desactivar a notificação áudio, marque a caixa de verificação **Som**.

MENSAGENS NA LINHA DE ESTADO

O Kaspersky Mobile Security 9 permite receber notificações emergentes na linha de estado sobre eventos da aplicação, por exemplo, ao iniciar a aplicação, ao expirar a validade da licença ou ao desactivar a protecção. Pode activar / desactivar a recepção de notificações sobre eventos da aplicação na linha de estado.

➤ *Para gerir notificações emergentes relativamente à operação da aplicação, proceda do modo seguinte:*

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

Este procedimento irá abrir a janela **Adicional**.

2. Desempenha acções dependendo das tarefas seguintes:
 - Para activar notificações emergentes na operação da aplicação, marque a caixa de verificação **Notificações**.
 - Para desactivar notificações emergentes, retire a selecção da caixa de verificação **Notificações**.

Ao utilizar o Kaspersky Mobile Security 9, o widget do ecrã inicial fica acessível (consulte a página [34](#)). Pretende-se que o widget do ecrã inicial indique o estado de protecção do seu dispositivo, a ocultação de informações confidenciais e a licença da aplicação.

Após instalar a aplicação, o widget automaticamente surge na janela principal do dispositivo. Pode adicionar um widget à janela principal ou eliminá-lo, assim como definir a indicação de ocultação de informações confidenciais no widget do ecrã Inicial (consulte a secção "Ocultar informações confidenciais" na página [67](#)).

➤ *Para gerir a apresentação do widget na janela principal, proceda do modo seguinte:*

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

Este procedimento irá abrir a janela **Adicional**.

2. Seleccionar **Widget**.

A janela do **Widget do ecrã inicial** abre.

3. Desempenha acções dependendo das tarefas seguintes:

- Para apresentar uma alteração no modo de ocultação de informações confidenciais no widget do ecrã Inicial, seleccione a caixa de verificação **Activar widget**.
- Para eliminar o widget do widget do ecrã Inicial, retire a selecção da caixa de verificação **Activar widget**.

➔ *Para definir o estado das informações confidenciais no widget do Ecrã inicial, proceda do modo seguinte:*

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

Este procedimento irá abrir a janela **Adicional**.

2. Seleccionar **Widget**.

A janela do **Widget do ecrã inicial** abre.

3. Desempenha acções dependendo das tarefas seguintes:

- Para apresentar uma alteração no modo de ocultação de informações confidenciais no widget do ecrã Inicial, seleccione a caixa de verificação **Apresentar estado da Protecção de Privacidade**.
- Para ocultar uma alteração no modo de ocultação de informações confidenciais no widget do ecrã Inicial, seleccione a caixa de verificação **Apresentar estado da Protecção de Privacidade**.

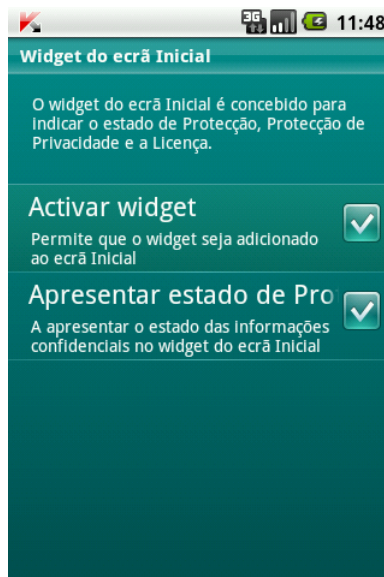


Figura 27. Definições do widget do ecrã inicial

CONTACTAR O SERVIÇO DE ASSISTÊNCIA TÉCNICA

Se já tiver adquirido o Kaspersky Internet Security, pode obter informações sobre o programa a partir do Serviço de Apoio Técnico, através do telefone ou da Internet.

Os especialistas do Serviço de Apoio Técnico responderão a todas as suas dúvidas sobre a instalação e a utilização da aplicação. Da mesma forma, irão ajudá-lo a eliminar as consequências das actividades de software maligno, caso o seu dispositivo tenha sido infectado.

Antes de contactar o Serviço de Apoio Técnico, leia as regras de Apoio para produtos da Kaspersky Lab (<http://support.kaspersky.com/support/rules>).

Enviar a sua dúvida por correio electrónico para o Serviço de Apoio Técnico

Pode encaminhar a sua dúvida para os especialistas do Serviço de Apoio Técnico preenchendo um formulário Web da Assistência Técnica, no endereço (<http://support.kaspersky.com/helpdesk.html?LANG=pt>).

Pode escrever a sua dúvida em russo, inglês, alemão, francês ou espanhol.

Para enviar uma mensagem de correio electrónico com a sua dúvida, é necessário incluir o **ID de Cliente** e a **palavra-passe** que recebeu quando efectuou o seu registo no Web site do Serviço de Apoio Técnico.

Se não for um utilizador registado de aplicações da Kaspersky Lab, pode preencher um formulário de registo (<https://support.kaspersky.com/en/personalcabinet/Registration/Form/?LANG=pt>). Durante o registo, introduza o *código de activação* da aplicação ou o *nome do ficheiro de chave*.

O Serviço de Apoio Técnico irá responder ao seu pedido no seu Armário Pessoal (<https://support.kaspersky.com/en/personalcabinet?LANG=pt>) e para o endereço de correio electrónico que tiver especificado na sua dúvida.

Na dúvida, descreva o problema ocorrido. Especifique as seguintes informações nos campos obrigatórios:

- **O tipo de pedido de ajuda.** Seleccione um tópico que melhor corresponda ao problema ocorrido, por exemplo, "Problema de Instalação/Remoção do Produto" ou "Problema de verificação/remoção de vírus pelo Antivírus". Se não encontrar um tópico apropriado, seleccione a opção "Questão geral".
- **O nome da aplicação e o número da respectiva versão.**
- **Texto do pedido.** Descreva o problema ocorrido, fornecendo tantos detalhes relevantes quando possível.
- **A sua ID de cliente e a respectiva palavra-passe.** Introduza o ID de cliente e a palavra-passe que recebeu quando efectuou o seu registo no Web site do Serviço de Apoio Técnico.
- **Endereço de e-mail.** O Serviço de Assistência Técnica irá enviar a resposta à sua questão para este endereço de correio electrónico.

Suporte Técnico por telefone

Se possuir um problema urgente, pode contactar o nosso Serviço de Suporte Técnico. Antes de contactar o Serviço de Apoio Técnico da sua área (http://support.kaspersky.com/support/support_local) ou internacional (<http://support.kaspersky.com/support/international>), recolha as informações (<http://support.kaspersky.com/support/details>) necessárias sobre o seu dispositivo e a aplicação antivírus instalada. Isto permitirá que os nossos especialistas o possam ajudar de forma mais rápida.

GLOSSÁRIO

A

ACTIVAR A APLICAÇÃO

Mudar a aplicação para o modo de funcionamento total. O utilizador precisa de uma licença para activar a aplicação.

ARQUIVO

Ficheiro que "contém" um ou vários outros objectos que também podem ser arquivos.

B

BASES DE DADOS ANTIVÍRUS

Bases de dados criadas pelos especialistas da Kaspersky Lab e que contêm uma descrição detalhada de todas as ameaças da segurança do computador actualmente conhecidas, assim como os métodos usados para a sua detecção e desinfecção. Estas bases de dados são constantemente actualizadas pela Kaspersky Lab, à medida que aparecem novas ameaças.

C

CÓDIGO SECRETO DA APLICAÇÃO

O código secreto impede o acesso não autorizado às definições da aplicação e às informações bloqueadas no dispositivo. O utilizador define-as ao iniciar a aplicação pela primeira vez e consiste em pelo menos quatro caracteres. O código secreto é pedido nas seguintes situações:

para acesso às definições da aplicação;

ao enviar um comando SMS a partir de outro dispositivo móvel para iniciar remotamente as seguintes funções: Bloqueio, Limpeza de Dados, Prot. Cartão SIM, Localização por GPS, Protecção de Privacidade.

D

DESINFECTAR OBJECTOS

Um método utilizado para processar objectos infectados, que resulta na recuperação completa ou parcial de dados, ou numa decisão de que os objectos não podem ser desinfectados. A desinfecção de objectos é efectuada de acordo com a base de dados da aplicação. Durante o processo de desinfecção, é possível que ocorra a perda de parte dos dados legítimos de um ficheiro.

E

ELIMINAR MENSAGENS SMS

Método de processamento de uma mensagem SMS com características de SPAM, apagando-a. Aconselha-se que utilize este método com mensagens SMS que indubitavelmente contenham spam.

ELIMINAÇÃO DE UM OBJECTO

O método de processamento de objectos que os apaga fisicamente da sua localização original. É aconselhável aplicar este método de processamento a todos os objectos maliciosos que não for possível desinfectar.

L

LISTA BRANCA

As entradas na lista contêm as seguintes informações:

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

Tipos de eventos que o Filtro de Chamadas e SMS entrega deste número. Estão disponíveis os seguintes tipos de eventos: chamadas e SMS, apenas chamadas e apenas SMS.

Expressão-chave que o Filtro de Chamadas e SMS utiliza para classificar uma SMS como solicitada (não spam). O Filtro de Chamadas e SMS apenas entrega SMS que contenham a expressão-chave, sendo que bloqueia todas as outras SMS.

LISTA NEGRA

As entradas na lista contêm as seguintes informações:

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

Tipos de eventos que o Filtro de Chamadas e SMS bloqueia deste número. Estão disponíveis os seguintes tipos de eventos: chamadas e SMS, apenas chamadas e apenas SMS.

Expressão-chave que o Filtro de Chamadas e SMS utiliza para classificar uma SMS como não solicitada (spam). O Filtro de Chamadas e SMS apenas bloqueia SMS que contenham a expressão-chave, sendo que entrega todas as outras SMS.

M

MÁSCARA DO NÚMERO DE TELEFONE

Colocar um número de telefone na Lista Negra ou Branca utilizando meta caracteres. Os dois meta caracteres básicos utilizados em máscaras de número de telefone são "*" e "?", (em que "*" representa qualquer número de caracteres e "?" corresponde a qualquer carácter individual). Por exemplo, *1234? na Lista Negra. O Filtro de Chamadas e SMS entrega chamadas ou SMS de um número no qual quaisquer símbolos sigam a figura 1234.

N

NÚMERO NÃO NUMÉRICO

Um número de telefone que inclui letras ou é constituído apenas por letras.

O

OBJECTO INFECTADO

Objecto que contém código malicioso. A aplicação detecta objectos infectados verificando o código binário dos mesmos e determinando que uma secção do código do objecto é idêntica a uma secção do código de uma ameaça conhecida. Os especialistas da Kaspersky Lab não recomendam a utilização destes objectos, uma vez que podem causar infecções no seu dispositivo.

KASPERSKY LAB

O Kaspersky Lab foi fundado em 1997. Actualmente, é a principal empresa de desenvolvimento de software de segurança de elevado desempenho, incluindo sistemas antivírus, anti-intrusão e contra correio electrónico não solicitado.

O Kaspersky Lab é uma empresa internacional. Estando sediado na Federação Russa, possui escritórios no Reino Unido, em França, na Alemanha, no Japão, nos países do Benelux, na China, na Polónia, na Roménia e nos EUA (Califórnia). Além disso, foi recentemente criado em França um novo departamento da empresa, o European Anti-Virus Research Centre (Centro Europeu de Pesquisa Antivírus). A rede de parceiros do Kaspersky Lab inclui mais de 500 empresas em todo o mundo.

Actualmente, o Kaspersky Lab emprega mais de mil especialistas altamente qualificados, incluindo 10 colaboradores detentores de Mestrados e 16 detentores de Doutoramentos. Todos os especialistas antivírus sénior do Kaspersky Lab são membros da CARO (Computer Anti-Virus Researchers Organization - Organização de Investigadores de Antivírus Informáticos).

O Kaspersky Lab oferece soluções de segurança líderes na sua gama, com base na sua experiência e conhecimento únicos, adquirida ao longo de 14 anos a combater vírus informáticos. Uma análise minuciosa das actividades relacionadas com vírus de computador permite aos especialistas da empresa antecipar tendências no desenvolvimento de malware e proporcionar aos nossos utilizadores uma protecção atempada contra novos tipos de ataque. Esta é a principal vantagem dos produtos e serviços do Kaspersky Lab. Os produtos da empresa irão permanecer sempre na vanguarda relativamente a outros vendedores que forneçam uma cobertura antivírus extensa tanto para utilizadores caseiros e empresariais.

Anos de trabalho árduo tornaram a empresa num dos principais produtores de software antivírus. O Kaspersky Lab foi a primeira empresa a desenvolver muitas das normas modernas do software antivírus. O produto de referência da empresa, o Kaspersky Anti-Virus, protege de uma forma fiável todos os tipos de sistemas de computador contra ataques de vírus, incluindo estações de trabalho, servidores de ficheiros, sistemas de correio, firewalls, portas de ligação à internet e PDAs. Além disso, os clientes da Kaspersky Lab desfrutam de uma ampla gama de serviços adicionais que asseguram tanto o funcionamento estável dos produtos da empresa como a total satisfação das necessidades empresariais específicas desses clientes. Um grande número de produtores de software em todo o mundo utiliza o kernel do Kaspersky Anti-Virus nos respectivos produtos, incluindo a Nokia ICG (EUA), a Aladdin (Israel), a Sybari (EUA), a G Data (Alemanha), a Deerfield (EUA), a Alt-N (EUA), a Microworld (Índia) e a BorderWare (Canadá).

Além disso, os clientes da Kaspersky Lab desfrutam de uma ampla gama de serviços adicionais que asseguram tanto o funcionamento estável dos produtos da empresa como a total satisfação das necessidades empresariais específicas desses clientes. Planeamos, instalamos e suportamos gamas antivírus empresariais. Neste âmbito, a base de dados das aplicações antivírus do Kaspersky Lab é actualizada de hora a hora. Da mesma forma, a empresa proporciona aos seus clientes um serviço de assistência técnica disponível 24 horas por dia em vários idiomas.

Se pretender esclarecer quaisquer questões, bem como enviar comentários ou sugestões, pode contactar-nos através dos nossos representantes ou, se preferir, directamente, através dos dados de contacto do Kaspersky Lab. As consultas detalhadas são fornecidas por telefone ou e-mail. Todas as suas questões serão respondidas na totalidade.

Web site da Kaspersky Lab

<http://www.kaspersky.pt/>

Enciclopédia de vírus:

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

Laboratório antivírus:

newvirus@kaspersky.com

(apenas para enviar objectos suspeitos em arquivos)

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

(para envio de pedidos a analistas de vírus)

Fórum Web da Kaspersky Lab:

<http://forum.kaspersky.com>

INFORMAÇÃO SOBRE CÓDIGO DE TERCEIROS

O código de terceiros é utilizado para criar a aplicação.

NESTA SECÇÃO

Código de programa distribuído	84
Outras informações	84

CÓDIGO DE PROGRAMA DISTRIBUÍDO

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

NESTA SECÇÃO

ADB.....	84
ADBWINAPI.DLL	Error! Bookmark not defined.
ADBWINUSBAPI.DLL	Error! Bookmark not defined.

OUTRAS INFORMAÇÕES

Informação adicional sobre código de terceiros.

Para verificação de assinaturas digitais, o Kaspersky Mobile Security utiliza a biblioteca de software de segurança de dados Crypto C da CryptoEx OOO.

Web site empresarial da CryptoEx OOO: <http://www.cryptoex.ru>

ÍNDICE

A

A determinar a localização do dispositivo	63
Activar	
Filtro de Chamadas e SMS.....	46
Protecção de Privacidade.....	68
Activar a aplicação	22
licença	28
Actualizar	
início agendado	76
Adicionar	
Lista Branca do Filtro de Chamadas e SMS.....	50
lista de números confidenciais de Protecção de Privacidade.....	72
Lista Negra do Filtro de Chamadas e SMS	47
Agendamento	
Actualização	76
Verificações a pedido	41
Anti-Roubo	57
Bloquear	58
Limpeza de Dados.....	59
Localização por GPS.....	63
Prot. Cartão SIM.....	62
Apagar	
Lista Branca do Filtro de Chamadas e SMS.....	52
lista de contactos confidenciais de Protecção de Privacidade.....	73
Lista Negra do Filtro de Chamadas e SMS	49
Arquivos	
Verificações a pedido	42

B

Bloquear	
chamadas de entrada.....	47
dispositivo.....	58
SMS de entrada.....	47

C

Código	
código de activação.....	23, 24
Código secreto da aplicação	25
Código secreto da aplicação.....	25, 26

D

Dados	
apagar remotamente	59
DADOS	
INFORMAÇÕES CONFIDENCIAIS.....	67
Desactivar	
Filtro de Chamadas e SMS.....	46
Protecção de Privacidade.....	68
DESINSTALAR	
APLICAÇÃO.....	21

E

Editar	
Lista Branca do Filtro de Chamadas e SMS.....	51

lista de contactos confidenciais de Protecção de Privacidade.....	73
Lista Negra do Filtro de Chamadas e SMS	48
Entrada	
Lista Branca do Filtro de Chamadas e SMS	50
Lista Negra do Filtro de Chamadas e SMS	47
Enviar comando SMS.....	65
F	
FILTRAGEM	
CHAMADAS DE ENTRADA	45
SMS DE ENTRADA.....	45
Filtro de Chamadas e SMS	45
acção no que diz respeito a SMS	54
acção no que diz respeito a uma chamada	55
Lista Branca.....	49
Lista Negra	47
modos.....	46
números não numéricos	53
números que não são dos Contactos	52
I	
Iniciar	
aplicação	27
INSTALAR A APLICAÇÃO.....	20
L	
Licença	
activar a aplicação.....	22
Contrato de Licença	28
informações	29
renovação.....	30
Limpar	
informações guardadas no dispositivo	59
Lista Branca	
Filtro de Chamadas e SMS.....	49
Lista Negra	
Filtro de Chamadas e SMS.....	47
M	
Modos	
Filtro de Chamadas e SMS.....	46
Protecção de Privacidade.....	67, 68
P	
Permitir	
chamadas de entrada.....	50
SMS de entrada.....	50
Protecção de Privacidade	67
lista de contactos confidenciais	72
modos.....	67
seleccionar informações e eventos a serem ocultos	71
Protecção Privacidade	
início automático.....	68
início remoto.....	69
R	
Renovar a licença	30

S

Som.....	78
----------	----

V

Verificações a pedido	
Acções a efectuar em objectos.....	43
arquivos.....	42
início agendado	41