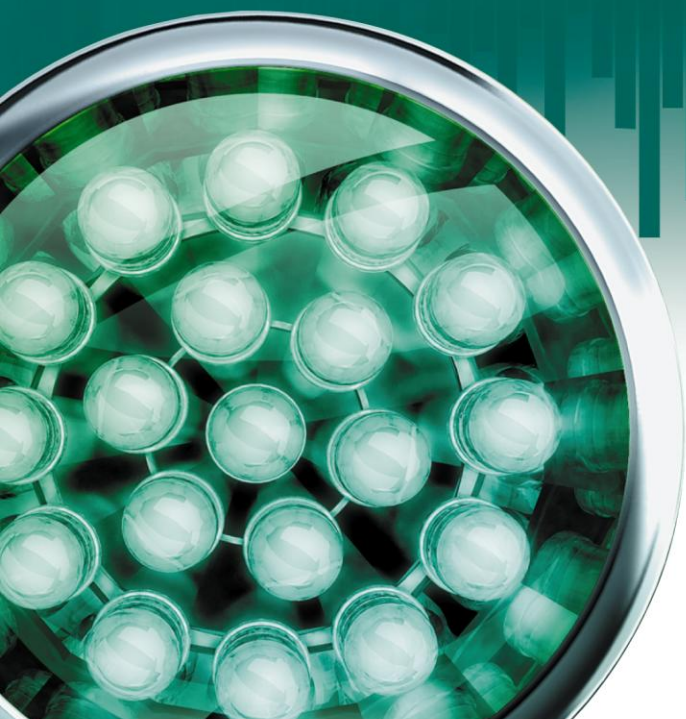


Gerenciador de Senhas Kaspersky

MANUAL DO USUÁRIO



Prezado usuário,

Obrigado por escolher nosso produto. Esperamos que este documento o ajude em seu trabalho e responda à maioria das dúvidas referentes a este produto de software.

Aviso! Este documento é propriedade da Kaspersky Lab: todos os seus direitos são reservados pelas leis de direitos autorais da Federação Russa e por tratados internacionais. A reprodução e distribuição ilegais deste documento ou de partes dele resultarão em responsabilidades civis, administrativas ou criminais relativas às leis da Federação Russa.

Qualquer tipo de reprodução ou distribuição de qualquer material, incluindo sua tradução, é permitido somente através da permissão por escrito da Kaspersky Lab.

Este documento e as imagens gráficas relacionadas a ele podem ser usados exclusivamente para fins informativos, não comerciais e pessoais.

Este documento pode ser alterado sem qualquer notificação. A versão mais recente deste documento está disponível no site da Kaspersky Lab, em <http://brazil.kaspersky.com/downloads/documentacao>.

A Kaspersky Lab não assume qualquer responsabilidade pelo conteúdo, qualidade, relevância ou precisão do material usado neste documento cujos direitos são de propriedade de terceiros, ou por possíveis danos associados ao uso desses documentos.

Este documento contém marcas registradas e marcas de serviço que são propriedade de seus respectivos proprietários.

Data de revisão: 19.02.2011

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

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

ÍNDICE

CONTRATO DE LICENÇA DO USUÁRIO FINAL DA KASPERSKY LAB.....	5
SOBRE ESTE MANUAL	10
Nesta documentação.....	10
Convenções da documentação	11
FONTES ADICIONAIS DE INFORMAÇÕES	12
Fontes de informações para você pesquisar	12
Discutindo os aplicativos da Kaspersky no fórum da Web	13
Entrando em contato com o Departamento de vendas	13
GERENCIADOR DE SENHAS KASPERSKY	14
ATIVANDO O APLICATIVO	15
INTERFACE DO GERENCIADOR DE SENHAS KASPERSKY.....	16
Ícone da área de notificação.....	16
Menu de contexto do Gerenciador de Senhas Kaspersky.....	16
Janela do Gerenciador de Senhas Kaspersky.....	17
Janela Banco de Dados de Senhas	18
Janela de configurações do aplicativo.....	19
Botão de Legenda	19
Plug-ins.....	19
Ponteiro	20
GERENCIAMENTO DO BANCO DE DADOS DE SENHAS	21
Acessando o Banco de Dados de Senhas	21
Adicionando dados pessoais	22
Conta	23
Nome de usuário.....	28
Identidade	28
Nota segura	29
Usando dados pessoais	30
Localizando senhas.....	30
Excluindo dados pessoais	31
Importando/exportando dados.....	31
Backup / Restauração do Banco de Dados de Senhas.....	33
CONFIGURANDO O APLICATIVO.....	35
Nome de usuário padrão	36
Contas mais usadas	37
Endereços Web ignorados	38
Endereços Web confiáveis	38
Teclas de atalho	39
Local do arquivo do Banco de Dados de Senhas.....	39
Criando novo Banco de Dados de Senhas.....	41
Local da cópia de backup.....	41
Selecionando o método de criptografia	42
Bloqueio automático do Banco de Dados de Senhas.....	43
Alterando o método de autorização do Gerenciador de Senhas Kaspersky	44

Usando dispositivos USB e Bluetooth para a autorização.....	44
Alterando a Senha Mestra.....	45
Navegadores da Web com suporte.....	45
Gerenciando modelos de Notas seguras.....	46
Hora de execução do aplicativo.....	47
Ação Ao clicar duas vezes.....	47
Notificações.....	48
Hora em que a senha foi armazenada na área de transferência.....	49
Exibindo o Botão de Legenda.....	49
CRIANDO SENHAS FORTES.....	50
USANDO A VERSÃO PORTÁTIL DO GERENCIADOR DE SENHAS KASPERSKY.....	51
Criando e conectando a versão portátil.....	51
Sincronização do Banco de Dados de Senhas.....	52
KASPERSKY LAB.....	54

CONTRATO DE LICENÇA DO USUÁRIO FINAL DA KASPERSKY LAB

IMPORTANTE ADVERTÊNCIA LEGAL PARA TODOS OS USUÁRIOS: LEIAM COM CUIDADO O SEGUINTE CONTRATO LEGAL ANTES DE COMEÇAR A USAR O APLICATIVO.

CLICANDO NO BOTÃO EU CONCORDO NA JANELA DE CONTRATO DE LICENÇA OU AO DIGITAR O(S) SÍMBOLO(S) CORRESPONDENTE(S) VOCÊ ESTARÁ CONCORDANDO EM VINCULAR-SE PELOS TERMOS E CONDIÇÕES DESTE CONTRATO. **ESTA AÇÃO SIMBOLIZA A SUA ASSINATURA E A SUA CONCORDÂNCIA EM VINCULAR-SE PELOS TERMOS DO PRESENTE CONTRATO, TORNANDO-SE PARTE DELE E CONCORDANDO SER ESTE CONTRATO EXECUTÁVEL COMO QUALQUER OUTRO CONTRATO NEGOCIADO E ASSINADO POR VOCÊ.** CASO VOCÊ NÃO CONCORDE COM TODOS OS TERMOS E CONDIÇÕES DO PRESENTE CONTRATO, CANCELE A INSTALAÇÃO DO APLICATIVO E NÃO O INSTALE.

APÓS CLICAR NO BOTÃO EU CONCORDO NA JANELA DE CONTRATO DE LICENÇA OU AO DIGITAR O(S) SÍMBOLO(S) CORRESPONDENTE(S), VOCÊ TERÁ O DIREITO DE USAR O APLICATIVO EM CONFORMIDADE COM OS TERMOS E CONDIÇÕES DESTE CONTRATO.

1. Definições

- 1.1. **Aplicativo** significa o aplicativo incluindo quaisquer atualizações e materiais relacionados.
- 1.2. **Titular** (proprietário de todos os direitos, quer sejam exclusivos ou não ao Aplicativo) significa a Kaspersky Lab ZAO, uma empresa constituída nos termos da legislação da Federação Russa.
- 1.3. **Computador(es)** significa(am) equipamento(s), incluindo computadores pessoais, computadores portáteis, estações de trabalho, assistentes digitais pessoais, 'telefones inteligentes', aparelhos de mão ou outros dispositivos eletrônicos para os quais o Aplicativo foi projetado, onde o Aplicativo será instalado e/ou usado.
- 1.4. **Usuário Final (Você / Seu)** significa instalação(ões) individual(ais) ou usar o Aplicativo em seu próprio nome ou de quem esteja legalmente usando uma cópia do Aplicativo; ou, se o Aplicativo está sendo baixado ou instalado em nome de uma organização, tal como um empregador, "Você" significa ainda a organização para a qual o Aplicativo é baixado ou instalado, declarando-se, para fins do presente instrumento, que tal organização tenha autorizado a pessoa aderindo a este contrato a fazê-lo em seu nome. Para os efeitos do presente documento o termo "organização", inclui, entre outros, qualquer parceria, sociedade de responsabilidade limitada, corporação, associação, sociedade de capital aberto, fundo fiduciário, empreendimento conjunto, organização do trabalho, organização sem personalidade jurídica ou autoridade governamental.
- 1.5. **Parceiro(s)** significa organização(ões) ou indivíduo(s) que distribui(em) o Aplicativo, tendo como base um contrato e licenciamento com o Titular.
- 1.6. **Atualização(ões)** significa todas as atualizações, revisões, "patches", aprimoramentos, reparos, modificações, cópias, complementações ou pacotes de manutenção da versão comprada do software.
- 1.7. **Manual do usuário** significa manual do usuário, guia do administrador, livro de referência e explicações correlatas ou outros materiais.

2. Licenciamento

2.1. O Titular concede a você uma licença vitalícia não exclusiva para armazenar, carregar, instalar, executar e exibir ("usar") o Aplicativo em um determinado número de computadores, a fim de usar o Aplicativo conforme descrito no Manual do usuário, de acordo com todos os requisitos técnicos descritos no Manual do usuário e de acordo com os termos e condições do presente Contrato (a "Licença"), sendo tal Licença aceita por você:

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

Aplicativo para múltiplos ambientes; Aplicativo para múltiplos idiomas; Aplicativo para mídia dupla; cópias múltiplas; pacotes. Caso você use diferentes versões do Aplicativo ou edições em diferentes idiomas do Aplicativo, caso receba o Aplicativo em múltiplos suportes, caso receba várias cópias do Aplicativo ou caso

tenha recebido o Aplicativo em conjunto com outro aplicativo, o número total permitido dos seus computadores nos quais todas as versões do Aplicativo são instaladas deve corresponder ao número de licenças que tenha obtido do Titular *uma vez que*, salvo se os termos e condições de licenciamento disponham de outra forma, cada licença comprada lhe dá o direito de instalar e usar o Aplicativo em tal número de Computador(es), conforme especificado nas Cláusulas 2.2 e 2.3.

2.2. Caso o Aplicativo tenha sido comprado em meio físico, Você tem o direito de usar o Aplicativo em determinado número de Computador(es), conforme especificado no pacote do Aplicativo.

2.3. Caso o Aplicativo tenha sido comprado pela Internet, Você tem o direito de usar o Aplicativo em determinado número de computadores que foi especificado quando Você comprou a licença para o Aplicativo.

2.4. Você tem o direito de fazer uma cópia do Aplicativo apenas para fins de cópia de segurança, e apenas para substituir a cópia legalmente de sua propriedade, caso essa cópia seja extraviada, destruída ou se tornar inutilizável. Tal cópia de segurança não pode ser utilizada para outros fins, devendo ser destruída quando você perder o direito ao uso do Aplicativo ou quando a Sua licença vencer ou for rescindida, por qualquer outro motivo, de acordo com a legislação em vigor no país da sua residência principal ou no país onde Você está usando o Aplicativo.

2.5. Você pode transferir a licença não exclusiva de uso do Aplicativo a outros indivíduos ou entidades legais no escopo da licença concedida a Você pelo Titular, contanto que o receptor concorde em se submeter a todos os termos e condições deste Contrato e substitua você completamente na licença concedida pelo Titular. Caso Você transfira os direitos concedidos pelo Titular de uso do Aplicativo Você deve destruir todas as cópias do Aplicativo, inclusive a de segurança. Se Você for receptor de uma licença transferida, Você deve concordar em obedecer a todos os termos e condições deste Contrato. Se você não concordar em se submeter a todos os termos e condições deste Contrato, Você não deverá instalar e/ou usar o Aplicativo. Você também concorda, como receptor de uma licença transferida, que Você não possui direitos melhores ou adicionais em relação ao Usuário Final original que comprou o Aplicativo do Titular.

2.6. Para executar o Aplicativo em modo completo, Você deve receber e instalar a chave da licença conforme descrito no Manual do usuário.

2.7. A partir da transição do Software para o modo completo (com a exceção de uma versão de teste do Aplicativo) Você tem direito a receber os seguintes serviços de acordo com os termos em <http://support.kaspersky.com/support/rules:>

- Atualizações do aplicativo na Internet, quando e como o Titular as publicar em sua página, ou por meio de outros serviços on-line. Quaisquer atualizações que você venha a receber tornam-se parte do Aplicativo, aplicando-se às mesmas os termos e condições do presente Contrato; e
- Assistência técnica na Internet e assistência técnica por linha telefônica direta.

3. Ativação repetida e período de uso da versão de teste

3.1. Caso você modifique o seu computador ou faça alterações em aplicativos de outros fornecedores nele instalados, o Titular poderá solicitar que Você repita a instalação da licença.

3.2. Você tem o direito de usar uma versão de teste do Aplicativo, conforme disposto na Cláusula 2.1, sem qualquer encargo, pelo período único de avaliação (30 dias) aplicável a partir do momento de ativação do Aplicativo, de acordo com o presente Contrato, *desde que* a versão de avaliação não lhe conceda nenhum direito a Atualizações e assistência técnica na Internet nem a assistência técnica por linha telefônica direta. Se o Titular definir outra duração para o período único de avaliação, Você será informado por uma notificação.

3.3. Você tem o direito de usar uma versão de teste do Aplicativo, conforme disposto na Cláusula 2.1, sem qualquer encargo, pelo período único adicional de avaliação (15 dias) aplicável a partir do final do período mencionado na Cláusula 3.2. Durante esse período, a funcionalidade do Aplicativo será limitada conforme descrito no Manual do usuário.

4. Assistência técnica

4.1. A assistência técnica descrita na Cláusula 2.6 do presente Contrato será fornecida a Você quando a mais recente

atualização do Aplicativo for instalada (com exceção de uma versão de avaliação do Aplicativo).

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

5. Limitações

5.1. Você não deve simular, clonar, alugar, emprestar, arrendar, vender, modificar, descompilar ou fazer engenharia reversa no Aplicativo, nem desmontar ou criar trabalhos derivados do Aplicativo ou de qualquer parte dele, com a única exceção de um direito não renunciável concedido a Você pela legislação aplicável, e você não deve reduzir de nenhuma maneira qualquer parte do Aplicativo para o formato humano legível ou

transferir o Aplicativo licenciado ou qualquer subconjunto do Aplicativo licenciado, nem permitir que terceiros o façam, exceto nos casos em que a restrição anterior seja expressamente proibida pela lei aplicável. Nem o código binário do Aplicativo nem o código-fonte pode ser usado ou submetido a engenharia reversa para recriar o algoritmo do programa, que é exclusivo do Titular. Todos os direitos não expressamente concedidos neste Contrato são reservados pelo Titular e/ou seus fornecedores, conforme aplicável. Qualquer uso não autorizado do Aplicativo resultará na rescisão imediata e automática do presente Contrato e da Licença aqui concedida, podendo resultar em processo penal e/ou cível contra Você.

5.2. Você não deve transferir os direitos de uso do Aplicativo a terceiros, salvo conforme estabelecido na Cláusula 2.5 do presente Contrato.

5.3. Você não deve fornecer o código de ativação e/ou o arquivo da chave de licença a terceiros, nem permitir que terceiros tenham acesso ao código de ativação e/ou a chave de licença, os quais são considerados dados confidenciais do Titular, e você tomará todas as precauções, dentro do razoável, para proteger o código de ativação e/ou a chave de licença, de boa-fé, já que você pode transferir o código de ativação e/ou a chave de licença a terceiros, conforme estipulado na Cláusula 2.5 do presente Contrato.

5.4. Você não pode alugar, arrendar ou emprestar o Aplicativo a terceiros.

5.5. Você não deve usar o Aplicativo para a criação de dados ou aplicativos usados para detecção, bloqueio ou tratamento das ameaças descritas no Manual do usuário.

5.6. O Titular tem o direito de bloquear o arquivo da chave ou rescindir a Sua Licença para uso do Aplicativo caso Você viole qualquer dos termos e condições deste Contrato, sem qualquer restituição a Você.

5.7. Caso Você esteja usando a versão de avaliação do Aplicativo, não terá o direito de receber a assistência técnica especificada na Cláusula 4 do presente Contrato, nem terá o direito de transferir a licença ou os direitos de uso do Aplicativo para qualquer terceiro.

6. Garantia restrita e exclusão

6.1. O Titular garante que o Aplicativo irá desempenhar substancialmente, de acordo com as especificações e descrições estabelecidas no Manual do usuário, *desde que, entretanto*, a referida garantia restrita não se aplique ao seguinte: (w) deficiências de seu computador e violação relacionada para as quais o Titular renuncia expressamente a qualquer responsabilidade da garantia; (x) avarias, defeitos ou falhas resultantes de uso indevido, abuso, acidente, negligência, instalação, operação ou manutenção imprópria; furto; vandalismo; atos fortuitos; atos de terrorismo; falhas ou picos de energia; acidente, alteração, modificações ou reparos não permitidos por qualquer terceiro que não seja o Titular, ou quaisquer outros terceiros ou Suas ações ou causas além do controle razoável pelo Titular; (y) qualquer defeito, não divulgado por Você ao Titular o mais rapidamente possível, após o defeito aparecer pela primeira vez; e (z) causados por incompatibilidade de componentes de equipamento e/ou aplicativo instalado em Seu computador.

6.2. Você reconhece, aceita e concorda que nenhum aplicativo está isento de erros, sendo aconselhado a realização de cópia de segurança no computador, com uma frequência e confiabilidade adequadas para Você.

6.3. O Titular não oferece qualquer garantia de que o Aplicativo irá funcionar corretamente em caso de violação dos termos e condições descritos no Manual do usuário ou no presente Contrato.

6.4. O Titular não garante proteção contra as ameaças descritas no Manual do usuário após o vencimento do prazo especificado nas Cláusulas 3.2 ou 3.3 do presente Contrato ou após a rescisão, por qualquer motivo, da Licença de uso do Aplicativo.

6.5. O APLICATIVO É FORNECIDO "TAL COMO SE ENCONTRA", E O TITULAR NÃO FAZ NENHUMA DECLARAÇÃO E NÃO DÁ NENHUMA GARANTIA QUANTO A SEU USO OU DESEMPENHO. SALVO POR QUALQUER GARANTIA, CONDIÇÃO, DECLARAÇÃO OU TERMO, NA MEDIDA EM QUE NÃO PODE SER EXCLUÍDA OU RESTRITA PELA LEGISLAÇÃO APLICÁVEL, O TITULAR E SEUS PARCEIROS NÃO DÃO NENHUMA GARANTIA, CONDIÇÃO, DECLARAÇÃO OU TERMO (EXPRESSO OU IMPLÍCITO, QUER POR ESTATUTO, LEI COMUM, PERSONALIZAÇÃO, USO OU DE ALGUMA OUTRA MANEIRA) QUANTO A QUALQUER ASSUNTO, INCLUINDO, ENTRE OUTROS, A NÃO VIOLAÇÃO DE DIREITOS DE TERCEIROS, COMERCIALIZIDADE, QUALIDADE SATISFATÓRIA, INTEGRAÇÃO OU APLICABILIDADE PARA DETERMINADO PROPÓSITO. VOCÊ ASSUME TODAS AS FALHAS E TODO O RISCO QUANTO AO DESEMPENHO E RESPONSABILIDADE DE SELEÇÃO DO APLICATIVO PARA ALCANÇAR SEUS RESULTADOS PRETENDIDOS, BEM COMO PARA A INSTALAÇÃO, USO E RESULTADOS OBTIDOS PELO APLICATIVO. SEM PREJUÍZO DAS DISPOSIÇÕES ANTERIORES, O TITULAR NÃO FAZ NENHUMA DECLARAÇÃO E NÃO DÁ NENHUMA GARANTIA QUE O APLICATIVO ESTARÁ LIVRE DE ERROS, INTERRUPÇÕES OU OUTRAS FALHAS, NEM QUE O APLICATIVO ATENDERÁ QUALQUER OU TODOS OS SEUS REQUISITOS, QUER OU NÃO DIVULGADOS AO TITULAR.

7. Exclusão e limitação da responsabilidade

7.1. NA MEDIDA DO PERMITIDO PELA LEGISLAÇÃO APLICÁVEL, EM NENHUM CASO O TITULAR OU SEUS PARCEIROS SERÃO RESPONSÁVEIS POR QUAISQUER DANOS ESPECIAIS, INCIDENTAIS, PUNITIVOS, INDIRETOS, CONSEQUÊNCIAS OU QUAISQUER DANOS (INCLUINDO, ENTRE OUTROS, DANOS POR PERDA DE RECEITA OU CONFIDENCIAIS OU OUTRAS INFORMAÇÕES, POR INTERRUPTÃO DOS NEGÓCIOS, POR PERDA DE PRIVACIDADE, POR CORRUPÇÃO, DANO E PERDA DE DADOS OU PROGRAMAS, POR NÃO CUMPRIMENTO DE QUALQUER DEVER INCLUINDO QUALQUER OBRIGAÇÃO LEGAL, DIREITO DE BOA-FÉ OU DIREITO DE CUIDADOS RAZOÁVEIS, POR NEGLIGÊNCIA, POR PREJUÍZOS ECONÔMICOS, E QUAISQUER OUTRAS PERDAS PECUNIÁRIAS OU OUTRA PERDA) DECORRENTES DE OU DE ALGUMA MANEIRA RELACIONADOS AO USO OU À IMPOSSIBILIDADE DE USAR O APLICATIVO, A PROVISÃO OU FALTA DE PRESTAÇÃO DE APOIO OU OUTROS SERVIÇOS, INFORMAÇÕES, APLICATIVO E CONTEÚDO RELACIONADO POR MEIO DO APLICATIVO OU DE OUTROS DECORRENTES DO USO DO APLICATIVO OU DE QUALQUER OUTRO RESULTANTE OU RELACIONADO COM QUALQUER DISPOSIÇÃO DO PRESENTE CONTRATO, OU DECORRENTE DE QUALQUER VIOLAÇÃO DE CONTRATO OU QUALQUER OFENSA (INCLUINDO NEGLIGÊNCIA, DETURPAÇÃO, QUALQUER RESPONSABILIDADE OU OBRIGAÇÃO RIGOROSA), OU QUALQUER VIOLAÇÃO DA GARANTIA DE DEVERES ESTATUTÁRIOS OU QUALQUER QUEBRA DA GARANTIA DO TITULAR OU QUALQUER UM DE SEUS PARCEIROS, MESMO SE O TITULAR OU QUALQUER PARCEIRO TENHA SIDO AVISADO DA POSSIBILIDADE DOS REFERIDOS DANOS.

VOCÊ CONCORDA QUE EM CASO DE O TITULAR E/OU SEUS PARCEIROS SEREM JULGADOS RESPONSÁVEIS, A RESPONSABILIDADE DO TITULAR E/OU DOS SEUS PARCEIROS ESTARÁ RESTRITA AOS CUSTOS DO APLICATIVO. EM NENHUM CASO, A RESPONSABILIDADE DO TITULAR E/OU SEUS PARCEIROS EXCEDERÁ O PREÇO PAGO AO TITULAR OU AO PARCEIRO PELO APLICATIVO (TAL COMO APLICÁVEL).

NADA NESTE CONTRATO EXCLUI OU LIMITA QUALQUER REIVINDICAÇÃO POR MORTE E LESÃO CORPORAL. AINDA NO CASO DE QUALQUER RENÚNCIA, EXCLUSÃO OU RESTRIÇÃO NESTE CONTRATO NÃO PODER SER EXCLUÍDA OU RESTRITA DE ACORDO COM A LEGISLAÇÃO APLICÁVEL, NESSE CASO, APENAS A REFERIDA RENÚNCIA, EXCLUSÃO OU RESTRIÇÃO NÃO IRÁ SE APLICAR A VOCÊ, E VOCÊ CONTINUARÁ VINCULADO POR TODAS AS RENÚNCIAS, EXCLUSÕES E RESTRIÇÕES REMANESCENTES.

8. GNU e outras licenças de terceiros

8.1. O Aplicativo pode incluir alguns programas de aplicativo que são licenciados (ou sublicenciados) para o usuário sob Licença Pública Geral GNU (GNU General Public License, GPL) ou outras licenças similares de aplicativo livre, que, entre outros direitos, permitem ao usuário copiar, modificar e redistribuir determinados programas, ou partes dos mesmos, bem como ter acesso ao código-fonte ("Aplicativo com Código Aberto"). Caso essas licenças exijam que, para qualquer aplicativo que é distribuído a alguém em formato binário executável, o código-fonte também seja disponibilizado a esses usuários, então ele deve ser disponibilizado por meio do envio de uma solicitação para source@kaspersky.com ou o código fonte fornecido juntamente com o Aplicativo. Se quaisquer licenças de Aplicativo com Código Aberto exigirem que o Titular propicie direitos para usar, copiar ou modificar um programa de Aplicativo com Código Aberto que é mais abrangente que os direitos concedidos no presente Contrato, os referidos direitos devem ter primazia sobre os direitos e restrições no presente instrumento.

9. Titularidade da propriedade intelectual

9.1. Você concorda que o Aplicativo e a autoria, sistemas, ideias, métodos de funcionamento, documentação e outras informações contidas no Aplicativo, são propriedade intelectual e/ou segredos industriais valiosos do Titular ou de seus parceiros, e que o Titular e seus parceiros, conforme o caso, são protegidos pelo direito civil e penal e pela lei de direitos autorais, segredos industriais, marcas e patentes da Federação Russa, da União Europeia e dos EUA, bem como de outros países e tratados internacionais. O presente Contrato não concede a Você nenhum direito à propriedade intelectual, incluindo todas as marcas comerciais ou marcas de serviço do Titular e/ou seus parceiros ("Marcas"). Você poderá usar as marcas comerciais apenas nas saídas impressas produzidas pelo Aplicativo, de acordo com a prática aceita de marcas comerciais, incluindo a identificação do nome do proprietário da marca comercial. Essa utilização de qualquer marca comercial não lhe dá qualquer direito de propriedade na referida marca. O Titular e/ou seus parceiros possuem e detêm todos os direitos, títulos e interesses relativos ao Aplicativo, incluindo, entre outros, quaisquer correções de erros, melhorias, atualizações ou outras modificações ao Aplicativo, sejam realizadas pelo Titular ou por qualquer terceiro, e todos os direitos autorais, patentes, direitos a segredos comerciais, marcas comerciais e outros direitos de propriedade intelectual contidos neste instrumento. A sua posse, instalação ou uso do Aplicativo não transfere para você qualquer título de propriedade intelectual sobre o Aplicativo, e você não poderá adquirir direitos sobre o Aplicativo, salvo conforme expressamente

previsto no presente Contrato. Todas as cópias do Aplicativo feitas em virtude deste instrumento devem conter as mesmas advertências sobre a propriedade que aparecem no Aplicativo. Salvo conforme indicado neste documento, este Contrato não lhe concede direitos de propriedade intelectual ao Aplicativo, e Você reconhece que a Licença, conforme definido mais pormenorizadamente a seguir, concedida ao abrigo do presente Contrato, só lhe garante um direito de uso restrito, nos termos e condições do presente Contrato. O Titular reserva todos os direitos não expressamente concedidos a você no presente Contrato.

9.2. Você concorda em não modificar ou alterar o Aplicativo por qualquer forma. Você não pode remover ou alterar qualquer advertência de direitos autorais ou outras advertências sobre a propriedade de quaisquer cópias do Aplicativo.

10. Lei aplicável; arbitragem

10.1. Este Contrato será regido e interpretado de acordo com as leis da Federação Russa, sem referência a conflitos de leis e princípios. Este Contrato não será regido pela Convenção das Nações Unidas sobre Contratos para a Venda Internacional de Mercadorias, cuja aplicação está expressamente excluída. Qualquer litígio decorrente da interpretação ou aplicação dos termos e condições deste Contrato ou qualquer violação destes deve, se não for resolvida por negociação direta, ser resolvida no Tribunal de Arbitragem Comercial Internacional da Câmara de Comércio e Indústria da Federação Russa em Moscou, Federação Russa. Qualquer adjudicação proferida pelo árbitro será final e vinculativa para as partes, podendo ainda qualquer julgamento sobre tal decisão arbitral ser executado em qualquer tribunal de jurisdição competente. Nada na presente Seção 11 deverá impedir uma Parte de buscar ou obter reparação justa em tribunal competente, quer antes, durante ou depois dos processos de arbitragem.

11. Prazo para interposição de ações judiciais

11.1. Nenhuma ação, independentemente da forma, decorrente das transações no âmbito do presente Contrato, pode ser interposta por qualquer uma das partes aqui mencionadas após 1 (um) ano de a ação ter ocorrido, ou foi constatado ter ocorrido, salvo ação por violação dos direitos de propriedade intelectual, a qual pode ser instaurada dentro do máximo prazo legal aplicável.

12. Totalidade do contrato; divisibilidade; princípio da não renúncia

12.1. Este Contrato é o contrato integral entre você e o Titular, substituindo quaisquer outros contratos, propostas, comunicações ou publicidade anterior, sendo verbais ou escritos, com relação ao Aplicativo ou ao objeto do presente Contrato. Você reconhece que leu este Contrato, compreende o mesmo e concorda em vincular-se por seus termos e condições. Caso qualquer disposição do presente Contrato seja constatada por um tribunal de jurisdição competente como inválida, nula ou inexecutável, por qualquer motivo, no todo ou em parte, essa disposição será interpretada de maneira mais restritiva para que se torne legal e aplicável, e o Contrato não irá sucumbir em seu todo por conta da mesma, permanecendo o restante do Contrato em plena vigência e efeito até o limite máximo permitido pela lei ou por similitude, preservando simultaneamente, na medida do possível, a sua intenção original. Nenhuma renúncia de qualquer disposição ou condição aqui contida será válida, a menos que seja feita por escrito e assinada por você e por um representante autorizado do Titular, sendo que nenhuma renúncia de qualquer violação de quaisquer disposições do presente Contrato constituirá renúncia quanto a qualquer violação prévia, concomitante ou posterior. A falha por parte do Titular em insistir ou aplicar o desempenho rigoroso de qualquer disposição do presente Contrato ou de qualquer direito não deve ser interpretada como renúncia de qualquer disposição ou direito.

13. Informações para contato do Titular

Caso tenha quaisquer perguntas relativas a este Contrato, ou caso deseje entrar em contato com o Titular, por qualquer motivo, favor entrar em contato com o nosso Departamento de Atendimento ao Cliente:

Kaspersky Lab ZAO, 10 build. 1 1st Volokolamsky Proezd
Moscou, 123060
Federação Russa
Tel.: +7-495-797-8700
Fax: +7-495-645-7939
Correio eletrônico: info@kaspersky.com
Página na Internet: www.kaspersky.com

© 1997-2011 Kaspersky Lab ZAO. Todos os Direitos Reservados. O Aplicativo e qualquer documentação que o acompanha são protegidos pelas leis de direitos autorais e tratados internacionais sobre direitos autorais, bem como outras leis e tratados sobre propriedade intelectual.

SOBRE ESTE MANUAL

Este documento é o Manual para a instalação, configuração e operação do Gerenciador de Senhas Kaspersky. O documento foi criado para um público abrangente. É necessário que os usuários do aplicativo consigam operar um computador pessoal em nível básico: estar familiarizados com a interface do sistema operacional Microsoft Windows e em sua navegação, além de saber como usar programas conhecidos de email e Internet, como o Microsoft Office Outlook e o Microsoft Internet Explorer.

O objetivo do documento:

- ajudar os usuários a ativar e configurar o programa em relação às tarefas desejadas;
- fornecer uma fonte de informações facilmente disponível sobre problemas relacionados ao aplicativo;
- fornecer fontes alternativas de informações sobre o aplicativo e as formas de obter suporte técnico.

NESTA SEÇÃO:

Nesta documentação [10](#)

Convenções da documentação [11](#)

NESTA DOCUMENTAÇÃO

O Manual do Usuário do Gerenciador de Senhas Kaspersky consiste nas seguintes seções principais:

Fontes adicionais de informações

Esta seção contém uma descrição dos dados sobre as fontes de informações adicionais referentes ao aplicativo e um recurso na Internet onde é possível discutir o aplicativo, compartilhar ideias, fazer perguntas e obter respostas.

Gerenciador de Senhas Kaspersky

Esta seção descreve os novos recursos do aplicativo e fornece informações resumidas sobre seus componentes e suas funções básicas.

Ativando o aplicativo

Esta seção contém informações referentes aos conceitos básicos usados no contexto de licenciamento do aplicativo, além de instruções para ajudá-lo a ativar o programa.

Interface do Gerenciador de Senhas Kaspersky

Esta seção contém uma descrição dos componentes básicos da interface gráfica do usuário do aplicativo.

Gerenciamento do Banco de Dados de Senhas

Esta seção contém informações sobre como criar e usar dados para preencher formulários automaticamente em sites e programas.

Configurando o aplicativo

Esta seção contém informações sobre como configurar o programa para obter eficiência máxima.

Criando senhas fortes

Esta seção contém informações sobre como usar o gerador de senhas fortes.

Usando a versão portátil do Gerenciador de Senhas Kaspersky

Esta seção contém informações sobre como criar e usar a versão portátil do Gerenciador de Senhas Kaspersky.

CONVENÇÕES DA DOCUMENTAÇÃO

As convenções da documentação usadas neste Manual estão descritas na tabela a seguir.

Table 1. Convenções da documentação

TEXTO DE EXEMPLO	DESCRIÇÃO DAS CONVENÇÕES DA DOCUMENTAÇÃO
Observe que...	Os avisos estão realçados em vermelho e dispostos em quadros. Os avisos contêm informações importantes, por exemplo, relacionadas às operações do computador fundamentais para sua segurança.
É recomendável usar...	As observações estão dispostas em quadros. As observações contêm informações adicionais e de referência.
Exemplo: ...	Os exemplos são fornecidos por seção sobre fundo amarelo e sob o título "Exemplo".
<i>Atualização</i> significa...	Os termos novos são realçados em itálico.
ALT+F4	Os nomes de teclas do teclado são exibidos em uma fonte em negrito e em letras maiúsculas. Os nomes das teclas seguidos de um sinal de "adição" indicam o uso de uma combinação de teclas.
Ativar	Os nomes de elementos da interface, como campos de entrada, comandos de menus, botões, etc., são realçados por uma fonte em negrito.
➡ <i>Para configurar a programação da tarefa:</i>	As frases introdutórias das instruções são exibidas em itálico.
help	Os textos da linha de comando ou de mensagens exibidas na tela utilizam uma fonte especial.
<Endereço IP do computador>	As variáveis são colocadas entre colchetes angulares. Em vez das variáveis, os valores correspondentes devem ser colocados em cada caso e os colchetes angulares são omitidos.

FONTES ADICIONAIS DE INFORMAÇÕES

Se houver dúvidas sobre a escolha, a compra, a instalação ou o uso do Gerenciador de Senhas Kaspersky, existem várias fontes de informações disponíveis de acordo com sua conveniência. Você pode escolher a mais adequada, de acordo com a importância e a urgência de sua pergunta.

NESTA SEÇÃO:

Fontes de informações para pesquisar sozinho.....	12
Discutindo os aplicativos da Kaspersky no fórum da Web.....	13
Entrando em contato com o Departamento de vendas.....	13

FONTES DE INFORMAÇÕES PARA VOCÊ PESQUISAR

A Kaspersky Lab oferece as seguintes fontes de informações sobre o aplicativo:

- página do aplicativo no site da Kaspersky Lab;
- página do aplicativo no site do Serviço de Suporte Técnico (na Base de Dados de Conhecimento);
- página do Serviço de Suporte do FastTrack
- sistema de Ajuda.

Página do aplicativo no site da Kaspersky Lab

Esta página <http://brazil.kaspersky.com/produtos/produtos-para-usuarios-domesticos/password-manager> fornece informações gerais sobre o aplicativo, seus recursos e opções.

Página do aplicativo no site do serviço de Suporte técnico (Base de dados de conhecimento)

Nesta página <http://support.kaspersky.com/kpm>, você encontra os artigos criados pelos especialistas do Serviço de Suporte Técnico.

Esses artigos contêm informações úteis, recomendações e perguntas frequentes sobre a compra, a instalação e o uso do aplicativo. Eles são classificados por assunto; por exemplo, Gerenciando a licença do produto, Configurando a atualização ou Eliminando falhas de operação. Os artigos podem responder às perguntas referentes a este aplicativo e também a outros produtos da Kaspersky Lab. Eles também podem conter notícias do Serviço de Suporte Técnico.

Serviço de Suporte do FastTrack

Nesta página de serviço, você encontra o banco de dados de perguntas frequentes com respostas referentes à operação do aplicativo. Para usar esse serviço, você precisará de uma conexão com a Internet.

- Para ir para a página do serviço, na janela principal do aplicativo, clique no link **Suporte** e, na janela que é aberta, clique no botão **Suporte do FastTrack**.

Sistema de Ajuda

O pacote de instalação do aplicativo inclui o arquivo da Ajuda completa e contextual, que contém informações sobre como gerenciar a proteção do computador (exibir o status de proteção, verificar diversas áreas do computador quanto à presença de vírus e executar outras tarefas). Além disso, no arquivo da Ajuda completa e contextual, você pode encontrar informações sobre cada janela do aplicativo, como a lista de suas configurações corretas e sua descrição, além da lista de tarefas que podem ser executadas.

Para abrir o arquivo de Ajuda, na janela desejada, clique no botão **Ajuda** ou pressione a tecla **F1**.

DISCUTINDO OS APLICATIVOS DA KASPERSKY NO FÓRUM DA WEB

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

Nesse fórum, é possível exibir os tópicos existentes, deixar seus comentários, criar novos tópicos e usar o mecanismo de pesquisa.

ENTRANDO EM CONTATO COM O DEPARTAMENTO DE VENDAS

Se você tiver dúvidas sobre como selecionar ou comprar o Gerenciador de Senhas Kaspersky, ou como prorrogar sua licença, ligue para o Departamento de Vendas no nosso escritório central em Moscou, pelos telefones:

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

O serviço está disponível em russo e em inglês.

Você também pode enviar suas dúvidas para os especialistas do Departamento de Vendas através do email sales@kaspersky.com.

GERENCIADOR DE SENHAS KASPERSKY

O Gerenciador de Senhas Kaspersky armazena e protege todos os seus dados pessoais (como senhas, nomes de usuário, contas em programas de mensagens na Internet, contatos, números de telefone, etc.). O Gerenciador de Senhas Kaspersky anexa as senhas e contas aos aplicativos do Microsoft Windows e às páginas da Web em que são usadas. Todas as informações são armazenadas em formato criptografado no Banco de Dados de Senhas, cujo acesso é protegido por uma Senha Mestra. Esses dados pessoais poderão ser acessados facilmente se o Banco de Dados de Senhas estiver desbloqueado. Depois de executar uma página da Web ou um aplicativo, o Gerenciador de Senhas Kaspersky insere automaticamente a senha, o nome de usuário e outros dados pessoais. Assim, você não precisa lembrar todas as senhas, basta lembrar uma.

O Gerenciador de Senhas Kaspersky é carregado por padrão ao iniciar o sistema. Esse componente é incorporado ao aplicativo, o que permite que os dados pessoais sejam gerenciados diretamente na janela do aplicativo.

O Gerenciador de Senhas Kaspersky monitora as ações de aplicativos com senhas e evita a interceptação e o roubo de dados pessoais. Esse componente verifica os aplicativos que usam senhas ou as solicitam a outros aplicativos antes de solicitar que você permita ou bloqueie uma ação suspeita.

Além disso, o Gerenciador de Senhas Kaspersky pode:

- salvar e usar suas senhas (veja a página [30](#));
- localizar contas, senhas, nomes de usuário e outras informações pessoais no Banco de Dados de Senhas (veja a página [30](#));
- gerar senhas fortes (veja a página [49](#)) ao registrar novas contas;
- salvar todas as senhas em dispositivos removíveis (veja a página [50](#));
- restaurar o Banco de Dados de Senhas da cópia de backup (veja a página [33](#));
- proteger senhas contra o acesso não autorizado (veja a página [21](#)).

ATIVANDO O APLICATIVO

O procedimento de ativação do aplicativo consiste em registrar uma chave de licença. O direito de usar a versão atual do aplicativo é garantido com base na chave de licença.

Cada versão do aplicativo tem sua própria chave de licença, que consiste em uma combinação de caracteres exclusiva. Sua chave de licença será recebida por email quando você comprar o Gerenciador de Senhas Kaspersky.

A chave de licença deve ser usada para a versão atual do aplicativo e para todas as atualizações.

Antes de instalar as atualizações da versão atual do aplicativo, verifique se a chave de licença foi salva.

O Gerenciador de Senhas Kaspersky é executado no modo totalmente funcional durante 30 dias a partir do momento da instalação. Quando a versão de avaliação expirar, algumas funções do aplicativo ficarão indisponíveis. Você pode ativar a licença durante a instalação inicial do Gerenciador de Senhas Kaspersky na janela do Assistente de Instalação (veja a página 36) ou a qualquer momento dentro do período de 30 dias, antes da expiração da versão de avaliação. Se você não tiver comprado a licença do aplicativo antes da ativação, poderá fazê-lo ao ativar o aplicativo.

Você também pode comprar a licença do Gerenciador de Senhas Kaspersky de uma das seguintes maneiras:

- na Loja Virtual da Kaspersky Lab;
- no menu de contexto do Gerenciador de Senhas Kaspersky – para fazer isso, selecione o item **Ativação** no menu de contexto do aplicativo;
- na janela de informações do aplicativo – para fazer isso, selecione o item **Ajuda** → **Sobre o Gerenciador de Senhas Kaspersky** no menu de contexto do aplicativo;
- ao desbloquear o Banco de Dados de Senhas usando a Senha Mestra – para fazer isso, clique no link **Comprar Chave de Licença online** na janela de desbloqueio;
- clicando no Botão de Legenda – para fazer isso, selecione **Ativação** no menu do Botão de Legenda.

Você pode ativar o aplicativo de uma das seguintes maneiras:

- No menu de contexto do aplicativo. Para fazer isso, selecione o item **Ajuda** → **Inserir Chave de Licença** no menu de contexto do aplicativo.
- Na janela de informações do aplicativo. Para fazer isso, selecione o item **Ajuda** → **Sobre o Gerenciador de Senhas Kaspersky** no menu de contexto do aplicativo.
- Ao desbloquear o Banco de Dados de Senhas usando a Senha Mestra. Para fazer isso, clique no link **Inserir sua Chave de Licença para ativar a versão comercial** na janela de desbloqueio.

➡ *Para ativar o aplicativo:*

1. No menu de contexto do Gerenciador de Senhas Kaspersky, selecione o item **Ajuda** → **Inserir Chave de Licença**.
2. Na janela que será aberta, alterne para a compra da licença, se necessário. Para fazer isso, clique no link **Comprar online**. Depois de comprar a licença, insira a chave de licença que você recebeu e a confirme.

INTERFACE DO GERENCIADOR DE SENHAS KASPERSKY

Neste capítulo, vamos examinar mais detalhadamente os principais princípios de trabalho com o Gerenciador de Senhas Kaspersky.



NESTA SEÇÃO:

Ícone da área de notificação	16
Menu de contexto do Gerenciador de Senhas Kaspersky	16
Janela do Gerenciador de Senhas Kaspersky	17
Janela Banco de Dados de Senhas	18
Janela de configurações do aplicativo	19
Botão de Legenda	19
Plug-ins	19
Ponteiro	20

ÍCONE DA ÁREA DE NOTIFICAÇÃO

Imediatamente depois de iniciar o Gerenciador de Senhas Kaspersky, seu ícone será exibido na área de notificação da barra de tarefas do Microsoft Windows.

Dependendo da situação, o ícone do Gerenciador de Senhas Kaspersky terá os seguintes formatos:

-  ativo (verde) – o Gerenciador de Senhas Kaspersky está desbloqueado, o acesso a seus dados pessoais é permitido;
-  inativo (vermelho) – o Gerenciador de Senhas Kaspersky está bloqueado, seus dados pessoais estão inacessíveis.

É possível acessar os seguintes itens da interface clicando no ícone:

- menu de contexto (veja a página [16](#));
- Ponteiro do Gerenciador de Senhas Kaspersky.

MENU DE CONTEXTO DO GERENCIADOR DE SENHAS KASPERSKY

O menu de contexto do Gerenciador de Senhas Kaspersky dá acesso às principais tarefas e contém os seguintes itens:

- **Bloquear/Desbloquear** – permitir ou bloquear o acesso a seus dados pessoais.

- **Contas** – acessar rapidamente as contas mais usadas. O número de contas no Banco de Dados de Senhas é especificado entre colchetes. A lista de contas mais usadas é criada automaticamente. A lista estará disponível se estiver configurada para ser exibida no menu de contexto (veja a página [37](#)). Quando o aplicativo é executado pela primeira vez, a lista não estará disponível, pois nenhum registro terá sido usado.
- **Notas Seguras** – acessar rapidamente as notas particulares. O número de notas seguras no Banco de Dados de Senhas é especificado entre colchetes.
- **Adicionar Conta** – adicionar uma nova conta ao Gerenciador de Senhas Kaspersky.
- **Gerenciador de Senhas** – alternar para a janela principal do aplicativo (veja a página [17](#)).
- **Configurações** – configurar o aplicativo.
- **Versão portátil** – executar o Assistente para Criação da Versão Portátil (veja a página [50](#)).
- **Gerador de Senhas** – criar senhas fortes (veja a página [49](#)).
- **Ajuda** – exibir o sistema de Ajuda do Kaspersky Password Manager.
- **Sair** – fechar o aplicativo. Quando esta opção está selecionada, o aplicativo é descarregado da RAM do computador.

Se o aplicativo não estiver desbloqueado, o acesso a seus dados pessoais estará bloqueado. Nesse caso, o menu de contexto conterá apenas os seguintes itens: **Desbloquear**, **Gerador de Senhas**, **Ajuda** e **Sair**.

➔ *Para abrir o menu de contexto,*

passa o cursor sobre o ícone do Gerenciador de Senhas Kaspersky na área de notificação da barra de tarefas e clique nele com o botão direito do mouse.

JANELA DO GERENCIADOR DE SENHAS KASPERSKY

A janela do **Gerenciador de Senhas Kaspersky** consiste em três partes:

- um botão para bloquear e desbloquear o Banco de Dados de Senhas (veja a página [21](#));
- botões de legenda para acessar as principais funções do Gerenciador de Senhas Kaspersky: criar senhas, identidades, gerenciar o Banco de Dados de Senhas, configurar o aplicativo, criar e sincronizar a versão portátil do Gerenciador de Senhas Kaspersky (indisponível quando o Banco de Dados de Senhas está bloqueado);
- o botão Gerador de senhas (veja a página [49](#)).

Você também pode usar os seguintes botões e links:

- **Ajuda** – exibe o sistema de Ajuda do Gerenciador de Senhas Kaspersky;
- **Voltar** – alterna para a janela principal do Gerenciador de Senhas Kaspersky.

JANELA BANCO DE DADOS DE SENHAS

A janela Banco de Dados de Senhas consiste em três partes:

- na parte superior da janela, é possível selecionar rapidamente as funções do Gerenciador de Senhas Kaspersky e executar as principais tarefas;
- a parte central da janela contém uma lista de todas as contas e outros dados pessoais, e permite gerenciar suas informações pessoais;
- a parte inferior da janela contém links para gerenciar o Banco de Dados de Senhas como um todo.

Você também pode usar o campo de pesquisa na parte superior da janela. O campo de pesquisa ajuda a localizar as informações necessárias no Banco de Dados de Senhas usando uma palavras-chave.

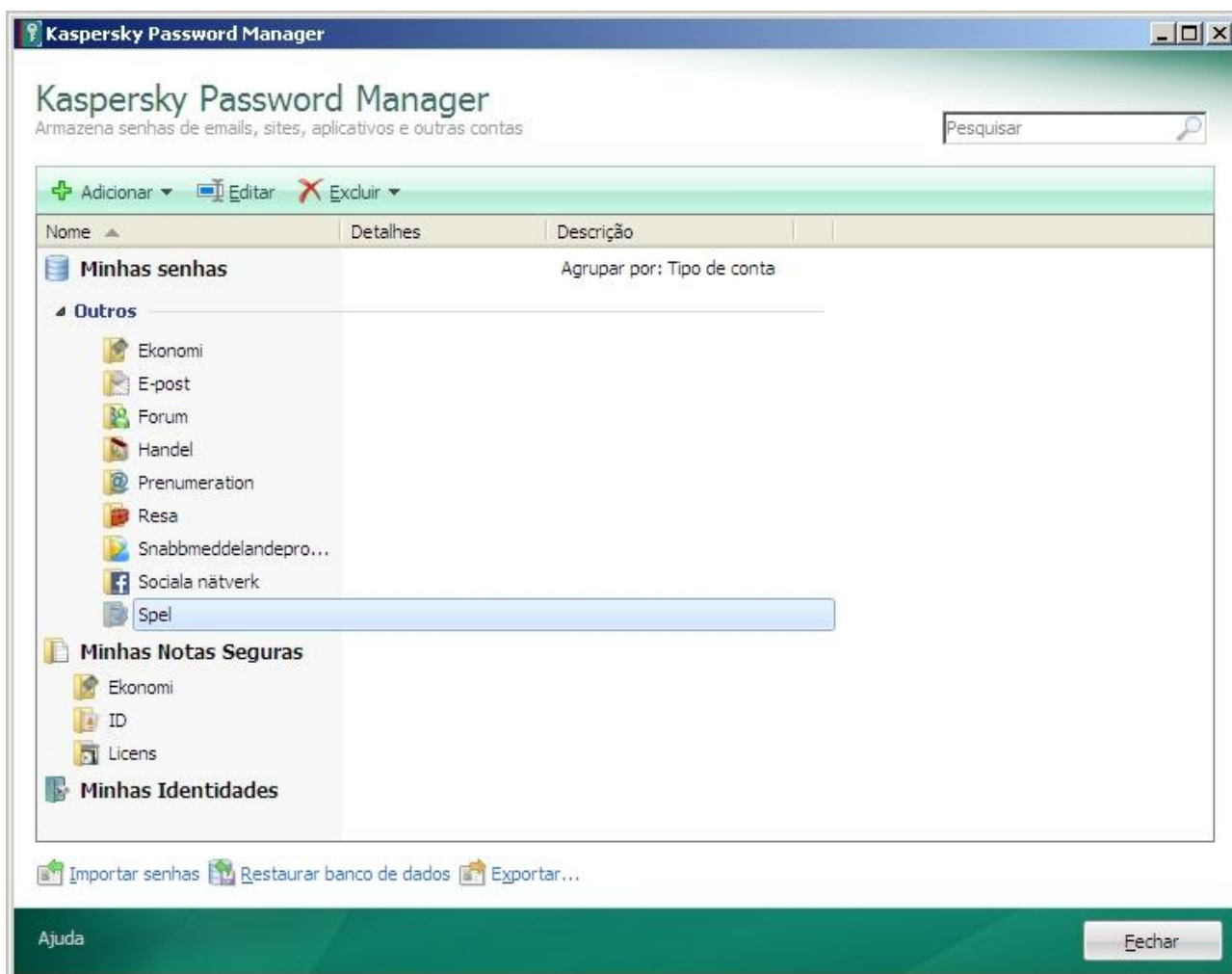


Figura 1. Janela Banco de Dados de Senhas

JANELA DE CONFIGURAÇÕES DO APLICATIVO

A janela de configurações do Gerenciador de Senhas Kaspersky pode ser aberta das seguintes maneiras:

- no menu de contexto do Gerenciador de Senhas Kaspersky (veja a página [16](#)) – para fazer isso, selecione **Configurações** no menu de contexto do Gerenciador de Senhas Kaspersky;
- na janela principal do Gerenciador de Senhas Kaspersky – para fazer isso, clique no botão **Configurações**.


A janela de configurações do aplicativo consiste em duas partes:

- à esquerda da janela há uma lista de funções do aplicativo;
- à direita da janela há uma lista de configurações da função, tarefa, etc. escolhida.


BOTÃO DE LEGENDA

O Botão de Legenda permite trabalhar com dados pessoais na janela do aplicativo/navegador. Esse botão está localizado no canto superior direito do aplicativo.

Ao clicar no Botão de Legenda, é aberto um menu com uma lista de nomes de usuário relacionados ao aplicativo/à página da Web. Ao selecionar um nome de usuário, o Gerenciador de Senhas Kaspersky preenche automaticamente os campos de autorização usando os dados do Banco de Dados de Senhas.

O Botão de Legenda está ativo  quando o Gerenciador de Senhas Kaspersky não está bloqueado (veja a página [21](#)). Clique nele para:

- **Adicionar Conta** – adicionar uma nova conta.
- **Editar Conta** – adicionar um nome de usuário/editar a conta ativa. O item de menu está disponível quando a conta está ativada.
- **Contas da Web** – exibir a lista de todas as contas da Web e abrir uma delas. O número de contas no Banco de Dados de Senhas é especificado entre colchetes.
- Lista de contas mais usadas – abre uma conta da lista. A lista é gerada automaticamente com base na frequência com que as contas são usadas. A lista estará disponível se estiver configurada para ser exibida no menu de contexto (veja a página [37](#)).
- **Identidades** – exibir a lista de Identidades criadas e selecionar uma Identidade para o formulário de registro.
- **Ajuda** – alternar para o sistema de ajuda do aplicativo.

O Botão de Legenda está inativo  quando o Gerenciador de Senhas Kaspersky está bloqueado. Nesse caso, nenhuma ação será executada ao clicar no botão. O botão inativo é exibido na janela do aplicativo quando as configurações do Botão de Legenda são configurados adicionalmente (veja a página [49](#)).

PLUG-INS

O Gerenciador de Senhas Kaspersky possui plug-ins incorporados em aplicativos que exigem autorização. Você pode instalar plug-ins de forma independente para os navegadores necessários. Os plug-ins instalados fornecem acesso a funções do Gerenciador de Senhas Kaspersky a partir da interface do aplicativo/navegador.

PONTEIRO

O ponteiro do Gerenciador de Senhas Kaspersky permite escolher rapidamente o aplicativo/a página da Web para entrada automática de dados pessoais.

➡ *Para usar o ponteiro do Gerenciador de Senhas Kaspersky:*

1. Aponte o cursor do mouse para o ícone do Gerenciador de Senhas Kaspersky na área de notificação da barra de tarefas e aguarde alguns segundos.
2. Quando ele for exibido, arraste o ponteiro do Gerenciador de Senhas Kaspersky para a janela do aplicativo/página da Web desejada. O Gerenciador de Senhas Kaspersky define automaticamente a ação que deve ser executada com o aplicativo/a página da Web escolhida.

GERENCIAMENTO DO BANCO DE DADOS DE SENHAS

O Banco de Dados de Senhas armazena todas as contas para aplicativos e páginas da Web com um ou vários nomes de usuário, além de Identidades (cartões que contêm, por exemplo, informações de contato, números de telefone, números de programas de mensagens na Internet, etc.).

Você poderá usar o Banco de Dados de Senhas se ele estiver desbloqueado (veja a página [21](#)). Antes de inserir alterações no Banco de Dados de Senhas, é recomendável definir as configurações de backup (veja a página [41](#)). Se esses dados forem alterados ou excluídos acidentalmente, use a Restauração do Banco de Dados de Senhas (veja a página [33](#)).

Você pode executar as seguintes ações:

- adicionar (veja a página [22](#)), alterar, excluir (veja a página [31](#)) dados particulares;
- importar/exportar (veja a página [31](#)), restaurar (veja a página [33](#)) o Banco de Dados de Senhas.

NESTA SEÇÃO:

Acessando o Banco de Dados de Senhas	21
Adicionando dados pessoais.....	22
Usando dados pessoais	30
Localizando senhas	30
Excluindo dados pessoais.....	31
Importando/exportando dados	31
Backup / Restauração do Banco de Dados de Senhas	33

ACESSANDO O BANCO DE DADOS DE SENHAS

Para acessar o Banco de Dados de Senhas, selecione um dos seguintes métodos de autorização:

- **Proteção da Senha Mestra.** A Senha Mestra é usada para acessar o Banco de Dados de Senhas.
- **Dispositivo USB.** Para acessar o Banco de Dados de Senhas, conecte qualquer dispositivo USB ao computador. Quando o dispositivo USB estiver desativado, o Banco de Dados de Senhas será bloqueado automaticamente.
- **Dispositivo Bluetooth.** Para acessar o Banco de Dados de Senhas, conecte um dispositivo Bluetooth ao computador. Quando o dispositivo Bluetooth estiver desativado, o Banco de Dados de Senhas será bloqueado automaticamente.
- **Sem autorização.** O acesso ao Banco de Dados de Senhas estará desprotegido.

Por padrão, a proteção é definida pela Senha Mestra, ou seja, você precisa lembrar apenas de uma senha.

A Senha Mestra é a ferramenta básica que protege seus dados pessoais. Se você tiver selecionado um método de autorização que usa um dispositivo e ele não estiver disponível (ou for perdido), você poderá usar a Senha Mestra para acessar seus dados pessoais.

Por padrão, o Gerenciador de Senhas Kaspersky bloqueia o Banco de Dados de Senhas quando o aplicativo é executado e depois de um tempo especificado durante o qual o computador não é usado (veja a página [43](#)). O aplicativo poderá ser usado somente se o Banco de Dados de Senhas estiver desbloqueado.

Você também pode bloquear/desbloquear o Banco de Dados de Senhas usando um dos seguintes métodos:

- na janela do Gerenciador de Senhas Kaspersky (veja a página [17](#));
- usando um dispositivo USB ou Bluetooth - somente para autorização com um dispositivo USB ou Bluetooth;
- clicando duas vezes no ícone do aplicativo (veja a página [47](#)) - nesse caso, a ação Ao clicar duas vezes deve ser configurada adicionalmente;
- no menu de contexto do Gerenciador de Senhas Kaspersky (veja a página [16](#));
- pressionando o atalho CTRL+ALT+L (veja a página [39](#)).

Para inserir a Senha Mestra, use um teclado virtual que permita a inserção de senhas sem pressionar o teclado.

➤ *Para bloquear um aplicativo no menu de contexto do aplicativo:*

1. Clique com o botão direito do mouse no ícone do Gerenciador de Senhas Kaspersky na área de notificação da barra de tarefas.
2. No menu que é aberto, selecione o item **Bloquear**.

➤ *Para desbloquear o Banco de Dados de Senhas no menu de contexto:*

1. Clique com o botão direito do mouse no ícone do Gerenciador de Senhas Kaspersky na área de notificação da barra de tarefas.
2. No menu exibido, selecione **Desbloquear**.
3. Insira a Senha Mestra na janela exibida.

ADICIONANDO DADOS PESSOAIS

Será possível adicionar dados pessoais se o Banco de Dados de Senhas não estiver bloqueado (veja a página [21](#)). Ao executar um aplicativo/uma página da Web, uma nova conta é reconhecida automaticamente se ela não tiver sido encontrada no Banco de Dados de Senhas. Após a autorização no aplicativo/na página da Web, o Gerenciador de Senhas Kaspersky poderá então adicionar dados pessoais ao Banco de Dados de Senhas.

Os seguintes tipos de dados pessoais estão disponíveis no Banco de Dados de Senhas:

- **Conta.** Combinação de um nome de usuário e senha para autorização na página da Web ou no programa.
- **Grupo de contas.** Usado para organizar contas no Banco de Dados de Senhas.
- **Nome de usuário.** Por padrão, o Gerenciador de Senhas Kaspersky oferece a opção de criar uma conta com um nome de usuário. Um nome de usuário adicional é usado quando os aplicativos ou páginas da Web permitem a criação de vários nomes de usuário para acessar seus recursos.
- **Identidade.** Usada para armazenar dados como sexo, data de nascimento, informações de contato, número de telefone, local de trabalho, número de programas de mensagens na Internet, endereço da página na Web, etc. É possível criar várias identidades para separar informações pessoais e comerciais.

- **Nota Segura.** Usada para armazenar qualquer informação.

CONTA

O Gerenciador de Senhas Kaspersky reconhece automaticamente uma nova conta se ela não tiver sido encontrada no Banco de Dados de Senhas. Após a autorização no aplicativo/na página da Web, o Gerenciador de Senhas Kaspersky permite salvar dados no Banco de Dados de Senhas. Também é possível adicionar uma nova conta ao Banco de Dados de Senhas manualmente.

A conta contém os seguintes dados:

- tipo de conta (conta de aplicativo ou conta da Internet);
- nome do usuário/vários nomes de usuário;
- senha;
- caminho do aplicativo/endereço de Internet da página da Web (dependendo do tipo de conta);
- configurações que definem as relações entre a conta e o objeto;
- configurações de ativação da conta;
- comentários;
- configurações de preenchimento de campos adicionais na página da Web.

O Gerenciador de Senhas Kaspersky permite usar uma ou várias contas para autorização no programa ou no site.

O Gerenciador de Senhas Kaspersky permite especificar um escopo para cada conta com base no caminho do aplicativo ou no endereço de Internet da página da Web.

Você pode adicionar uma conta de diversas maneiras:


- clicando no Botão de Legenda – para fazer isso, selecione **Adicionar Conta** no menu do Botão de Legenda;
- no menu de contexto do Gerenciador de Senhas Kaspersky – para fazer isso, selecione **Adicionar Conta** no menu de contexto do Gerenciador de Senhas Kaspersky;
- na janela principal do Gerenciador de Senhas Kaspersky;

➡ *Para adicionar uma nova conta na janela principal:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, clique no botão **Banco de Dados de Senhas**.
4. Na parte superior da janela que é aberta, clique no botão **Adicionar** e selecione o item **Adicionar Conta**.
5. No Assistente para Criação de Contas que é aberto, selecione o tipo de conta (Contas da Web, Contas de Aplicativo ou modo especializado) e clique em **Avançar**.
 - Se você tiver selecionado uma conta da Internet ou uma conta de aplicativo, especifique o site ou o aplicativo para o qual a conta será usada e clique em **Avançar**.
 - Se você tiver selecionado o modo avançado, na guia **Links**, especifique o caminho do aplicativo/da página da Web e defina as configurações de uso da conta.

6. Na parte superior do campo **Nome da Conta**, insira ou edite o nome da nova conta.
7. Na guia **Informações do Login**, insira o nome de usuário (login) e a senha.

O nome de usuário pode consistir em uma ou em várias palavras. Para especificar palavras-chave (veja a página [24](#)) para o nome de usuário, clique em .

Para copiar um nome de usuário/uma senha para a área de transferência, clique no botão .

Para copiar um nome de usuário de outra conta, siga o link **Usar o Login compartilhado de outra Conta**.


Para criar uma senha automaticamente, clique no link **Criar nova senha** (veja a página [49](#)).


8. Na guia **Edição manual de formulário**, modifique as configurações de preenchimento de outros campos da página da Web, se necessário.
9. Se necessário, na guia **Comentários**, insira algum texto explicativo para a conta. Para exibir comentários em uma notificação depois de ativar a conta, marque a caixa **Mostrar comentários na notificação**.

PESQUISA DE PALAVRAS-CHAVE

É possível usar palavras-chave para fazer uma pesquisa rápida de dados pessoais no Banco de Dados de Senhas. Elas são geradas para cada nome de usuário. É recomendável atribuir palavras-chave ao adicionar uma conta (veja a página [23](#))/um nome de usuário (veja a página [28](#)).

➡ *Para especificar palavras-chave para o nome de usuário:*


1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, clique no botão **Banco de Dados de Senhas**.
4. Selecione um nome de usuário na lista **Minhas senhas** e, na parte superior da janela, clique no botão **Editar**.
5. Na janela que é aberta, clique em  ao lado do campo **Login** e preencha o campo **Descrição**.


Se foi escolhida uma conta com um nome de usuário, na janela **Conta com Login único**, na guia **Informações do login**, clique em .

ADICIONANDO UM CAMINHO AO PROGRAMA/PÁGINA DA WEB


Para conectar uma conta a um aplicativo ou uma página da Web, você deve criar um link. Para uma página da Web, um link é um endereço Web. Para um aplicativo, um link é um caminho para o arquivo executável do aplicativo no computador. Sem esses dados, a conta não será anexada a nenhum aplicativo/nenhuma página da Web.

É possível anexar a conta a um programa/uma página da Web das seguintes maneiras:


- seguindo o link  na lista dos sites escolhidos do navegador ou na lista de aplicativos no computador;
- especificando manualmente o caminho do aplicativo/da página da Web;
- usando o ponteiro do Gerenciador de Senhas Kaspersky.

Para verificar o caminho inserido, inicie o aplicativo/a página da Web clicando em .

➤ *Para selecionar um link na lista:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, clique no botão **Banco de Dados de Senhas**.
4. Na parte superior da janela, clique no botão **Adicionar** e selecione o item **Adicionar Conta**.
5. Na janela que é aberta, na guia **Links**, no campo **Link**, clique em .
6. Na janela que é aberta, no campo **Link**, insira o caminho do aplicativo/da página da Web.

Para especificar uma página da Web da lista de páginas salvas (Favoritos), na lista **Marcadores**, clique no link **Copiar link de Favoritos**. Para copiar o caminho da página da Web da janela do navegador, clique no link **Use o caminho para o aplicativo vinculado**.

Para criar um link para o aplicativo, no campo **Link**, clique no botão  e especifique o caminho do arquivo executável do aplicativo.

➤ *Para especificar o caminho do programa/da página da Web manualmente:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, clique no botão **Banco de Dados de Senhas**.
4. Na parte superior da janela, clique no botão **Adicionar** e selecione o item **Adicionar Conta**.
5. Na janela que é aberta, na guia **Link**, no campo **Link**, insira o caminho do programa/endereço da página da Web. O endereço da página da Web deve iniciar com <http://www>.

➤ *Para inserir o caminho do programa/da página da Web usando o ponteiro do Gerenciador de Senhas Kaspersky:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, clique no botão **Banco de Dados de Senhas**.
4. Na parte superior da janela, clique no botão **Adicionar** e selecione o item **Adicionar Conta**.
5. Na janela que é aberta, na guia **Links**, no campo **Link**, insira o caminho do programa/da página da Web movendo o ponteiro do Gerenciador de Senhas Kaspersky para a janela do aplicativo/navegador.

SELECIONANDO UM MÉTODO PARA ANEXAR A CONTA

Para determinar quais dados de conta devem ser inseridos automaticamente cada vez que o aplicativo/a página da Web for iniciado, o Gerenciador de Senhas Kaspersky usa o caminho do aplicativo/o endereço de Internet da página da Web.

Como o Gerenciador de Senhas Kaspersky permite usar várias contas para um único aplicativo/site, você deve especificar um escopo para cada conta.

O Gerenciador de Senhas Kaspersky permite criar um escopo para cada conta com base no caminho do aplicativo/endereço de Internet da página da Web. O escopo pode ser configurado ao criar a conta (veja a página [23](#)). Você pode alterar as configurações no futuro.

Dependendo do objeto (aplicativo ou site), as formas como as contas são usadas variam.

As seguintes opções estão disponíveis para o aplicativo:

- Usar a conta para o aplicativo. A conta será usada em todas as caixas de diálogo do aplicativo que tiverem campos para inserir dados pessoais.
- Reconhecer por cabeçalho da janela. A conta será usada somente na janela do aplicativo específica.

Por exemplo, um aplicativo pode usar várias contas. Para contas diferentes, apenas os cabeçalhos das janelas serão diferentes em um aplicativo. O Gerenciador de Senhas Kaspersky inserirá automaticamente os dados da conta de acordo com o cabeçalho da janela do aplicativo.

As seguintes opções estão disponíveis para usar uma conta para páginas da Web:

- Apenas para a página da Web específica. O Gerenciador de Senhas Kaspersky adiciona automaticamente o nome de usuário e a senha aos campos de identificação apenas na página da Web específica.

Por exemplo, se a conta estiver relacionada a uma página da Web com o endereço <http://www.web-site.com/login.html>, ela não será válida para outros sites, como <http://www.web-site.com/pointer.php>.

- Para sites de um diretório. O Gerenciador de Senhas Kaspersky adiciona automaticamente o nome de usuário e a senha aos campos de identificação de todas as páginas da Web na pasta mais recente.

Por exemplo, se o endereço do site <http://www.web-site.com/cgi-bin/login.html> foi inserido, a conta será usada para páginas da Web na pasta *cgi-bin*.

- No site: <nome de domínio de terceiro nível e inferiores>. Esta conta é usada para qualquer página da Web no domínio (domínio de terceiro nível e inferiores).

Por exemplo, o Gerenciador de Senhas Kaspersky adiciona automaticamente dados de identidade nas seguintes páginas da Web: <http://www.domain1.domain2.web-site.com/login.html> ou <http://www.domain1.domain2.web-site.com/index.php>. No entanto, a conta não será usada em páginas da Web com endereços que têm domínios de quarto nível diferentes: <http://www.domain3.domain2.web-site.com/pointer.php> ou <http://www.domain4.domain2.web-site.com/pointer.php>.

- No site: <nome do site>. A conta será usada em todas as páginas da Web com campos para inserir nomes de usuário e senhas.

Por exemplo, o Gerenciador de Senhas Kaspersky adiciona automaticamente cartões de identidade nas seguintes páginas da Web: <http://www.domain1.domain2.web-site.com/login.html>, <http://www.domain2.domain2.web-site.com/index.php>, <http://www.domain3.domain2.web-site.com/index.php> ou <http://www.domain4.domain2.web-site.com/index.php>.

➔ *Para definir parâmetros para usar uma conta:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, clique no botão **Banco de Dados de Senhas**.
4. Selecione uma conta na lista **Minhas senhas** e clique no botão **Editar**.
5. Na janela que é aberta, na guia **Links**, selecione uma das opções para usar a conta.

ATIVÇÃO AUTOMÁTICA DA CONTA

Por padrão, a ativação automática da conta está ativa. O Gerenciador de Senhas Kaspersky insere apenas o nome de usuário e a senha nos campos de identificação. Você pode definir parâmetros adicionais de ativação da conta (veja a página [23](#)).

Um intervalo de endereços Web nos quais a ativação automática é usada é especificado adicionalmente para a página da Web.

As seguintes opções estão disponíveis para a ativação da conta:

- Para a página da Web escolhida. A conta será ativada somente para a página da Web específica.
- Para o site. A conta será ativada em todas as páginas do site.

➔ *Para definir a ativação automática da conta:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, clique no botão **Banco de Dados de Senhas**.
4. Selecione uma conta na lista **Minhas senhas** e clique no botão **Editar**.
5. Na janela que é aberta, na guia **Links**, marque a caixa **Ativar automaticamente a Conta após o carregamento**.

Além disso, especifique um dos métodos para ativar a conta para a página da Web.

PREENCHENDO CAMPOS ADICIONAIS

Durante a autorização em um site, frequentemente são solicitados outros dados, além do nome de usuário e da senha. O Gerenciador de Senhas Kaspersky pode preencher os campos adicionais automaticamente. Você pode definir opções de preenchimento automático de campos adicionais para a conta.

Será possível definir opções para campos adicionais se o caminho do aplicativo/endereço do site for especificado.

Para definir opções para campos, o Gerenciador de Senhas Kaspersky carrega a página da Web temporariamente e analisa todos os campos e botões. Os campos e botões são mesclados em grupos para cada página da Web.

O Gerenciador de Senhas Kaspersky salva arquivos e imagens temporariamente no computador a partir da página da Web carregada.

➔ *Para definir opções de campos adicionais:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, clique no botão **Banco de Dados de Senhas**.
4. Selecione uma conta na lista **Minhas senhas** e clique no botão **Editar**.
5. Na janela que é aberta, na guia **Edição manual de formulário**, clique no botão **Editar campos do formulário**.
6. Na parte superior da janela **Edição manual de formulário**, marque a caixa ao lado do campo ou botão desejado.
7. Ative o campo na coluna **Valor** do campo ou botão escolhido clicando duas vezes e defina os valores do campo.

CRIANDO UM GRUPO DE CONTAS

O uso de grupos de contas pode ajudar a organizar informações no Banco de Dados de Senhas. Um grupo consiste em uma pasta com contas adicionadas a ela.

Os grupos recém-criados são exibidos no menu de contexto do Gerenciador de Senhas Kaspersky: o item **Contas** →<Nome do grupo>.

➤ *Para criar um grupo de contas:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, clique no botão **Banco de Dados de Senhas**.
4. Na parte superior da janela, clique no botão **Adicionar** e selecione o item **Adicionar Grupo**.
5. Insira o nome do novo grupo.
6. Adicione contas da lista **Minhas senhas** arrastando-as para a pasta criada.


NOME DE USUÁRIO


Frequentemente são usados vários nomes de usuário para determinados aplicativos/sites. O Gerenciador de Senhas Kaspersky permite salvar vários nomes de usuário para uma conta. O Gerenciador de Senhas Kaspersky reconhece automaticamente um nome de usuário quando ele é usado pela primeira vez e oferece a opção de adicioná-lo a uma conta para um aplicativo/site. Você pode adicionar um novo nome de usuário manualmente para uma conta e então alterá-lo. É possível usar o mesmo nome de usuário para contas diferentes.

Você pode adicionar um novo nome de usuário para uma conta das seguintes maneiras:

- Clicando no Botão de Legenda. Para fazer isso, no menu do Botão de Legenda, selecione o item **Editar Conta** → **Adicionar Conta**.
- Na janela principal do aplicativo.

➤ *Para adicionar um nome de usuário para uma conta:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, clique no botão **Banco de Dados de Senhas**.
4. Selecione uma conta na lista **Minhas senhas**, clique no botão **Adicionar** e selecione o item **Adicionar Conta**.
5. Na janela que é aberta, insira o nome de usuário e a senha. O nome de usuário pode consistir em uma ou em várias palavras. Para especificar palavras-chave para um nome de usuário, clique em  e preencha o campo **Descrição**.

Para copiar um nome de usuário/uma senha para a área de transferência, clique em . Para criar uma senha automaticamente, siga o link **Gerar senha** (veja a página [49](#)).

Para copiar um nome de usuário de outra conta, siga o link **Usar o Login compartilhado de outra Conta**.

IDENTIDADE

Além do nome de usuário e da senha, frequentemente são usados outros dados pessoais para o registro no site; por exemplo, nome completo, ano de nascimento, sexo, endereço de email, número de telefone, país de residência, etc. O Gerenciador de Senhas Kaspersky pode armazenar todos esses dados em um Banco de Dados de Senhas criptografado, na forma de Identidades. Durante o registro em um novo site, o Gerenciador de Senhas Kaspersky preenche automaticamente o formulário de registro usando os dados de uma Identidade escolhida. Você pode usar

várias identidades para salvar informações particulares e comerciais separadamente. É possível alterar os parâmetros da Identidade posteriormente.

➤ *Para criar uma Identidade:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, clique no botão **Banco de Dados de Senhas**.
4. Clique no botão **Adicionar Identidade** na parte superior da janela.
5. Na janela que é aberta, no campo **Nome**, insira o nome da identidade.
6. Insira valores para os campos desejados e os ative clicando duas vezes na coluna **Valor**.

NOTA SEGURA

As Notas seguras foram criadas para armazenar informações de texto em formato criptografado (por exemplo, dados de passaporte, dados de contas bancárias, etc.) e para acessar rapidamente os dados salvos. O Gerenciador de Senhas Kaspersky inclui um conjunto de ferramentas de edição de texto padrão para ajudar a editar o texto da Nota segura. Ao criar uma Nota segura, você pode usar modelos com um conjunto de tipos de dados padrão (veja a página [46](#)).

Você pode alterar as configurações de Nota segura no futuro.

➤ *Para criar uma Nota segura do início:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, clique no botão **Banco de Dados de Senhas**.
4. Clique no botão **Criar Nota Segura** na parte superior da janela.
5. Na janela que é aberta, no campo **Nome**, insira o nome da Nota segura.
6. Insira as informações desejadas no editor de texto.

➤ *Para criar uma Nota segura com base em um modelo:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, clique no botão **Banco de Dados de Senhas**.
4. Clique no botão **Criar Nota Segura** na parte superior da janela.
5. Na janela que é aberta, no campo **Nome**, insira o nome da Nota segura.
6. Na parte inferior da janela, clique no botão **Selecionar modelo** e selecione o modelo desejado.
7. Preencha os dados exigidos e formate o texto, se necessário.

➤ *Para exibir a Nota segura,*

abra o menu de contexto do Gerenciador de Senhas Kaspersky e selecione **Notas Seguras** → <nome do grupo> → <nome da Nota segura>.

USANDO DADOS PESSOAIS

O Gerenciador de Senhas Kaspersky anexa as contas aos aplicativos/às páginas da Web em que são usadas. O Banco de Dados de Senhas procura automaticamente as contas anexadas quando os aplicativos/as páginas da Web são executados. Se for encontrada uma conta, os dados pessoais são inseridos automaticamente. Se não houver uma senha anexada no Banco de Dados de Senhas, o Gerenciador de Senhas Kaspersky oferecerá automaticamente a adição de uma senha ao Banco de Dados de Senhas (veja a página [23](#)).

Alguns aplicativos/sites podem usar vários nomes de usuário. O Gerenciador de Senhas Kaspersky permite salvar vários nomes de usuário para uma conta.

Se um novo nome de usuário for usado durante a autorização, o Gerenciador de Senhas Kaspersky oferecerá adicioná-lo à conta (veja a página [28](#)) para o aplicativo ou a página da Web aberta. Quando o aplicativo/a página da Web for executada novamente, uma janela com uma lista de nomes de usuário dessa conta será exibida ao lado dos campos de entrada de dados pessoais.

Além do nomes de usuário e da senha, frequentemente outros dados são usados para registro no site (por exemplo, nome completo, sexo, país, cidade, telefone, email, etc.). O Gerenciador de Senhas Kaspersky pode armazenar esses dados em um Banco de Dados de Senhas criptografado, na forma de Identidades.

Para separar informações particulares e comerciais, você pode criar várias Identidades (veja a página [28](#)). Então, quando você se registrar no programa/site, o Gerenciador de Senhas Kaspersky usará automaticamente o cartão escolhido para preencher o formulário de registro. O uso de Identidades economiza o tempo de preencher formulários de registro idênticos.

Durante a autorização no aplicativo/na página da Web, o Gerenciador de Senhas Kaspersky inserirá os dados pessoais automaticamente somente se o Banco de Dados de Senhas estiver desbloqueado.

É possível usar uma conta das seguintes maneiras:

- Execute o aplicativo/a página da Web. O formulário de autorização será preenchido automaticamente usando os dados da conta.
- Use o ponteiro do Gerenciador de Senhas Kaspersky. Para fazer isso, mova o cursor do mouse sobre o ícone do aplicativo na área de notificação da barra de tarefas e ative a conta arrastando o ponteiro do Gerenciador de Senhas Kaspersky para a janela do aplicativo/navegador desejado.
- Selecione a conta na lista de contas mais usadas. Para fazer isso, abra o menu de contexto do Gerenciador de Senhas Kaspersky e, nas contas mais usadas, selecione o registro desejado.
- Use o menu de contexto do Gerenciador de Senhas Kaspersky. Para fazer isso, abra o menu de contexto do Gerenciador de Senhas Kaspersky e selecione o item **Contas** → **<Nome da conta>**.

➔ *Para usar uma Identidade:*

1. Clique no Botão de Legenda no canto superior direito da janela do aplicativo/navegador.
2. No menu que é aberto, selecione o item **Identidades** → **<Nome da identidade>**. O Gerenciador de Senhas Kaspersky preenche automaticamente os campos do registro na página da Web usando os dados da Identidade.

LOCALIZANDO SENHAS

Uma pesquisa de dados pessoais pode ser comprometida nos seguintes casos:

- Algumas senhas não estão associadas com aplicativos/sites.
- O Banco de Dados de Senhas contém um grande número de contas.

O Gerenciador de Senhas Kaspersky localiza senhas rapidamente usando os seguintes parâmetros:

- nome da conta;
- nome de usuário;
- palavras-chave (veja a página [24](#)) (os parâmetros de pesquisa de palavras-chave são definidos adicionalmente para cada nome de usuário);
- endereço Web (para endereços Web).

A pesquisa é executada pelo nome completo e pelas letras iniciais e quaisquer caracteres incluídos no nome da conta ou link.

➤ *Para localizar uma conta/senha:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, clique no botão **Banco de Dados de Senhas**.
4. Na parte superior da janela, insira o texto no campo de pesquisa.

EXCLUINDO DADOS PESSOAIS

Antes de alterar dados pessoais, o Gerenciador de Senhas Kaspersky cria automaticamente uma cópia de backup do Banco de Dados de Senhas. Se esses dados forem alterados ou excluídos acidentalmente, use a Restauração do Banco de Dados de Senhas (veja a página [33](#)).

No Banco de Dados de Senhas, é possível excluir um ou todos os elementos.

➤ *Para excluir um elemento do Banco de Dados de Senhas:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, clique no botão **Banco de Dados de Senhas**.
4. Selecione um item na lista **Minhas senhas**, clique no botão **Excluir** e escolha **Excluir**.

➤ *Para excluir todos os elementos do Banco de Dados de Senhas:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, clique no botão **Banco de Dados de Senhas**.
4. Selecione um item na lista **Minhas senhas**, clique no botão **Excluir** e escolha **Excluir tudo**.

IMPORTANDO/EXPORTANDO DADOS

O Gerenciador de Senhas Kaspersky pode importar e exportar seu Banco de Dados de Senhas e objetos individuais do Banco de Dados de Senhas (Identidades, contas de usuário e Notas seguras).

Você pode importar as duas senhas de outros aplicativos de gerenciamento de senhas (por exemplo, Internet Explorer, Mozilla Firefox, KeePass), além de senhas que foram exportadas anteriormente usando o Gerenciador de Senhas Kaspersky.

As senhas são importadas de arquivos *.xml e *.ini.

O Gerenciador de Senhas Kaspersky pode exportar o Banco de Dados de Senhas para arquivos *.xml, *.html ou *.txt.

A exportação de senhas para um arquivo é conveniente para abrir senhas de acesso geral, imprimir o Banco de Dados de Senhas ou salvar uma cópia de backup do Banco de Dados de Senhas em um arquivo em outro formato para o Gerenciador de Senhas Kaspersky.

As senhas exportadas são armazenadas em arquivos não criptografados e não são protegidas do acesso não autorizado. Portanto, é recomendável considerar as formas de proteção dos arquivos exportados antecipadamente.

O Banco de Dados de Senhas é modificado ao ser importado. Você pode escolher uma das seguintes ações a serem executadas com o Banco de Dados de Senhas:

- **Substituir.** O Banco de Dados de Senhas atual será substituído pelo importado (todas as senhas armazenadas no Banco de Dados de Senhas do Gerenciador de Senhas Kaspersky antes da importação serão excluídas).
- **Mesclar.** As senhas importadas serão adicionadas ao Banco de Dados de Senhas. Ao mesclar, você tem a opção de importar contas no Gerenciador de Senhas Kaspersky.
- **Cancelar.** A importação de senhas será cancelada.

➔ *Para importar senhas de um arquivo:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, clique no botão **Banco de Dados de Senhas**.
4. Na parte inferior da janela, clique no link **Importar senhas**.
5. Na janela **Recuperar senhas não protegidas** que é aberta, selecione o aplicativo do qual as senhas serão importadas e clique em **Importar senhas**.
6. Na janela que é aberta, especifique o arquivo com as senhas que você deseja importar e clique em **Abrir**.
7. Na janela que é aberta, selecione a ação que deve ser executada com o Banco de Dados de Senhas.

➔ *Para salvar o Banco de Dados de Senhas em um arquivo:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, clique no botão **Banco de Dados de Senhas**.
4. Na parte inferior da janela, clique no link **Exportar**.
5. Na janela que é aberta, selecione o modo de exportação (exportar todo o Banco de Dados de Senhas ou objetos selecionados) e clique em **Avançar**.
6. Na janela que é aberta, selecione as configurações de exportação dos dados:
 - Se desejar proteger os dados que estão sendo exportados, selecione **Exportação segura** e especifique a senha para a proteção dos dados.

- Se desejar exportar os dados para um arquivo não protegido, selecione **Exportar sem criptografia** e especifique o formato do arquivo para exportação.
 - Para programar uma alteração de senha para dados exportados, marque a caixa de seleção **Use uma data de lembrete para ser notificado sobre a expiração de itens exportados** e escolha a data de expiração da senha. O Gerenciador de Senhas Kaspersky informará sobre a necessidade de alterar a senha.
7. Na janela que é aberta, especifique o caminho de exportação do arquivo e clique no botão **Avançar**.
 8. Na janela que é aberta, marque as configurações de exportação dos dados e inicie a exportação.

BACKUP / RESTAURAÇÃO DO BANCO DE DADOS DE SENHAS

Antes que o Banco de Dados de Senhas seja alterado, uma cópia de backup é criada automaticamente. O caminho da cópia de reserva é definido por padrão, mas você pode alterá-lo (veja a página [41](#)). A restauração de senhas é útil nos seguintes casos:

- se as alterações mais recentes precisarem ser canceladas;
- se o Banco de Dados de Senhas foi substituído ou excluído;
- se o Banco de Dados de Senhas atual ficou inacessível/danificado depois de uma falha de hardware ou do sistema.

Todos os dados na cópia de backup são armazenados em formato criptografado. O Gerenciador de Senhas Kaspersky registra todas as alterações do Banco de Dados de Senhas. No aplicativo, as cópias de backup são exibidas em uma lista e classificadas de acordo com sua data, iniciando da mais recente. Para cada cópia de backup, são fornecidos os seguintes dados:

- local;
- data e hora de criação;
- alterações em relação à versão anterior.

Você pode usar as cópias de backup para resolver as seguintes tarefas:

- restaurar um Banco de Dados de Senhas a partir de uma cópia de backup;
- excluir cópias de um armazenamento de backup;
- alterar o local das cópias de backup (veja a página [41](#)).

➡ *Para restaurar o Banco de Dados de Senhas:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, clique no botão **Banco de Dados de Senhas**.
4. Na parte inferior da janela, clique no link **Restaurar banco de dados**.
5. Na janela **Restaurar** que é aberta, selecione a data da cópia de backup na lista e, na parte superior da janela, clique em **Restaurar**.
6. Confirme a restauração clicando em **OK**.

➤ *Para remover cópias de backup desnecessárias:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, clique no botão **Banco de Dados de Senhas**.
4. Na parte inferior da janela, clique no link **Restaurar banco de dados**.
5. Na janela **Restaurar** que é aberta, na lista de cópias de backup, selecione as versões das cópias de backup que devem ser excluídas. Para selecionar várias versões, mantenha pressionada a tecla **CTRL**.
6. Clique em **Excluir**.
7. Na janela que é aberta, confirme a exclusão dos dados clicando em **OK**.

CONFIGURANDO O APLICATIVO

As configurações do aplicativo poderão ser definidas somente se o Banco de Dados de Senhas estiver desbloqueado (veja a página [21](#)). Ao editar as configurações, você pode:

- definir a hora em que o aplicativo é executado (veja a página [47](#));
- ativar notificações (veja a página [48](#));
- especificar o nome de usuário (veja a página [36](#)) que será usado por padrão ao criar uma nova conta;
- definir a hora em que a senha foi armazenada na área de transferência (veja a página [49](#));
- criar uma lista de contas mais usadas (veja a página [37](#));
- criar uma lista de sites ignorados (veja a página [38](#)), para os quais as funções do Gerenciador de Senhas Kaspersky não devem se aplicar;
- criar uma lista de sites confiáveis (veja a página [38](#)), para os quais o Gerenciador de Senhas Kaspersky permitirá o re-endereçamento;
- especificar uma combinação de teclas para executar as funções do Gerenciador de Senhas Kaspersky rapidamente (veja a página [39](#));
- alterar o caminho de armazenamento do Banco de Dados de Senhas (veja a página [39](#)) e das cópias de backup (veja a página [41](#));
- alterar o método de criptografia de dados (veja a página [42](#));
- definir o bloqueio automático do Banco de Dados de Senhas (veja a página [43](#));
- Alterar a Senha Mestra (veja a página [45](#));
- configurar o acesso o Banco de Dados de Senhas (veja a página [44](#));
- alterar o local do Botão de Legenda, criar uma lista de aplicativos compatíveis com o Botão de Legenda (veja a página [49](#));
- criar uma lista de aplicativos compatíveis (veja a página [45](#)).

➡ *Para editar as configurações do Gerenciador de Senhas Kaspersky:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. Na janela do Gerenciador de Senhas Kaspersky que é aberta, selecione a seção que deve ser editada.
5. À direita da janela, insira as alterações das configurações da seção escolhida.

NESTA SEÇÃO:

Assistente de Configuração	36
Nome de usuário padrão.....	36
Contas mais usadas.....	37
Endereços Web ignorados.....	38
Endereços Web confiáveis.....	38
Teclas de atalho.....	39
Local do arquivo do Banco de Dados de Senhas	39
Criando novo Banco de Dados de Senhas	41
Local da cópia de backup.....	41
Selecionando o método de criptografia.....	42
Bloqueio automático do Banco de Dados de Senhas	43
Alterando o método de autorização do Gerenciador de Senhas Kaspersky	44
Usando dispositivos USB e Bluetooth para a autorização	44
Alterando a Senha Mestra.....	45
Navegadores da Web com suporte.....	45
Gerenciando modelos de Notas seguras	46
Hora de execução do aplicativo	47
Ação Ao clicar duas vezes	47
Notificações.....	48
Hora em que a senha foi armazenada na área de transferência	49
Exibindo o Botão de Legenda	49

NOME DE USUÁRIO PADRÃO

O Gerenciador de Senhas Kaspersky permite especificar um nome de usuário que será exibido automaticamente no campo **Login** ao criar uma nova conta (veja a página [23](#)).

➤ *Para definir o nome de usuário padrão:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. À esquerda da janela que é aberta, selecione a seção **Geral**.

5. À direita da janela, preencha o campo **Login Padrão**.

CONTAS MAIS USADAS

O Gerenciador de Senhas Kaspersky fornece acesso rápido às contas. A lista de contas mais usadas é exibida na janela principal do aplicativo. Ela também pode ser exibida no menu de contexto e no menu do Botão de Legenda.

Essa lista contém os nomes de aplicativos/páginas da Web que você executa com mais frequência. Os itens da lista são organizados em ordem alfabética ou por frequência de uso.

A lista de contas mais usadas estará disponível no menu se o Banco de Dados de Senhas não estiver bloqueado (veja a página [21](#)).

Você pode definir as seguintes opções da lista:

- **Número de itens na lista** – o número máximo de contas mais usadas que são exibidas no menu de contexto do aplicativo;
- **Mostrar a lista no menu da bandeja do sistema** – a lista de contas mais usadas estará acessível no menu de contexto do Gerenciador de Senhas Kaspersky;
- **Exibir no menu do Botão de Legenda** – a lista de contas mais usadas estará acessível no menu do Botão de Legenda (na janela do aplicativo/navegador).

➔ *Para exibir as contas mais usadas no menu de contexto:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. À esquerda da janela, selecione a seção **Contas mais usadas**.
5. À direita da janela, marque a caixa **Mostrar a lista no menu da bandeja do sistema**.

Para exibir a lista de contas mais usadas no menu do Botão de Legenda, marque também a caixa **Exibir no menu do Botão de Legenda**.

Se a caixa **Mostrar a lista no menu da bandeja do sistema não estiver marcada, as outras opções da lista não poderão ser modificadas.**

6. Especifique o número de contas no campo **Tamanho da lista**.
7. Se necessário, modifique os itens da lista manualmente. Para remover um item da lista, selecione a conta desejada e clique em **Excluir**. Para excluir todos os itens da lista, clique em **Limpar**.

ENDEREÇOS WEB IGNORADOS

Você pode especificar uma lista de endereços Web nos quais o Gerenciador de Senhas Kaspersky não será usado. A entrada automática do nome de usuário e da senha fica desativada para os sites nessa lista. Além disso, o Gerenciador de Senhas Kaspersky não se oferecerá mais para criar uma nova conta (veja a página [23](#)) / um novo nome de usuário (veja a página [28](#)) para esses sites.

➤ *Para criar uma lista de endereços ignorados:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. À esquerda da janela, selecione a seção **Endereços Web ignorados**.
5. À direita da janela, clique em **Adicionar**, insira o endereço Web e pressione **ENTER**.

Para alterar um endereço Web, selecione-o na lista e clique em **Editar**. Para excluir um endereço Web da lista, selecione-o e clique em **Excluir**.

ENDEREÇOS WEB CONFIÁVEIS

O Gerenciador de Senhas Kaspersky protege seus dados pessoais de ataques de phishing. Se durante a autorização você for redirecionado para outro site, o aplicativo o notificará a respeito.

Frequentemente, os remetentes de phishing usam o redirecionamento para sites que dão acesso a contas bancárias (como sites de bancos virtuais, sistemas de pagamento, etc.). Na página de autorização oficial da empresa, os usuários são redirecionados para um site falso com aparência semelhante à da página oficial. Todos os dados inseridos na página falsa caem nas mãos dos invasores.

Muitas vezes, o redirecionamento é instalado oficialmente nos sites. Se não desejar que o Gerenciador de Senhas Kaspersky considere o re-endereçamento como um ataque de phishing, você poderá criar uma lista de endereços confiáveis. A lista de endereços confiáveis inclui os sites para os quais os dados pessoais inseridos são transferidos. Durante a autorização, o Gerenciador de Senhas Kaspersky não o notificará sobre a transferência de dados pessoais para o site confiável.

O Gerenciador de Senhas Kaspersky permite a transferência de dados pessoais de outros sites para o site confiável. Antes de adicionar um site à lista de endereços confiáveis, certifique-se de sua confiabilidade.

Você pode adicionar um site à lista de endereços confiáveis das seguintes maneiras:

- diretamente, durante a autorização no site;
- manualmente, na janela **Configurações do Gerenciador de Senhas Kaspersky**.

Para adicionar um site à lista de endereços confiáveis durante a autorização no site, aguarde para ser redirecionado de um site para outro e, em seguida, na janela do Gerenciador de Senhas Kaspersky, marque a caixa **Sempre confiar em site de <nome do site>**.

➤ *Para criar uma lista de endereços confiáveis manualmente:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.

4. À esquerda da janela, selecione a seção **Endereços Web confiáveis**.
5. À direita da janela, clique em **Adicionar**. O campo na lista **Endereços Web confiáveis** ficará ativo. Em seguida, insira o endereço Web e pressione **ENTER**.

Para alterar o endereço Web, selecione-o na lista e clique em **Editar**. Para excluir o endereço Web da lista, selecione-o e clique em **Excluir**.

TECLAS DE ATALHO

É conveniente usar teclas de atalho para acessar rapidamente determinadas funções do aplicativo.

Você pode especificar teclas de atalho para as seguintes ações:

- Bloquear/Desbloquear o Gerenciador de Senhas Kaspersky (veja a página [21](#)).
- Insira a senha.

Para acessar funções rapidamente, você pode especificar uma tecla ou uma combinação de duas ou três teclas.

Evite combinações de teclas usadas pelo Microsoft Windows para acessar funções.

➤ *Para especificar um atalho:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. À esquerda da janela, selecione a seção **Teclas de atalho**.
5. À direita da janela, defina a combinação de teclas desejada para cada ação.

LOCAL DO ARQUIVO DO BANCO DE DADOS DE SENHAS

O Banco de Dados de Senhas do Gerenciador de Senhas Kaspersky é um arquivo criptografado (veja a página [42](#)) que armazena todos os seus dados pessoais (contas, nomes de usuário, senhas e Identidades).

Os caminhos padrão em diferentes versões do Microsoft Windows são os seguintes:


- Microsoft Windows XP: C:\Documents and Settings\Nome_do_usuario\Meus Documentos\Passwords Database\;
- Microsoft Windows Vista: C:\Users\Nome_do_usuario\Documentos\Passwords Database\;
- Microsoft Windows 7: C:\Users\Nome_do_usuario\Meus Documentos\Passwords Database\.

Você pode usar diversas mídias para armazenar o Banco de Dados de Senhas: disco removível, disco local ou unidade de rede.


As seguintes ações são possíveis ao alterar o caminho ou o nome do Banco de Dados de Senhas:

- **Copiar** – cria uma cópia do Banco de Dados de Senhas com o caminho especificado. Essa cópia se tornará o Banco de Dados de Senhas ativo.
- **Mover** – o Banco de Dados de Senhas ativo será salvo com o caminho especificado.
- **Criar novo Banco de Dados de Senhas** – cria uma cópia vazia do Banco de Dados de Senhas que se tornará ativo.

➔ *Para mover ou renomear o Banco de Dados de Senhas:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. À esquerda da janela, selecione a seção **Minhas senhas**.
5. À direita da janela, em **Local**, clique no  localizado à direita do campo **Caminho**.
6. Na janela **Selecionar Banco de Dados de Senhas**, especifique o nome e o caminho do arquivo e clique no botão **Abrir**.
7. Na janela **Local do Banco de Dados de Senhas** que é aberta, selecione a ação que deve ser executada com o Banco de Dados de Senhas.
8. Na janela **Gerenciador de Senhas Kaspersky**, insira a Senha Mestra para confirmar as alterações.


➔ *Para alterar o Banco de Dados de Senhas atual:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. À esquerda da janela, selecione a seção **Minhas senhas**.
5. À direita da janela, em **Local**, clique no  localizado à direita do campo **Caminho**.
6. Na janela **Selecionar Banco de Dados de Senhas**, especifique o arquivo do Banco de Dados de Senhas e clique no botão **Abrir**.
7. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, insira a Senha Mestra para acessar o Banco de Dados de Senhas escolhido.

CRIANDO NOVO BANCO DE DADOS DE SENHAS

O Gerenciador de Senhas Kaspersky permite usar vários Bancos de Dados de Senhas de forma consistente. A criação de um novo Banco de Dados de Senhas permite que seus dados pessoais sejam separados e salvos em dois ou mais Bancos de Dados de Senhas. Se necessário, um Banco de Dados de Senhas antigo pode ser restaurado. O Gerenciador de Senhas Kaspersky poderá criar um novo Banco de Dados de Senhas, caso o Banco de Dados de Senhas atual esteja danificado ou não possa ser restaurado de uma cópia de backup.

➤ *Para criar um novo Banco de Dados de Senhas:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. À esquerda da janela, selecione a seção **Minhas senhas**.
5. À direita da janela, em **Local**, clique no  localizado à direita do campo **Caminho**.
6. Na janela **Selecionar Banco de Dados de Senhas**, especifique o local e o nome de arquivo do Banco de Dados de Senhas, e clique em **Abrir**.
7. Na janela **Local do Banco de Dados de Senhas** que é aberta, selecione a ação **Novo Banco de Dados de Senhas**.
8. Na janela **Novo Banco de Dados de Senhas**, em **Senha**, defina a senha de acesso ao novo banco de dados e a insira novamente no campo **Confirmar senha**.

Se a senha reinserida estiver incorreta, ela será realçada em vermelho.

Em **Algoritmo de criptografia**, selecione o provedor de criptografia e o método de criptografia desejado (veja a página [42](#)).

9. Na janela exibida, insira a nova Senha Mestra para confirmar a criação de um novo Banco de Dados de Senhas.

LOCAL DA CÓPIA DE BACKUP

Antes de salvar as alterações de seus dados pessoais, o Gerenciador de Senhas Kaspersky faz cópias de backup do Banco de Dados de Senhas automaticamente. Isso evita a perda de dados, em caso de falha do sistema ou técnica. O Gerenciador de Senhas Kaspersky cria uma cópia completa do Banco de Dados de Senhas antes de implementar as alterações.

Se o Banco de Dados de Senhas for danificado, você poderá restaurar os dados da cópia de backup mais recente do Banco de Dados de Senhas (veja a página [33](#)).


Você pode usar diversas mídias para armazenar a cópia de backup do Banco de Dados de Senhas: disco removível, disco local ou unidade de rede.

Por padrão, dependendo do sistema operacional, a cópia de backup é salva no seguinte caminho:

- Microsoft Windows XP: C:\Documents and Settings\Nome_do_usuario\Meus Documentos\Passwords Database\;
- Microsoft Windows Vista: C:\Users\Nome_do_usuario\Documentos\Passwords Database\;

- Microsoft Windows 7: C:\Users\Nome_do_usuario\Meus Documentos\Passwords Database\.

➡ Para alterar o caminho do arquivo de backup:

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. À esquerda da janela, selecione a seção **Minhas senhas**.
5. À direita da janela, em **Backup**, clique no botão  localizado à direita do campo **Caminho**.
6. Na janela **Procurar pasta**, selecione a pasta para a cópia de backup do Banco de Dados de Senhas.

SELECIONANDO O MÉTODO DE CRIPTOGRAFIA

A função da criptografia é proteger as informações do acesso e da distribuição não autorizados. O principal objetivo da codificação é transferir mensagens criptografadas através de canais desprotegidos.

As chaves são necessárias para a criptografia e a descryptografia. Uma chave é um componente essencial de uma codificação. Se uma única chave for usada para a criptografia e a descryptografia, ela é chamada de chave simétrica. Se forem usadas duas chaves, ela é assimétrica. As codificações simétricas podem ser em bloco ou em fluxo. Qualquer informação (independentemente do formato dos dados de origem) é interpretada em código binário. Uma codificação em bloco presume que todos os dados serão divididos em blocos e cada um deles passará então por uma transformação independente. Em uma codificação em fluxo, o algoritmo é aplicado a cada bit de informações.

O Gerenciador de Senhas Kaspersky oferece os seguintes algoritmos simétricos:

- **DES**. Codificação em bloco com a chave de tamanho padrão de 56 bits. Pelos padrões atuais, o DES não fornece um alto nível de proteção. Esse algoritmo é usado quando a confiabilidade não é o principal requisito.
- **3DES**. Um algoritmo em bloco criado com base no DES. Resolve os principais pontos fracos de seu predecessor, o tamanho pequeno da chave. As chaves 3DES são três vezes maiores que as usadas pelo DES ($56 \times 3 = 168$ bits). A velocidade de operação é três vezes menor que a do DES, mas o nível de segurança é muito maior. O 3DES é usado com mais frequência, pois o DES não é suficientemente resistente às técnicas de violação modernas.
- **DUAS CHAVES 3DES**. Um algoritmo em bloco criado com base no DES. Trata-se de um algoritmo 3DES que usa um tamanho de chave de 112 bits (56×2).
- **RC2**. Um algoritmo de codificação em bloco com uma chave de comprimento variável processa rapidamente uma grande quantidade de informações. É um algoritmo mais rápido que o DES. Em termos de segurança e resistência, é comparável ao 3DES.
- **RC4**. Uma codificação em fluxo com uma chave de comprimento variável. O tamanho da chave pode variar de 40 a 256 bits. As vantagens do algoritmo estão em sua alta velocidade e o tamanho variável da chave. Por padrão, o Gerenciador de Senhas Kaspersky usa o RC4 para criptografar os dados.
- **AES**. Um algoritmo simétrico de codificação em bloco com um comprimento de chave de 128, 192, 256 bits. Esse algoritmo garante um alto nível de segurança e é um dos mais usados.

O Microsoft Windows usa um provedor de criptografia para executar as operações criptográficas. Cada provedor de criptografia é compatível com diversos algoritmos de criptografia com um comprimento de chave especificado. O Gerenciador de Senhas Kaspersky usa os seguintes provedores de criptografia internos do Microsoft Windows:

- Microsoft Base Cryptographic Provider;
- Microsoft Enhanced Cryptographic Provider;

- Microsoft Enhanced RSA and AES Cryptographic Provider (Prototype);
- Microsoft RSA/Schannel Cryptographic Provider;
- Microsoft Strong Cryptographic Provider.

➔ *Para alterar o algoritmo de criptografia:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. À esquerda da janela, selecione a seção **Minhas senhas**.
5. À direita da janela, em **Criptografia**, clique em **Alterar**.
6. Na janela **Algoritmo de criptografia** que é aberta, especifique as configurações da criptografia.

BLOQUEIO AUTOMÁTICO DO BANCO DE DADOS DE SENHAS

O Gerenciador de Senhas Kaspersky bloqueia automaticamente o Banco de Dados de Senhas depois de executar um aplicativo e depois de um tempo especificado durante o qual o computador não foi usado. Você pode especificar o intervalo de tempo após o qual o Banco de Dados de Senhas será bloqueado. O valor do intervalo varia de 1 a 60 minutos. É recomendável bloquear o Banco de Dados de Senhas depois de 5-20 minutos de inatividade do computador. Também é possível desativar o bloqueio automaticamente do Banco de Dados de Senhas.

O Gerenciador de Senhas Kaspersky bloqueia o Banco de Dados de Senhas automaticamente depois de um período definido de inatividade do computador. Se o bloqueio automático do computador estiver desativado, seus dados estarão desprotegidos caso você saia de perto do computador sem bloqueá-lo manualmente.

➔ *Para modificar o intervalo após o qual o Banco de Dados de Senhas é bloqueado:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. À esquerda da janela, selecione a seção **Minhas senhas**.
5. À direita da janela, em **Bloqueio automático**, use a lista suspensa para selecionar o tempo depois do qual o Banco de Dados de Senhas será bloqueado.

Para desativar o bloqueio do Banco de Dados de Senhas, selecione **Nunca**.

ALTERANDO O MÉTODO DE AUTORIZAÇÃO DO GERENCIADOR DE SENHAS KASPERSKY

A autorização permite controlar o acesso a seus dados pessoais. Você escolhe o método de autorização ao iniciar o Gerenciador de Senhas Kaspersky pela primeira vez, mas, se necessário, o método de autorização pode ser alterado.

➤ *Para alterar o método de autorização:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. À esquerda da janela, selecione a seção **Método de autorização**.
5. À direita da janela, em **Método de autorização**, selecione uma opção de autorização na lista suspensa.


CONSULTE TAMBÉM:

Usando dispositivos USB e Bluetooth para a autorização [44](#)

USANDO DISPOSITIVOS USB E BLUETOOTH PARA A AUTORIZAÇÃO


Para acessar o Banco de Dados de Senhas (veja a página [44](#)), o Gerenciador de Senhas Kaspersky permite usar diversos dispositivos USB e Bluetooth.

➤ *Para usar um dispositivo USB para acessar o Banco de Dados de Senhas:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. À esquerda da janela, selecione a seção **Método de autorização**.
5. À direita da janela, em **Método de autorização**, selecione o **Dispositivo USB** na lista suspensa.
6. Conecte o dispositivo removível ao computador.
7. Selecione um dispositivo na lista **Unidades de disco** e clique no botão **Definir**. O ícone  é exibido ao lado do dispositivo escolhido. Se o dispositivo conectado não for exibido na lista, marque a caixa **Mostrar dispositivos adicionais**. Se necessário, é possível alterar o dispositivo de autorização clicando em **Redefinir**.

➤ *Para usar um dispositivo Bluetooth para acessar o Banco de Dados de Senhas:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.

4. À esquerda da janela, selecione a seção **Método de autorização**.
5. À direita da janela, em **Método de autorização**, selecione o **Dispositivo Bluetooth** na lista suspensa.
6. Ative o Bluetooth no computador e no dispositivo.
7. Selecione um dispositivo na lista **Fones e modems** e clique no botão **Definir**. O ícone  é exibido ao lado do dispositivo escolhido. Se necessário, é possível alterar o dispositivo de autorização clicando em **Redefinir**.

ALTERANDO A SENHA MESTRA

A Senha Mestra é criada ao iniciar o Gerenciador de Senhas Kaspersky pela primeira vez. Você pode alterá-la posteriormente.

Ao alterar a Senha Mestra, o Gerenciador de Senhas Kaspersky solicita a confirmação da senha de entrada (a nova senha deve ser inserida novamente). A nova senha não pode ser salva sem a confirmação. Se a senha de confirmação não corresponder à senha inserida, a senha confirmada será realçada em vermelho. Nesse caso, uma mensagem de aviso será exibida quando você tentar salvar a nova senha.

➤ *Para alterar a Senha Mestra:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. À esquerda da janela, selecione a seção **Método de autorização**.
5. À direita da janela, em **Proteção por senha**, clique em **Alterar**.
6. Na janela **Proteção por senha** que é aberta, insira a nova senha nos campos **Senha** e **Confirmar senha**.

NAVEGADORES DA WEB COM SUPORTE

Para garantir que a ativação automática da conta e o Botão de Legenda (veja a página [49](#)) funcionem corretamente em vários navegadores e programas de email, o Gerenciador de Senhas Kaspersky solicita a instalação de extensões adicionais (plug-ins). Por padrão, os plug-ins são instalados quando o Gerenciador de Senhas Kaspersky é executado pela primeira vez. Você pode instalar plug-ins adicionais.

O Gerenciador de Senhas Kaspersky contém uma lista de navegadores da Web e programas de email em que um status é atribuído a cada programa, **Instalado** ou **Não instalado**, dependendo do plug-in necessário estar instalado ou não.

É recomendável fechar todos os programas para os quais o plug-in será instalado.

➤ *Para instalar um plug-in para um navegador ou programa de email:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. À esquerda da janela, selecione a seção **Navegadores com suporte**.

5. À direita da janela, selecione um programa na lista de **Navegadores com suporte e extensões disponíveis** e clique em **Instalar**.
6. Siga as instruções do **Assistente de Instalação**. Quando o plug-in estiver instalado, o programa será movido automaticamente para o grupo **Instalado**. O status **Instalado** será atribuído a ele. Você pode excluir um plug-in instalado clicando em **Desinstalar**.

GERENCIANDO MODELOS DE NOTAS SEGURAS

Você pode editar modelos predefinidos de Notas seguras (veja a página [29](#)), criar novos modelos, usar uma Nota segura existente como modelo.

➤ *Para alterar um modelo predefinido de Nota segura:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. Selecione a seção **Gerenciar modelos** à esquerda da janela.
5. À direita da janela, selecione um modelo na lista e clique no botão **Editar**.
6. Faça as alterações desejadas no editor de texto.

➤ *Para criar um modelo de Nota segura:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. Selecione a seção **Gerenciar modelos** à esquerda da janela.
5. À direita da janela, clique em **Adicionar**.
6. Na janela que é aberta, no campo **Nome**, insira o nome de um novo modelo de Nota segura.
7. Insira as informações desejadas no editor de texto.

➤ *Para usar uma Nota segura existente como modelo:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela **Gerenciador de Senhas Kaspersky** que é aberta, clique no botão **Banco de Dados de Senhas**.
4. Na janela que é aberta, selecione a Nota segura desejada na lista e, na parte superior da janela, clique no botão **Editar**.
5. Na parte inferior da janela que é aberta, clique no botão **Salvar como modelo**.
6. Na janela que é aberta, no campo **Nome**, insira o nome de um novo modelo de Nota segura.

HORA DE EXECUÇÃO DO APLICATIVO

O Gerenciador de Senhas Kaspersky é carregado por padrão ao iniciar o sistema. Você pode alterar as configurações de execução do programa.

➤ *Para executar o programa manualmente:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. À esquerda da janela, selecione a seção **Geral**.
5. À direita da janela, na seção **Geral**, desmarque a caixa **Carregar o Gerenciador de Senhas Kaspersky ao iniciar o Windows**.

AÇÃO AO CLICAR DUAS VEZES

O Gerenciador de Senhas Kaspersky permite selecionar a ação que será executada ao clicar duas vezes no ícone do aplicativo na área de notificação da barra de tarefas do Microsoft Windows (veja a página [16](#)). Você pode selecionar uma das seguintes ações:

- abra a janela principal do Gerenciador de Senhas Kaspersky (veja a página [17](#));
- bloquear/desbloquear o Gerenciador de Senhas Kaspersky (esta ação é definida por padrão).

➤ *Para definir a tarefa que deve ser executada ao clicar duas vezes no ícone do aplicativo na área de notificação da barra de tarefas:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. À esquerda da janela, selecione a seção **Geral**.
5. À direita da janela, selecione a ação na lista suspensa **Ao clicar duas vezes**.

NOTIFICAÇÕES

Quando o Gerenciador de Senhas Kaspersky estiver em execução, ocorrerão vários eventos de caráter informativo. Para manter-se atualizado, utilize o serviço de notificações. Os usuários são notificados dos eventos por prompts e mensagens pop-up.

Os seguintes tipos de notificações são implementados no aplicativo:

- **Execução do aplicativo.** Uma mensagem é exibida ao reiniciar o aplicativo, quando o aplicativo já foi iniciado e o Banco de Dados de Senhas não está bloqueado.
- **Ativação da conta.** Uma mensagem é exibida quando a conta é ativada.
- **Limpar área de transferência.** O Gerenciador de Senhas Kaspersky pode armazenar a senha temporariamente na área de transferência. Isso é conveniente quando é necessário copiar e colar dados no campo selecionado. Quando o tempo especificado expirar (veja a página [49](#)), a senha será excluída da área de transferência.
- **Bloqueio automático do Gerenciador de Senhas Kaspersky.** É exibida uma mensagem quando o Gerenciador de Senhas Kaspersky bloqueia automaticamente o Banco de Dados de Senhas. Por padrão, o Gerenciador de Senhas bloqueia o Banco de Dados de Senhas automaticamente após a inicialização do sistema operacional e depois de um tempo especificado (veja a página [43](#)) durante o qual o computador não é usado.
- **Exportando senhas para arquivo não criptografado.** Uma mensagem de aviso informa que, depois da exportação, as senhas serão salvas em um arquivo não criptografado e, conseqüentemente, estarão acessíveis para qualquer usuário que trabalhe no computador. É recomendável que antes de exportar os dados você considere as formas de proteger o arquivo com as senhas.
- **Edição manual de formulário.** Para definir parâmetros para campos adicionais, o aplicativo solicita permissão para usar o navegador padrão. A mensagem avisa que imagens e arquivos do sistema (cookies) serão salvos no computador.
- **Dificuldades para preencher as informações de login da Conta.** Essa mensagem avisa que não é possível inserir dados pessoais automaticamente durante a autorização.

➡ *Para receber notificações:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. À esquerda da janela, selecione a seção **Geral**.
5. À direita da janela, clique no botão **Configurações de notificação** na seção **Geral**.
6. Na janela que é exibida, marque ou desmarque a caixa ao lado dos tipos de notificações desejados.

HORA EM QUE A SENHA FOI ARMAZENADA NA ÁREA DE TRANSFERÊNCIA

O Gerenciador de Senhas pode copiar a senha para a área de transferência por um período especificado. Isso é conveniente para executar ações rapidamente com senhas (por exemplo, quando você precisa usar uma senha criada para se registrar em um site/aplicativo). Você pode definir o tempo que a senha ficará salva na área de transferência. Quando esse tempo acabar, a senha será excluída automaticamente da área de transferência. Isso evitará que as senhas sejam interceptadas e roubadas, pois não será possível copiá-las da área de transferência quando o tempo especificado expirar.

➤ *Para alterar o tempo de backup da senha na área de transferência:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. À esquerda da janela, selecione a seção **Geral**.
5. À direita da janela, em **Área de Transferência**, defina o tempo em segundos.

EXIBINDO O BOTÃO DE LEGENDA

Se, além do menu do Gerenciador de Senhas Kaspersky, o aplicativo com o qual você está trabalhando tiver outros menus incorporados, será possível definir a posição do Botão de Legenda em relação aos outros botões. Além disso, você pode gerar uma lista de navegadores nos quais o Botão de Legenda (veja a página [19](#)) é usado.

➤ *Para alterar as configurações de exibição do Botão de Legenda:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
3. Na janela que é aberta, clique no botão **Configurações**.
4. À esquerda da janela, selecione a seção **Botão de Legenda**.
5. À direita da janela, em **Exibição do Botão de Legenda**, defina os parâmetros desejados de acordo com a tarefa:
 - para alterar o local do Botão de Legenda, no campo **Mover botão para a esquerda**, insira o número da posição do botão (quantos botões estarão localizados à direita do Botão de Legenda);
 - para evitar que o Botão de Legenda seja exibido ao bloquear o Banco de Dados de Senhas, marque a caixa **Ocultar se o Gerenciador de Senhas Kaspersky estiver bloqueado**;
 - para criar uma lista de navegadores nos quais o Botão de Legenda está disponível, na seção **Botão de Legenda em navegadores da Web**, marque a caixa ao lado do navegador desejado na lista.

CRIANDO SENHAS FORTES

A segurança dos dados depende diretamente da força de suas senhas. Os dados podem estar em risco nos seguintes casos:

- uma senha é usada para todas as contas;
- a senha é simples;
- a senha usa informações fáceis de adivinhar (como os nomes ou datas de nascimento de familiares).


Para garantir a segurança dos dados, o Gerenciador de Senhas Kaspersky permite que sejam criadas senhas únicas e confiáveis para as contas usando o Gerador de Senhas.

Uma senha é considerada forte quando consiste em mais de quatro caracteres e contém símbolos especiais, números e letras maiúsculas e minúsculas.

A segurança da senha é determinada pelos seguintes parâmetros:

- **Comprimento** – o número de símbolos da senha. Esse valor pode variar de 4 a 99 símbolos. Quando mais longa a senha, mais forte ela é considerada.
- **A-Z** – letras maiúsculas.
- **a-z** – letras minúsculas.
- **0-9** – números.
- **Símbolos especiais** – símbolos especiais.
- **Excluir símbolos semelhantes** – não é permitido usar símbolos idênticos em uma senha.

➡ *Para criar uma senha forte usando o Gerador de Senhas:*

1. Abra o menu de contexto do Gerenciador de Senhas Kaspersky e selecione **Gerador de Senhas**.
2. Na janela do **Gerador de Senhas**, especifique o número de símbolos da senha no campo **Comprimento da senha**.
3. Se necessário, você pode especificar outras configurações para o Gerador de Senhas em **Adicional**, marcando/desmarcando as caixas ao lado das configurações desejadas.
4. Clique em **Gerar**. A senha criada é exibida no campo **Senha**. Para exibir a senha criada, marque a caixa **Mostrar senha**.
5. Copie a senha na área de transferência usando o botão  e a insira no campo de entrada de senha no aplicativo/na página da Web pressionando **CTRL+V**. A senha criada será salva na área de transferência.
6. Para salvar as configurações especificadas para uso posterior, marque a caixa **Por padrão**.

USANDO A VERSÃO PORTÁTIL DO GERENCIADOR DE SENHAS KASPERSKY

O Gerenciador de Senhas Kaspersky permite armazenar todas as suas senhas em uma mídia removível (por exemplo, um cartão de memória ou um celular, se ele puder ser usado como cartão de memória). Para fazer isso, crie uma versão portátil do Gerenciador de Senhas Kaspersky em um dispositivo removível. A versão portátil do aplicativo é criada no computador em que a versão completa do Gerenciador de Senhas Kaspersky foi instalada. A versão portátil do aplicativo apresenta todas as funcionalidades do Gerenciador de Senhas Kaspersky.

A versão portátil permite usar o Gerenciador de Senhas Kaspersky em um computador público (por exemplo, em um cybercafé ou uma biblioteca) em que o Gerenciador de Senhas Kaspersky não está instalado. Assim que um dispositivo removível é conectado ao computador, o Gerenciador de Senhas Kaspersky é iniciado automaticamente. Assim que o dispositivo removível é desativado, o Gerenciador de Senhas Kaspersky é fechado automaticamente, removendo todos os seus dados do computador público.

Além disso, você pode usar a versão portátil para sincronizar seus Bancos de Dados de Senhas, caso o Gerenciador de Senhas Kaspersky esteja instalado e seja usado simultaneamente em vários computadores (por exemplo, no seu computador em casa e no escritório).

NESTA SEÇÃO:

Criando e conectando a versão portátil.....	51
Sincronização do Banco de Dados de Senhas	52

CRIANDO E CONECTANDO A VERSÃO PORTÁTIL

Para que a versão portátil do Gerenciador de Senhas Kaspersky seja executada corretamente em um computador público, é recomendável instalar os plug-ins adicionais para o navegador da Web.

É possível instalar um plug-in das seguintes maneiras:

- Na janela do Assistente de Instalação do plug-in. Para fazer isso, siga as etapas do Assistente de Instalação do plug-in na primeira execução da versão portátil do Gerenciador de Senhas Kaspersky.
- No menu do Botão de Legenda na janela do navegador da Web. Para fazer isso, no menu do Botão de Legenda, selecione o item **O plug-in de preenchimento automático do Gerenciador de Senhas Kaspersky não está instalado**.

Ao executar o aplicativo pela primeira vez em um computador público, o Assistente de Instalação da versão portátil do Gerenciador de Senhas Kaspersky é iniciado automaticamente.

Você pode aplicar as seguintes configurações avançadas ao uso da versão portátil do aplicativo:

- criar um atalho da versão portátil na área de trabalho, que permite executar o aplicativo posteriormente da área de trabalho do computador;
- usar o Teclado Virtual – abre o teclado virtual para inserir dados pessoais.

➔ *Para criar uma versão portátil do Gerenciador de Senhas Kaspersky:*

1. Abra a janela principal do aplicativo.
2. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.

3. Na janela que é aberta, clique no botão **Versão Portátil**.
4. Na janela que é aberta, selecione o dispositivo no qual você deseja instalar a versão portátil do Gerenciador de Senhas Kaspersky e clique em **Avançar**.
5. Na janela que é aberta, configure a versão portátil:
 - Para não precisar inserir a Senha Mestra para acessar a versão portátil do Gerenciador de Senhas Kaspersky, marque a caixa **Nunca solicitar a Senha Mestra**.
 - Para que a Versão Portátil seja iniciada automaticamente quando um dispositivo removível é conectado ao computador, marque a caixa de seleção **Ativar a execução automática do Gerenciador de Senhas do dispositivo removível**.
6. Clique no botão **Executar**. Clique em **Concluir** quando a instalação for concluída.

➔ *Para usar a versão portátil do aplicativo:*

1. Conecte o dispositivo removível ao computador.
2. Execute a versão portátil do Gerenciador de Senhas Kaspersky da unidade removível selecionada, se ela não tiver sido iniciada automaticamente ao conectar a mídia.
3. Ao executar a versão portátil pela primeira vez, você poderá instalar plug-ins de preenchimento automático e desativar os gerenciadores de senha integrados para os navegadores da Web instalados no computador.
4. Insira as Senha Mestra na janela exibida.

A versão portátil do Gerenciador de Senhas Kaspersky está pronta para ser usada.

SINCRONIZAÇÃO DO BANCO DE DADOS DE SENHAS

Se você usar o Gerenciador de Senhas Kaspersky em computadores diferentes, precisará manter todos os Bancos de Dados de Senhas atualizados. Usando a versão portátil, é possível sincronizar os dados e usar o Banco de Dados de Senhas atualizado em todos os computadores em que o Gerenciador de Senhas Kaspersky está instalado. Para fazer isso, sincronize o Banco de Dados de Senhas da versão portátil com o Banco de Dados de Senhas em um computador e, em seguida, sincronize-o novamente em outro computador.

➔ *Para sincronizar o Banco de Dados de Senhas da versão portátil com o Banco de Dados de Senhas em um dos computadores:*

1. Conecte o dispositivo removível ao computador.
2. Abra a janela principal do aplicativo.
3. Na parte inferior da janela, clique no botão **Gerenciador de Senhas Kaspersky**.
4. Na janela que é aberta, clique no botão **Versão Portátil**.
5. Na janela que é aberta, selecione um dispositivo no qual a versão portátil do Gerenciador de Senhas Kaspersky está instalada e clique no botão **Avançar**.
6. Na janela que é aberta, selecione o modo de sincronização do Banco de Dados de Senhas:
 - Para adicionar os dados do banco de dados do Gerenciador de Senhas Kaspersky instalado no computador ao Banco de Dados de Senhas da versão portátil, selecione a opção **Mesclar Bancos de Dados de Senhas**.

O banco de dados do Gerenciador de Senhas Kaspersky instalado no computador não será alterado. Para adicionar os dados mesclados, repita a sincronização selecionando a opção **Use o banco de dados da**

Versão Portátil.

- Para substituir o Banco de Dados de Senhas da Versão Portátil pelo Banco de Dados de Senhas do Gerenciador de Senhas Kaspersky instalado no computador, selecione a opção **Usar o banco de dados do Gerenciador de Senhas Kaspersky instalado neste computador**.
 - Para substituir o Banco de Dados de Senhas do Gerenciador de Senhas Kaspersky instalado no computador pelo Banco de Dados de Senhas da versão portátil, selecione a opção **Usar o Bancos de Dados de Senhas da Versão Portátil**.
7. Clique no botão **Avançar**.
 8. Na janela que é aberta, configure a versão portátil:
 - Para não precisar inserir a Senha Mestra para acessar a versão portátil do Gerenciador de Senhas Kaspersky, marque a caixa **Nunca solicitar a Senha Mestra**.
 - Para que a Versão Portátil seja iniciada automaticamente quando um dispositivo removível é conectado ao computador, marque a caixa de seleção **Ativar a execução automática do Gerenciador de Senhas do dispositivo removível**.
 9. Clique no botão **Executar**. Clique no botão **Concluir** quando a sincronização for concluída.

KASPERSKY LAB

A Kaspersky Lab foi fundada em 1997. Atualmente, é a empresa russa líder no desenvolvimento de uma grande variedade de produtos de software de segurança de informações de alto desempenho, incluindo sistemas antivírus, antispam e anti-hacking.

A Kaspersky Lab é uma empresa internacional. Sediada na Federação Russa, a empresa possui escritórios no Reino Unido, França, Alemanha, Japão, Holanda, China, Polônia, Romênia e EUA (Califórnia). Um novo escritório da empresa foi aberto recentemente na França, o Centro Europeu de Pesquisa Antivírus. A rede de parceiros da Kaspersky Lab inclui mais de 500 empresas no mundo inteiro.

Atualmente, a Kaspersky Lab emprega mais de mil especialistas altamente qualificados, incluindo 10 detentores de mestrado e 16 detentores de PhD. Todos os especialistas sênior em antivírus da Kaspersky Lab fazem parte da CARO (Computer Anti-Virus Researchers Organization).

Os bens mais valiosos de nossa empresa são o conhecimento exclusivo e a especialização coletiva acumulada nos 14 anos de combate contínuo aos vírus de computador. Uma análise completa das atividades de vírus de computador permite aos especialistas da empresa prever as tendências de desenvolvimento de malware e fornecer aos nossos usuários uma proteção oportuna contra os novos tipos de ataques. Essa vantagem é a base dos produtos e serviços da Kaspersky Lab. Os produtos da empresa estão sempre um passo à frente de outros fornecedores, oferecendo proteção antivírus abrangente aos nossos clientes.

Os anos de muito trabalho tornaram a empresa um dos principais desenvolvedores de software antivírus. A Kaspersky Lab foi a primeira empresa a desenvolver vários dos padrões modernos dos software antivírus. O principal produto da empresa, o Kaspersky Anti-Virus, protege de forma confiável todos os tipos de sistemas de computador contra ataques de vírus, incluindo estações de trabalho, servidores de arquivos, sistemas de email, firewalls, gateways da Internet e computadores portáteis. Suas ferramentas de gerenciamento fáceis de usar maximizam a automação da proteção antivírus de computadores e redes corporativas. Diversos desenvolvedores de todo o mundo usam o kernel do Kaspersky Anti-Virus em seus produtos, incluindo Nokia ICG (EUA), Aladdin (Israel), Sybari (EUA), G Data (Alemanha), Deerfield (EUA), Alt-N (EUA), Microworld (Índia) e BorderWare (Canadá).

Os clientes da Kaspersky Lab dispõem de vários serviços adicionais que asseguram o funcionamento estável dos produtos da empresa e a conformidade total com seus requisitos empresariais específicos. Nós projetamos, implementamos e damos suporte a sistemas corporativos de antivírus. O banco de dados de antivírus da Kaspersky Lab é atualizado de hora em hora. A empresa fornece aos seus clientes serviço de suporte técnico 24 horas em vários idiomas.

Caso tenha dúvidas, comentários ou sugestões, você pode entrar em contato conosco através de nossos distribuidores ou diretamente com a Kaspersky Lab. Será um prazer ajudá-lo em qualquer assunto relacionado aos nossos produtos, por telefone ou email. Você receberá respostas completas e abrangentes a todas as suas perguntas.

Site oficial da Kaspersky Lab: <http://brazil.kaspersky.com/>

Enciclopédia de vírus: <http://www.securelist.com/>

Laboratório de antivírus: newvirus@kaspersky.com
(somente para o envio de objetos suspeitos em arquivos comprimidos)
<http://support.kaspersky.com/virlab/helpdesk.html?LANG=pt>
(para consultas de analistas de vírus)

Fórum da Kaspersky Lab na Web: <http://forum.kaspersky.com>