Manual do Usuário

Nextel Proteção Online – Versão 13.0

1 Índice

1 Índice 2
2 Nextel Proteção Online 4
2.1 Instalação da Central de Serviços 6
2.2 Instalação automática do Nextel Proteção Online 9
3 INTERFACE DO NEXTEL PROTEÇÃO ONLINE 13
3.1 PAINEL SUPERIOR DA INTERFACE DO NEXTEL PROTEÇÃO ONLINE 14
3.1.1 NEXTEL 14
3.1.2 PROTEÇÃO EM NUVEM 15
3.1.3 Relatórios 16
3.1.4 Configurações 17
3.2 PAINEL CENTRAL DA INTERFACE DO NEXTEL PROTEÇÃO ONLINE 18
3.2.2 Status do Computador 18
3.3 PAINEL INFERIOR DA INTERFACE DO NEXTEL PROTEÇÃO ONLINE 19
4 CONFIGURAÇÕES 20
4.1 CENTRO DE PROTEÇÃO 20
4.1.1 CONFIGURAÇÕES GERAIS 20
4.1.2 Antivírus de Arquivos: 22
4.1.3 Antivírus de E-mail: 25
4.1.4 Antivírus da Web: 28
4.1.5 Antivírus de IM: 31
4.1.6 Controle de Aplicativos: 33
4.1.7 Inspetor do Sistema: 35
4.1.8 Firewall: 38
4.1.9 Bloqueador de Ataques de Rede: 39
4.1.10 Antispam: 40
4.1.11 Antibanner: 42
4.1.12 Banco Seguro: 44
4.1.13 Inserção segura de dados: 45
4.2 VERIFICAÇÃO 47

4.2.1 Configurações Gerais: 47
4.2.2 Verificação Completa 49
4.2.3 Verificação de Áreas Críticas 52
4.2.4 Verificação Personalizada....55
4.2.5 Verificação de Vulnerabilidades 57
4.3 ATUALIZAÇÃO....59
4.3.1 Configurações de Atualização....59
4.4 CONFIGURAÇÕES AVANÇADAS 60
4.4.1 Ameaças e Exclusões....60
4.4.2 Autodefesa 61
4.4.3 Economia de Bateria 62
4.4.4 Compatibilidade....63
4.4.5 Rede 64
4.4.6 Notificações 66
4.4.7 Relatórios e Quarentena 68
4.4.8 Feedback 70
4.4.9 Perfil de Jogo 71
4.4.10 Aparência....72
4.4.11 Controle dos Pais 74
4.4.12 Gerenciar Configurações 75
5 CONFIGURAÇÃO DO PAINEL INFERIOR DA INTERFACE DO NEXTELPROTECT:....76
5.1 Verificação....77
5.2 Atualização 78
5.3 Banco Seguro....79
5.4 Controle dos Pais 80
5.4.1 Configurando o Controle para Pais 81
5.5 Atividade de Aplicativos....97
5.6 Monitor de rede 98
5.7 Teclado Virtual 101
5.8 Quarentena 102
5.9 Ferramentas 103

2 Nextel Proteção Online

A Kaspersky Lab desenvolveu o Kaspersky Internet Security, um produto que protege o que é precioso para você em seu PC, como suas fotos, músicas, seus documentos e seus filhos. Seu PC fica protegido contra vírus, spyware, cavalos de troia, spam, hackers, rootkits e outras ameaças. Com os recursos de segurança automáticos, o Kaspersky Internet Security elimina a sobrecarga da proteção do PC, é um produto fácil de baixar, instalar e executar. Para que você possa trabalhar, fazer compras e realizar operações bancárias on-line sem preocupações. Nesta apostila, o produto será apresentado como **"Nextel Proteção Online"** que é a marca registrada ao produto Kaspersky Internet Security para os clientes NEXTEL.

Assim como toda solução antivírus de qualidade, o Nextel Proteção Online tem como objetivo a prevenção de desastres ou danos que possam ser causados por softwares maliciosos ou não autorizados.

É importante lembrar que para o correto funcionamento da solução, o sistema operacional deve ser mantido sempre com as últimas atualizações de segurança instaladas, requisito importante a ser verificado logo na instalação.

REQUISITOS MÍNIMOS DE SISTEMA:

- Processador: 1 GHz 32 bits (x86)/64 bits (x64) ou superior;
- Memória mínima: 512 MB;
- Espaço em disco: 1 GB (32 bits) ou 2 GB (64 bits);
- Conexão à internet para validação da assinatura e atualizações;

SISTEMAS OPERACIONAIS COMPATÍVEIS:

Windows 8, Windows 8 Pro, Windows 7 (todas as versões), Windows Vista (todas as versões), Windows XP (SP2).

Observação na Instalação do Nextel Proteção Online:

Um detalhe importante a observar ao iniciar a instalação do Nextel Proteção Online é a verificação de softwares conflitantes. São exemplos destes, softwares antivírus e firewall de outros fabricantes, inclusive firewall do Windows. Normalmente, o programa de instalação do Nextel Proteção Online remove o software conflitante automaticamente, mas em alguns casos, essa remoção automatizada não será concluída com sucesso. Nesse caso, é necessário verificar se o fabricante do software em questão fornece alguma ferramenta equivalente a **Uninstallation Tool**.

Segue os links para download da ferramenta de desinstalação automatizada dos fabricantes mais populares:

Produto	Link para Ferramenta de Desinstalação	Link para Instruções de Desinstalação
AVIRA	http://dlpro.antivir.com/package/removaltool/win32/en/removaltool-win32-en.exe	http://www.avira.com/pt-br/support-download-avira-antivir-removal-tool
ESET NOD	http://download.eset.com/special/ESETUninstaller.exe	http://kb.eset.com/esetkb/index?page=content&id=SOLN3160
AVAST	http://files.avast.com/files/eng/aswclear.exe	http://www.avast.com/pt-br/uninstall-utility
F-Secure	ftp://ftp.f-secure.com/support/tools/uitool/UninstallationTool.zip	http://support.f-secure.com/enu/corporate/downloads/removeav.shtml
NORTON	ftp://ftp.symantec.com/public/english_us_canada/removal_tools/Norton_Removal_Tool.exe	https://support.norton.com/sp/pt/br/home/current/solutions/v24120365_NIS_OEM_2012_pt_pt
McAfee	http://download.mcafee.com/products/licensed/cust_support_patches/MCPR.exe	http://service.mcafee.com/FAQDocument.aspx?id=TS101331&lc=1046
AVG	http://aa-download.avg.com/filedir/util/avgrem/avg_remover_stf_x64_2013_3341.exe	http://www.avg.com/us-en/utilities
BIT DEFENDER	http://www.bitdefender.com/files/KnowledgeBase/file/BitDefender_Uninstall_Tool.exe	http://www.bitdefender.com/support/How-to-uninstall-Bitdefender-333.html
PANDA	http://resources.downloads.pandasecurity.com/sop/UNINSTALLER_08.exe	http://www.pandasecurity.com/homeusers/downloads/docs/product/help/ap/2013/br/100.htm
G Data	http://mirror.gdata.de/dl_files/pushfile.php?fHash=e99ef52c3c52bbfc509f1274081bc077	http://www.gdatasoftware.co.uk/support/downloads/tools.html

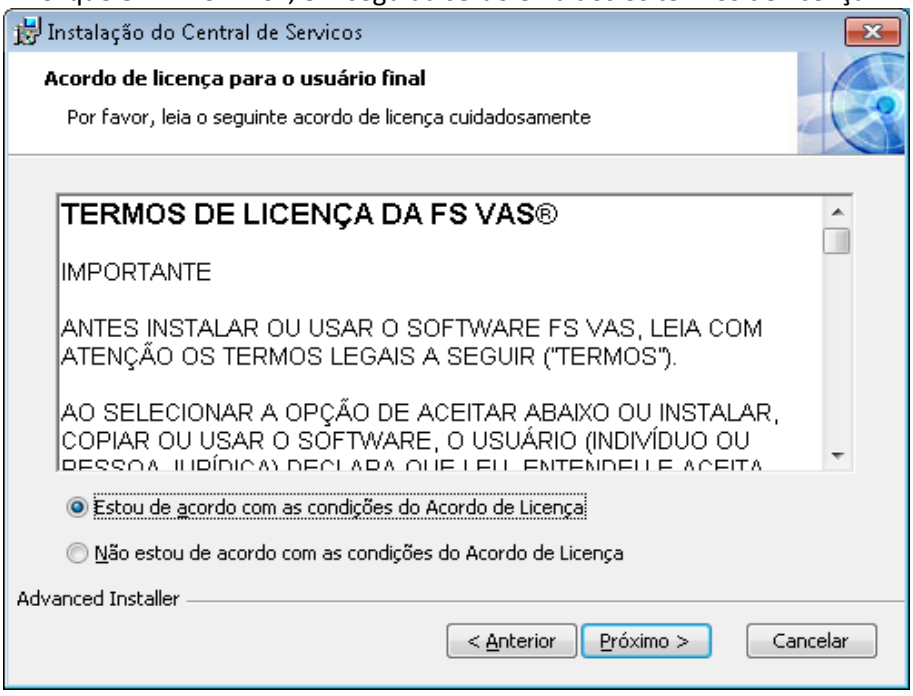
- Lembrando que é recomendado verificar as instruções contidas na página disponibilizada pelo fabricante para compreender o processo de desinstalação automática. Normalmente é necessário apenas executar o arquivo especificado.

2.1 Instalação da Central de Serviços

Para realizar o download do Nextel Proteção Online é necessário a instalação da Central de Serviços. Pela central de serviços é possível instalar e autenticar o Nextel Proteção Online com a chave de ativação.

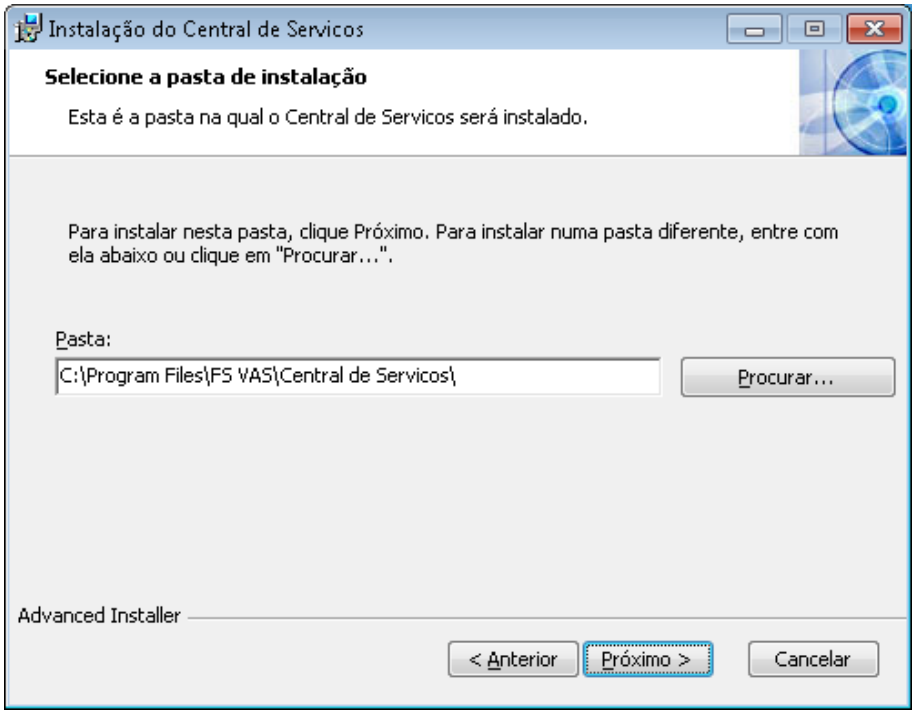
Ao baixar a Central de Serviços, aparecerá a interface de instalação:

Clique em “Próximo”, em seguida serão exibidos os termos de licença:



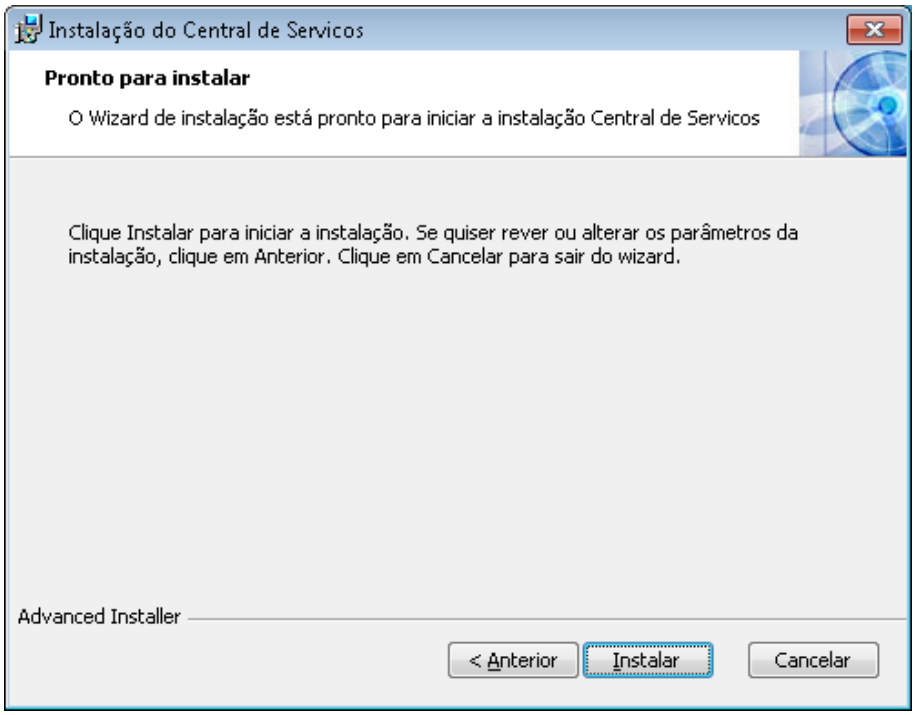
O usuário deve ler atentamente o contrato, selecionar “Estou de acordo com as condições do Acordo de Licença” e clicar em “Próximo”.

Na etapa seguinte, deve escolher a pasta de instalação:

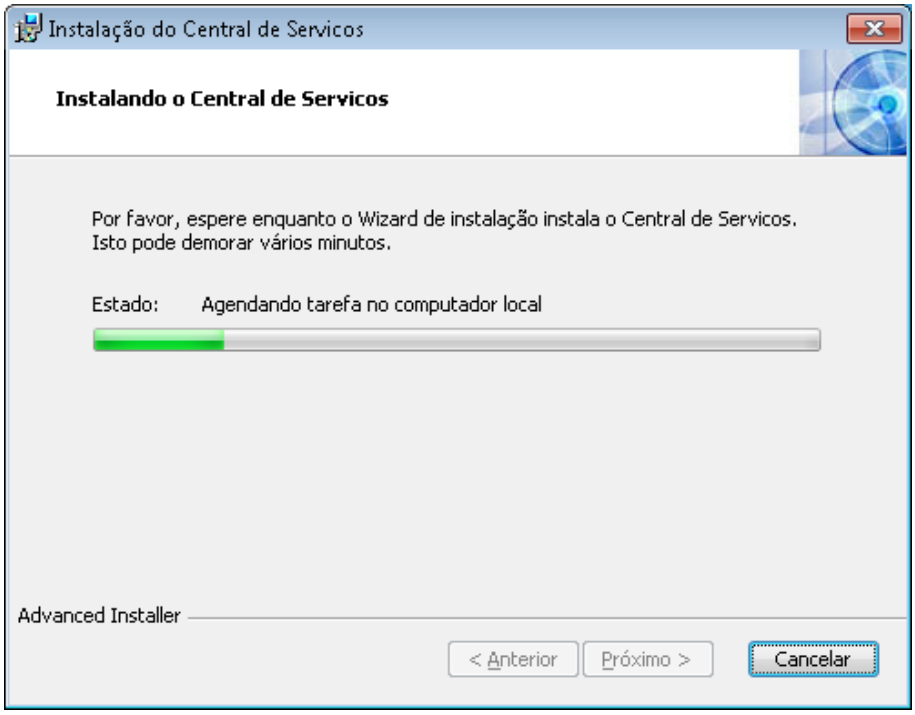


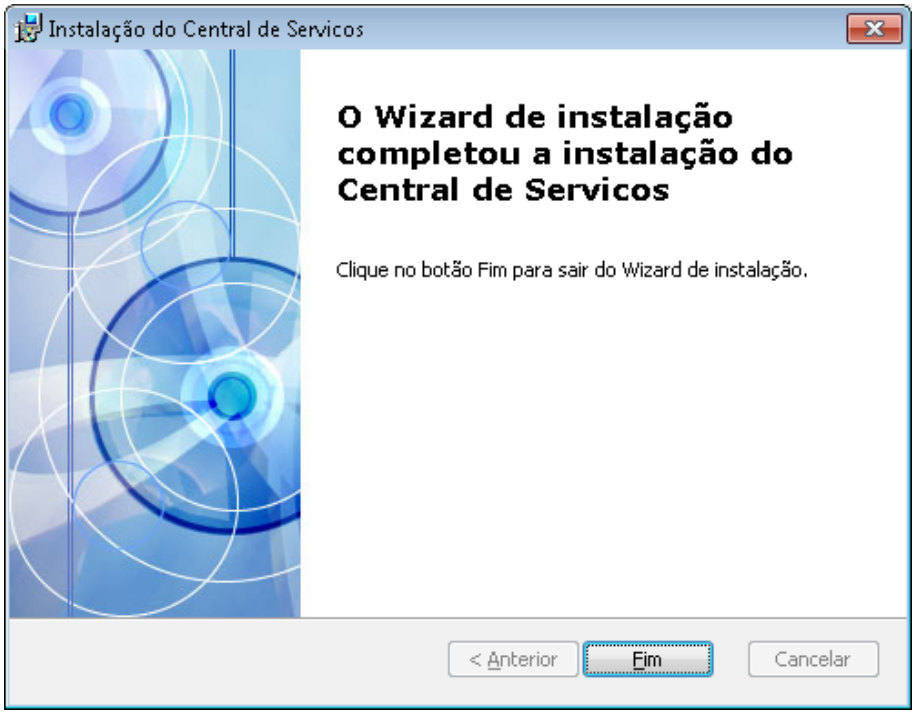
Após selecionar a pasta para a instalação, clique em “próximo” para prosseguir.

O aplicativo está pronto para instalação, Clique em instalar:



O programa começará a instalação:





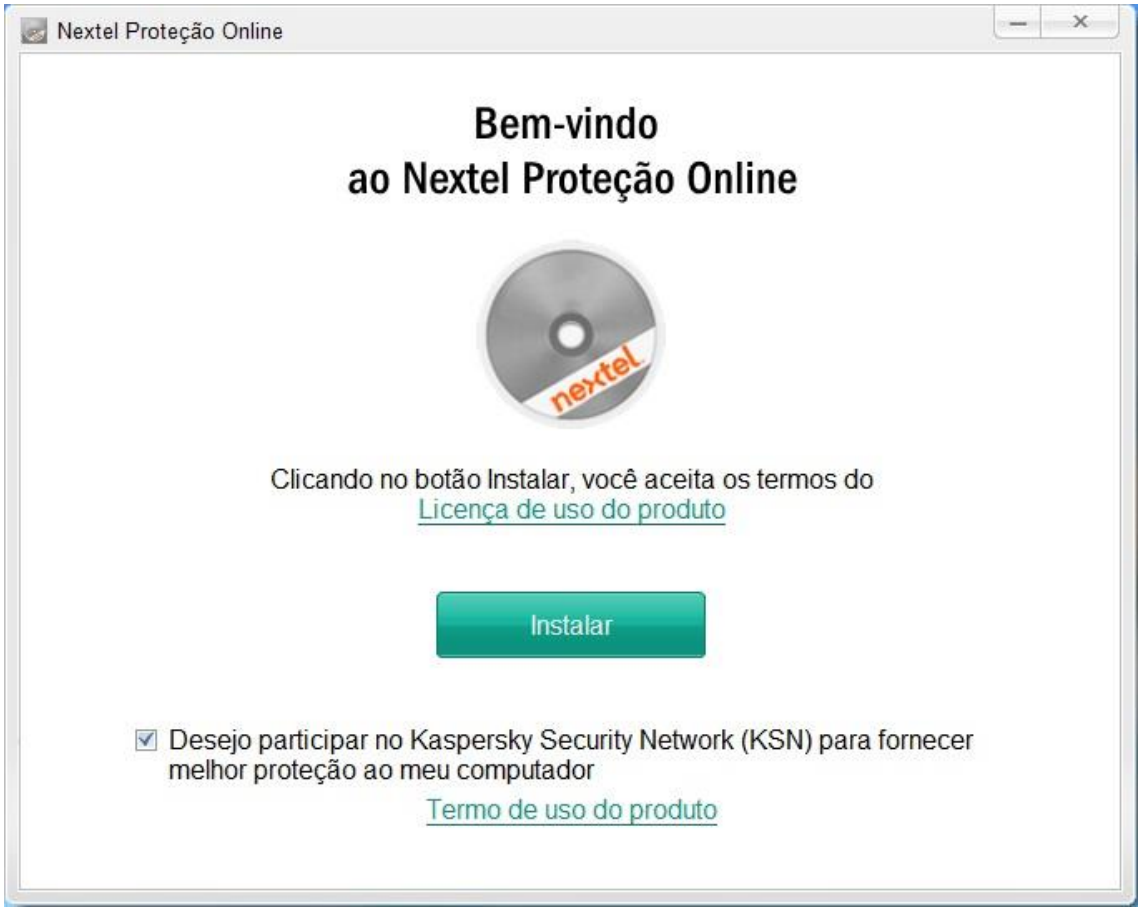
Clique no botão “Fim”.

A janela de instalação automática do Nextel Proteção Online será iniciada automaticamente conforme veremos nas telas seguintes:

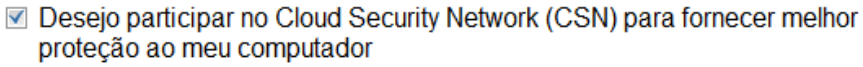
2.2 Instalação automática do Nextel Proteção Online

Uma tela de boas-vindas será exibida.

Leia atentamente o “Contrato de Licença do Usuário Final”:



É recomendável marcar a opção:



Kaspersky Security Network (KSN) significa: Rede de Segurança na Nuvem

O Nextel Proteção Online (KSN) reúne milhões de usuários em todo o mundo para detectar novas ameaças rapidamente e determinar a reputação de programas e sites.

Com o seu consentimento, a informação sobre as tentativas de infectar o seu computador e atividade de programa suspeito é enviado a Nextel Proteção Online Lab. Esta informação é imediatamente processada pelo sistema especialista automatizado em apenas 40 segundos.

Um programa antivírus padrão precisa de pelo menos 4 horas para (detectar, bloquear e gravar em um banco de dados de assinatura) os mais de 35 mil programas maliciosos que surgem a cada dia.

Métodos pró-ativos alternativos e tecnologias de nuvem são necessários para garantir mais rapidez e uma proteção mais eficaz contra as ameaças mais recentes.

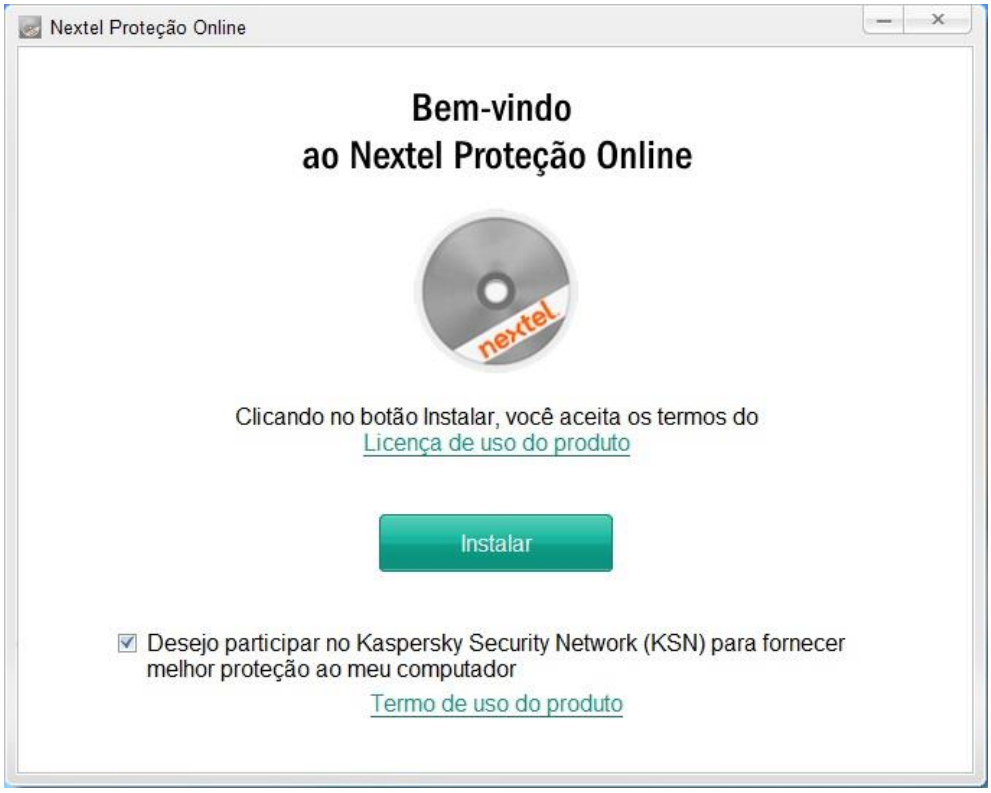
É por isso que especialistas do Nextel Proteção Online desenvolveram uma proteção híbrida que combina ferramentas anti-malware tradicionais com tecnologias de nuvem. Estas tecnologias de proteção em nuvem são baseadas em dados recolhidos no âmbito do Nextel Proteção Online.

A Tecnologia Cloud (KSN) vai:

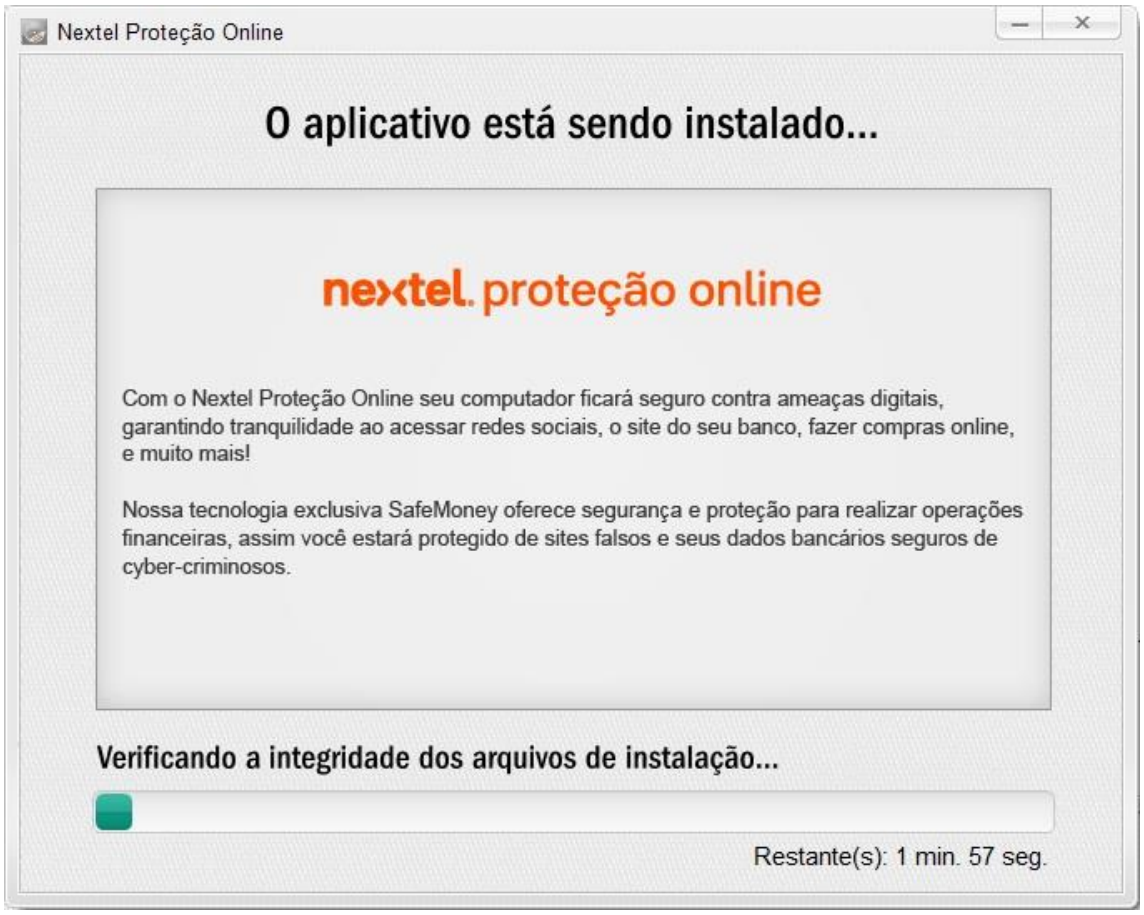
- Fornecer proteção contra as mais recentes ameaças.
- Liberar espaço no disco rígido. Com banco de dados na nuvem, não são armazenados no seu computador.
- Reduzir o tráfego ao atualizar bancos de dados de antivírus.
- Melhorar o desempenho do computador: informações baseadas em nuvem significa que não há necessidade de analisar todas as atividades de aplicação.

*A descrição detalhada da tecnologia envolvida pode ser encontrada em: www.securelist.com

Para prosseguir clique em: Instalar.

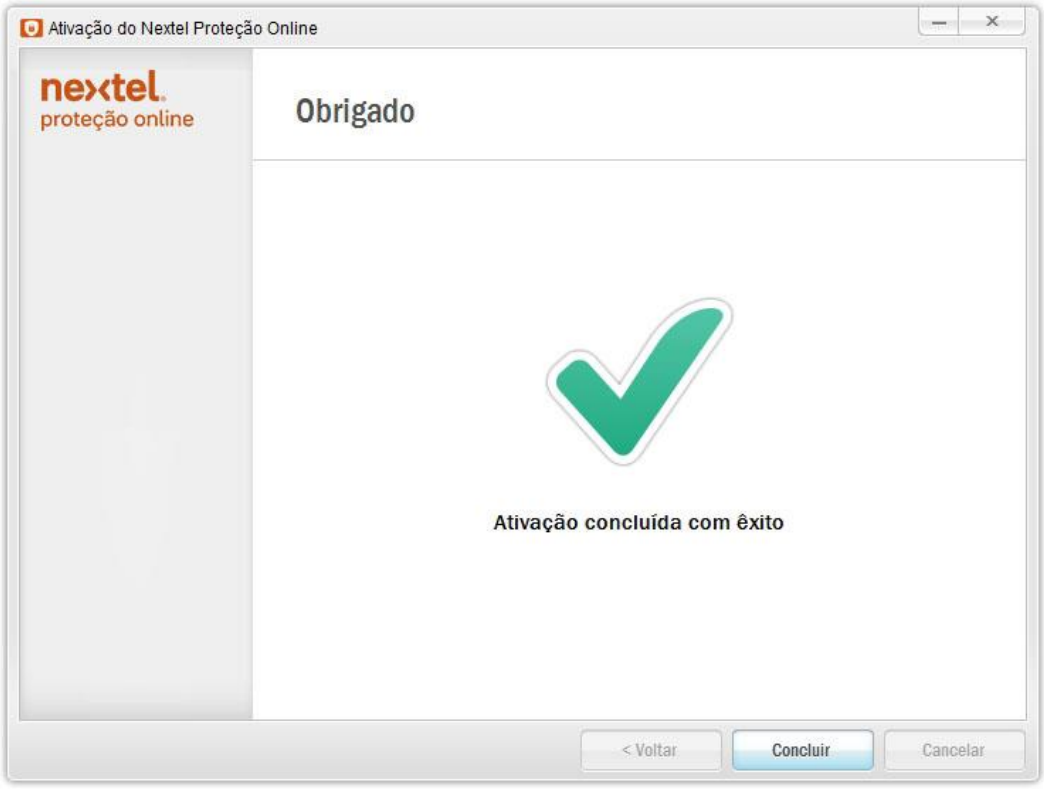


Conforme a tela abaixo, o aplicativo está sendo instalado:



O aplicativo foi instalado com êxito, marque a caixa “Iniciar Nextel Proteção Online” e clique em: Concluir.

Carregando o Nextel Proteção Online:



A ativação foi concluída com êxito, para avançar clique em: Concluir.

3 INTERFACE DO NEXTEL PROTEÇÃO ONLINE

Nas páginas seguintes vamos conhecer as seguintes partes da interface Nextel Proteção Online:

- Superior
- Central
- Inferior

3.1 PAINEL SUPERIOR DA INTERFACE DO NEXTEL PROTEÇÃO ONLINE

3.1.1 NEXTEL

Ao clicar no ícone “ palavra ” será apresentado um breve resumo sobre a versão do Nextel Proteção Online:

Após ler, clique em fechar.

3.1.2 PROTEÇÃO EM NUVEM

Exibe o status de acesso aos serviços do Nextel Proteção Online disponíveis na Internet. Ao clicar neste botão, é aberta uma janela que descreve os serviços e as informações recebidas deles. Conforme tela seguinte:

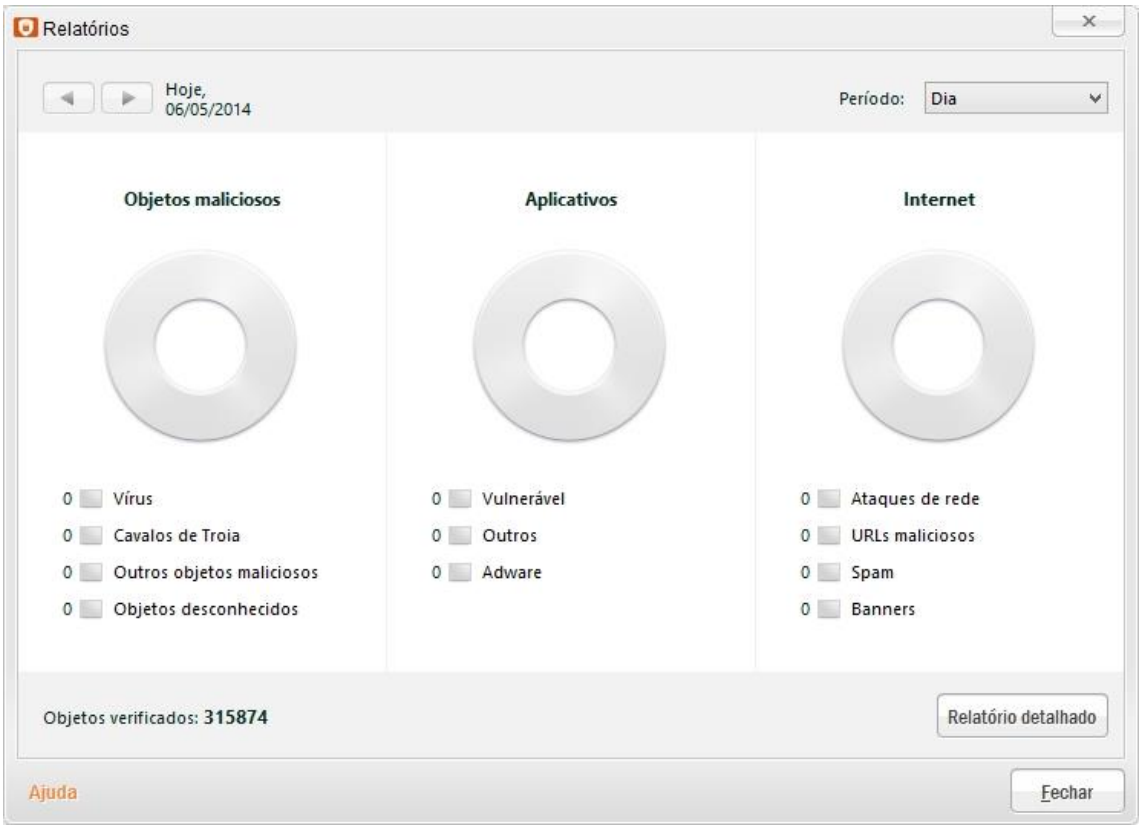
Essa tela aborda o mesmo assunto com informações que tratamos no tema "**Kaspersky Security Network" (KSN). Rede De Segurança Na Nuvem.**

A Kaspersky Security Network é necessária para garantir mais rapidez e proteção mais eficaz contra as ameaças mais recentes.

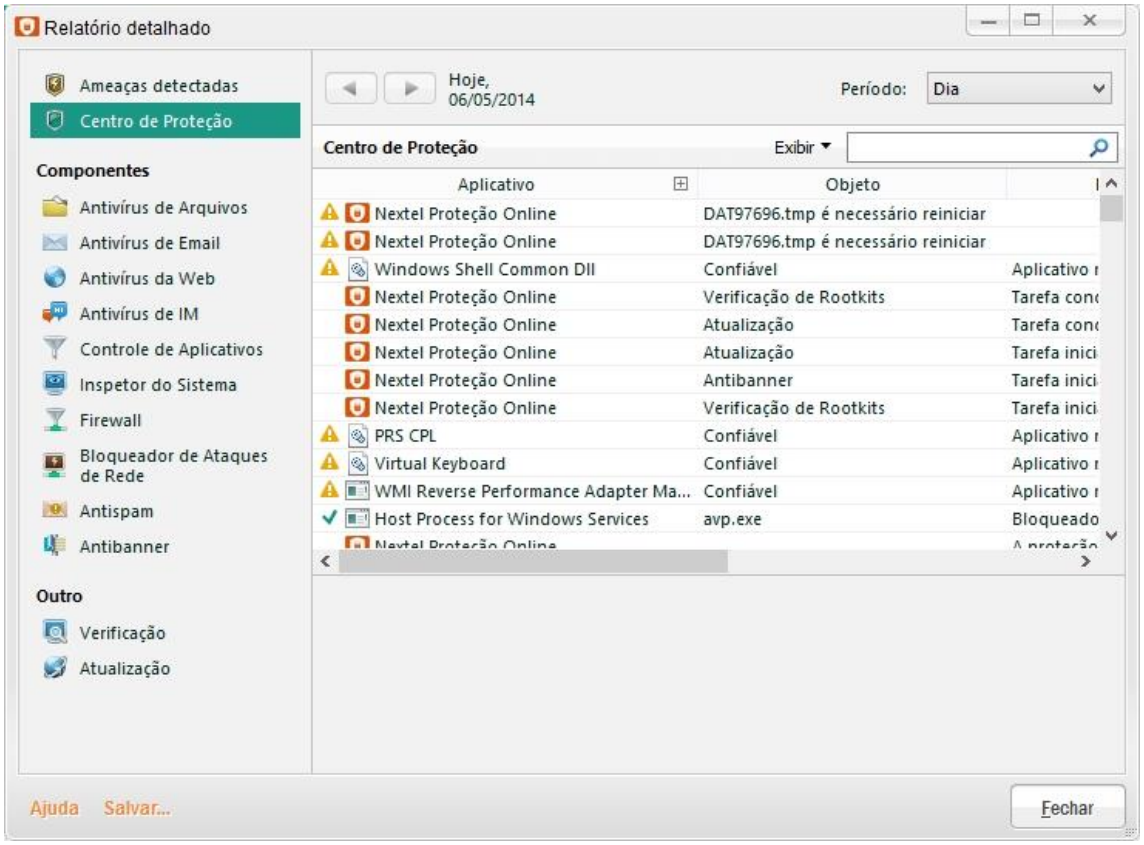
Consulte o Tema 2.2 da página 9 ou clique no botão "Saiba Mais".

3.1.3 Relatórios

- Período: Serão apresentados por período toda à verificação feita pelo Nextel Proteção Online. Você pode criar relatórios referentes aos seguintes períodos: dia, semana, mês, ano e período completo.



“Relatório detalhado”: Para obter um relatório detalhado sobre o funcionamento dos componentes e a execução de tarefas por item e período conforme a tela abaixo:



3.1.4 Configurações

O usuário configura as ferramentas do Nextel Proteção Online. Essas configurações serão explicadas de forma detalhada nos próximos passos.

3.2 PAINEL CENTRAL DA INTERFACE DO NEXTEL PROTEÇÃO ONLINE

3.2.2 Status do Computador

O centro da interface informa o status de proteção do computador como um todo. Por exemplo: “O computador está protegido” ou “A segurança do computador está em risco”.

Mais detalhes são mostrados na lista que inclui os seguintes itens:

- ✓ Ameaças: Informações sobre ameaças à segurança do computador;
- ✓ Componentes de proteção: Informações sobre o funcionamento dos componentes de proteção, como o Antivírus de Arquivos ou o Antivírus da Web;
- ✓ Bancos de dados: Informações sobre a condição dos bancos de dados de antivírus do aplicativo;
- ✓ Assinatura: Informações sobre o número de dias restantes até a expiração da licença.

3.3 PAINEL INFERIOR DA INTERFACE DO NEXTEL PROTEÇÃO ONLINE

No painel inferior da interface temos atalhos das ferramentas Nextel Proteção Online. Atalhos dos quais abordaremos de forma detalhada no decorrer da apostila.

- Ao clicar nos botões Seta para a esquerda ou Seta para a direita é possível se mover pela lista de componentes.

- Ao clicar nos botões Seta para cima e Seta para baixo é possível expandir e ocultar a lista completa de componentes.

- Ao clicar no botão com o nome de um componente, a janela de gerenciamento desse componente é aberta.

No rodapé da lista de atalhos temos os botões:

- Ajuda: Em todas as telas da interface temos a opção (Ajuda) que oferece informações detalhadas de cada componente do Nextel Proteção Online.

- Suporte: A seção Suporte contém as informações necessárias ao Serviço de Suporte Técnico: número da versão do Nextel Proteção Online, data e hora da versão dos bancos de dados do aplicativo, versão do sistema operacional, chave de ativação com informações sobre a licença atual, sugestões de configuração de aplicativos, artigos técnicos sobre como configurar e usar o Nextel Proteção Online, Fórum de usuários onde é possível deixar seus comentários, criar novos tópicos e procurar informações.

- Meu NEXTEL: Redireciona para o Portal https://meuNextel.Nextel.com.br/login

- Gerenciar Assinatura: fornece informações sobre:

a. Chave (Informações da Licença com informações sobre a licença atual);
b. Status da chave;
c. Tipo de licença;
d. Número de hosts abrangidos pela licença;
e. Data de ativação e data de expiração da licença.

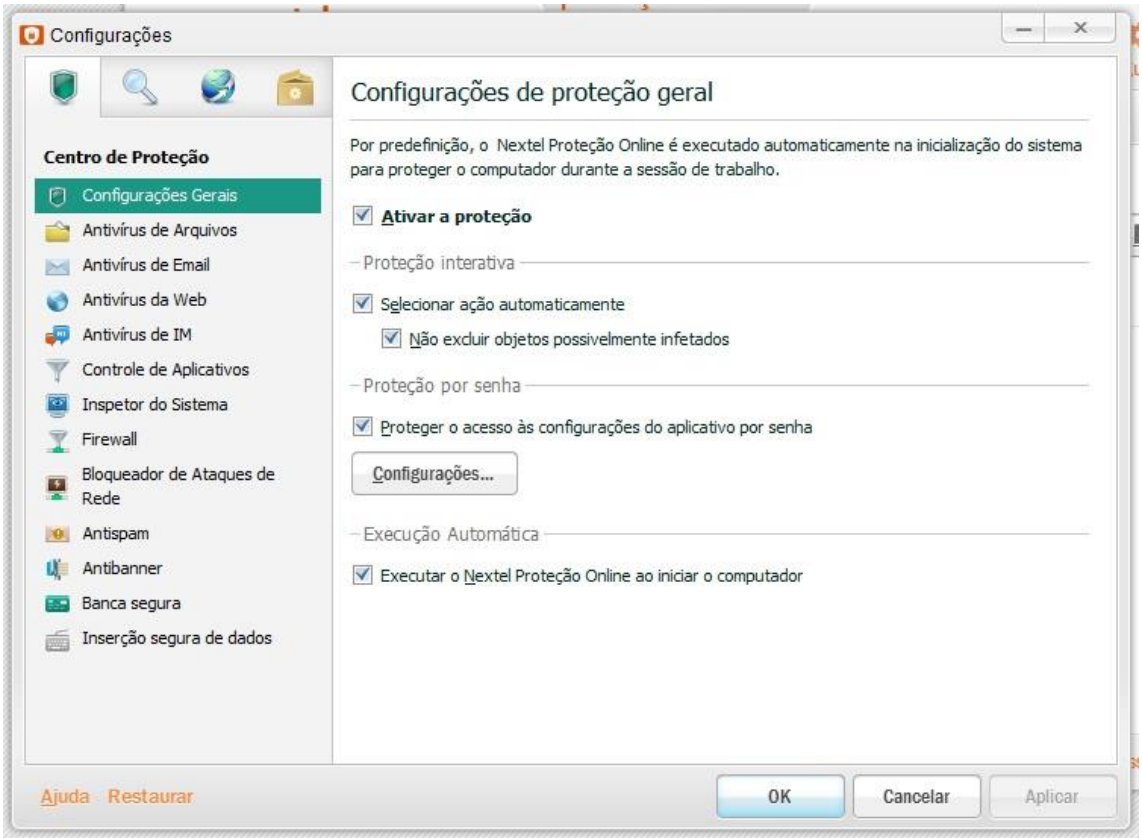
Agora que a interface foi apresentada, vamos conhecer de forma detalhada a configuração dos componentes do Nextel Proteção Online:

4 CONFIGURAÇÕES

O usuário configura as ferramentas do Nextel Proteção Online. Essas configurações serão explicadas de forma detalhada nos próximos passos.

4.1 CENTRO DE PROTEÇÃO

4.1.1 CONFIGURAÇÕES GERAIS



“Ativar a Proteção”: Para que o computador esteja protegido é necessário manter essa opção marcada, ao desabilitar essa opção, desativará todos os componentes de proteção do Nextel Proteção Online deixando o computador vulnerável.

- Proteção Interativa -

“Selecionar ação automaticamente”: O antivírus é capaz de detectar e tomar uma ação se um programa é ***Confiável*** (a execução é permitida), ***Suspeito*** (a execução é realizada mediante interação do usuário) ou ***Malicioso*** (a execução é bloqueada automaticamente).

Neste caso a ação adotada pelo software quando um arquivo malicioso for encontrado serão: (*Colocar em quarentena, Limpar o arquivo, Excluir o arquivo*).

Ao desmarcar essa opção o sistema interage com o usuário de modo a adotar uma ação quando um arquivo malicioso for encontrado.

“Não excluir objetos possivelmente infectados”: Mesmo que esteja no automático, essa opção mantem os arquivos suspeitos para o usuário resolver a ação a ser tomada. Aplicando as regras do automático apenas nos arquivos confiáveis ou maliciosos.

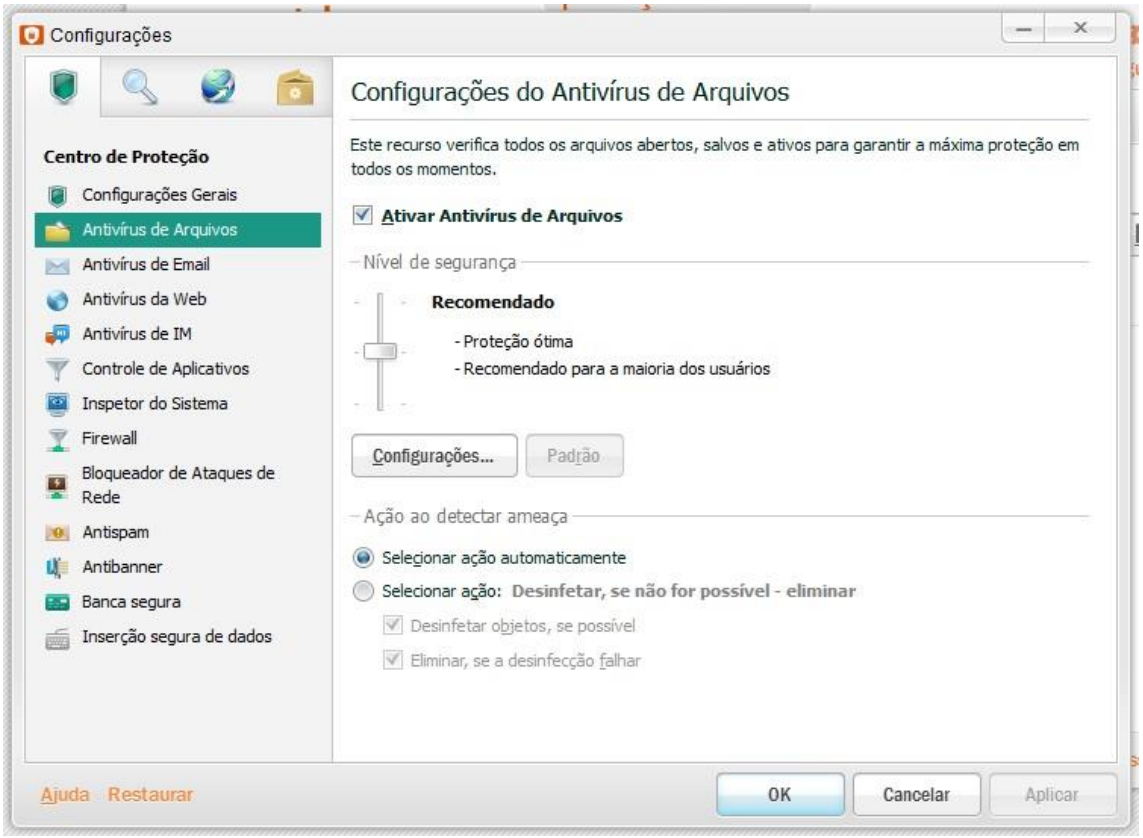
- Proteção por Senha -

“Proteger o acesso às configurações do aplicativo por senha”: Clique no botão “configurações” e insira uma senha de administrador do Nextel Proteção Online, é necessário manter essa opção marcada para garantir que somente o administrador ative, desative ou faça alterações nas configurações do Nextel Proteção Online.

- Execução Automática -

“Executar o Nextel Proteção Online ao iniciar o computador”: É necessário manter essa opção marcada para que o computador esteja protegido desde o seu iniciar, caso contrário o mesmo estará desprotegido até que o usuário clique manualmente e execute o Nextel Proteção Online.

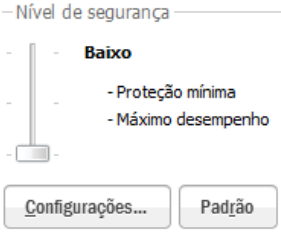
4.1.2 Antivírus de Arquivos:



"Ativar Antivírus de Arquivos": Se estiver marcado, o Antivírus de Arquivos será executado ao iniciar o sistema operacional, sendo executado na memória do computador verificando todos os arquivos abertos, salvos ou executados. Se estiver desmarcada, o Antivírus de Arquivos estará desativado. Esta caixa vem marcada por padrão, recomenda-se mantê-la marcada para garantir uma proteção efetiva.

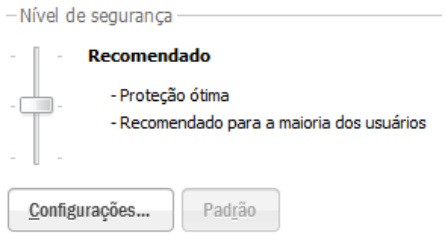
- Nível de Segurança: Temos três níveis para ajustar de acordo com o perfil do usuário -

Baixo: Neste nível de segurança, o Antivírus de Arquivos verifica apenas os arquivos com extensões especificadas em todos os discos rígidos, unidades removíveis e de rede do computador, além de executar uma análise heurística superficial. Os arquivos compostos não são verificados.



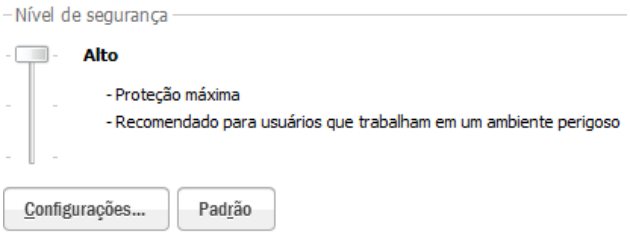
O nível de segurança Baixo permite a velocidade de verificação máxima, embora tenha uma proteção menor.

Recomendado: É o nível recomendado para a maioria dos usuários. Garante um equilíbrio ideal entre desempenho e segurança do sistema. O componente Antivírus de Arquivos verificará apenas os formatos de arquivo especificados em todos os discos rígidos, unidades de rede e mídias de armazenamento removível do computador; além de executar a análise heurística superficial.



Os objetos OLE são verificados. Os pacotes de instalação e arquivos comprimidos não são verificados. Esse é o nível de segurança Padrão (por esse motivo o botão "Padrão" está apagado, pois o mesmo já está acionado).

Alto: Neste nível de segurança, o Antivírus de Arquivos aplica o controle mais rígido a todos os arquivos abertos, salvos e executados. Verifica: todos os tipos de arquivos em todas as unidades, unidades de rede e mídia de armazenamento removíveis do computador.



Verifica também: arquivos comprimidos, pacotes de instalação e objetos OLE incorporados. Esse é o nível de segurança recomendado para usuários que trabalham em ambientes perigosos, com maior risco de ataques de invasores.

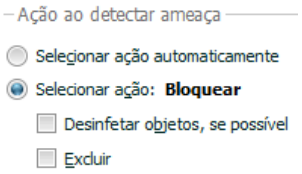
*Dúvidas sobre o botão "Configurações" deverão ser esclarecidas através do atendimento de suporte nível 2.

- Ação ao detectar ameaça -

"Selecionar ação automaticamente": Ao detectar objetos perigosos, o Antivírus de Arquivos executará automaticamente uma ação: Para objetos maliciosos, a ação é Desinfetar ou Excluir se a desinfecção falhar, para objetos provavelmente infetados, a ação é Ignorar. Antes de tentar desinfetar ou excluir um objeto infectado, o Antivírus de Arquivos cria uma cópia de backup para posterior restauração ou desinfecção.

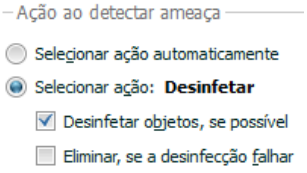
“Selecionar ação”: Temos quatro opções para ajustar de acordo com o perfil do usuário:

Bloquear: O Antivírus de Arquivos bloqueia o acesso ao objeto. As informações sobre esse evento são registradas em um relatório (Negação de acesso de aplicativos externos a um objeto). Um objeto bloqueado não pode ser lido, executado, alterado ou excluído. Esta ação será executada se as caixas de seleção “Desinfetar” e “Excluir” estiverem desmarcados.

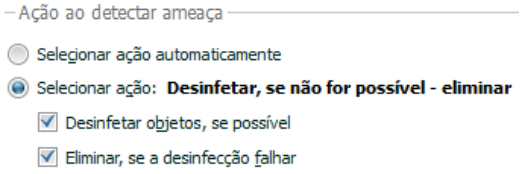


Desinfetar: O Antivírus de Arquivos tenta desinfetar todos os objetos infectados ou provavelmente infectados detectados. Se a desinfecção falhar, o Antivírus de Arquivos os moverá para a Quarentena.

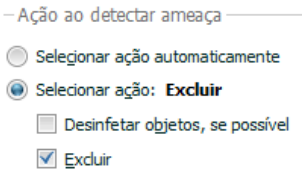
A ação será executada se a caixa “Eliminar, se a desinfecção falhar” estiver desmarcada.



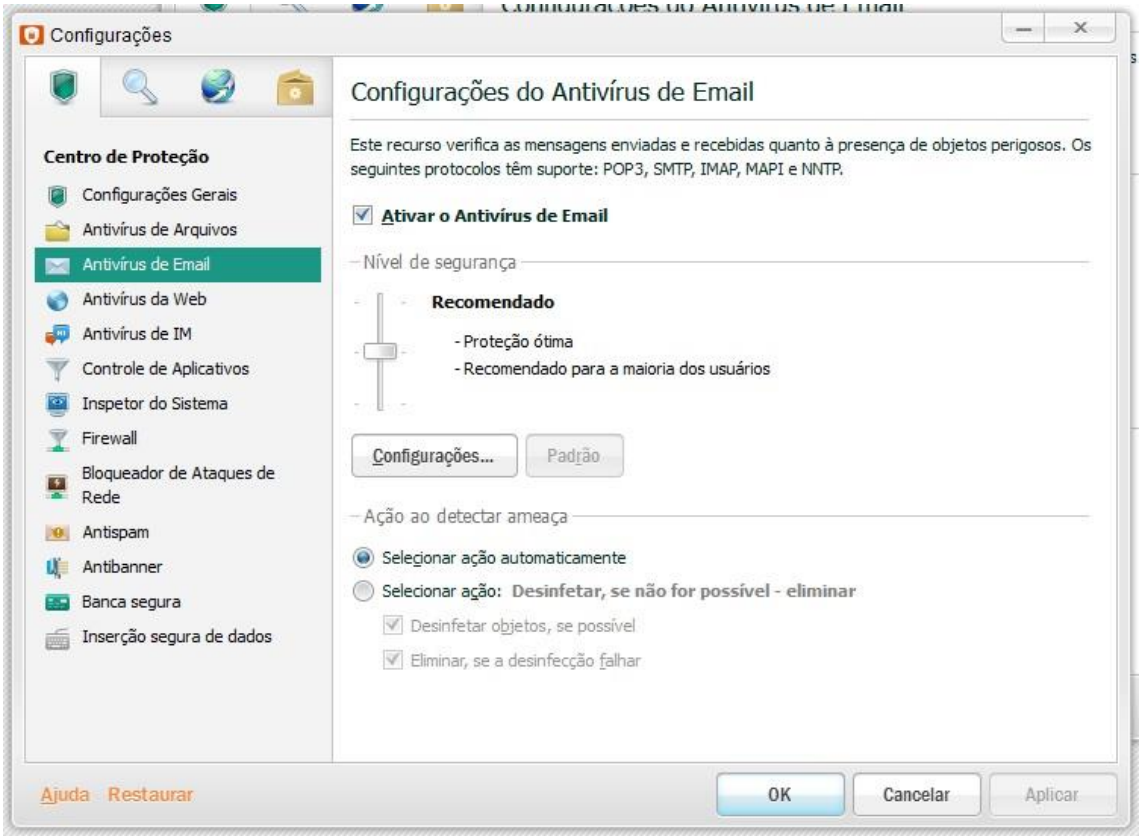
Desinfetar, se não for possível – Eliminar: O Antivírus de Arquivos tenta desinfetar todos os objetos infectados ou provavelmente infectados detectados. Se a desinfecção falhar, o Antivírus de Arquivos os excluirá. A ação é realizada se as caixas “Desinfetar” e “Eliminar, se a desinfecção falhar” forem selecionadas.



Excluir: O Antivírus de Arquivos exclui objetos infetados. Esta ação será executada se a caixa “Desinfetar” estiver desmarcada e a caixa “Excluir” estiver selecionada.

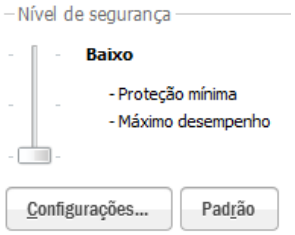


4.1.3 Antivírus de E-mail:



"Ativar o Antivírus de Email": Se estiver marcado, o Antivírus de Email será carregado ao iniciar o sistema operacional, sendo executado continuamente, verificando os emails dos protocolos POP3, SMTP, IMAP, MAPI e NNTP, além das conexões seguras (SSL) para POP3, SMTP e IMAP. Se a caixa estiver desmarcada, o Antivírus de Email estará desativado.

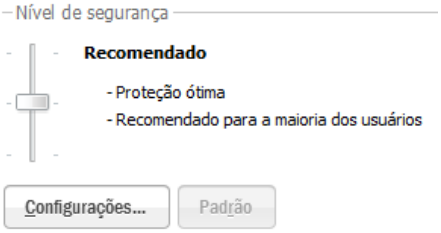
- Nível de Segurança: O usuário tem três níveis para ajustar de acordo com suas condições de trabalho e sua situação atual:



Baixo: O Antivírus de Email verifica apenas as mensagens recebidas e executa a análise heurística superficial. Os arquivos anexos inseridos não são verificados. O Antivírus de Email verificará os emails com velocidade máxima e o menor comprometimento de recursos do sistema. O analisador heurístico permite a detecção de objetos de cujo comportamento no sistema pode causar uma ameaça à segurança. Por exemplo, um objeto pode ser considerado provavelmente infetado se contiver sequências de comandos típicos de objetos maliciosos (abrir arquivo, escrever no arquivo).

O nível de segurança Baixo é usado ao trabalhar em um ambiente protegido confiável. Um exemplo de um ambiente como esse pode ser uma rede corporativa com segurança de email centralizada.

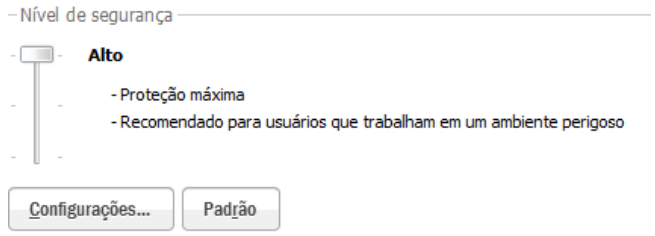
Recomendado: Este nível de segurança garante um equilíbrio ideal entre desempenho e segurança do sistema. O Antivírus de Email verificará as mensagens enviadas e recebidas e executará a análise heurística de média intensidade.



O analisador heurístico permite a detecção de objetos de cujo comportamento no sistema pode causar uma ameaça à segurança. Por exemplo, um objeto pode ser considerado provavelmente infetado se contiver sequências de comandos típicos de objetos maliciosos (abrir arquivo, escrever no arquivo).

Este nível é o modo de segurança padrão (por esse motivo o botão “Padrão” está apagado, pois o mesmo está acionado). É o nível recomendado para a maioria dos usuários.

Alto: O Antivírus de Email aplica o controle mais rígido às mensagens de email. O Antivírus de Email verifica as mensagens enviadas e recebidas e executa a análise heurística profunda.



O analisador heurístico permite a detecção de objetos de cujo comportamento no sistema pode causar uma ameaça à segurança. Por exemplo, um objeto pode ser considerado provavelmente infetado se contiver sequências de comandos típicos de objetos maliciosos (abrir arquivo, escrever no arquivo).

O nível de segurança Alto é aplicado ao trabalhar em um ambiente perigoso. Um exemplo desse tipo de ambiente é uma conexão com um serviço de email gratuito, de uma rede que não tem uma proteção de email centralizada.

*Dúvidas sobre o botão “Configurações” deverão ser esclarecidas através do atendimento de suporte nível 2.

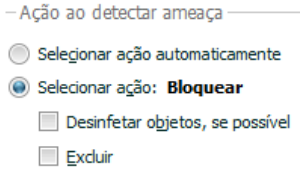
- Ação ao detectar ameaça:

“Selecionar ação automaticamente”: Ao detectar objetos perigosos, o Antivírus de Email executará automaticamente uma ação. Para objetos infetados, a ação é Desinfetar. Excluir se a desinfecção falhar e, para objetos provavelmente infectados a ação é Ignorar. Antes de tentar desinfetar ou excluir um objeto infectado, o Antivírus de Email cria uma cópia de backup para posterior restauração ou desinfecção.

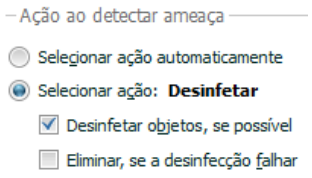
A ação automática pode ser desmarcada para o usuário configurar a forma de adotar uma ação quando um arquivo malicioso for encontrado.

“Selecionar ação”: Temos quatro opções para ajustar de acordo com o perfil do usuário:

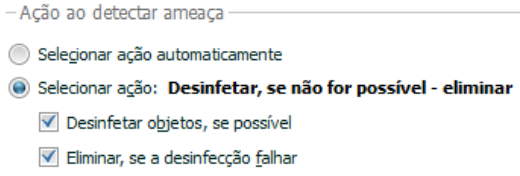
Bloquear: O Antivírus de Email bloqueia o acesso ao objeto. As informações relevantes são registradas no relatório. Negação de acesso de aplicativos externos a um objeto. Um objeto bloqueado não pode ser lido, executado, alterado ou excluído. Esta ação será executada se as caixas de seleção Desinfetar e Excluir estiverem desmarcados.



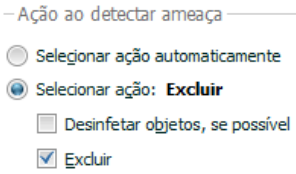
Desinfetar: O Antivírus de Email tenta desinfetar automaticamente todos os objetos infectados ou possivelmente infectados detectados. Se a desinfecção falhar, o Antivírus de Email marca esta mensagem como contendo um objeto infectado/perigoso, mas não executa ações adicionais neste objeto. A ação será executada se a caixa Eliminar se a desinfecção falhar estiver desmarcado.



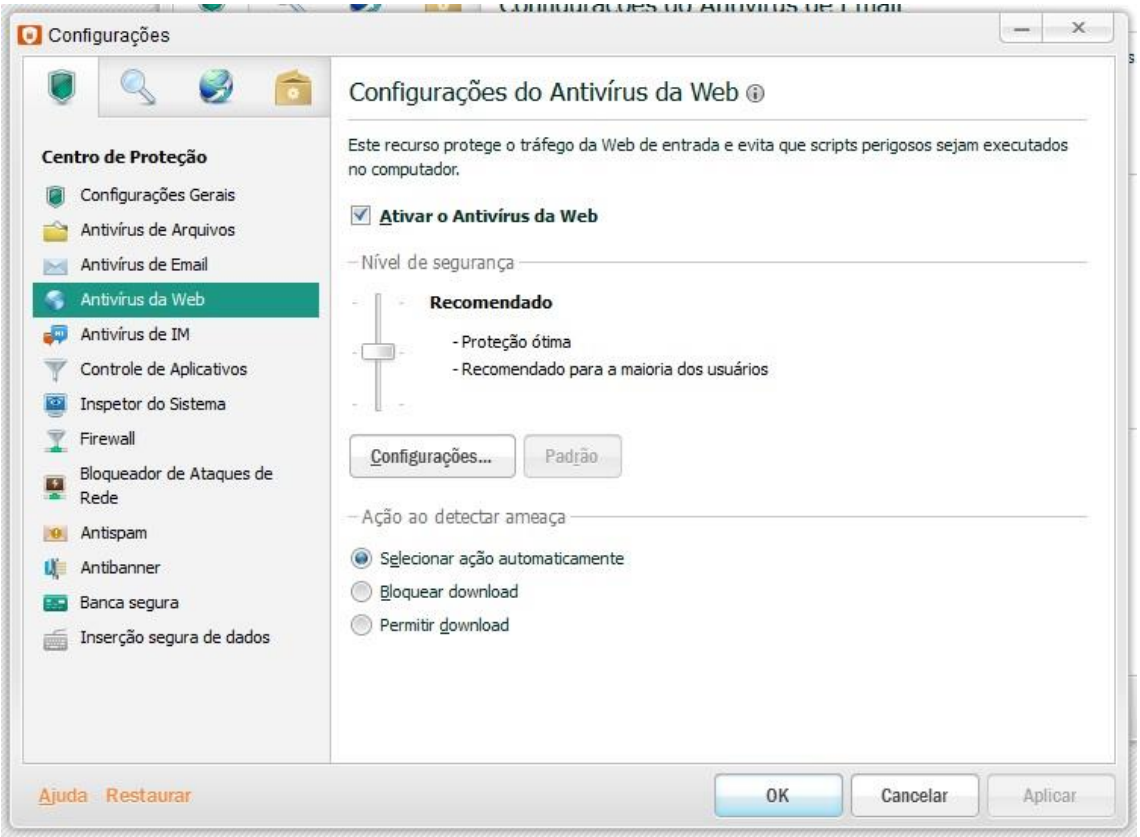
Desinfetar, se não for possível Eliminar: O Antivírus de Email tenta desinfetar automaticamente todos os objetos infectados ou possivelmente infectados detectados. Se a desinfecção falhar, o Antivírus de Email os excluirá. A ação é realizada se as caixas Desinfetar e Eliminar forem selecionados.



Excluir: O Antivírus de Email exclui objetos infetados. Esta ação será executada se a caixa Desinfetar estiver desmarcado.



4.1.4 Antivírus da Web:

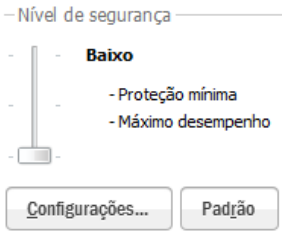


"Ativar o Antivírus da Web": Esta caixa ativa/desativa a proteção em tempo real. O Antivírus da Web protegerá os dados recebidos pelo computador através dos protocolos HTTP e FTP, O aplicativo controlará evitando que scripts perigosos sejam executados no computador, os interceptará e verificará a presença de vírus. Dependendo dos resultados da verificação, você poderá bloquear ou permitir a execução do script.

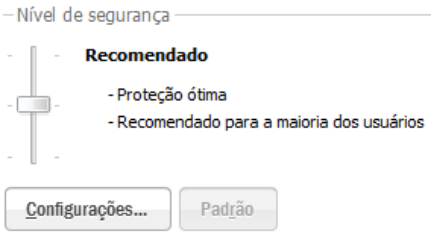
Se a caixa estiver desmarcada, o Antivírus da Web estará desativado. Esta caixa vem marcada por padrão.

- Nível de Segurança: Temos três níveis para ajustar de acordo com o perfil do usuário -

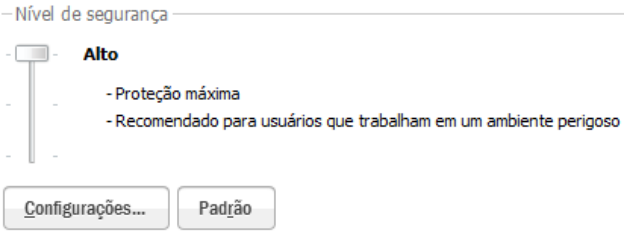
Baixo: Nível de segurança que garante a velocidade máxima ao verificar scripts e o tráfego da Web. O Antivírus da Web não verifica arquivos comprimidos e executa uma análise heurística superficial.



Recomendado: Nível de segurança que garante a proteção e a velocidade ideais ao verificar scripts e o tráfego da Web. O Antivírus da Web verifica arquivos comprimidos incorporados com tamanho não superior a 1 MB e realiza análise heurística de nível médio. Este é o modo de segurança padrão (por esse motivo o botão "Padrão" está apagado, pois o mesmo está acionado).



Alto: O Antivírus da Web aplica o controle mais rígido aos scripts e objetos recebidos por HTTP e FTP. Realiza a verificação detalhada de todos os objetos usando o conjunto completo de bancos de dados do aplicativo e verifica todos os arquivos comprimidos incorporados com tamanho não superior a 1 MB.



O Antivírus da Web executa a análise heurística com seu nível de verificação mais profundo.

Por exemplo, um objeto pode ser considerado provavelmente infetado se contiver sequências de comandos típicos de objetos maliciosos (abrir arquivo, escrever no arquivo).

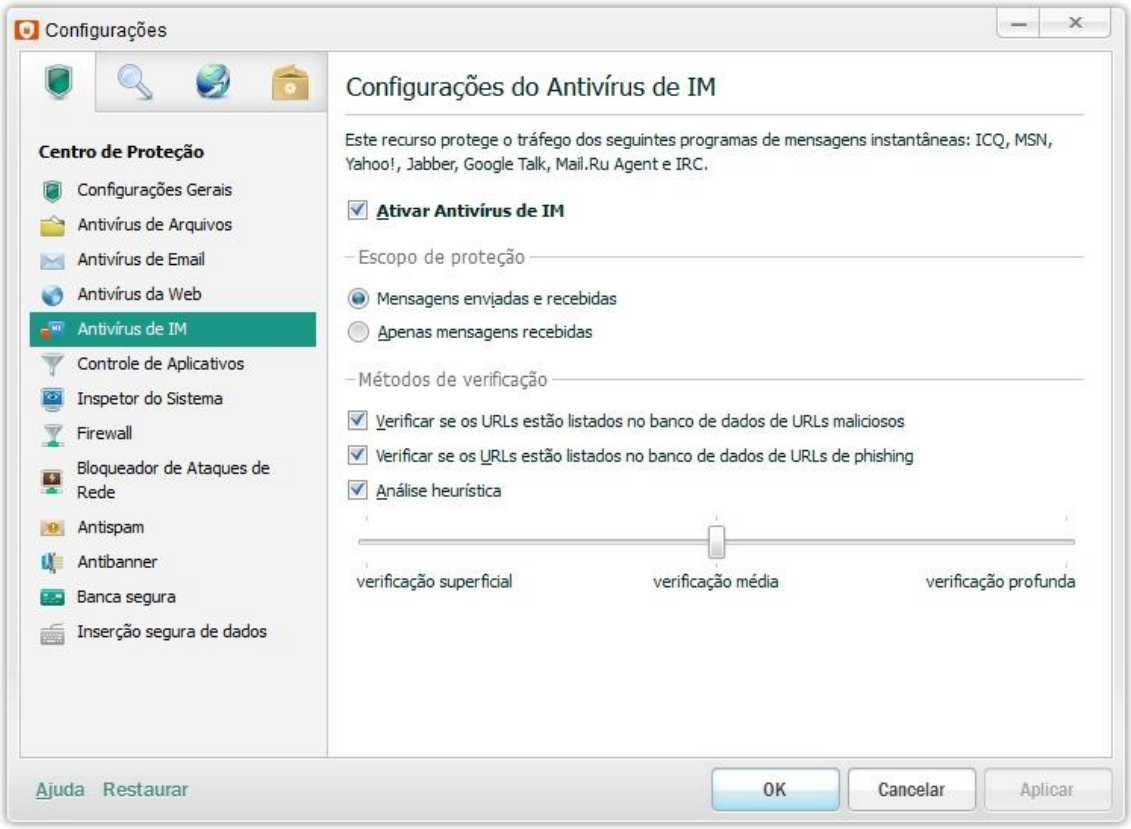
- Ação ao detectar ameaça –

“Selecionar ação automaticamente”: O Antivírus da Web seleciona uma ação automática de acordo com suas configurações atuais. Se um recurso da Web estiver listado entre as exclusões ou não contiver nenhum objeto malicioso, o Antivírus da Web permitirá que você o carregue. Se o Antivírus da Web detectar uma ameaça na verificação, ele bloqueará o download do objeto.

“Bloquear download”: Se for detectada uma ameaça, o Antivírus da Web bloqueará o acesso ao objeto e exibirá uma mensagem sobre isso na tela.

“Permitir download”: Se for detectada uma ameaça, o Antivírus da Web permitirá o download do objeto.

4.1.5 Antivírus de IM:



"Ativar Antivírus de IM": Se a caixa estiver marcada, o Antivírus de IM será executado ao iniciar o sistema operacional, permanecerá permanentemente na RAM do computador e verificará todas as mensagens enviadas e recebidas transferidas por programas de IM (Skype, Facebook Chat IM, Jabber, Google Talk, Mail.Ru Agent ou IRC). Esta caixa vem marcada por padrão.

- Escopo de proteção -

“Mensagens enviadas e recebidas”: O Antivírus de IM verifica as mensagens enviadas e recebidas quanto à presença de objetos perigosos ou URLs contidos nos bancos de dados de endereços maliciosos e de phishing.

“Apenas mensagens recebidas”: O Antivírus de IM verifica apenas as mensagens recebidas.

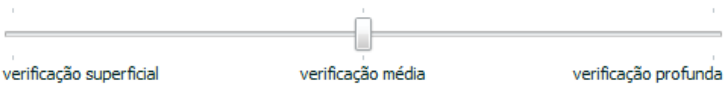
- Métodos de verificação -

"Verificar se os URLs estão listados no banco de dados de URLs maliciosos": A caixa ativa/desativa a verificação da inclusão dos links contidos em mensagens instantâneas na lista de endereços maliciosos. A lista é criada pelos especialistas da Nextel Proteção Online Lab e faz parte do kit de distribuição do aplicativo. Esta caixa vem marcada por padrão.

"Verificar se os URLs estão listados no banco de dados de URLs de phishing": A caixa ativa/desativa a verificação da inclusão dos links contidos em mensagens instantâneas na lista de endereços de phishing. Os bancos de dados do Nextel Proteção Online incluem todos os sites conhecidos no momento por serem usados como sites de phishing. A Nextel Proteção Online Lab complementa essa lista com endereços obtidos de uma organização internacional, o Anti-Phishing Working Group. A lista de endereços é atualizada com a atualização dos bancos de dados do Nextel Proteção Online. Esta caixa vem marcada por padrão.

"Análise Heurística": Esta caixa ativa/desativa o uso da análise heurística ao verificar mensagens e URLs enviados por programas de IM. Uma tecnologia de detecção de informações sobre ameaças que ainda não foram adicionadas aos bancos de dados da Nextel Proteção Online Lab. O analisador heurístico permite a detecção de objetos de cujo comportamento no sistema pode causar uma ameaça à segurança. Por exemplo, um objeto pode ser considerado provavelmente infetado se contiver sequências de comandos típicos de objetos maliciosos (abrir arquivo, escrever no arquivo). Esta caixa vem marcada por padrão.

“Barra deslizante”: Altera o nível de detalhamento da verificação de mensagens de programas de IM. O nível de detalhamento define o equilíbrio entre a profundidade das pesquisas de novas ameaças, a carga sobre os recursos do sistema operacional e o tempo necessário para a verificação.



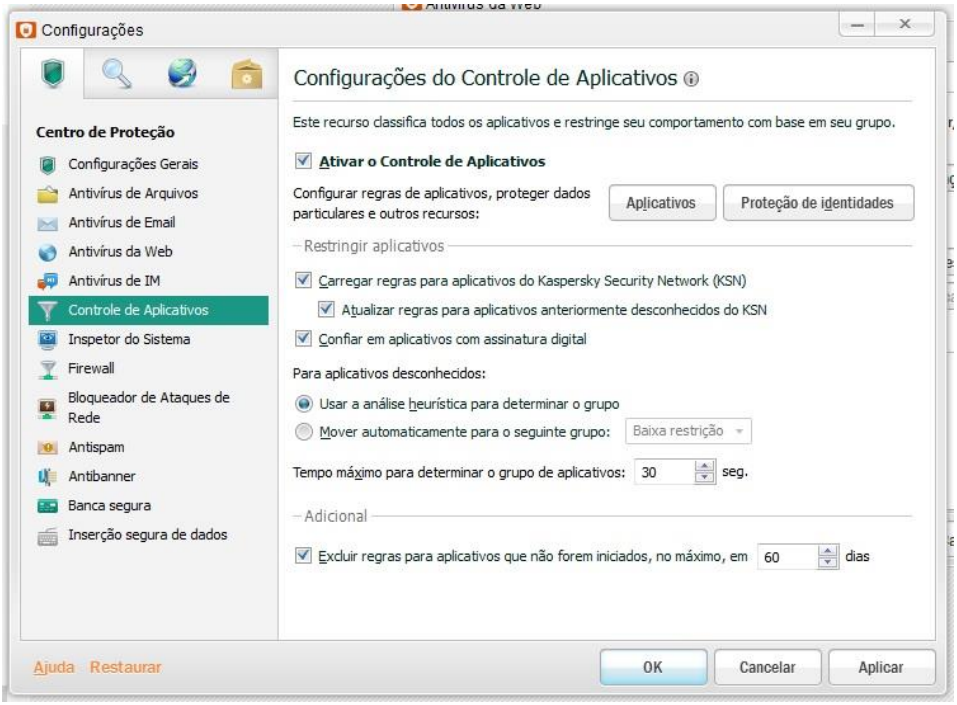
Estão disponíveis os seguintes níveis de verificação:

- **Verificação superficial:** O analisador heurístico verifica as mensagens de programas de IM quanto à presença de ameaças usando um conjunto de sinais mínimo. A verificação é mais rápida e consome menos recursos, com um número mais baixo de falsos positivos.

- **Verificação média:** O analisador heurístico verifica as mensagens de programas de IM quanto à presença de ameaças, usando um conjunto de sinais que permite manter o equilíbrio necessário entre velocidade e nível de detalhamento da verificação, além de evitar um impacto excessivo de possíveis falsos positivos. Este é o nível padrão.

- **Verificação profunda:** O analisador heurístico verifica as mensagens de programas de IM quanto à presença de ameaças usando um conjunto de sinais máximo. A verificação é realizada em detalhe, consome menos recursos e demora mais tempo. É provável serem detectados falsos positivos.

4.1.6 Controle de Aplicativos:



“Ativar o Controle de Aplicativos”: Esta caixa ativa/desativa o Controle de Aplicativos.

“Aplicativos”: Neste botão, a janela Aplicativos é aberta. Nesta janela, você pode editar a lista de regras para aplicativos.

"Proteção de identidades": Neste botão, a janela Proteção de Identidades Digitais é aberta. Nesta janela, é possível criar uma usita de dados pessoais e uma lista de configurações e recursos do sistema operacional cujo acesso deve ser monitorado pelo Controle de Aplicativos.

- Restringir aplicativos -

“Carregar regras para aplicativos do Kaspersky Security Network (KSN)”: O Controle de Aplicativos enviará uma solicitação ao banco de dados do (CSN) para definir o grupo do aplicativo. Se a caixa estiver desmarcada, o Controle de Aplicativos não pesquisará informações no banco de dados do (CSN) para definir o grupo de confiança do aplicativo. Esta caixa vem marcada por padrão.

“Atualizar regras para aplicativos anteriormente desconhecidos do CSN”: As regras de controle para aplicativos anteriormente desconhecidos do (CSN) serão atualizadas automaticamente. Se a caixa estiver desmarcada, a atualização automática de regras para aplicativos anteriormente desconhecidos será desativada. Esta caixa vem marcada por padrão.

“Confiar em aplicativos com assinatura digital”: Os aplicativos com assinaturas digitais serão considerados confiáveis pelo Controle de Aplicativos. O Controle de Aplicativos move esses aplicativos para o grupo Confiável e não verifica sua atividade. Se a caixa estiver desmarcada, os aplicativos com assinaturas digitais não serão considerados confiáveis pelo Controle de Aplicativos e suas atividades serão verificadas. Esta caixa vem marcada por padrão.

- Para aplicativos desconhecidos:

“Usar a análise heurística para definir o grupo”: O Controle de Aplicativos usa a análise heurística para definir o grupo de um aplicativo desconhecido. Após a verificação dos aplicativos, o Controle de Aplicativos os coloca em um grupo.

“Mover automaticamente para o seguinte grupo”: O Controle de Aplicativos coloca automaticamente um aplicativo desconhecido em um dos três grupos de confiança selecionados na lista suspensa. A lista contém os seguintes grupos de confiança: Baixa Restrição, Alta Restrição e Não Confiáveis.

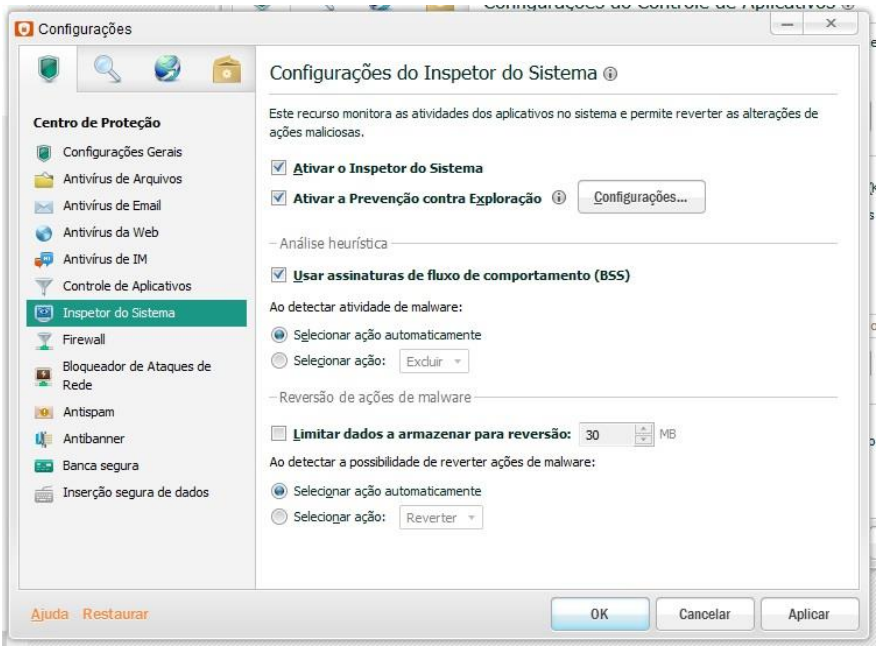
- Tempo máximo para definir o grupo de aplicativos: É o período durante o qual o Controle de Aplicativos verifica os aplicativos em execução usando a análise heurística. O período é definido em segundos.
  Por padrão, o Controle de Aplicativos analisa cada aplicativo por 30 segundos. Se, quando esse período expirar, o Controle de Aplicativos não puder determinar claramente a classificação de ameaça do aplicativo, o componente o moverá para o grupo Baixa Restrição.
  O Controle de Aplicativos continuará verificando o aplicativo em segundo plano e, em seguida, ele será incluído em um grupo de confiança.

- Adicional -

“Excluir regras para aplicativos que não foram iniciados, no máximo, em 60 dias”: Esta caixa ativa/desativa a opção de excluir automaticamente as regras para aplicativos que não foram executadas durante o período especificado. O período é especificado em dias.

Por padrão, o Controle de Aplicativos exclui as regras para aplicativos que não foram executados por mais de 60 dias. Esta caixa vem marcada por padrão.

4.1.7 Inspetor do Sistema:



“Ativar Inspetor do Sistema”: O Inspetor do Sistema coletará e salvará dados de todos os eventos que ocorrem no sistema (como a modificação de um arquivo, a modificação de chaves do Registro, a execução de drivers, a tentativa de desligar o computador). Esses dados são usados para rastrear a atividade maliciosa de aplicativos e restaurar o sistema ao estado anterior ao surgimento de um aplicativo malicioso (reversão das ações do aplicativo malicioso).

O Inspetor do Sistema coleta dados de diversas fontes, inclusive outros componentes do Nextel Proteção Online. Esta caixa vem marcada por padrão.

“Ativar Prevenção de Exploração”: O Nextel Proteção Online rastreia os arquivos executados por aplicativos vulneráveis. Se detectar uma tentativa para executar um arquivo executável a partir de um aplicativo vulnerável que não tenha sido iniciado pelo usuário, o aplicativo bloqueia a execução do arquivo.

As informações sobre o bloqueio do arquivo executável executado são registradas no relatório de Prevenção de Exploração. Esta caixa vem marcada por padrão.

"Configurações": Ao clicar nesse botão, a janela Configurações da Prevenção de Exploração é aberta. Nesta janela você pode configurar o comportamento do Inspetor do Sistema quando este detectar qualquer atividade perigosa de aplicativos. Dúvidas deverão ser esclarecidas através do atendimento de suporte nível 2.

- Análise heurística -

"Usar assinatura de fluxo de comportamento (BSS)": Esta caixa ativa/desativa o uso a tecnologia BSS (Behavior Stream Signatures), que permite analisar as atividades do aplicativo de acordo com as informações coletadas. Se a caixa estiver marcada, o Inspetor do Sistema analisará as atividades do aplicativo de acordo com as informações coletadas e os padrões atualizáveis de atividades perigosas (BSS). O Inspetor do Sistema verifica o nível de semelhança entre as ações do aplicativo e as de um aplicativo malicioso. Se o Inspetor do Sistema analisar a atividade de um aplicativo e considerar que este é malicioso, aplica a ação especificada ao aplicativo (por exemplo, fecha o aplicativo).

Se a caixa estiver desmarcada, o Inspetor do Sistema não analisará as atividades do aplicativo, apenas coletando e armazenando informações sobre a atividade de todos os aplicativos. Esta caixa vem marcada por padrão.

- Ao detectar atividade de malware:

"Selecionar ação automaticamente": Se o Inspetor do Sistema analisar a atividade de um aplicativo e considerar que este é malicioso, reverte as ações do aplicativo e notifica o usuário sobre esse evento. O Inspetor do Sistema adiciona informações sobre o evento e os resultados do processamento ao relatório. No modo de proteção automática, esta opção está selecionada por padrão.

"Selecionar ação":

- **Excluir** – o Inspetor do Sistema exclui o aplicativo malicioso.
- **Encerrar o aplicativo malicioso** – o Inspetor do Sistema encerra todos os processos do aplicativo malicioso.
- **Ignorar** – o Inspetor do Sistema não executa nenhuma ação com o aplicativo.

- Reversão de ações de malware –

“Limitar dados a armazenar para reversão”: Essa caixa ativa/desativa a limitação imposta ao volume de informações armazenadas para reverter ações de um aplicativo malicioso. Esta caixa vem desmarcada por padrão.

No campo de entrada de dados deslizante, junto da caixa de seleção, você pode especificar o volume de memória que o Inspetor do sistema deve usar para reverter as ações de aplicativos maliciosos. O valor é especificado em megabytes. Valor padrão: 20 MB.

- Ao detectar possibilidade de reverter ações de malware:

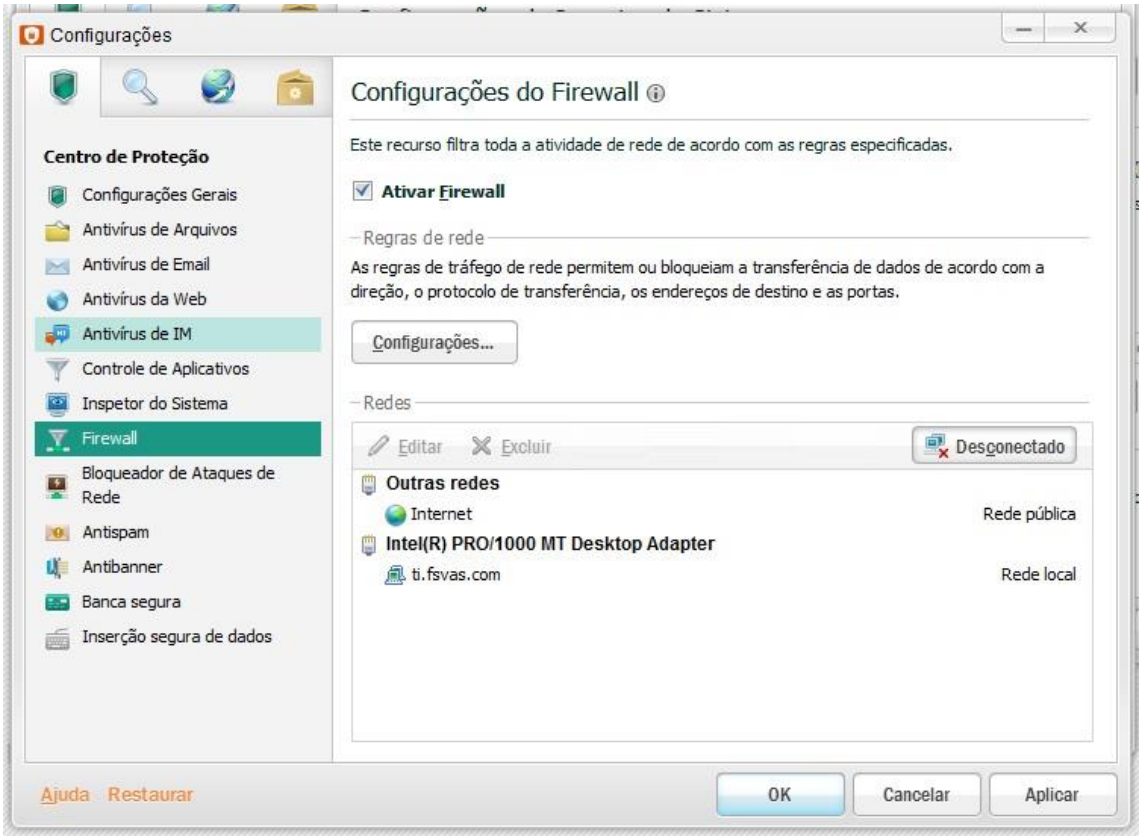
“Selecionar ação automaticamente”: Se as atividades dos componentes: Inspetor do Sistema, Defesa Proativa ou Antivírus de Arquivos ou a execução de uma tarefa de verificação indicar ser necessária uma reversão das ações de um aplicativo, o Inspetor do Sistema a executará automaticamente. Esta opção está selecionada por padrão.

“Selecionar ação”: Se as ações dos componentes: Inspetor do Sistema, Defesa Proativa ou Antivírus de Arquivos ou a execução da tarefa de verificação indicar ser necessária uma reversão, o Inspetor do Sistema executará uma das seguintes ações predefinidas, selecionada na lista suspensa:

- **Reverter** – o Inspetor do Sistema reverte as ações do aplicativo malicioso. Esta ação é selecionada por padrão.

- **Não reverter** – o Inspetor do Sistema salva as informações sobre a atividade maliciosa do aplicativo, mas não revertem suas ações.

4.1.8 Firewall:



“Ativar Firewall”: Esta caixa ativa/desativa o Firewall e vem marcada por padrão.

- Regras de rede: é possível definir as regras de acordo com as quais o Firewall regula as atividades de aplicativos.

Ao clicar no botão **“Configurações”** a janela Firewall é aberta. Nesta janela, é possível definir regras de pacotes e regras para aplicativos, expandir o intervalo de endereços de rede e alterar a lista de recursos cuja atividade de rede é monitorada pelo Firewall.

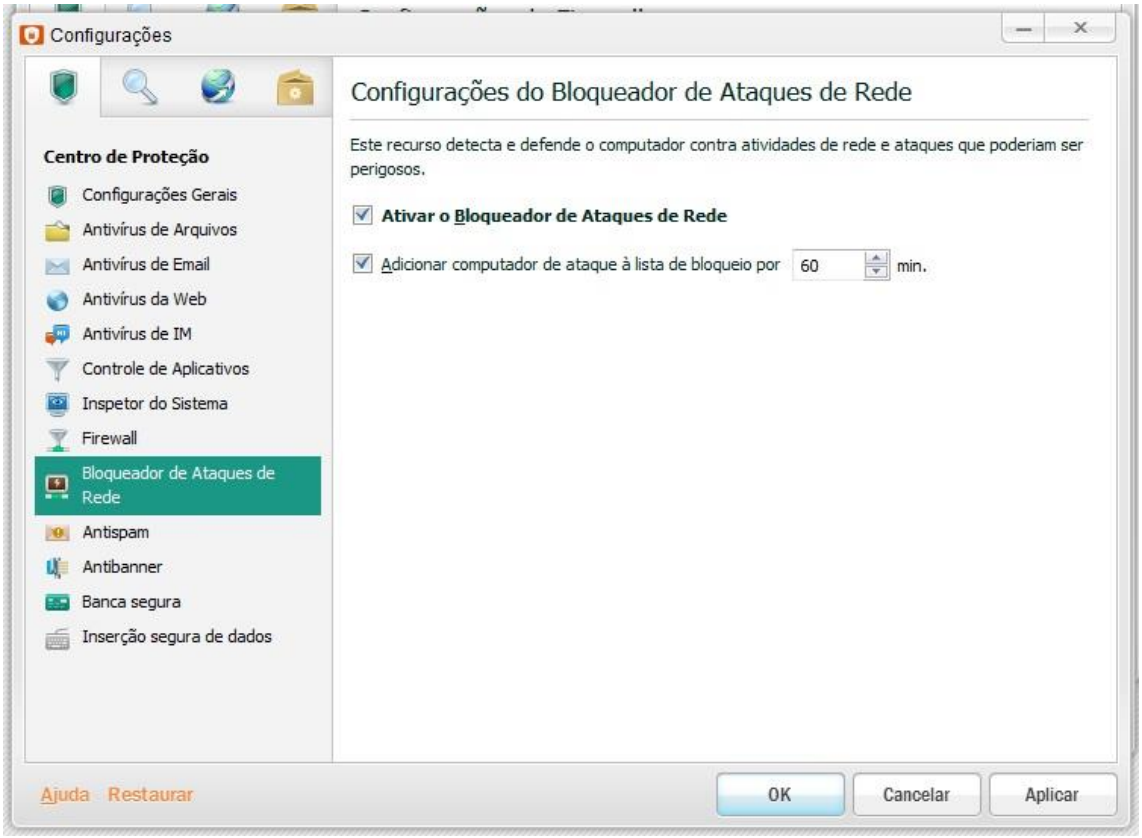
- Redes: Na seção Redes, é possível definir as configurações do controle das conexões de rede detectadas pelo Firewall no computador.

“Editar”: Este botão abre a janela Conexão de rede (se houver uma conexão selecionada) ou Adaptador de rede (se houver um adaptador selecionado). Na janela Conexão de rede, é possível ajustar as configurações para controlar conexões de rede. Na janela Adaptador de rede, é possível configurar o controle das conexões de rede estabelecidas usando um adaptador de rede selecionado. O botão está disponível para conexões ativas e inativas.

“Excluir”: Ao clicar neste botão, o Firewall exclui a conexão da lista.

“Desconectado”: As conexões ativas e inativas são exibidas na lista Redes.

4.1.9 Bloqueador de Ataques de Rede:



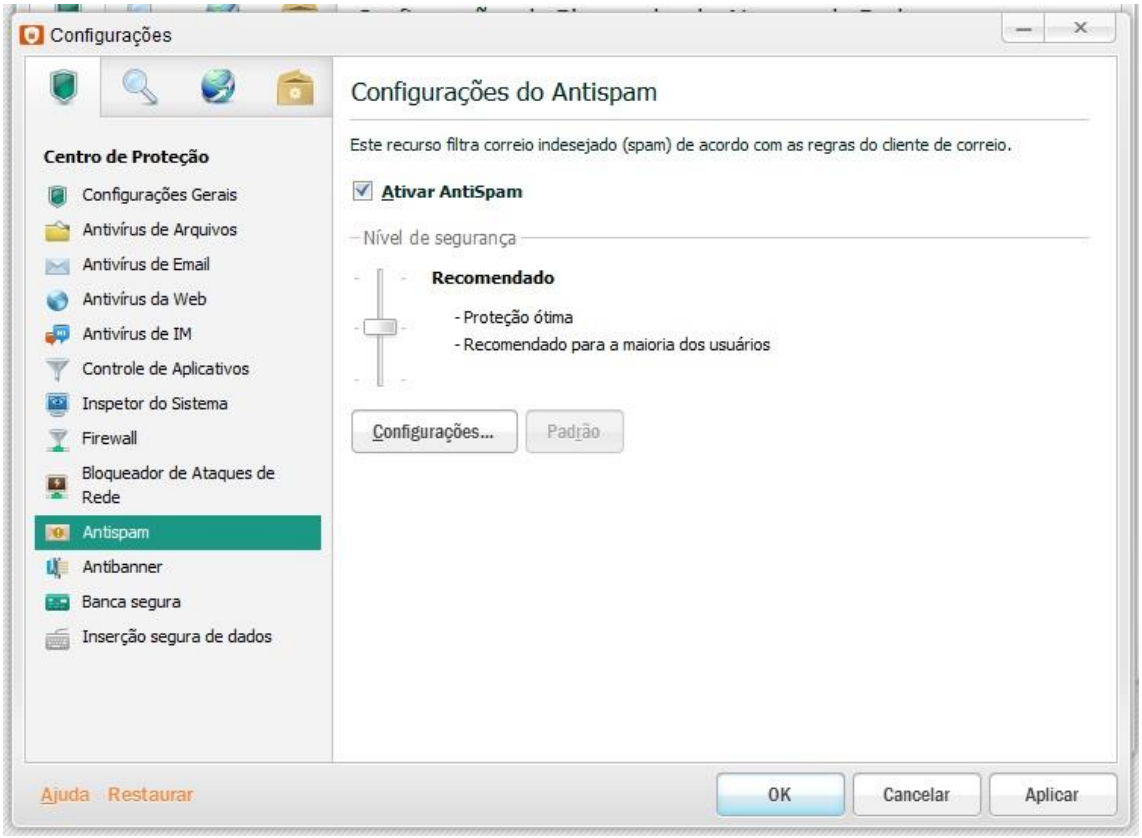
"Ativar Bloqueador de Ataques de Rede": O Bloqueador de Ataques de Rede será carregado ao iniciar o sistema operacional e verificará atividades características de ataques de rede no tráfego de rede de entrada. Ao detectar uma tentativa de ataque ao computador, o Nextel Proteção Online bloqueia toda a atividade de rede do computador que está atacando o seu.

Se a caixa estiver desmarcada, o Bloqueador de Ataques de Rede estará desativado. Esta caixa vem marcada por padrão.

"Adicionar o computador de ataque à lista de computadores bloqueados por 60 min": Esta caixa ativa/desativa a opção para o Bloqueador de Ataques de Rede bloquear a atividade de rede de um computador de ataque durante o intervalo de tempo especificado. O período de tempo é especificado em minutos.

Por padrão, o Bloqueador de Ataques de Rede bloqueia a atividade do computador de ataque por uma hora.

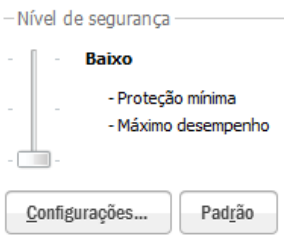
4.1.10 Antispam:



"Ativar Antispam": O Antispam detectará os emails não solicitados (spam) e os processará de acordo com as regras do programa de email. Isso economiza tempo ao trabalhar com emails. Esta caixa vem marcada por padrão.

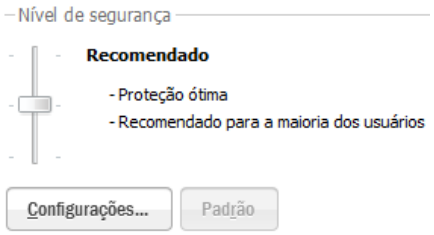
- Nível de segurança: Na seção Nível de segurança, é possível selecionar uma coleção de configurações predefinidas do Antispam. O usuário deve decidir o nível de segurança a ser selecionado de acordo com suas condições de trabalho e sua situação atual.

"**Baixo**": Nível de segurança em que o Antispam aplica o nível mínimo de filtragem de spam. Se o nível de segurança Baixo for definido, o Antispam considerará as mensagens com taxas de spam entre 80 e 99 como spam provável e as mensagens com taxas de spam superiores a 99 como spam. Esta configuração define as condições para a filtragem de emails que passaram pela verificação profunda de elementos das listas de endereços e frases permitidos/bloqueados. A classificação dessas mensagens como spam não é totalmente segura. Assim, o Antispam calcula a probabilidade de a mensagem ser spam.

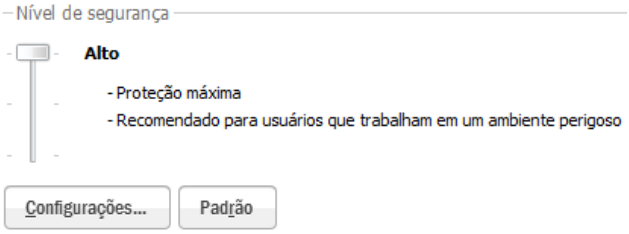


A Taxa de spam é o valor da probabilidade que define se uma mensagem é spam ou não. Se os resultados da verificação da mensagem mostrarem que sua taxa de spam é maior que o valor limite, o Antispam considerará a mensagem como spam ou spam provável. É recomendável definir o nível de segurança Baixo ao trabalhar em um ambiente seguro (por exemplo, ao usar um email corporativo criptografado). A definição do nível de segurança Baixo pode reduzir a frequência de casos em que emails íntegros são reconhecidos como spam ou spam provável.

"**Recomendado**": Este nível de segurança garante um equilíbrio ideal entre desempenho e segurança. É adequado para a maioria das situações. Essa é a configuração padrão (por esse motivo o botão "Padrão" está apagado, pois o mesmo já está acionado).



"**Alto**": Nível de segurança em que o Antispam aplica o nível máximo de filtragem de spam. O Antispam considera uma mensagem como spam provável quando sua taxa de spam excede 50, e como spam quando sua taxa de spam excede 80.

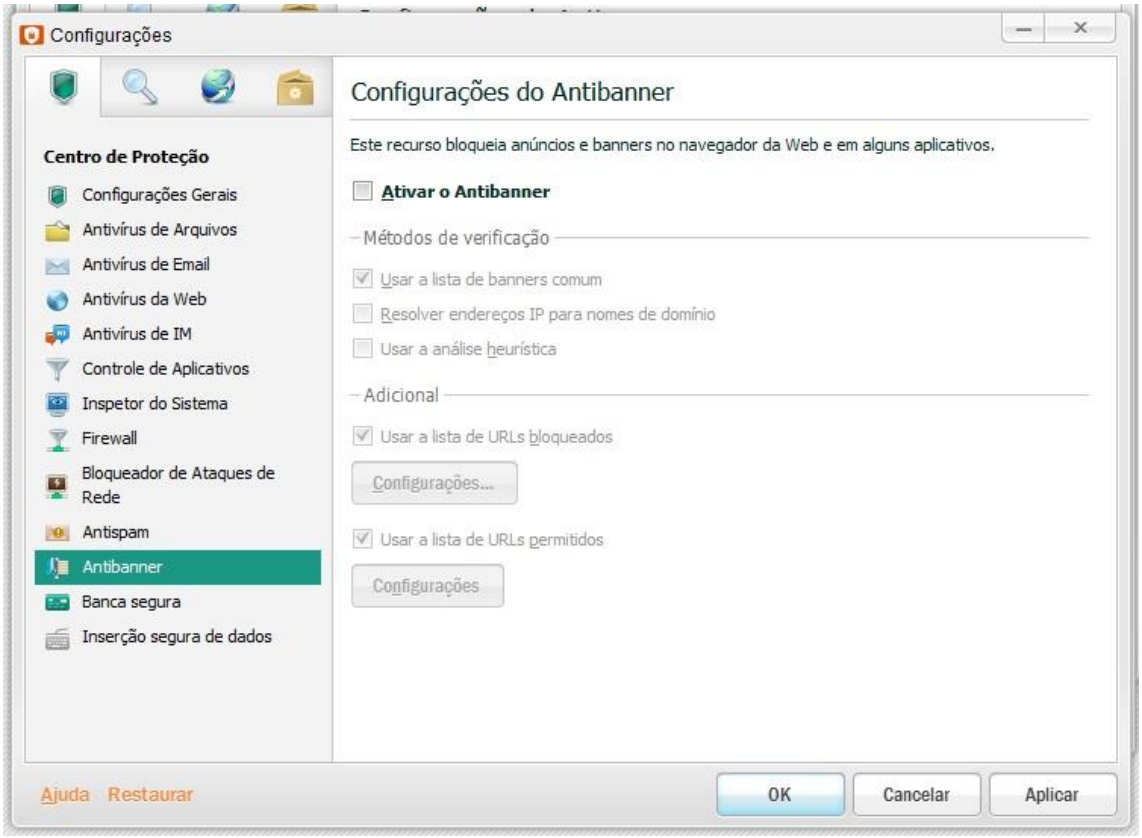


Esta configuração define as condições para a filtragem de emails que passaram pela verificação profunda de elementos das listas de endereços e frases permitidos/bloqueados. A classificação dessas mensagens como spam não é totalmente segura. Assim, o Antispam calcula a probabilidade de a mensagem ser spam.

A Taxa de spam é o valor da probabilidade que define se uma mensagem é spam ou não. Se os resultados da verificação da mensagem mostrarem que sua taxa de spam é maior que o valor limite, o Antispam considerará a mensagem como spam ou spam provável.

É recomendável definir o nível de segurança Alto ao trabalhar em um ambiente perigoso (por exemplo, ao usar um serviço de email gratuito). A definição do nível de segurança Alto pode aumentar a frequência de casos em que emails íntegros são reconhecidos como spam.

4.1.11 Antibanner:



"Ativar Antibanner": Se a caixa estiver marcada, o Antibanner bloqueará os banners exibidos nas páginas da Web que são abertas e na interface de determinados aplicativos.

Por padrão, o Antibanner bloqueia os banners mais conhecidos, cujos URLs são fornecidos com o kit de distribuição do Nextel Proteção Online. Esta caixa vem desmarcada por padrão.

- Métodos de verificação -

"Usar a lista de banners comum": Se a caixa estiver marcada, o Antibanner bloqueará o download de banners de anúncios dos URLs que correspondem às máscaras na lista. Esta caixa vem marcada por padrão.

"Resolver endereços IP para nomes de domínio": Esta caixa ativa/desativa a resolução automática de endereços IP para URLs nas listas de endereços de banners permitidos/bloqueados (por exemplo, o endereço IP 195.27.181.34 para o URL www.Nextel.com.br). Com este recurso, é possível evitar repetir URLs. Esta caixa vem desmarcada por padrão.

“Usar Análise Heurística”: O analisador heurístico permite a detecção de objetos de cujo comportamento no sistema pode causar uma ameaça à segurança. Por exemplo, um objeto pode ser considerado provavelmente infetado se contiver sequências de comandos típicos de objetos maliciosos (abrir arquivo, escrever no arquivo).

Se a caixa estiver marcada, o Antibanner usará a análise heurística para verificar os banners cujos URLs não se encontram na lista fornecida com o kit de distribuição do Nextel Proteção Online. O Antibanner analisa as imagens baixadas para descobrir se elas têm recursos típicos de banners. Com base nessa análise, o Antibanner pode identificar uma imagem como um banner e bloqueá-la. Esta caixa vem desmarcada por padrão.

*Esta funcionalidade não está disponível no Microsoft Internet Explorer 10 aberto no Microsoft Windows 8.

- Adicional –

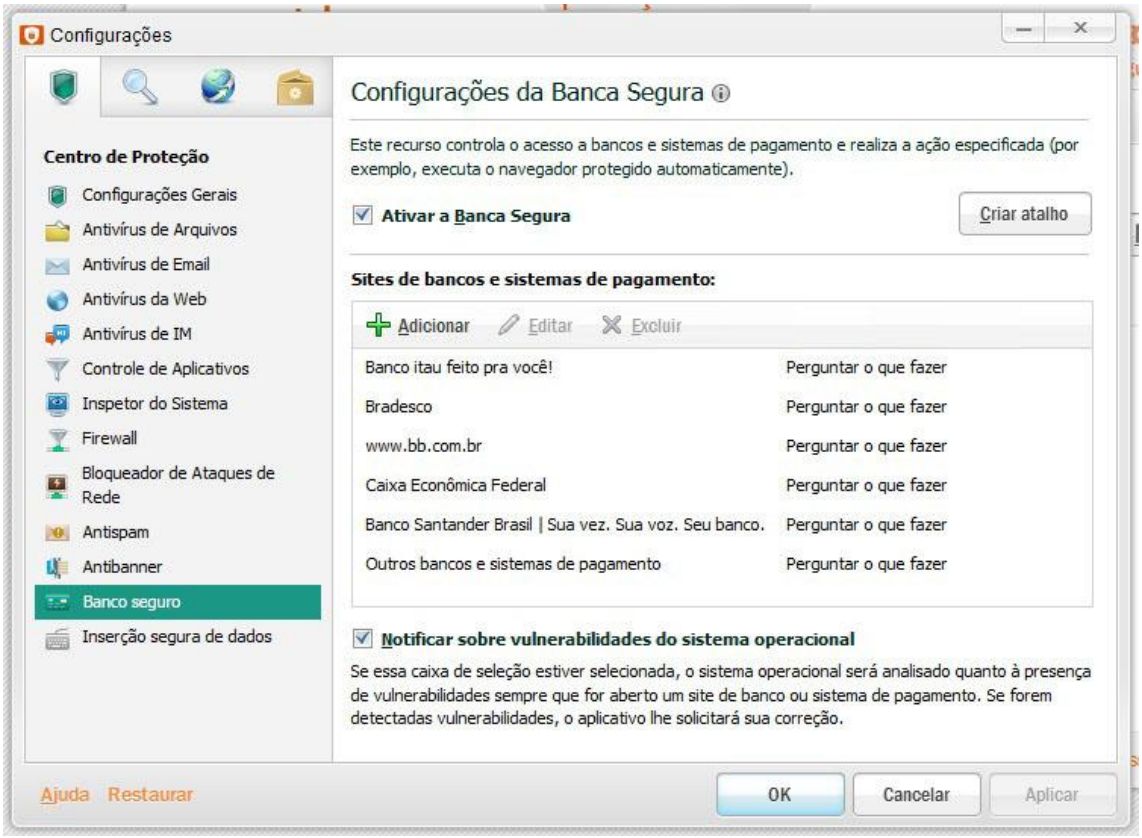
“Usar a lista de URLs bloqueados”: O Antibanner bloqueará os banners cujos URLs estão incluídos na lista de endereços bloqueados. Se a caixa estiver desmarcada, o Antibanner não verificará se o URL do banner está incluído na lista de endereços bloqueados. Esta caixa vem marcada por padrão.

“Configurações”: Ao clicar neste botão, é aberta a janela URLs bloqueados, na qual é possível criar uma lista de endereços de banners bloqueados. Nesta janela, é possível adicionar o URL de um banner ou uma máscara de URLs à lista de endereços bloqueados.

“Usar a lista de URLs permitidos”: O Antibanner não bloqueará o banner cujo URL está incluído na lista de endereços permitidos. Esta caixa vem marcada por padrão.

“Configurações” Ao clicar neste botão, é aberta a janela URLs permitidos, na qual é possível criar uma lista de endereços de banners permitidos. Nesta janela, é possível adicionar o URL de um banner ou uma máscara de URLs à lista de endereços permitidos.

4.1.12 Banco Seguro:



"Ativar o Banco seguro": O Nextel Proteção Online monitora todas as tentativas de acessar sites de bancos ou sistemas de pagamento e realiza a ação configurada como padrão ou especificada pelo usuário. Por padrão, quando é executado no modo Banco Seguro, o Nextel Proteção Online solicita ao usuário que confirme a inicialização da Execução Segura de Sites.

Se a caixa de seleção estiver desmarcada, o Nextel Proteção Online permite o acesso a sites de bancos e sistemas de pagamento usando um navegador da Web padrão. Esta caixa vem marcada por padrão.

"Criar atalho": Clicar nesse botão faz com que o Nextel Proteção Online crie um atalho para executar o Banco seguro. Esse atalho permite abrir uma janela com uma lista de sites de bancos ou sistemas de pagamento que requerem o navegador protegido para acesso.

- Sites de bancos e sistemas de pagamento: Contém uma lista de sites de bancos e sistemas de pagamento que, quando acessados, requerem que o Nextel Proteção Online execute a ação especificada pelo usuário. Para cada item na lista, é exibido o URL de um site e a ação realizada ao acessar esse site. Por padrão, a lista contém o item Outros bancos e sistemas de pagamento.

Contamos com três botões para customizar a lista de banco seguro:

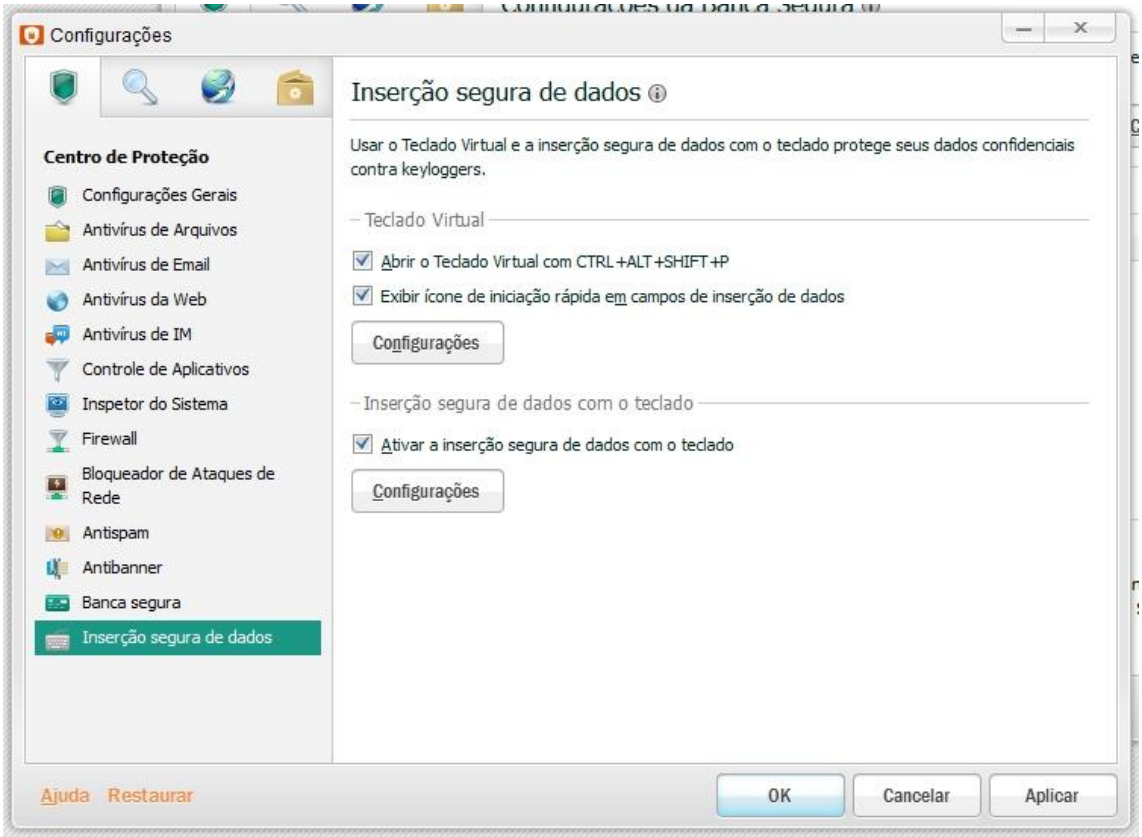
- Adicionar: Ao clicar neste botão, você pode adicionar o site de um banco ou sistema de pagamento ao qual, quando acessado, o Nextel Proteção Online executado no modo Banco Seguro aplica a ação especificada (por exemplo, executa a Execução Segura de Sites).

- Editar: Ao clicar neste botão você pode configurar um modo de execução do Banco seguro que deve ser usado ao acessar o site de um banco ou sistema de pagamento.

- Excluir: Clicar nesse botão remove o site selecionado de um banco ou sistema de pagamento da lista.

"Notificar sobre vulnerabilidades do sistema operacional": Ativa /Desativa a exibição de notificações que informam o usuário sobre o perigo das tentativas de acessar o site de um banco ou sistema de pagamento devido a uma vulnerabilidade no sistema operacional. O Nextel Proteção Online pergunta se deseja baixar a atualização necessária a partir do site do fornecedor do sistema operacional. Se a atualização automática do sistema operacional estiver desativada, o Nextel Proteção Online pergunta se deseja ativá-la. Esta caixa vem marcada por padrão.

4.1.13 Inserção segura de dados:



- Teclado Virtual –

“Abrir o Teclado Virtual com CTRL+ALT+SHIFT+P”: Esta caixa de seleção ativa/desativa o acesso rápido ao Teclado Virtual usando atalho de teclado CTRL+ALT+SHIFT+P. Esta caixa vem marcada por padrão.

“Exibir ícone de iniciação rápida em campos de inserção de dados”: Esta caixa de seleção ativa/desativa a exibição do ícone de início rápido do Teclado Virtual em campos de entrada de sites. Por padrão, a caixa fica desmarcada até que o computador seja reiniciado pela primeira vez após a instalação do aplicativo; após reiniciá-lo, a caixa fica selecionada.

“Configurações”: Ao clicar nesse botão você pode especificar os sites em que o ícone de iniciação rápida do Teclado Virtual deve ser exibido nos campos de entrada. Na janela pode também criar listas de sites nos quais a exibição do ícone de iniciação rápida do Teclado Virtual deve ser ativada ou desativada, independentemente das categorias de sites selecionadas.

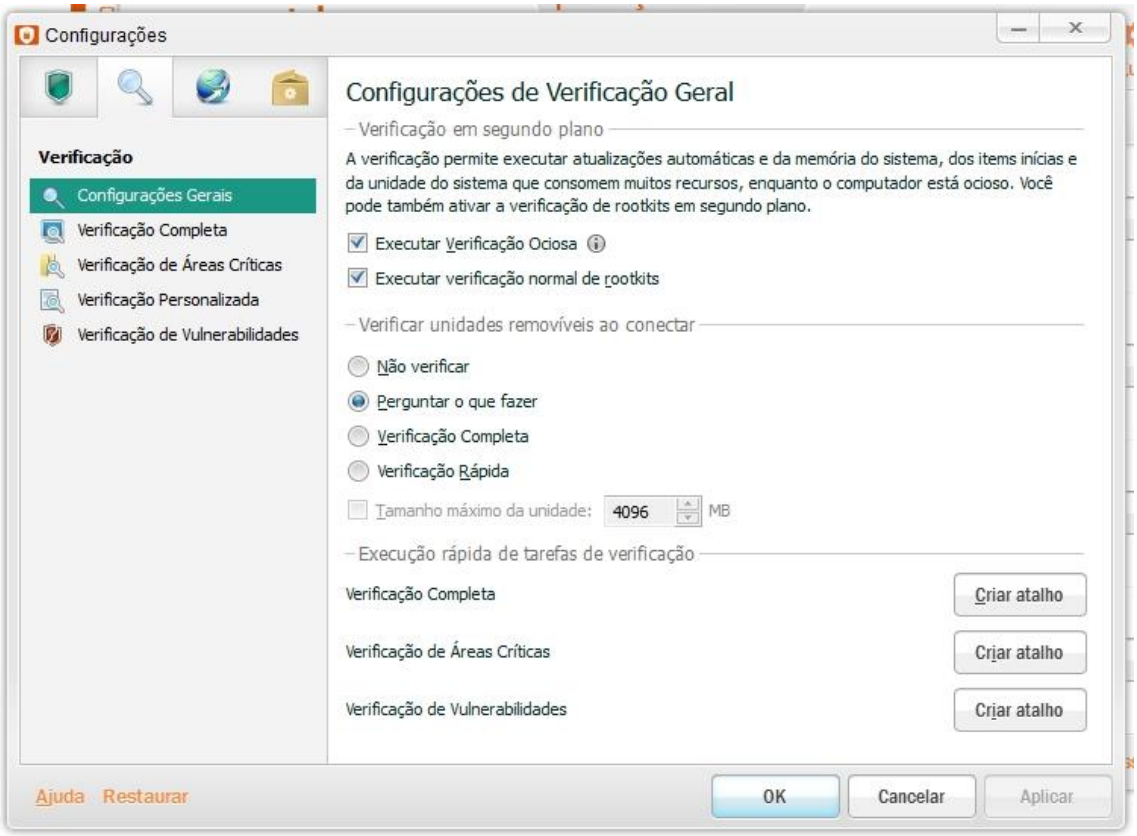
- Inserção segura de dados com o teclado -

“Ativar a inserção segura de dados com o teclado”: Esta caixa de seleção ativa/desativa a proteção da inserção de dados com o teclado do computador. Por padrão, a caixa fica desmarcada até que o computador seja reiniciado pela primeira vez após a instalação do aplicativo; após reiniciá-lo, a caixa fica selecionada.

“Configurações”: Ao clicar neste botão você pode especificar em que sites a inserção de dados com o teclado do computador deve ser protegida. Na janela também é possível criar listas de sites nos quais a proteção da inserção de dados com o teclado deve ser ativada ou desativada, independentemente das categorias de sites selecionadas.

4.2 VERIFICAÇÃO

4.2.1 Configurações Gerais:



- Verificação em segundo plano: é possível configurar as tarefas de atualização e verificação para um momento em que o computador não está sendo usado.

"Executar Verificação Ociosa": Esta caixa ativa/desativa a execução de tarefas (verificação da memória do sistema, da partição do sistema ou de objetos de inicialização) e de tarefas de atualização automática enquanto o computador está bloqueado ou a proteção de tela está ativada.

Se o computador estiver trabalhando com a bateria, o Nextel Proteção Online não executará nenhuma tarefa enquanto o computador estiver ocioso. Esta caixa vem marcada por padrão.

"Executar verificação normal de rootkits": Rootkits é o nome que se dá a um programa ou um conjunto de programas desenvolvidos para ocultar rastros de um invasor ou um malware no sistema operacional. Em sistemas operacionais baseados em Windows, um rootkit normalmente significa um programa que invade o sistema operacional e intercepta suas funções (APIs do Windows). Acima de tudo, a interceptação e modificação de funções de APIs de nível inferior permite que esse programa mascare sua presença no sistema.

Um rootkit pode geralmente mascarar a presença de quaisquer processos, pastas e arquivos que estão armazenados em uma unidade de disco, além de chaves de registro, caso sejam descritas na configuração do rootkit. Vários rootkits instalam seus próprios drivers e serviços no sistema operacional (eles também são "invisíveis"). Esta caixa vem marcada por padrão.

- Verificar unidades removíveis ao conectar -

"Não verificar": Quando você conecta uma unidade removível, o Nextel Proteção Online não a verifica e não pergunta o que fazer com ela.

"Perguntar o que fazer": Quando aparecer uma mídia removível no sistema, o Nextel Proteção Online perguntará o que fazer: Verificação Rápida, Verificação Completa ou Não verificar. Esta é a configuração padrão.

"Verificação Completa": Quando aparecer uma mídia removível no sistema, o Nextel Proteção Online executará uma verificação completa de todos os seus arquivos, de acordo com as configurações da tarefa de Verificação Completa.

"Verificação Rápida": Quando aparecer uma mídia removível no sistema, o Nextel Proteção Online executará uma verificação de todos os arquivos no disco rígido, de acordo com as configurações da tarefa de Verificação de Áreas Críticas.

"Tamanho máximo da unidade": O Nextel Proteção Online verificará as unidades removíveis que não excederem o tamanho máximo especificado. O tamanho da unidade removível é especificado em megabytes. Por padrão, o valor é definido como 4096 MB. Se a caixa estiver desmarcada, o Nextel Proteção Online verificará as unidades removíveis de qualquer tamanho. Esta caixa vem desmarcada por padrão.

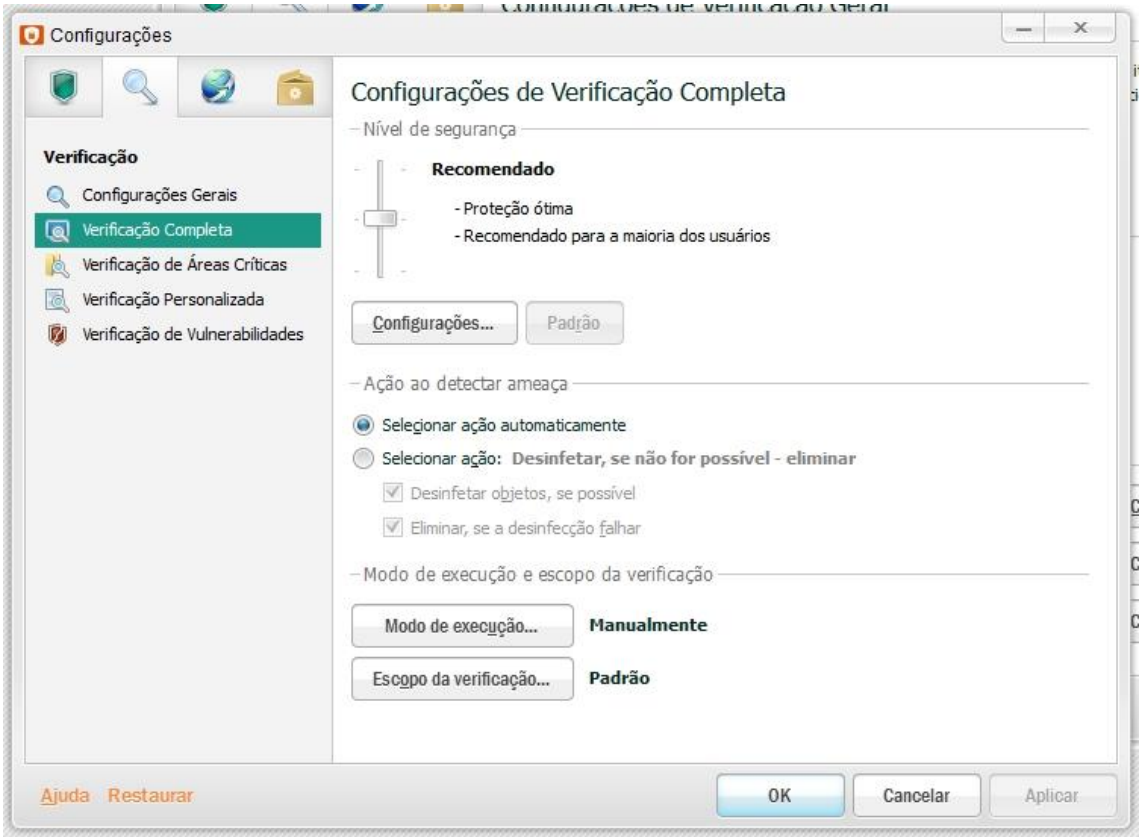
- Execução rápida de tarefas de verificação -

“Verificação Completa”: Criar Atalho, é possível selecionar uma pasta na qual você deve criar um atalho de início rápido para a verificação completa do computador quanto à presença de vírus e especificar o nome do arquivo do atalho. Por padrão, o Nextel Proteção Online cria um atalho denominado Full Scan.lnk na área de trabalho do computador.

“Verificação de Áreas Críticas”: Criar Atalho, é possível selecionar uma pasta na qual você deve criar um atalho de início rápido para a verificação das áreas críticas quanto à presença de vírus e especificar o nome do atalho. Por padrão, o Nextel Proteção Online cria um atalho denominado Critical Areas Scan.lnk na área de trabalho do computador.

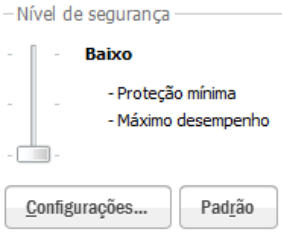
“Verificação de Vulnerabilidades”: Criar Atalho, é possível selecionar uma pasta na qual você deve criar um atalho de início rápido para a verificação de vulnerabilidades e especificar o nome do atalho. Por padrão, o Nextel Proteção Online cria um atalho denominado Vulnerability Scan.lnk na área de trabalho do computador.

4.2.2 Verificação Completa



- Nível de segurança: É possível selecionar as configurações de verificação predefinidas usando o controle deslizante. Você pode selecionar um dos três níveis de segurança criados pelos especialistas do Nextel Proteção Online ou ajustar você mesmo às configurações da verificação.

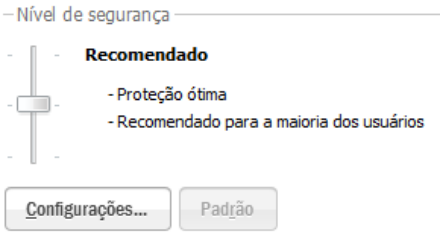
"**Baixo**": Este nível de segurança é a melhor opção para tratar aplicativos com requisitos de RAM significativos, pois o número de arquivos que devem ser verificados é menor nesse nível.



Ao contrário das configurações de verificação padrão, com as configurações de verificação desse nível de segurança, o Nextel Proteção Online verifica apenas os arquivos novos e alterados.

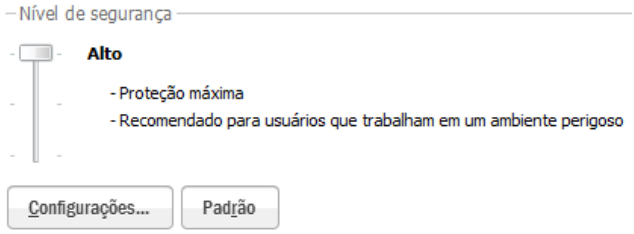
Se forem necessários mais de 180 segundos para verificar os arquivos, o Nextel Proteção Online excluirá esses arquivos da verificação.

"**Recomendado**": Este nível de segurança é adequado na maioria dos casos e recomendado pelos especialistas do Nextel Proteção Online. Garante um equilíbrio ideal entre desempenho e segurança.



Essa é a configuração padrão (por esse motivo o botão "Padrão" está apagado, pois o mesmo já está acionado).

"**Alto**": Esse nível de segurança deverá ser selecionado quando a probabilidade de infecção do computador for muito alta. Ao contrário das configurações de verificação padrão, com as configurações de verificação desse nível de segurança, o Nextel Proteção Online verifica todos os tipos de arquivos. Ao verificar arquivos compostos, o Nextel Proteção Online também verifica os arquivos com formato de email.



*Dúvidas sobre o botão "Configurações" deverão ser esclarecidas através do atendimento de suporte nível 2.

- Ação ao detectar ameaça -

"Selecionar ação automaticamente"; Ao detectar objetos perigosos, o Nextel Proteção Online executará automaticamente a ação: Para objetos infectados, ação é Desinfetar, se não for possível, excluir; para objetos provavelmente infectados, é Ignorar. Antes de tentar desinfetar ou excluir um objeto infectado, o Nextel Proteção Online cria uma cópia de backup para posterior restauração ou desinfecção.

"Selecionar ação"; Se for detectado um objeto perigoso, o Nextel Proteção Online automaticamente realiza a ação especificada:

- **Desinfetar, Eliminar se a desinfecção falhar:** O Nextel Proteção Online tenta desinfetar todos os objetos infectados ou provavelmente infectados detectados. Se a desinfecção falhar, o Nextel Proteção Online os excluirá.

- **Bloquear:** O Nextel Proteção Online bloqueia o acesso ao objeto. As informações sobre esse evento são registradas em um relatório. Negação de acesso de aplicativos externos a um objeto. Um objeto bloqueado não pode ser lido, executado, alterado ou excluído.

- **Desinfetar:** O Nextel Proteção Online tenta desinfetar todos os objetos infectados ou provavelmente infectados detectados. Se a desinfecção falhar, o Nextel Proteção Online os moverá para a Quarentena.

- **Excluir:** O Nextel Proteção Online exclui objetos infetados.

- Modo de execução e escopo da verificação -

"Modo de execução"; Ao clicar neste botão, o modo de execução da verificação completa atual é exibido à direita do botão. Os seguintes modos de execução da verificação completa estão disponíveis:

- **Manualmente**: O Nextel Proteção Online executa a tarefa de verificação no momento mais conveniente para você. Nesse modo, a verificação programada está desativada.

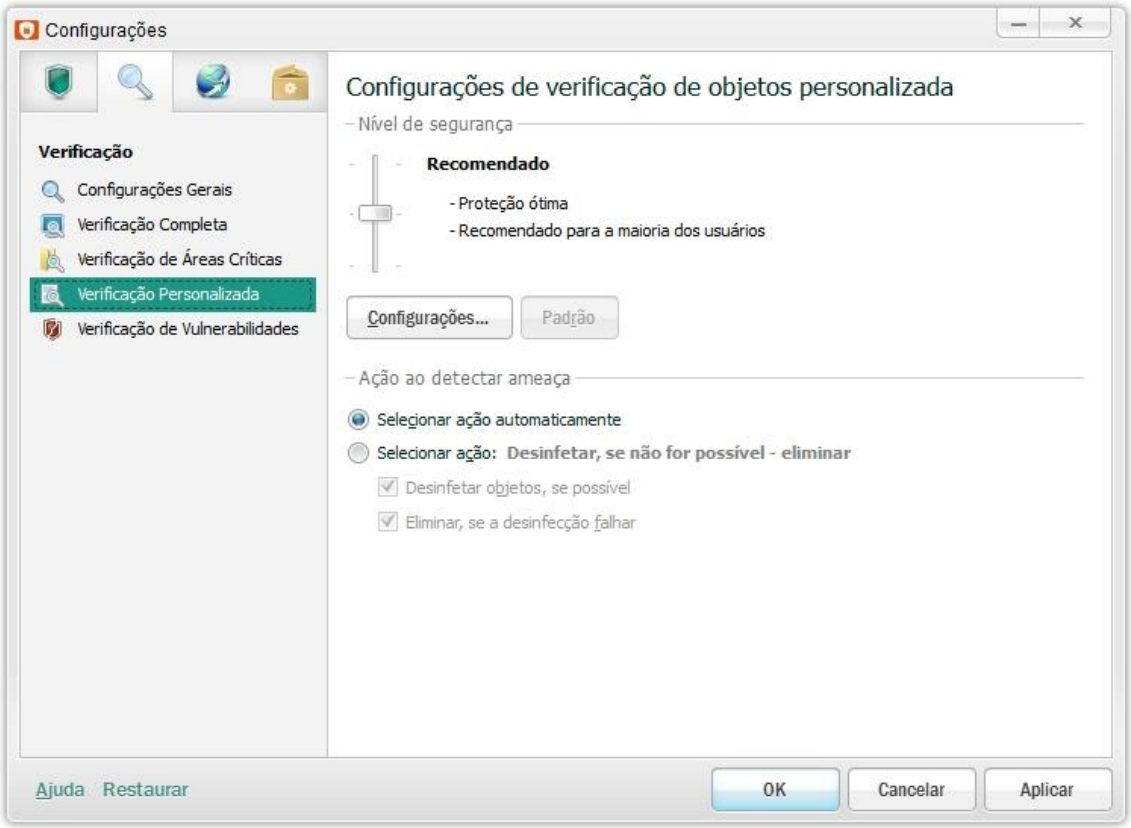
- **Por programação**: O Nextel Proteção Online executa a tarefa de acordo com a programação que você criou. Nesse modo, você também pode executar a verificação manualmente. A verificação programada está desativada por padrão.

“Escopo de verificação”: Ao clicar neste botão, é possível especificar os objetos (como arquivos ou pastas) que devem ser verificados pelo Nextel Proteção Online. O modo atual de criação da lista de objetos a serem verificados é exibido à direita do botão. Os seguintes métodos de criação da lista de objetos a serem verificados estão disponíveis:

- **Por padrão**: Ao executar a tarefa de Verificação Completa, o Nextel Proteção Online verifica a memória do sistema, os objetos de inicialização, o armazenamento de backup do sistema, os emails, os discos rígidos e as unidades removíveis.

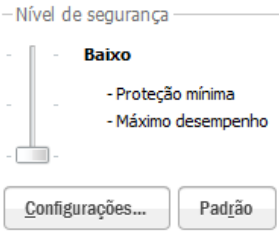
- **Personalizada**: O Nextel Proteção Online verifica os objetos especificados. Se o escopo de verificação estiver vazio ou não contiver nenhum objeto selecionado, a verificação completa não poderá ser iniciada.

4.2.3 Verificação de Áreas Críticas



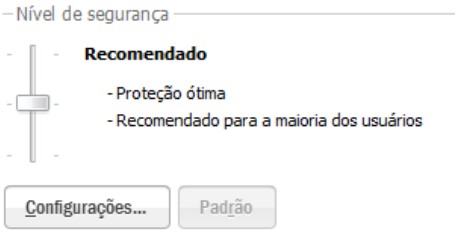
- Nível de segurança: É possível selecionar as configurações de verificação predefinidas usando o controle deslizante. Você pode selecionar um dos três níveis de segurança criados pelos especialistas da Nextel Proteção Online ou ajustar você mesmo às configurações da verificação.

"**Baixo**": Este nível de segurança é a melhor opção para tratar aplicativos com requisitos de RAM significativos, pois o número de arquivos que devem ser verificados é menor nesse nível. Ao contrário das configurações de verificação padrão, com as configurações de verificação desse nível de segurança, o Nextel Proteção Online verifica apenas os arquivos novos e alterados.



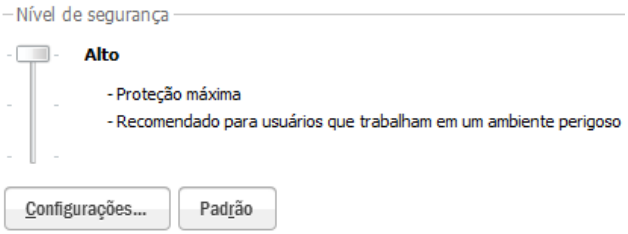
Se forem necessários mais de 180 segundos para verificar os arquivos, o Nextel Proteção Online excluirá esses arquivos da verificação.

"**Recomendado**": Este nível de segurança é adequado na maioria dos casos e recomendado pelos especialistas do Nextel Proteção Online. Garante um equilíbrio ideal entre desempenho e segurança.



Essa é a configuração padrão. (Por esse motivo o botão "Padrão" está apagado, pois o mesmo já está acionado).

"**Alto**": Esse nível de segurança deverá ser selecionado quando a probabilidade de infecção do computador for muito alta. Ao contrário das configurações de verificação padrão, com as configurações de verificação desse nível de segurança, o Nextel Proteção Online verifica todos os tipos de arquivos.



Ao verificar arquivos compostos, o Nextel Proteção Online também verifica os arquivos com formato de email.

- Ação ao detectar ameaça -

"Selecionar ação automaticamente": Ao detectar objetos perigosos, o Nextel Proteção Online executará automaticamente uma ação: Para objetos infectados, a ação é Desinfetar, se não for possível, Eliminar; para objetos provavelmente infectados, é Ignorar.

Antes de tentar desinfetar ou Eliminar um objeto infectado, o Nextel Proteção Online cria uma cópia de backup para posterior restauração ou desinfecção.

"Selecionar ação": Se for detectado um objeto perigoso, o Nextel Proteção Online automaticamente realiza uma ação especificada. A ação realizada pelo Nextel Proteção Online é definida numa combinação das caixas de seleção:

- **Desinfetar, Eliminar se a desinfecção falhar:** O Nextel Proteção Online tenta desinfetar todos os objetos infectados ou provavelmente infectados detectados. Se a desinfecção falhar, o Nextel Proteção Online os excluirá. A ação é realizada se as caixas Desinfetar e Eliminar se a desinfecção falhar for selecionado.

- **Bloquear:** O Nextel Proteção Online bloqueia o acesso ao objeto. As informações sobre esse evento são registradas em um relatório. Negação de acesso de aplicativos externos a um objeto. Um objeto bloqueado não pode ser lido, executado, alterado ou excluído. Esta ação será executada se as caixas de seleção Desinfetar e Eliminar estiverem desmarcados.

- **Desinfetar:** O Nextel Proteção Online tenta desinfetar todos os objetos infectados ou provavelmente infectados detectados. Se a desinfecção falhar, o Nextel Proteção Online os moverá para a Quarentena. A ação será executada se a caixa Excluir se a desinfecção falhar estiver desmarcado.

- **Excluir:** O Nextel Proteção Online exclui objetos infetados. Esta ação será executada se a caixa Desinfetar estiver desmarcado.

- Modo de execução e escopo da verificação -

"Modo de execução": Ao clicar neste botão, é possível configurar a execução da verificação de áreas críticas. O modo de execução da tarefa atual é exibido à direita do botão. Valores disponíveis:

- **Manualmente**: O Nextel Proteção Online executa a tarefa de verificação no momento mais conveniente para você. Nesse modo, a verificação programada está desativada. Este é o modo de execução padrão.

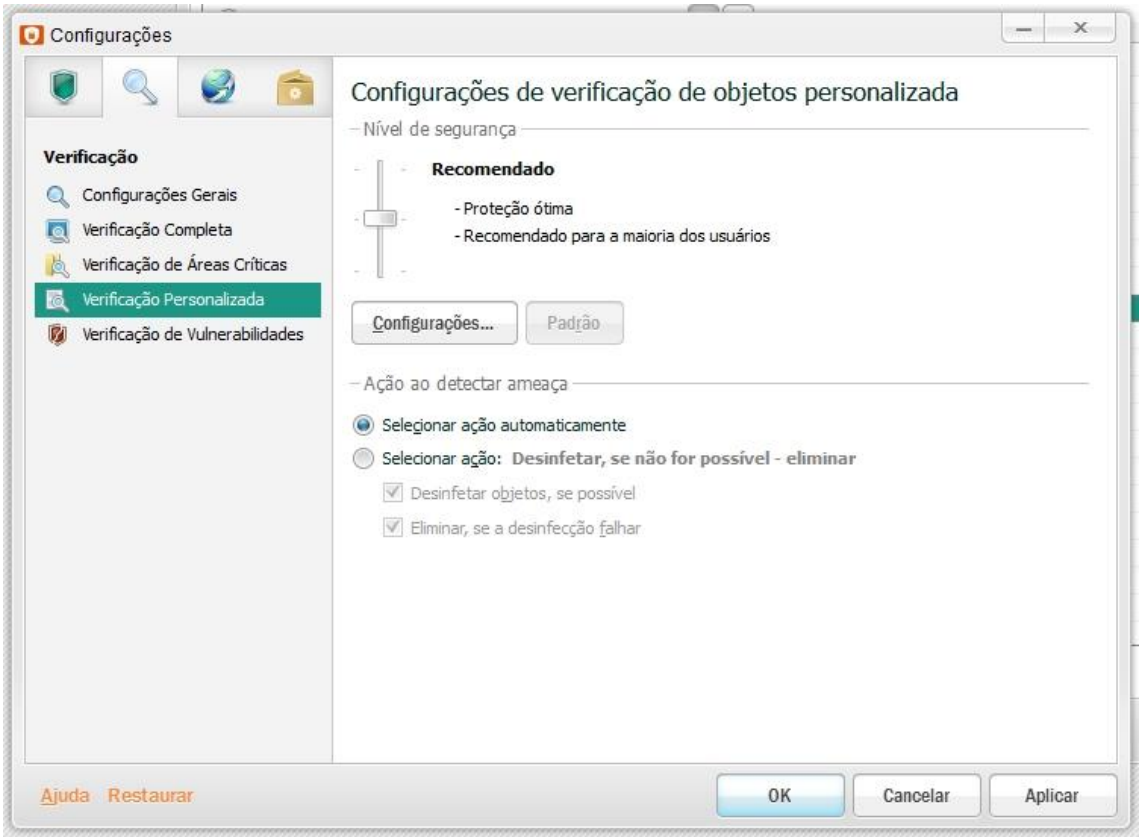
- **Por programação**: O Nextel Proteção Online executa a tarefa de acordo com a programação que você criou. Nesse modo, você também pode executar a verificação manualmente. A verificação programada está desativada por padrão.

"Escopo de verificação": Ao clicar neste botão, é possível especificar os objetos (como arquivos ou pastas) que devem ser verificados pelo Nextel Proteção Online. O modo atual de criação da lista de objetos a serem verificados é exibido à direita do botão. Os seguintes métodos de criação da lista de objetos a serem verificados estão disponíveis:

- **Por padrão**: Ao executar a tarefa de Verificação de Áreas Críticas, o Nextel Proteção Online verifica a memória do sistema e os objetos de inicialização. A lista de objetos é definida por padrão.

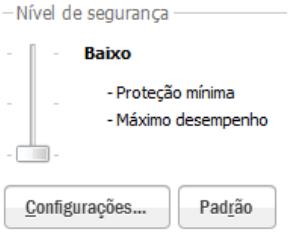
- **Personalizada**: O Nextel Proteção Online verifica os objetos especificados. Se o escopo de verificação estiver vazio ou não contiver nenhum objeto selecionado, a verificação de áreas críticas não poderá ser iniciada.

4.2.4 Verificação Personalizada



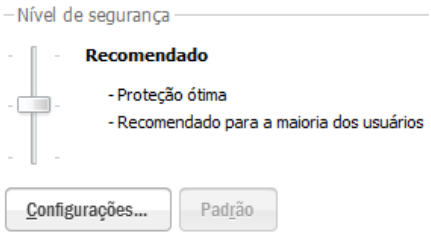
- Nível de segurança –

"**Baixo**": Este nível de segurança é a melhor opção para tratar aplicativos com requisitos de RAM significativos, pois o número de arquivos que devem ser verificados é menor nesse nível. Ao contrário das configurações de verificação padrão, com as configurações de verificação desse nível de segurança, o Nextel Proteção Online verifica apenas os arquivos novos e alterados. Se forem necessários mais de 180 segundos para verificar os arquivos, o Nextel Proteção Online excluirá esses arquivos da verificação.

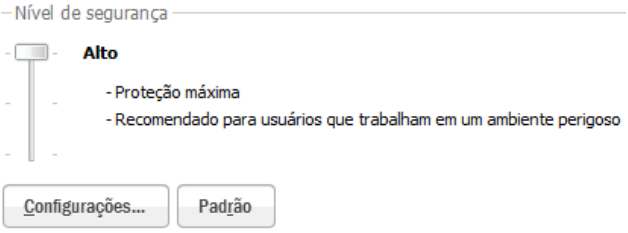


"**Recomendado**": Este nível de segurança é adequado na maioria dos casos e recomendado pelos especialistas do Nextel Proteção Online. Garante um equilíbrio ideal entre desempenho e segurança.

Essa é a configuração padrão (por esse motivo o botão "Padrão" está apagado, pois o mesmo já está acionado).



"**Alto**": Esse nível de segurança deverá ser selecionado quando a probabilidade de infecção do computador for muito alta. Ao contrário das configurações de verificação padrão, com as configurações de verificação desse nível de segurança, o Nextel Proteção Online verifica todos os tipos de arquivos.



Ao verificar arquivos compostos, o Nextel Proteção Online também verifica os arquivos com formato de email.

- Ação ao detectar ameaça -

"Selecionar ação automaticamente": Ao detectar objetos perigosos, o Nextel Proteção Online executará automaticamente uma ação: Para objetos infectados, a ação é Desinfetar, se não for possível, Eliminar; para objetos provavelmente infectados, é Ignorar. Antes de tentar desinfetar ou Eliminar um objeto infectado, o Nextel Proteção Online cria uma cópia de backup para posterior restauração ou desinfecção.

"Selecionar ação": Se for detectado um objeto perigoso, o Nextel Proteção Online automaticamente realiza uma ação especifica. A ação realizada é definida por combinação de caixas de seleção:

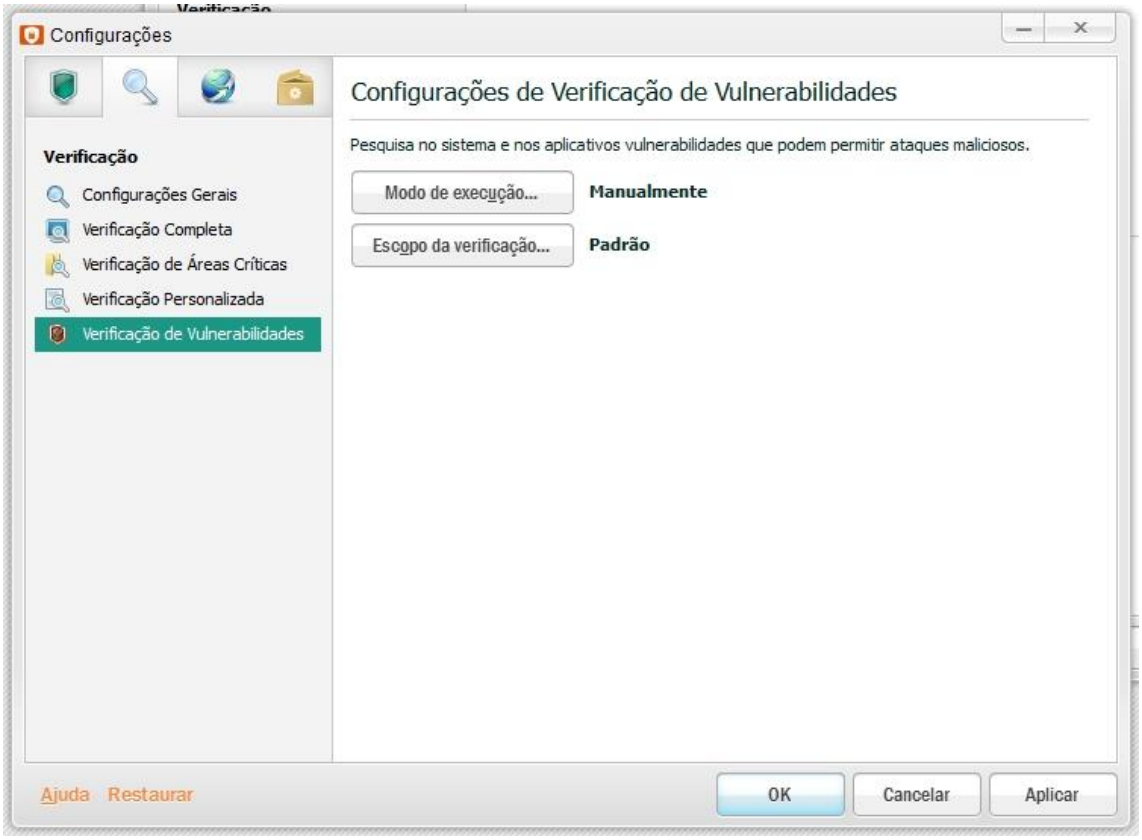
- **Desinfetar, Eliminar se a desinfecção falhar:** O Nextel Proteção Online tenta desinfetar todos os objetos infectados ou provavelmente infectados detectados. Se a desinfecção falhar, o Nextel Proteção Online os excluirá. A ação é realizada se as caixas Desinfetar e Eliminar se a desinfecção falhar for selecionado.

- **Bloquear:** O Nextel Proteção Online bloqueia o acesso ao objeto. As informações sobre esse evento são registradas em um relatório (Negação de acesso de aplicativos externos a um objeto). Um objeto bloqueado não pode ser lido, executado, alterado ou excluído. Essa ação será executada se as caixas Desinfetar e Eliminar estiverem desmarcados.

- **Desinfetar:** O Nextel Proteção Online tenta desinfetar todos os objetos infectados ou provavelmente infectados detectados. Se a desinfecção falhar, o Nextel Proteção Online os moverá para a Quarentena. A ação será executada se a caixa Excluir se a desinfecção falhar estiver desmarcado.

- **Excluir:** O Nextel Proteção Online exclui objetos infetados. Esta ação será executada se a caixa Desinfetar estiver desmarcado.

4.2.5 Verificação de Vulnerabilidades



“Modo de execução”: Ao clicar neste botão, é possível configurar o modo de execução da tarefa de verificação de vulnerabilidades. O modo de execução atual da tarefa de verificação de vulnerabilidades é exibido à direita do botão. Os seguintes modos de execução da tarefa estão disponíveis:

- **Manualmente**: O Nextel Proteção Online executa a verificação de vulnerabilidades no momento mais conveniente para você. Nesse modo, a execução da tarefa programada está desativada. Este é o modo de execução padrão.

- **Por programação**: O Nextel Proteção Online executa a tarefa de acordo com a programação que você criou. Nesse modo, você também pode executar a verificação de vulnerabilidades manualmente. Por padrão, a verificação de vulnerabilidades programada está desativada.

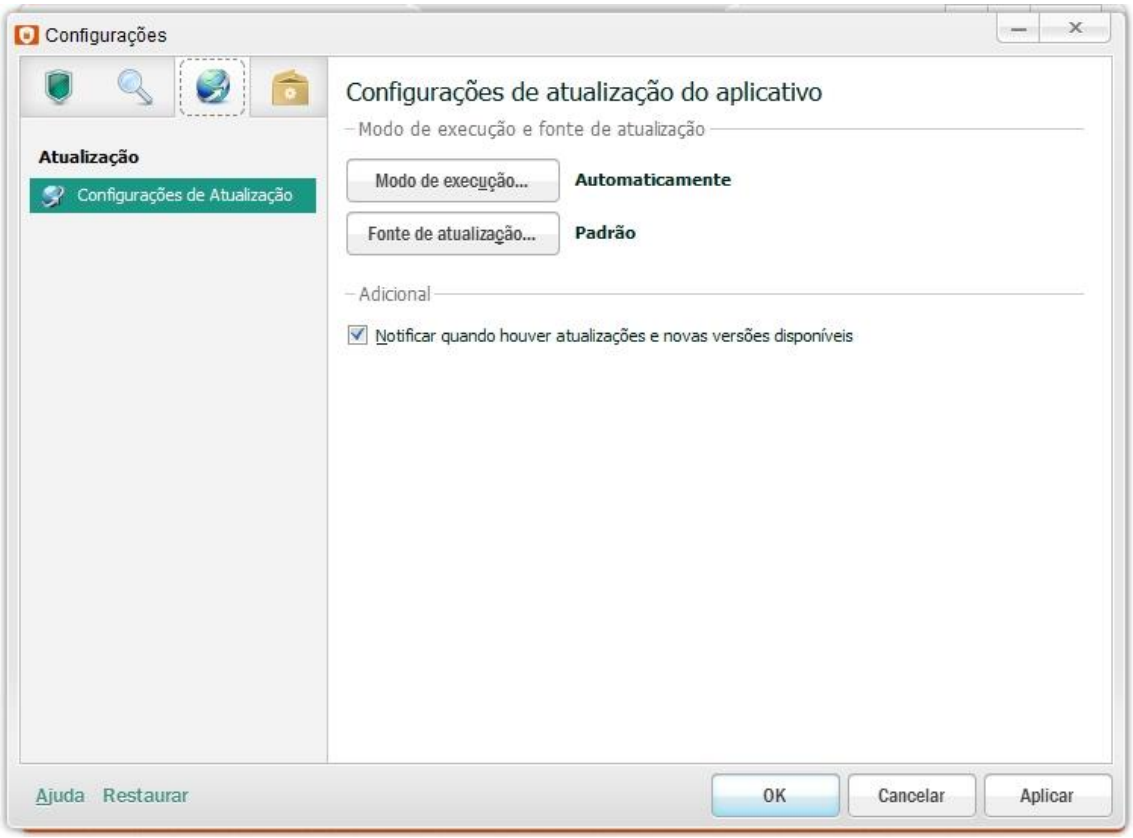
“Escopo de verificação”: Ao clicar neste botão, é possível especificar os objetos (como arquivos ou pastas) que devem ser verificados pelo Nextel Proteção Online durante a verificação de vulnerabilidades. O modo atual de criação da lista de objetos a serem verificados é exibido à direita do botão. Valores disponíveis:

- **Por padrão**: Ao executar a tarefa de Verificação de Vulnerabilidades, o Nextel Proteção Online verifica os arquivos dos aplicativos instalados no computador. A lista de objetos é definida por padrão.

- **Personalizada**: O Nextel Proteção Online verifica os objetos especificados. Se o escopo de verificação estiver vazio e nenhum de seus objetos estiver marcado com uma caixa, a verificação de vulnerabilidades não será executada.

4.3 ATUALIZAÇÃO

4.3.1 Configurações de Atualização



- Modo de execução e fonte de atualização -

"Modo de execução": Ao clicar neste botão, é possível configurar a recuperação e a execução da instalação de atualizações. O modo de execução selecionado é exibido à direita do botão: Automaticamente, Manualmente ou Por programação.

"Fonte de atualização": Ao clicar neste botão, é possível criar uma lista de recursos dos quais o Nextel Proteção Online recupera as atualizações. A fonte de atualização selecionada é exibida à direita:

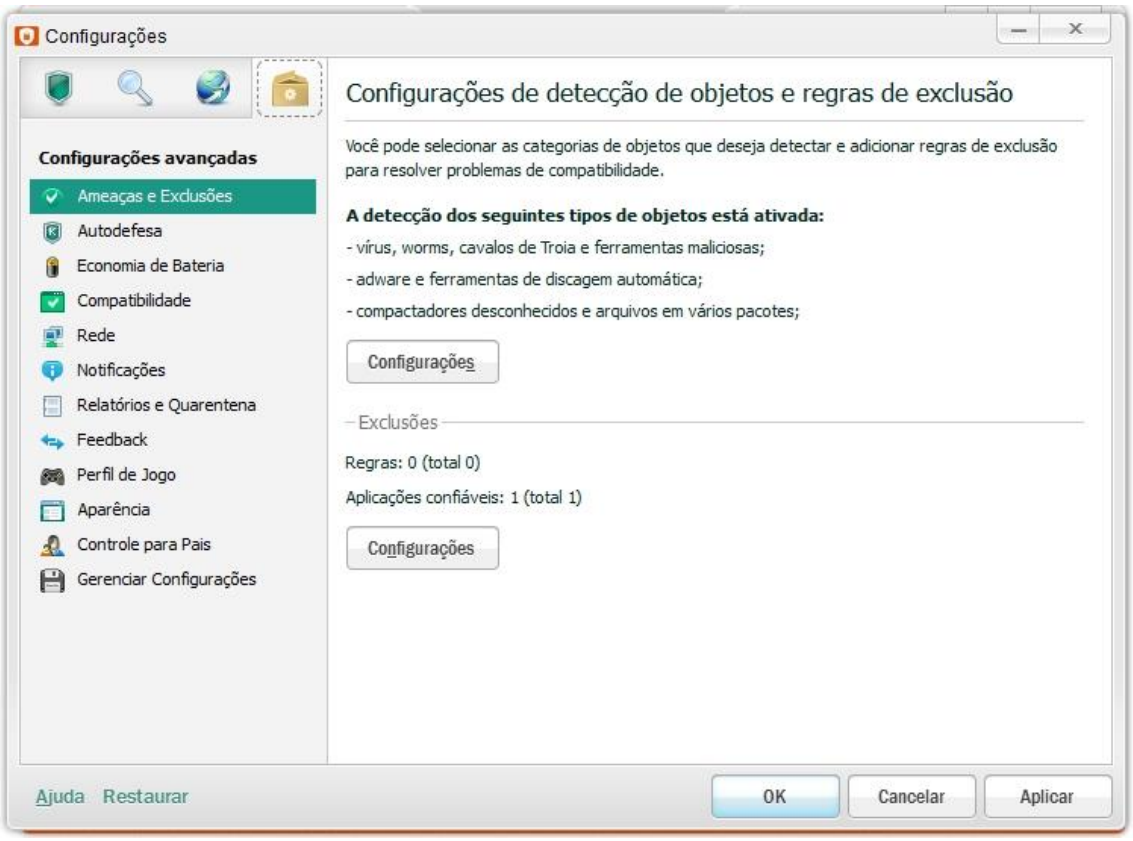
- **Por padrão**: Ao executar atualizações, o Nextel Proteção Online usa os servidores de atualização.
- **Definido pelo usuário**: Ao executar atualizações, o Nextel Proteção Online usa uma fonte especificada pelo usuário.

- Adicional: Você pode especificar as operações que serão executadas pelo Nextel Proteção Online após a atualização do banco de dados.

"Notificar quando houver atualizações e novas versões disponíveis": Esta caixa ativa/desativa a exibição de notificações que informam sobre o lançamento de atualizações e novas versões do aplicativo. Esta caixa vem marcada por padrão.

4.4 CONFIGURAÇÕES AVANÇADAS

4.4.1 Ameaças e Exclusões



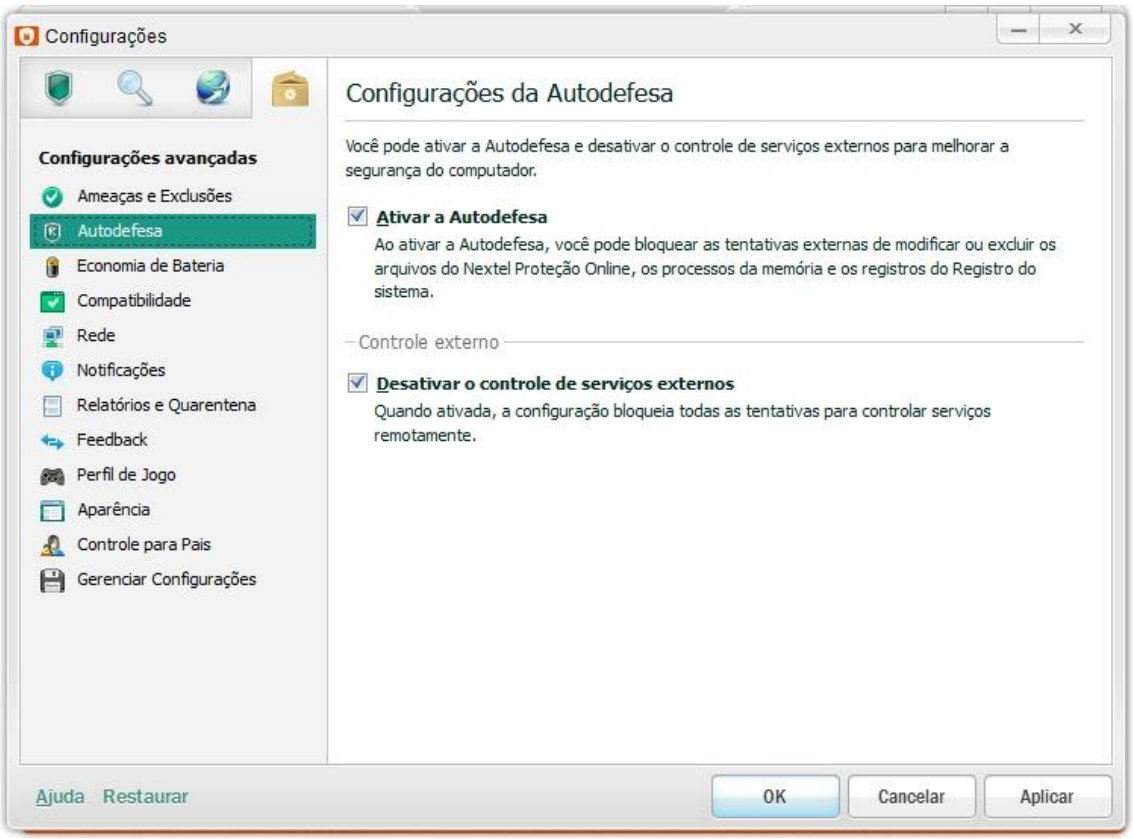
"Configurações": O botão está localizado sob a lista de tipos de objetos detectados pelo Nextel Proteção Online. Ao clicar neste botão, é possível selecionar os objetos que você deseja que o Nextel Proteção Online detecte. Dependendo das configurações definidas na janela (Objetos para detecção), o Nextel Proteção Online sempre detectará vírus, worms e cavalos de Troia.

- Exclusões -

"Configurações": Ao clicar nesse botão, a janela (Zona Confiável) é aberta. Nesta janela, é possível criar uma zona confiável, que é uma lista de objetos que não são monitorados pelo Nextel Proteção Online. Um objeto pode ser representado por um arquivo de um determinado formato, um grupo de arquivos determinados por uma máscara, uma área especificada (por exemplo, uma pasta ou um aplicativo), um processo de programa ou um objeto determinado pelo tipo de ameaça de acordo com a classificação da Enciclopédia de Vírus.

A zona confiável deve ser criada de acordo com as propriedades dos arquivos com os quais você lida e com os aplicativos instalados no computador. Talvez seja necessário criar uma zona confiável se, por exemplo, o Nextel Proteção Online bloquear o acesso a um aplicativo que você tem certeza de que é confiável.

4.4.2 Autodefesa

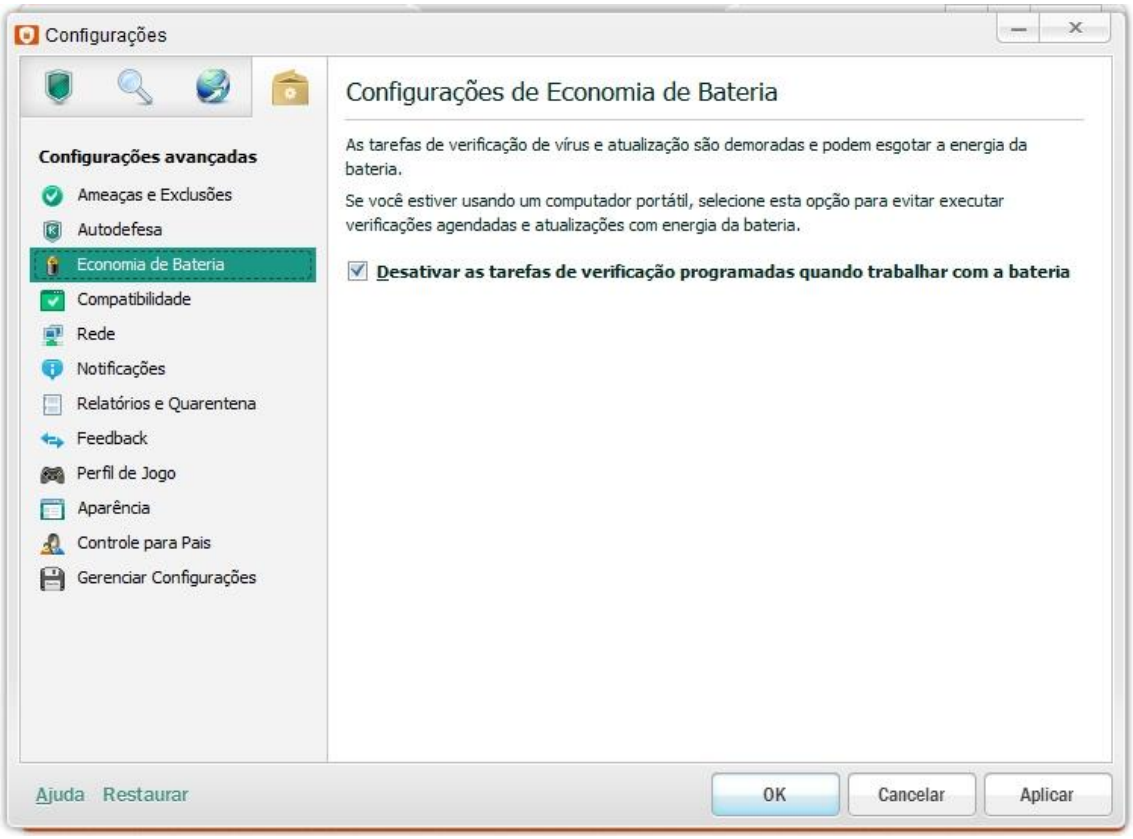


“Ativar Autodefesa”: Esta caixa ativa/desativa os mecanismos de proteção do Nextel Proteção Online contra alterações ou exclusão de seus próprios arquivos no disco rígido, nos processos da RAM e nos registros do Registro do sistema. Esta caixa vem marcada por padrão.

- Controle externo -

“Desativar controle de serviços externos”: Esta caixa ativa/desativa a opção de bloquear todas as tentativas de gerenciamento remoto dos serviços do aplicativo. Se for detectada uma tentativa de gerenciar o aplicativo remotamente, será exibida uma notificação sobre o ícone do Nextel Proteção Online na área de notificação da barra de tarefas do Microsoft® Windows® (se as notificações não estiverem desativadas). Esta caixa vem marcada por padrão.

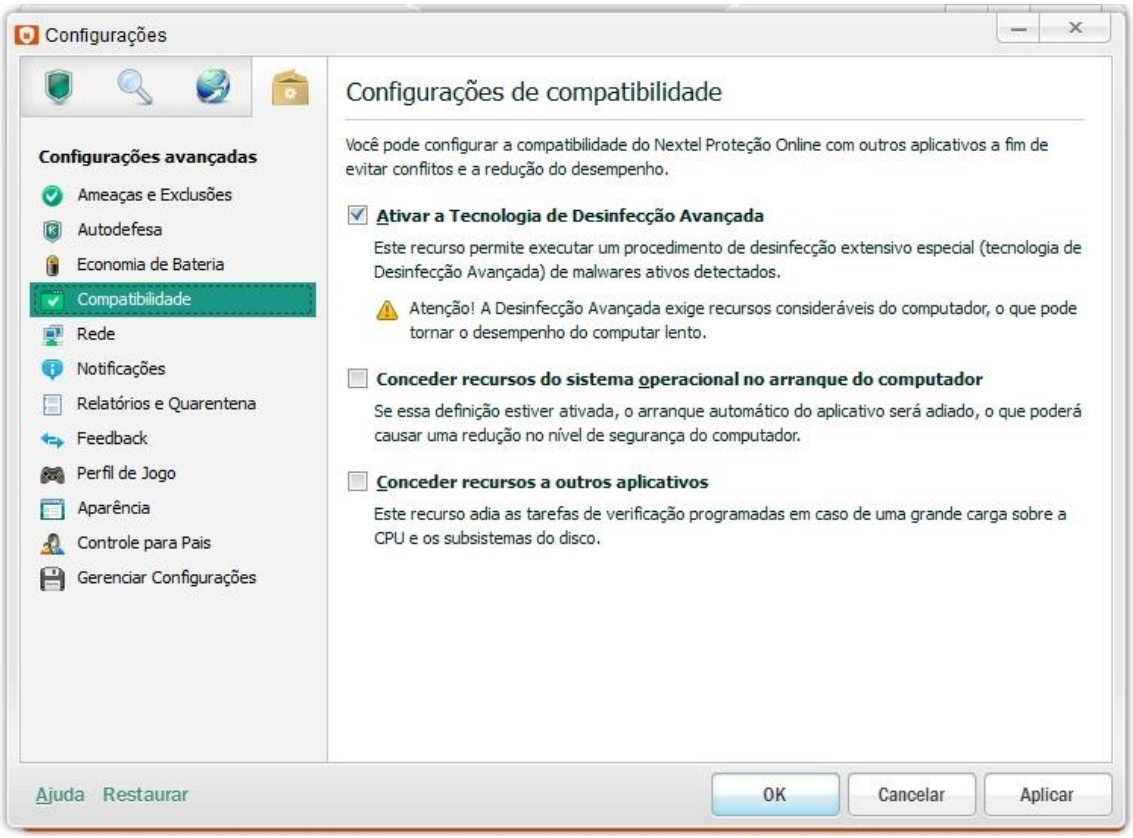
4.4.3 Economia de Bateria



"Desativar as tarefas de verificação programadas quando trabalhar com a bateria": A verificação de vírus e a atualização podem consumir uma quantidade significativa de recursos e tempo. Esta caixa ativa/desativa o modo de adiar as tarefas de verificação de vírus para economizar bateria em um computador portátil.

Se necessário, você mesmo pode atualizar o Nextel Proteção Online ou iniciar uma verificação de vírus. Esta caixa vem marcada por padrão.

4.4.4 Compatibilidade



"Ativar a Tecnologia de Desinfecção Avançada": Se a caixa estiver marcada, quando o Nextel Proteção Online detectar uma atividade maliciosa no sistema, ele permitirá que você execute um procedimento especial de desinfecção avançada que neutraliza e exclui a ameaça.

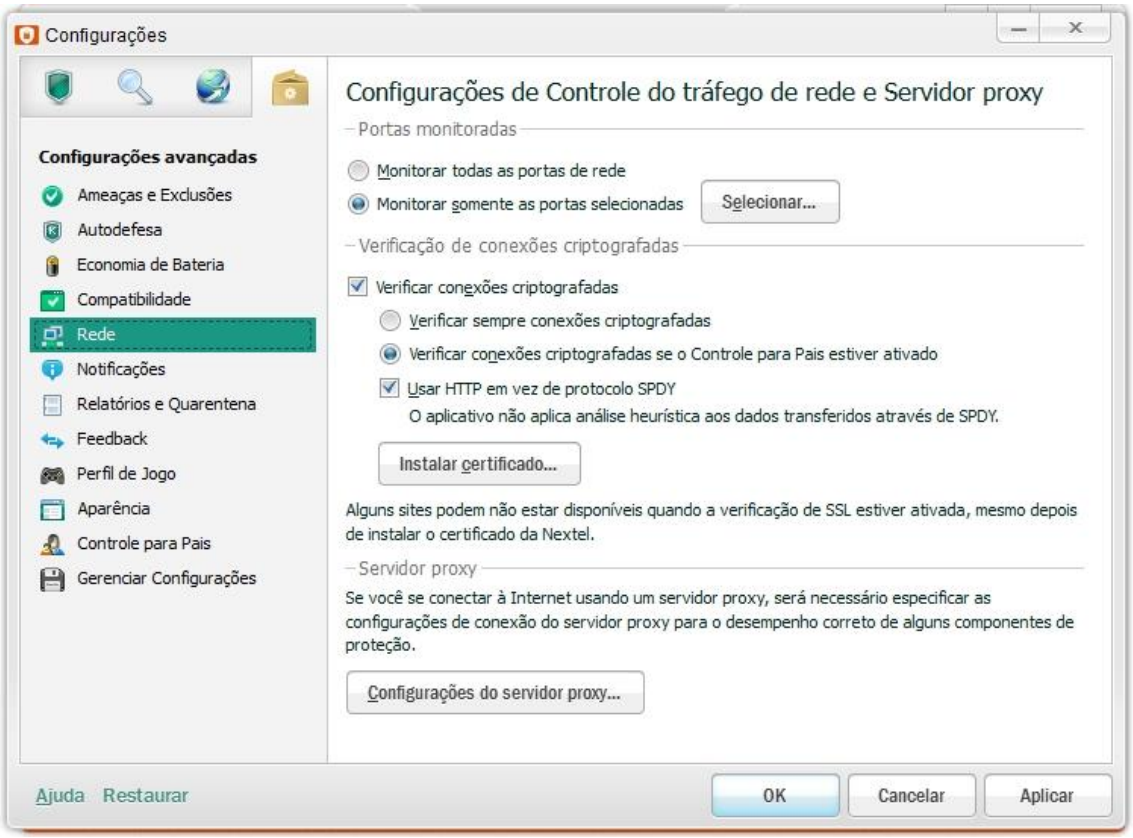
Ao concluir o procedimento, o computador é reiniciado. A Tecnologia de Desinfecção Avançada exige recursos significativos do computador, o que pode afetar seu desempenho. Esta caixa vem marcada por padrão.

“Conceder recursos do sistema operacional ao reiniciar o computador”: Se a caixa de seleção estiver marcada, a inicialização do Nextel Proteção Online é atrasada um pouco para permitir que o sistema operacional inicialize mais rápido.

Nós recomendamos que você evite este uso, já que neste caso o Nextel Proteção Online não verifica as conexões de rede que tiverem sido estabelecidas antes da inicialização do aplicativo. Por exemplo, o Nextel Proteção Online não interceptará as ações de programas maliciosos que recebem ou transmitem dados na inicialização do sistema operacional; ele também não controlará as mensagens de clientes de mensagens instantâneas. Recomenda-se deixar essa caixa desmarcada.

“Conceder recursos a outros aplicativos”: Quando o Nextel Proteção Online executa tarefas de verificação, pode haver um aumento da carga de trabalho na CPU e nos subsistemas de disco, o que afeta o desempenho de outros aplicativos. Se isso acontecer, o Nextel Proteção Online poderá pausar as tarefas de verificação e liberar recursos do sistema para os aplicativos do usuário. Isto ajuda a liberar a carga dos subsistemas da CPU e do disco.

4.4.5 Rede



- Portas monitoradas: É possível escolher o modo de monitoramento de portas que será usado pelo Antivírus de Email, pelo Antivírus da Web e pelo Antispam para verificar fluxos de dados.

“Monitorar todas as portas de rede”: Neste modo de monitoramento de portas, os componentes de proteção Antivírus de Email, Antispam e Antivírus da Web monitoram os fluxos de dados transferidos por todas as portas abertas do computador.

“Monitorar somente as portas selecionadas”: Neste modo de monitoramento de portas, os componentes de proteção Antivírus de Email, Antispam e Antivírus da Web monitoram os fluxos de dados transferidos pelas portas selecionadas do computador. Uma lista de portas usadas para transmitir o tráfego de email e da Web é fornecida com o kit de distribuição do aplicativo. Este modo de monitoramento de portas está selecionado por padrão.

“Selecionar” ao clicar neste botão, a janela Portas de rede é aberta. Nesta janela, também é possível criar uma lista de portas que devem ser monitoradas ou uma lista de aplicativos cujas portas o Nextel Proteção Online monitora.

- Verificação de conexões criptografadas -

“Verificar conexões criptografadas”: Nextel Proteção Online sempre usará certificado para garantir que a conexão seja realmente segura. As conexões que usam o protocolo SSL protegem o canal de troca de dados na Internet. O protocolo SSL permite identificar as partes que trocam dados usando certificados eletrônicos, codificar os dados transferidos e assegurar sua integridade durante a transferência.

- **“Verificar sempre conexões criptografadas”:** Se o Nextel Proteção Online detectar um certificado inválido ao se conectar com um servidor (por exemplo, quando ele for substituído com intenções maliciosas), o produto exibirá uma notificação solicitando que você aceite ou rejeite o certificado, ou apenas exiba suas informações. Se o Nextel Proteção Online estiver funcionando no modo de proteção automático, ele interromperá a conexão com um certificado inválido automaticamente, sem qualquer notificação. Esta opção é definida por padrão.

- **"Verificar conexões criptografadas se o Controle para Pais estiver ativado":** O Nextel Proteção Online usa certificado para verificar a segurança das conexões SSL apenas se o Controle para Pais estiver ativado. Se o Controle para Pais estiver desativado, o Nextel Proteção Online não verificará as conexões SSL.

- **“Usar HTTP em vez de SPDY”:** Esta caixa de seleção cobre o uso de protocolos HTTP e SPDY ao estabelecer uma conexão com um servidor remoto. Se a caixa de seleção estiver marcada ao estabelecer uma conexão com um servidor remoto, o Nextel Proteção Online troca conexões de SPDY para HTTP. Se o servidor remoto der suporte apenas a SPDY, o aplicativo não verifica os dados enviados / recebidos do servidor remoto.

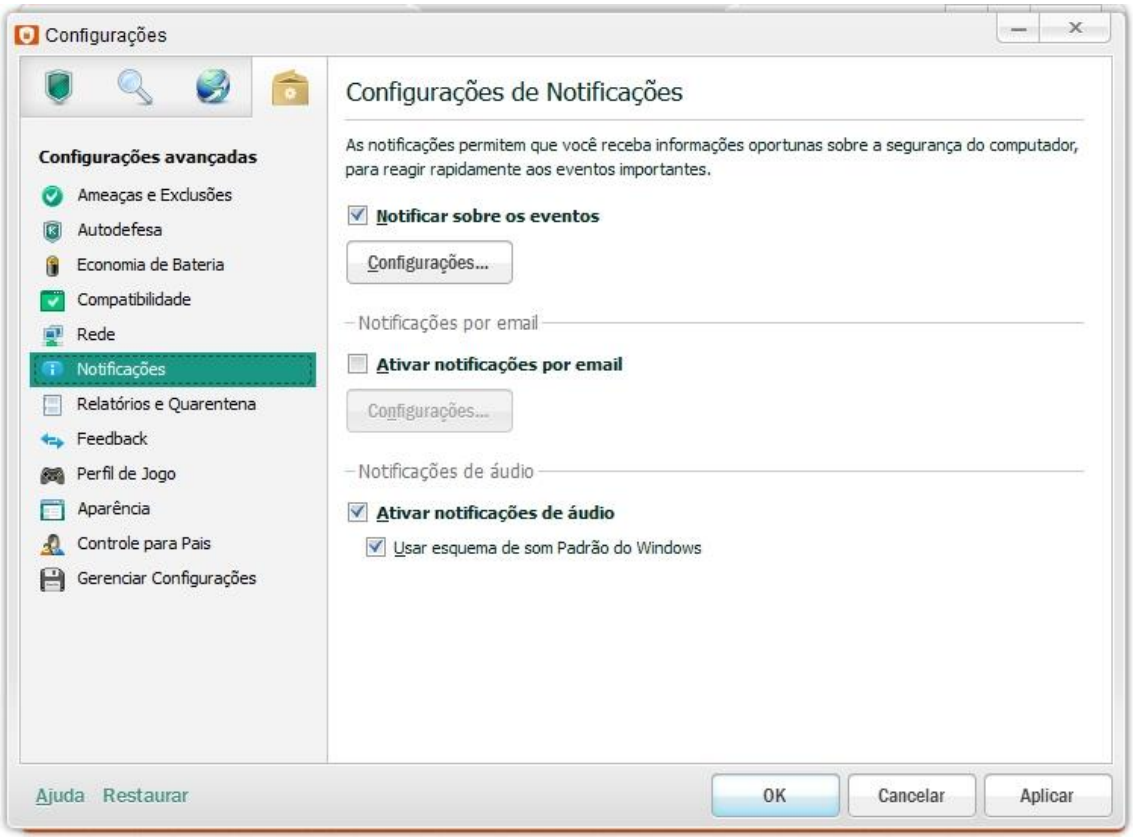
  Se a caixa de seleção não estiver marcada, o Nextel Proteção Online estabelece uma conexão com o servidor remoto usando o protocolo SPDY (desde que o servidor remoto suporte o protocolo). Nesse caso, o aplicativo não controla a transferência de dados por esta conexão. Não é recomendado usar esse modo, posto que corre o risco de fazer download de conteúdo potencialmente perigoso da internet para o computador do usuário tanto pelo SPDY quanto pelo HTTP.

- Servidor proxy -

“Configurações do servidor proxy”: Ao clicar no botão, a janela Configurações do servidor proxy é aberta. Nesta janela, é possível configurar a conexão com um servidor proxy.

Dúvidas sobre configurações deverão ser esclarecidas através do atendimento Suporte nível 2.

4.4.6 Notificações



“Notificar sobre os eventos”: Se a caixa estiver desmarcada, o Nextel Proteção Online não o notificará sobre os eventos ocorridos durante sua operação, mas registrará essas informações em um relatório. As notificações podem ser implementadas usando os seguintes métodos:

- Mensagens pop-up sob o ícone do Nextel Proteção Online na área de notificação da barra de tarefas.
- Notificações de áudio.
- Mensagens por email.

“Configurações”: Ao clicar nesse botão, a janela Notificações é aberta. Nesta janela, é possível selecionar tipos de eventos sobre os quais o Nextel Proteção Online deve notificá-lo e os tipos de notificações (notificação na tela, sinal sonoro, email).

- Notificações por email -

“Ativar notificações por email”: Esta caixa ativa/desativa a entrega de notificações por email. Esta caixa vem desmarcada por padrão.

“Configurações”: Ao clicar no botão, a janela Configurações de notificação por email é aberta. Nesta janela, é possível configurar o envio de notificações por email.

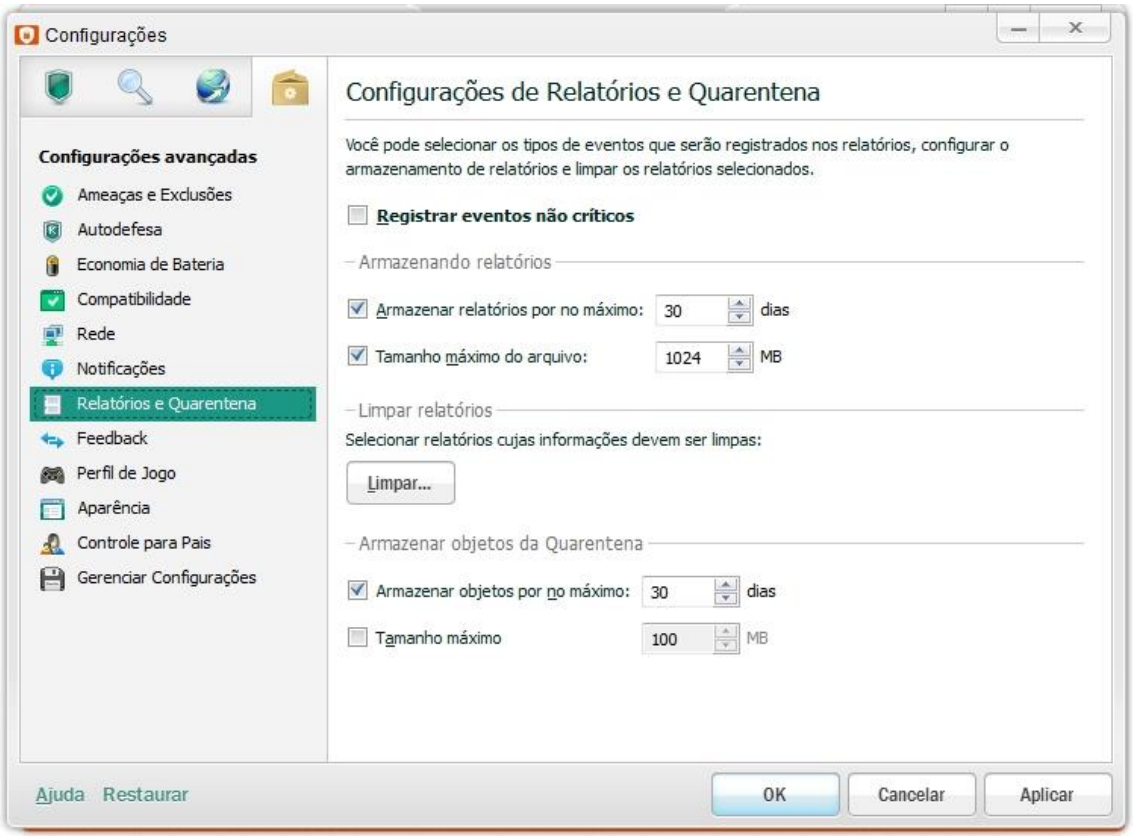
- Notificações de áudio -

“Ativar notificações de áudio”: Esta caixa ativa/desativa as notificações de áudio. Por padrão, todas as notificações são acompanhadas de um sinal sonoro.

“Usar esquema de som Padrão do Windows”: Se a caixa de seleção estiver marcada, serão usados os sons do esquema de som padrão do Microsoft Windows para notificações de áudio.

Se a caixa estiver desmarcada, o esquema de som das versões anteriores do Nextel Proteção Online será usado para notificações de áudio.

4.4.7 Relatórios e Quarentena



"Registrar eventos não-críticos": A caixa ativa/desativa a opção de adicionar informações sobre todos os eventos aos relatórios do Nextel Proteção Online. Esta caixa está desmarcada por padrão.

- Armazenando relatórios -

"Armazenar relatórios por no máximo": A caixa ativa/desativa a opção que define o tempo máximo de armazenamento dos relatórios. A duração do armazenamento é definida em dias. Se a caixa estiver marcada, os relatórios serão armazenados por no máximo 30 dias, por padrão. Quando esse intervalo de tempo expirar, o Nextel Proteção Online limpará os relatórios.

Se a caixa estiver desmarcada, a duração do armazenamento de relatórios não será restrita. Esta caixa vem marcada por padrão.

“Tamanho máximo de arquivo”: O tamanho máximo é especificado em megabytes. Se a caixa estiver marcada, o tamanho máximo padrão será 1024 MB. Quando o tamanho máximo for excedido, os registros mais antigos serão removidos do arquivo quando registros novos forem adicionados.

Se a caixa estiver desmarcada, o tamanho do arquivo de relatório não será restrito. Esta caixa vem marcada por padrão.

- Limpar relatórios -

“Limpar”: Ao clicar no botão, a janela Limpando relatórios é aberta. Na janela, é possível selecionar os relatórios que devem ser excluídos. Por padrão, o Nextel Proteção Online exclui os relatórios de tarefas de verificação, relatórios de atualização, relatórios sobre a aplicação de regras do Firewall e relatórios do Controle para Pais.

- Armazenando objetos da Quarentena -

“Armazenar objetos por no máximo”: A caixa ativa/desativa a opção que define o tempo máximo de armazenamento dos objetos em quarentena e das cópias de objetos no Backup. A duração do armazenamento é definida em dias.

Se a caixa de seleção estiver selecionada, a duração padrão de armazenamento é de 30 dias. Quando este período terminar, o Nextel Proteção Online exclui os objetos. Se a caixa estiver desmarcada, a duração do armazenamento de objetos não será restrita. Esta caixa vem marcada por padrão.

“Tamanho máximo”: A caixa ativa/desativa a opção que define o tamanho máximo do armazenamento de dados. O tamanho do armazenamento é especificado em megabytes.

Se a caixa estiver marcada, o tamanho máximo padrão do armazenamento será 100 MB. Quando o tamanho máximo for excedido, os registros mais antigos serão removidos do armazenamento quando registros novos forem adicionados. Se a caixa estiver desmarcada, o tamanho do armazenamento não será restrito. Esta caixa vem desmarcada por padrão.

4.4.8 Feedback

"Concordo em participar do programa Kaspersky Security Network": Esta caixa ativa/desativa a opção de enviar estatísticas para acelerar a coleta de dados sobre os tipos e fontes de novas ameaças, além de desenvolver métodos para neutralizá-las:

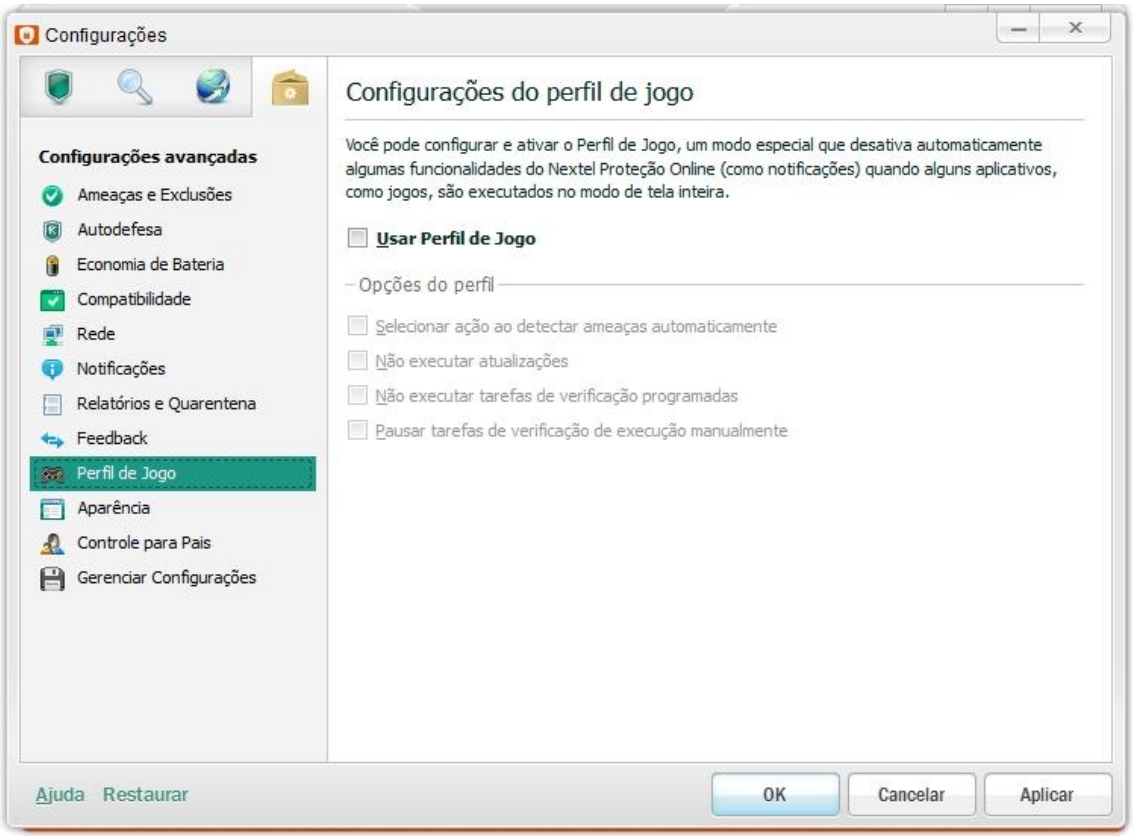
- O identificador Nextel Proteção Online descreve as configurações de hardware do computador e não contém informações particulares.

- Informações sobre as ameaças detectadas pelos componentes do aplicativo. O conteúdo das informações depende do tipo de ameaça detectada.

- Informações sobre o sistema operacional: versão do sistema operacional, service packs instalados, serviços e drivers baixados, versões de navegadores e programas de email, plug-ins de navegadores, número da versão do Nextel Proteção Online instalada no computador.

A caixa será marcada por padrão se você tiver concordado em participar do Kaspersky Security Network na instalação inicial.

4.4.9 Perfil de Jogo



"Usar Perfil de Jogo": O Perfil de Jogo foi criado para aplicativos de jogos em execução no modo de tela inteira. Ele permite modificar simultaneamente as configurações de todos os componentes do Nextel Proteção Online ao alternar seus aplicativos de jogos para o modo de tela inteira e reverter às alterações feitas ao sair desse modo. Esta caixa vem desmarcada por padrão.

- Opções do perfil -

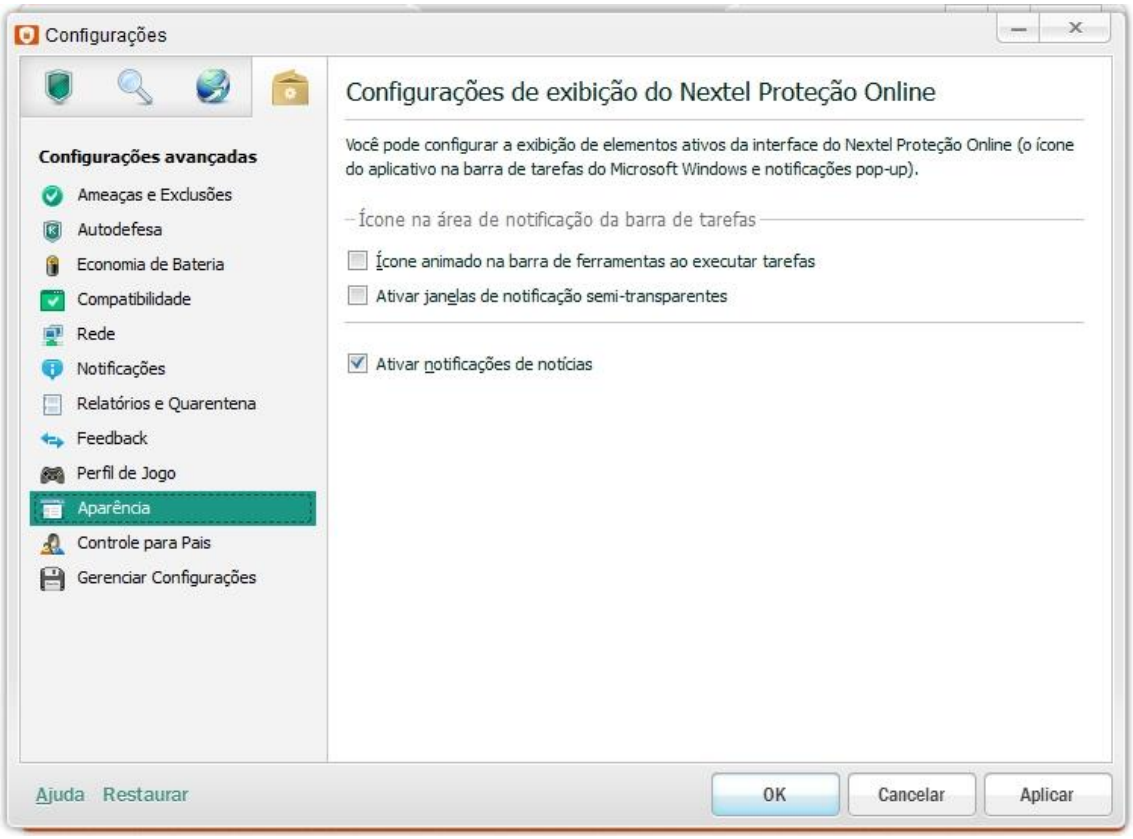
"Selecionar ação ao detectar ameaças automaticamente": Se a caixa estiver marcada, o Nextel Proteção Online será alternado para o modo de proteção automática e não exibirá nenhuma notificação na tela quando houver aplicativos de jogos em execução no modo de tela inteira. Esta caixa vem marcada por padrão.

“Não executar atualizações”: Esta caixa ativa/desativa a opção de pausar as atualizações programadas do Nextel Proteção Online. Esta opção permite evitar que os aplicativos de jogos em execução no modo de tela inteira fiquem lentos. Esta caixa vem marcada por padrão.

“Não executar tarefas de verificação programadas”: A caixa ativa/desativa a opção de pausar a execução de tarefas de verificação programadas. Esta opção permite evitar que os aplicativos de jogos em execução no modo de tela inteira fiquem lentos. Esta caixa está marcada por padrão. Esta caixa estará disponível quando a caixa Usar Perfil de Jogo estiver marcado.

“Pausar tarefas de verificação de execução manualmente”: Esta caixa ativa/desativa a opção de pausar a verificação iniciada manualmente. Esta opção permite evitar que os aplicativos de jogos em execução no modo de tela inteira fiquem lentos. Esta caixa vem marcada por padrão.

4.4.10 Aparência



- Ícone na área de notificação da barra de tarefas -

“Ícone animado na barra de ferramentas ao executar tarefas”: A caixa ativa/desativa a animação do ícone do Nextel Proteção Online. Se a caixa de seleção estiver marcada, o ícone na área de notificação da barra de tarefas do Windows® mudará de acordo com a operação executada no momento pelo Nextel Proteção Online.

Por exemplo, se o Nextel Proteção Online estiver baixando atualizações, o ícone exibirá um globo girando em miniatura.

Se a caixa estiver desmarcada, a animação estará desativada. Nesse caso, o ícone do Nextel Proteção Online exibirá apenas o status de proteção do computador: se a proteção estiver ativada, o ícone ficará colorido; se estiver pausada ou desativada, será cinza. Esta caixa vem desmarcada por padrão.

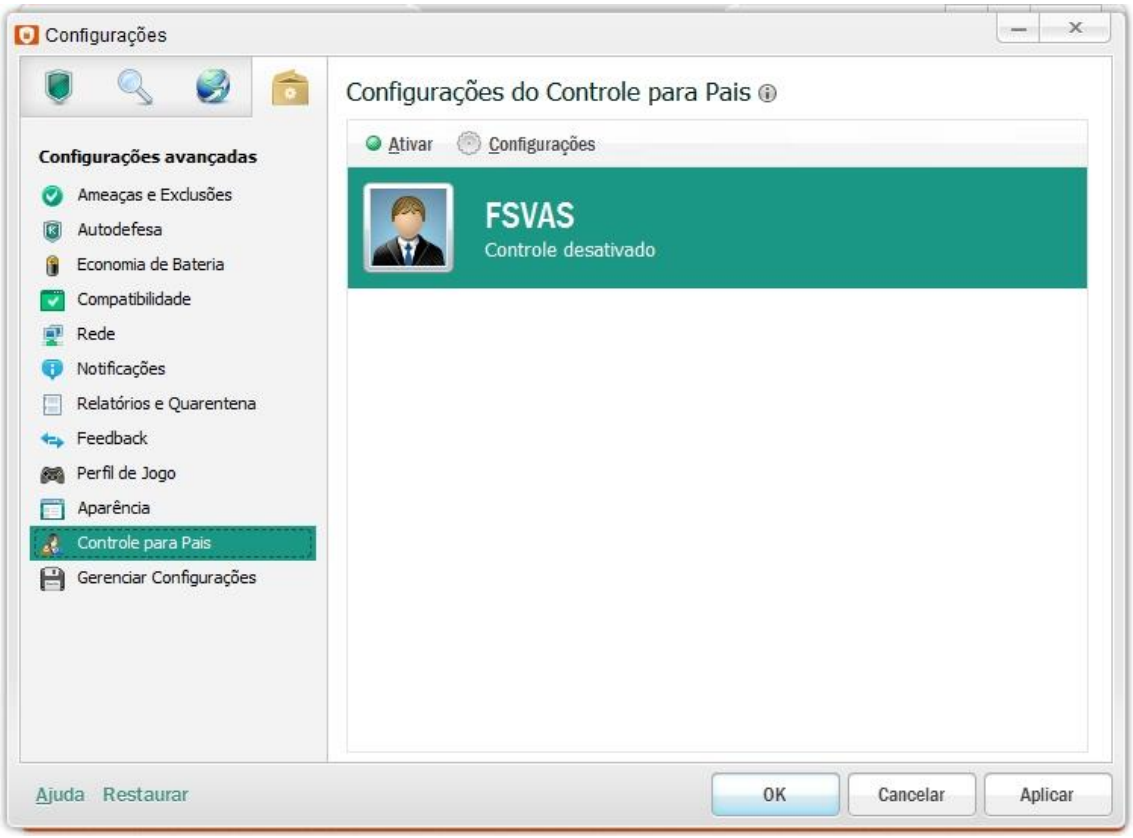
“Ativar janelas de notificação semitransparentes”: As janelas de notificações do aplicativo podem ser exibidas sobre o ícone do Nextel Proteção Online na área de notificação da barra de tarefas do Windows®.

Se a caixa estiver marcada, as janelas de notificações serão semitransparentes; assim, a área da tela sob elas ainda estarão visíveis. A janela de notificações ficará sólida quando o cursor estiver sobre ela.

Se a caixa estiver desmarcada, as janelas de notificações serão sólidas. Esta caixa vem desmarcada por padrão.

“Ativar notificações de notícias”: Esta caixa ativa/desativa a exibição de notícias do Nextel Proteção Online e suas notificações. Esta caixa vem marcada por padrão.

4.4.11 Controle dos Pais



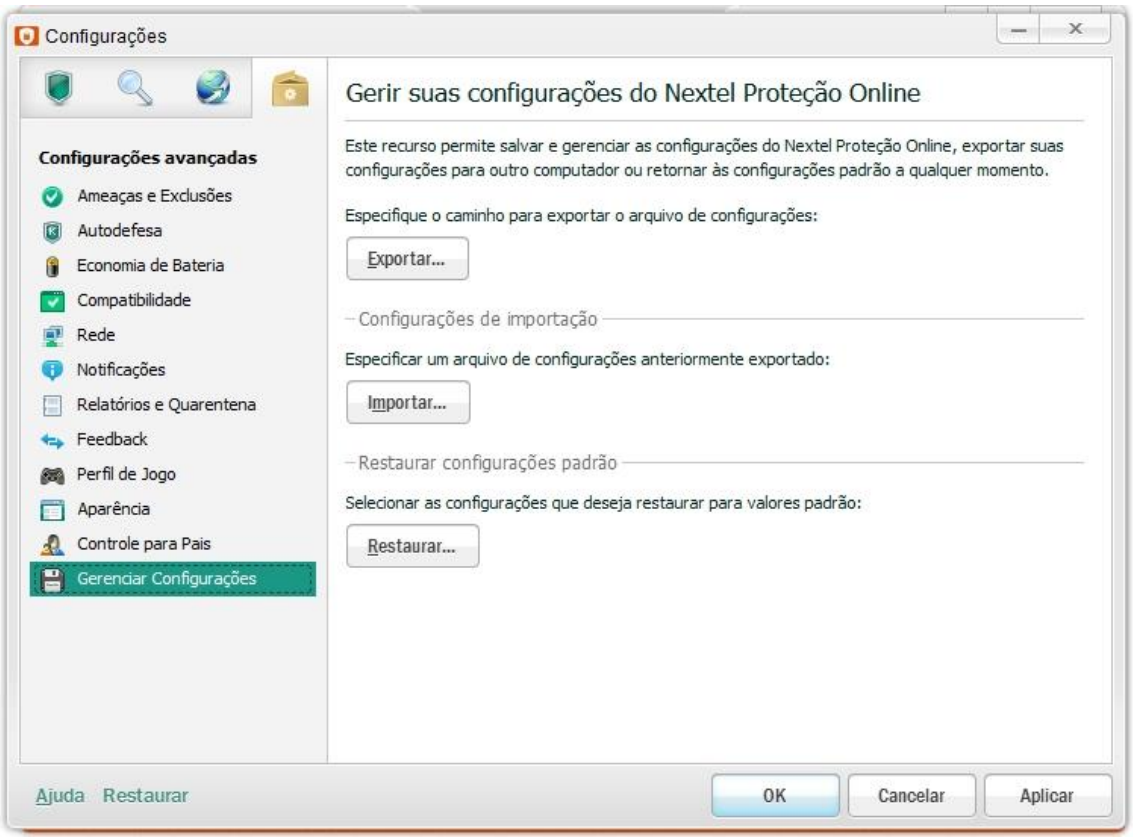
Contém informações sobre as contas de usuário:

- Imagem do usuário selecionada nas configurações do Controle para Pais.
- Status do controle do usuário conforme definido para o Controle para Pais (Ativado ou Desativado).

“Ativar/Desativar”: Este botão ativa/desativa o controle do usuário selecionado. Se não for definida uma senha para restringir o acesso ao Nextel Proteção Online, ao clicar pela primeira vez no botão Controlar, será aberta uma janela que permite a criação dessa senha.

“Configurações": Clicar nesse botão o leva para a configuração da conta do usuário selecionado.

4.4.12 Gerenciar Configurações



"Exportar": Este botão abre a janela Especifique um arquivo de configuração. Nesta janela, é possível especificar o nome de um arquivo de configuração no qual serão salvas as configurações do Nextel Proteção Online. Além disso, você pode selecionar uma pasta para armazenar o arquivo.

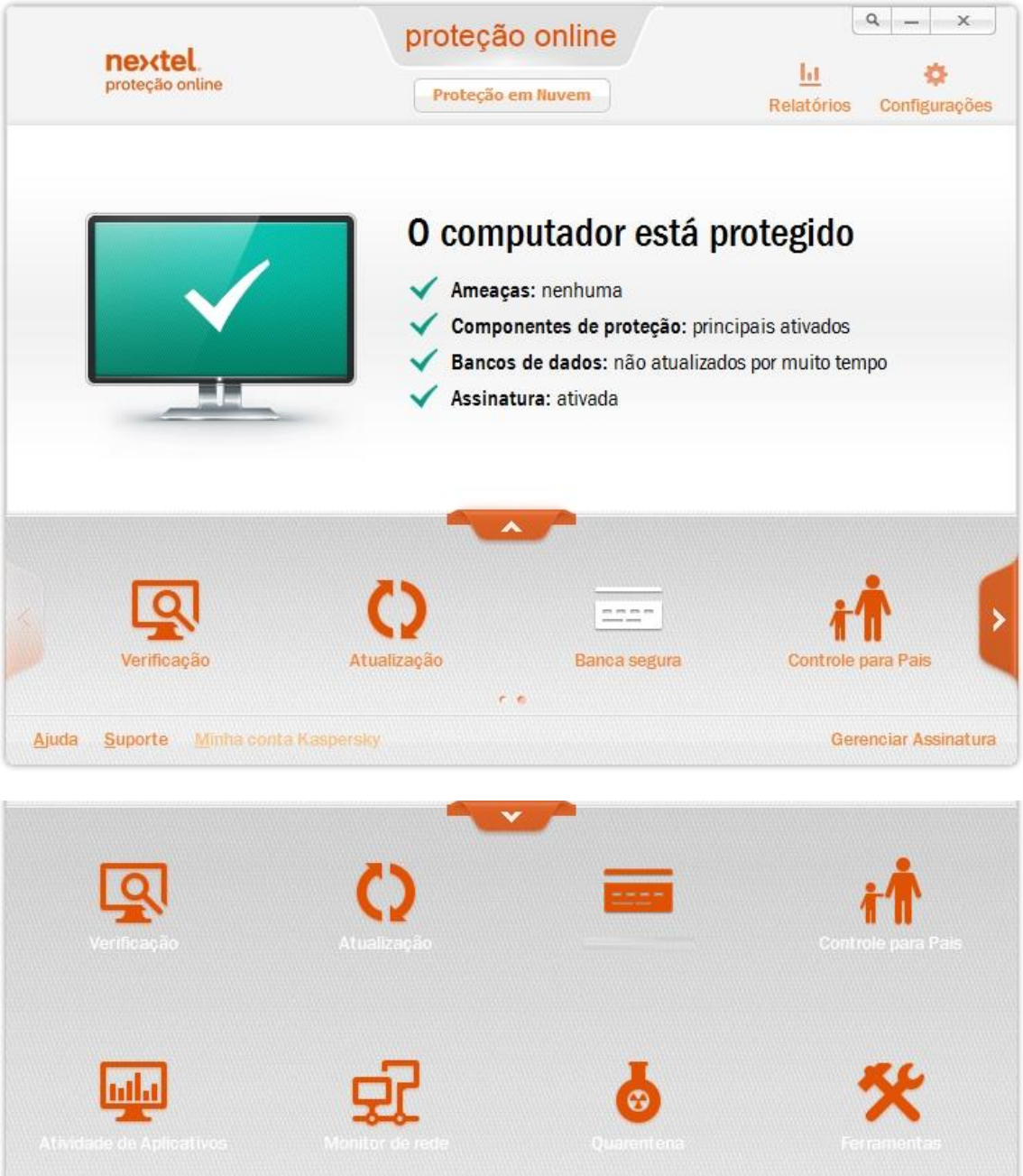
- Configurações de importação -

"Importar": Este botão abre a janela (Especifique um arquivo de configuração). Nesta janela, é possível selecionar um arquivo com as configurações que devem ser aplicadas ao Nextel Proteção Online.

- Restaurar configurações padrão -

"Restaurar": Este botão abre a janela do Assistente de Instalação do Nextel Proteção Online. Na janela Restaurar configurações do Assistente de Configuração, é possível restaurar as configurações recomendadas do Nextel Proteção Online.

5 CONFIGURAÇÃO DO PAINEL INFERIOR DA INTERFACE DO NEXTELPROTECT:



No Painel inferior da interface temos atalhos dos componentes e ferramentas Nextel Proteção Online.

Ao clicar no botão com o nome de um componente ou ferramenta, a janela de gerenciamento do mesmo será aberta.

Confira passo a passo esse gerenciamento:

5.1 Verificação

“Verificação Completa” foi criada para iniciar e interromper a verificação completa, além de exibir informações sobre seu andamento durante a execução e após sua interrupção.

"Verificação de Áreas Críticas" foi criada para iniciar e interromper a verificação de áreas críticas, além de exibir suas informações enquanto ela estiver em andamento ou após sua interrupção.

“Verificação de Vulnerabilidades” foi criada para iniciar e interromper a verificação de vulnerabilidades, corrigir as vulnerabilidades detectadas e exibir informações sobre a verificação de vulnerabilidades enquanto ela estiver em andamento ou após sua interrupção.

“Verificação Personalizada” foi criada para executar a verificação personalizada de pastas e arquivos. Para verificar um arquivo ou pasta, você pode especificar o local usando o link procurar.

5.2 Atualização

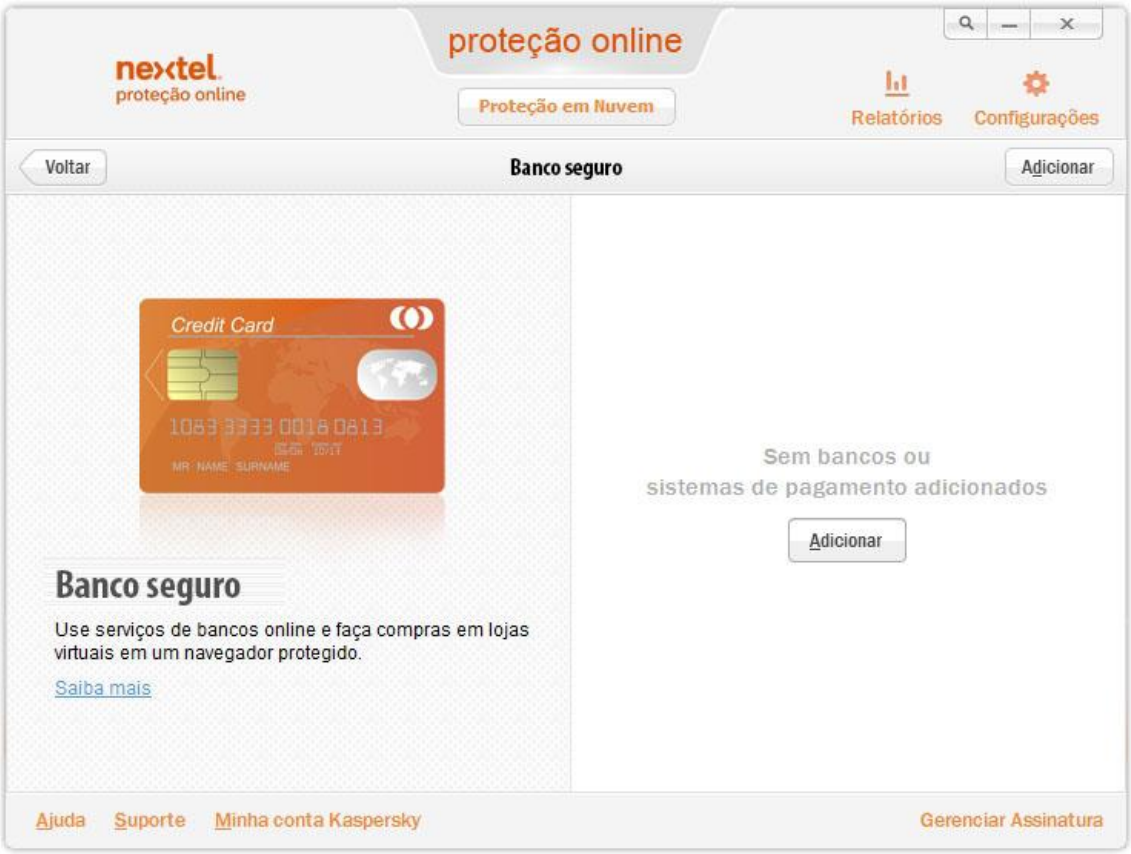
- **Última atualização:** Hora da última atualização, na qual é possível exibir informações sobre as atualizações concluídas dos bancos de dados.

- **Assinaturas:** Especifica o número de assinaturas ou fragmentos de malware que ativam sua detecção.

- **Modo de execução:** É aberta a janela Atualização na guia Modo de execução. Nesta janela, é possível configurar o modo de execução das atualizações.

- **Atualizar:** Ao clicar nesse botão, é iniciada a atualização dos bancos de dados e módulos do aplicativo. Este botão não estará disponível se a reversão para os bancos de dados anteriores estiver em andamento, ou seja, se os bancos de dados do aplicativo estiverem sendo retornados a sua condição antes da execução da última atualização.
  Ao clicar no botão Seta para baixo é aberto um menu que permite aceder à configuração da atualização. Ao selecionar Configurações, é aberta a janela (atualização) na qual é possível selecionar um modo de execução e uma fonte de atualização.

5.3 Banco Seguro



"Adicionar": Ao clicar neste botão, a janela Site de Banco seguro é aberta. Nessa janela você pode adicionar o site de um banco ou sistema de pagamento ao qual, quando acessado, o Nextel Proteção Online executado no modo Banco Seguro aplica a ação especificada (por exemplo: Execução Segura de Sites).

"Saber mais": O link abre a janela do navegador da Web exibindo uma página da Web do site do Serviço de Suporte Técnico que fornece informações detalhadas sobre o Banco Seguro.

5.4 Controle dos Pais

Esta janela exibe as seguintes informações dos usuários:

- Ícone da conta selecionada nas configurações do Controle para Pais.
- Ativar/Desativar o Controle para Pais da conta selecionada.
- Status de controle: É aberta a janela de configuração do Controle para Pais.

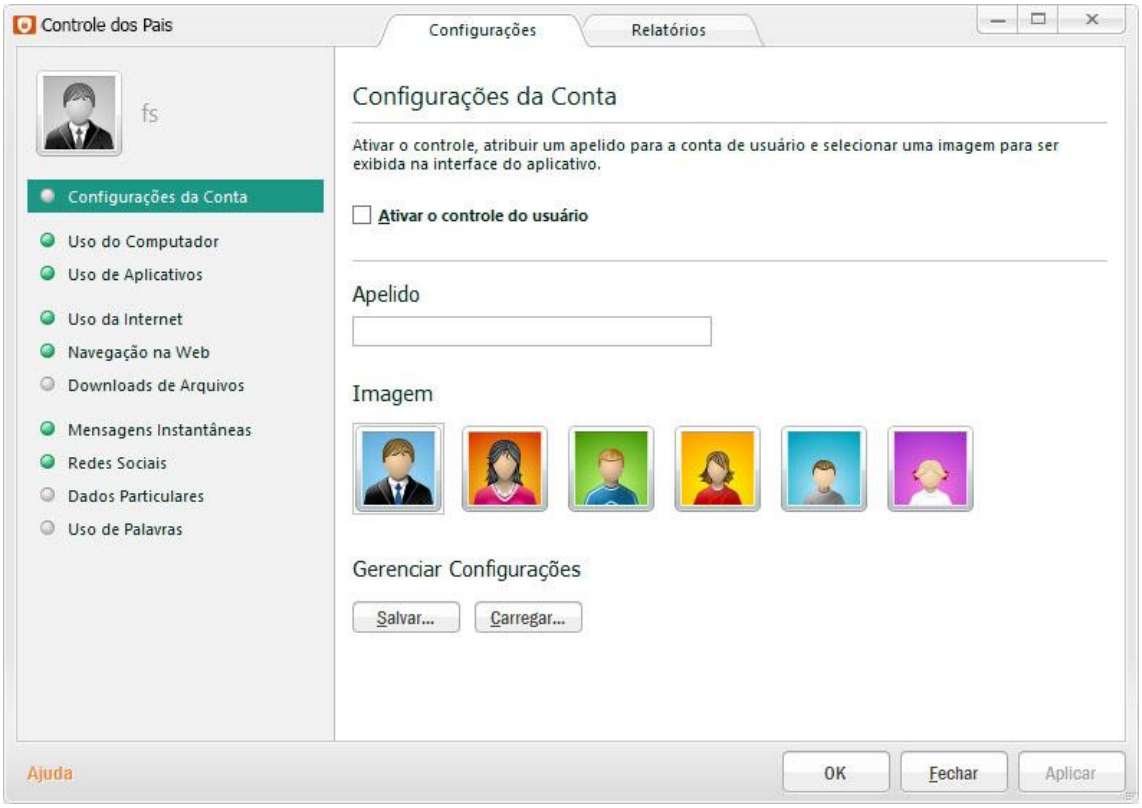
5.4.1 Configurando o Controle para Pais

Para configurar o Controle para Pais em uma conta clique no botão  .

Na janela Controle para Pais temos na parte esquerda da janela uma sessão de componentes do Controle dos Pais e as configurações de cada componente na parte direita da janela.

Vamos abordar cada componente da sessão nas telas seguintes.

5.4.1.1 Configurações da Conta:



Nessa seção é possível ativar / desativar o Controle para Pais da conta selecionada e configurar sua exibição na interface do Controle para Pais:

- Ativar controle para o usuário: Esta caixa ativa/desativa o Controle para Pais da conta selecionada.

Se a caixa estiver marcada, o Controle para Pais será ativado para a conta de usuário escolhida de acordo com suas configurações.

Se a caixa estiver desmarcada, o Controle para Pais será desativado para a conta escolhida, independentemente das configurações do Controle para Pais.

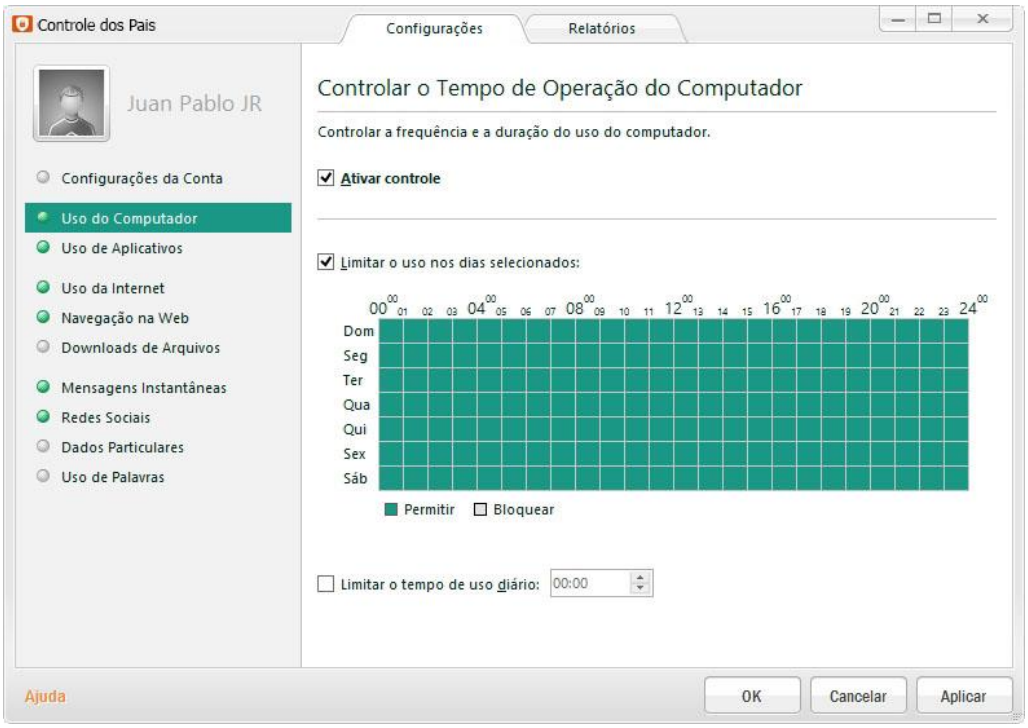
- Apelido: O nome de conta usado na lista de contas e nos relatórios.

- Imagem: Lista de imagens para contas de usuário. A imagem selecionada é exibida ao lado do nome da conta nas listas e nos relatórios do usuário.Na seção Gerenciar Configurações, é possível salvar ou carregar as configurações do Controle para Pais em arquivo.

- Salvar: Ao clicar neste botão, as configurações do Controle para Pais da conta escolhida serão gravadas em arquivo.

- Carregar: Ao clicar no botão, é aberta a janela “Carregar configurações do Controle para Pais” na qual é possível baixar as configurações do Controle para Pais da conta das seguintes fontes:
  - Um arquivo de configuração;
  - Um perfil de usuário existente;
  - Um modelo padrão (por exemplo, criança, adolescente).

5.4.1.2 Uso do Computador



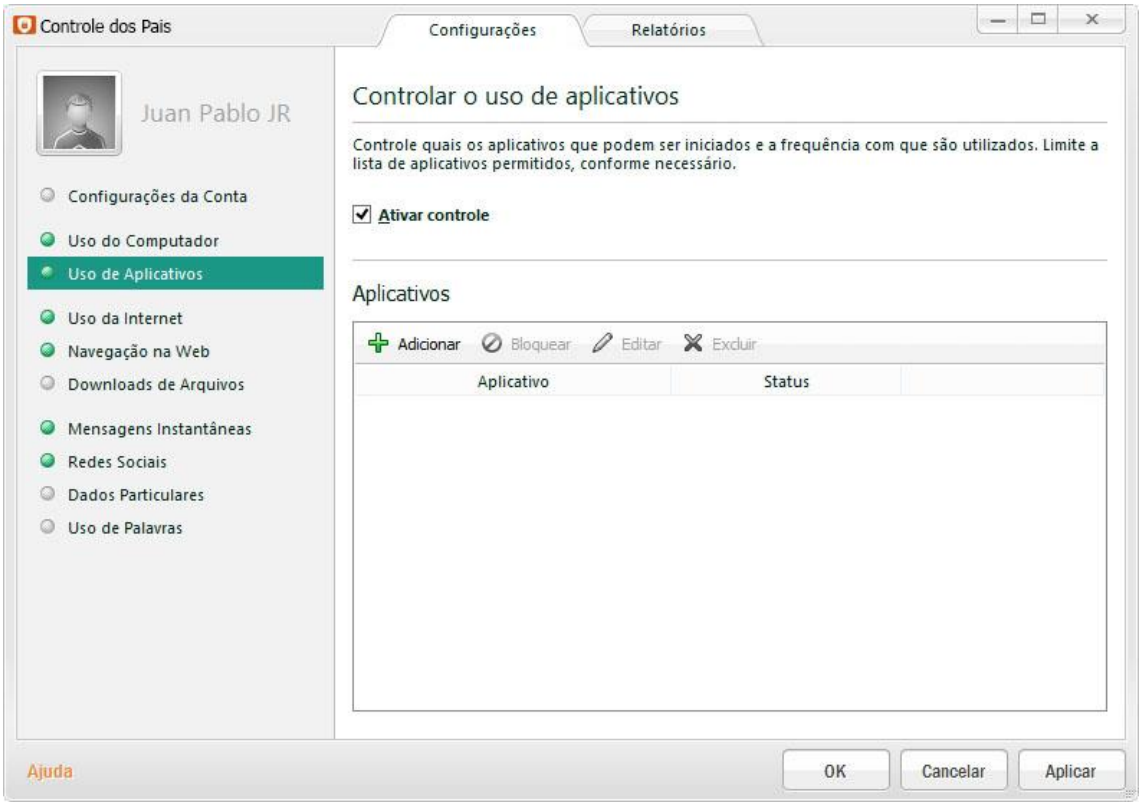
Na seção “Controlar o Tempo de Operação do Computador” é possível limitar o tempo de uso do computador para um usuário selecionado:

- Ativar controle: Esta caixa ativa/desativa o controle do tempo de uso do computador para a conta selecionada. Se a caixa estiver marcada, informações sobre o tempo gasto no computador para a conta selecionada serão exibidas no Relatório de Uso do Computador.

- Limitar uso nos dias selecionados: você pode configurar uma programação de acesso do usuário ao computador (especificando dias da semana e horários do dia) e limitar o tempo total de uso do computador a cada 24 horas. Para fazer isso, é necessário usar o calendário e a caixa Limitar o uso nos dias selecionados. Se a caixa estiver desmarcada, as estatísticas de uso do computador não serão mantidas para a conta selecionada e o usuário poderá trabalhar no computador sem limites de tempo.

- Limitar o tempo de uso diário: Se a caixa estiver marcada, você poderá especificar o tempo máximo de uso do computador permitido a cada 24 horas. O tempo de uso total é inserido no formato hh:mm. Se a caixa estiver desmarcada, o tempo total de uso do computador a cada 24 horas não será registrado.

5.4.1.3 Uso de Aplicativos:



Na seção “Controlar o Uso de Aplicativos” é possível limitar a execução de aplicativos:

- Ativar controle: Esta caixa ativa/desativa o controle da execução de aplicativos para a conta selecionada.

  Se a caixa estiver marcada, as informações sobre os aplicativos que são iniciados para a conta selecionada serão exibidas no Relatório de Uso de Aplicativos. Você também pode bloquear ou permitir a execução de aplicativos especificados ou definir um limite de tempo para executar aplicativos permitidos usando a lista Aplicativos.

  Se a caixa estiver desmarcada, as estatísticas de execução de programas não serão mantidas para a conta escolhida, e o usuário poderá executar todos os aplicativos sem limitações.

- Aplicativos: Você pode usar esta lista para permitir/bloquear a execução de aplicativos ou definir um limite de tempo para a execução de aplicativos permitidos.

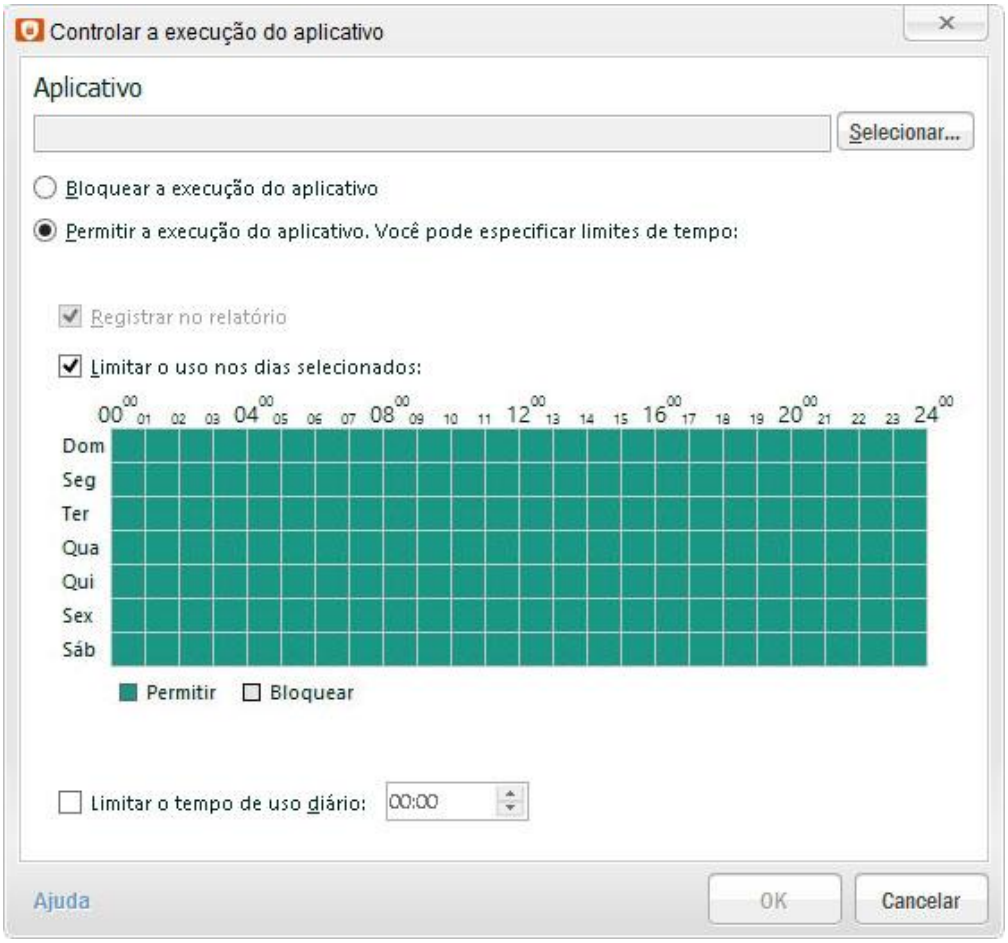
  - Adicionar: Ao clicar neste botão, é aberta a janela “Controlar a execução do aplicativo” na qual é possível adicionar aplicativos à lista Aplicativos e definir limites de tempo para a execução de aplicativos. (Veja mais na próxima imagem).

- Bloquear/Permitir: Este botão permite bloquear/permitir a execução do aplicativo selecionado.

- Editar: Ao clicar neste botão, é aberta a janela Controlar a execução do aplicativo, na qual é possível alterar as configurações de uso do aplicativo selecionado.

- Excluir: Ao clicar neste botão, o aplicativo selecionado é removido da lista de Aplicativos.

- Adicionar:



- Selecionar: Ao clicar neste botão, é aberto um menu que inclui os seguintes itens:

✓ Aplicativos – abre a janela Selecionar aplicativo, na qual é possível selecionar um aplicativo da lista.
✓ Procurar – abre a janela do navegador na qual é possível encontrar e selecionar o arquivo executável de um aplicativo.

- Bloquear a execução do aplicativo: Ao selecionar esta opção, a execução do aplicativo é bloqueada.

- Permitir a execução do aplicativo: Ao selecionar esta opção, a execução do aplicativo é permitida. Além disso, você pode configurar uma programação de execução do aplicativo e limitar o tempo total de uso do aplicativo a cada 24 horas.

- Registrar no relatório: Esta caixa ativa/desativa o registro de uso de aplicativo em log.

  Se a caixa estiver marcada, as informações sobre a execução do aplicativo serão exibidas no relatório Aplicativo em execução para a conta selecionada.

  Se a caixa estiver desmarcada, não serão mantidas estatísticas de execução do aplicativo para a conta selecionada.

- Limitar o uso nos dias selecionados: Esta caixa ativa/desativa as restrições impostas sobre o uso do aplicativo permitido em dias da semana e horários especificados.

  Se a caixa estiver marcada, você poderá configurar uma programação de uso do computador: definir um ou vários intervalos para cada dia da semana em que o uso do aplicativo é permitido ou bloqueado, levando em conta o limite imposto sobre o tempo total de uso do computador a cada 24 horas.

  Você pode configurar a programação de uso do aplicativo usando uma tabela. As linhas da tabela correspondem aos dias da semana e as colunas correspondem a intervalos de 1 hora na escala de tempo. A escala de tempo pode ser de 12 ou de 24 horas, dependendo das configurações regionais do sistema operacional. As cores das células da tabela refletem os limites impostos: o cinza indica que o uso do aplicativo está bloqueado; o verde indica que está permitido.

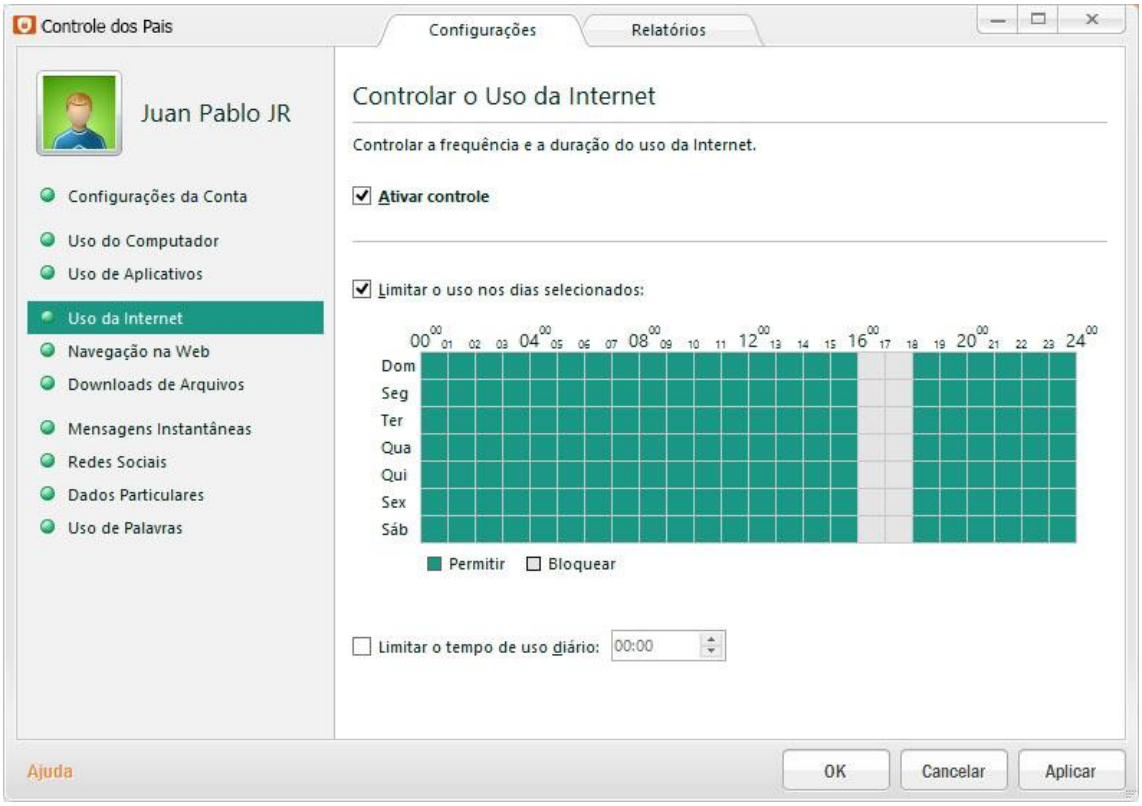
  Se a caixa estiver desmarcada, a programação de limites não será observada.

- Limitar o tempo de uso diário: Esta caixa ativa/desativa os limites de tempo impostos sobre o uso do aplicativo a cada 24 horas.

  Se a caixa estiver marcada, você poderá especificar o tempo máximo de uso do aplicativo permitido a cada 24 horas. O tempo de uso total do aplicativo é inserido no formato hh:mm.

  Se a caixa estiver desmarcada, o tempo total de uso do aplicativo a cada 24 horas não será registrado.

5.4.1.4 Uso da Internet



Na seção Controlar o Uso da Internet, é possível limitar o tempo de uso da Internet do usuário selecionado. O Nextel Proteção Online controla as conexões através de HTTP, HTTPS e FTP.

- Ativar controle: Esta caixa ativa/desativa o controle do tempo de uso da Internet para a conta selecionada.

  Se a caixa estiver marcada, informações sobre as sessões da Internet para a conta selecionada serão exibidas no Relatório de Uso da Internet.

  Se a caixa estiver desmarcada, as estatísticas de uso da Internet não serão mantidas para a conta selecionada e o usuário poderá acessar na Internet sem limites de tempo.

- Limitar o uso nos dias selecionados: Esta caixa ativa/desativa as restrições impostas sobre o uso da Internet em dias da semana e horários especificados.

  Se a caixa estiver marcada, você poderá configurar uma programação de uso da Internet: definir um ou vários intervalos para cada dia da semana, especificando se o uso da Internet é permitido ou bloqueado levando em conta o limite imposto sobre o tempo total de uso da Internet a cada 24 horas.

Você pode configurar a programação de uso da Internet usando uma tabela. As linhas da tabela correspondem aos dias da semana e as colunas correspondem a intervalos de 1 hora na escala de tempo. A escala de tempo pode ser de 12 ou de 24 horas, dependendo das configurações regionais do sistema operacional. As cores das células da tabela refletem os limites impostos: o cinza indica que o uso da Internet está bloqueado; o verde indica que está permitido.

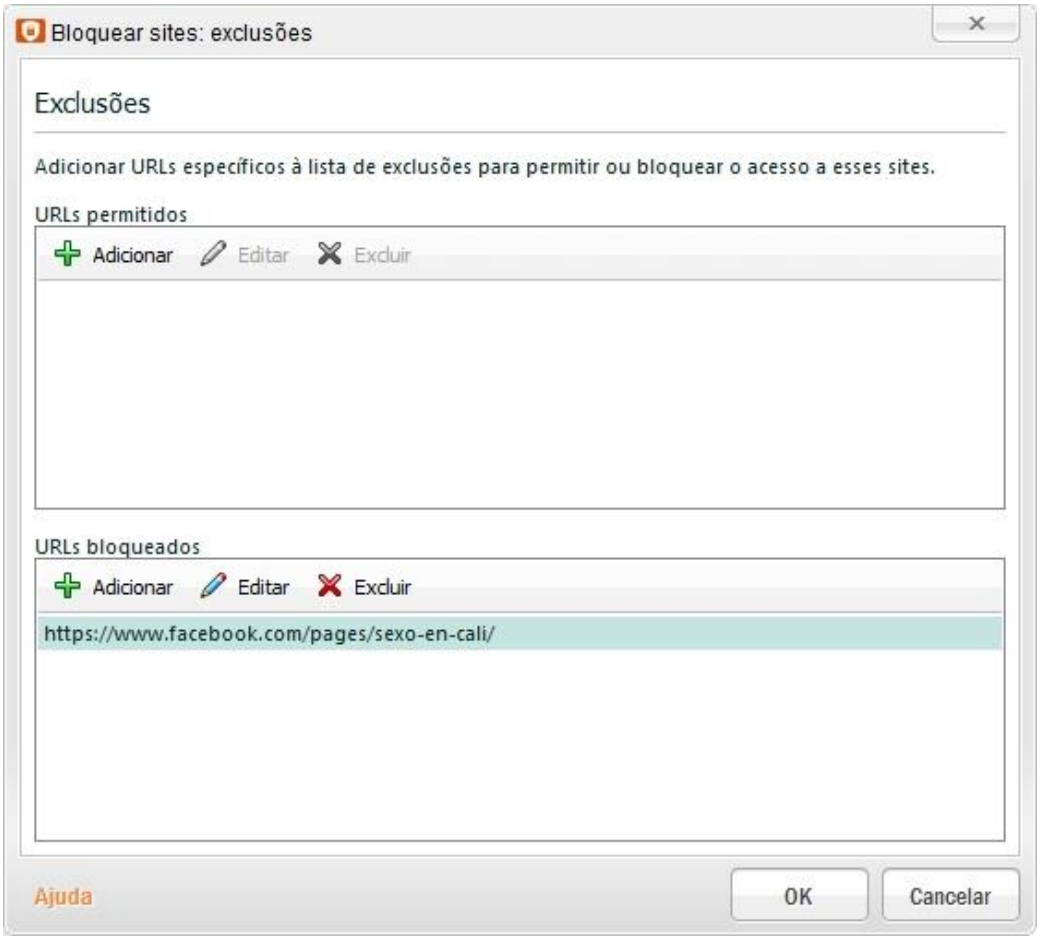
Se a caixa estiver desmarcada, a programação de limites não será observada.

- Limitar o tempo de uso diário: Esta caixa ativa/desativa os limites de tempo impostos sobre o uso da Internet a cada 24 horas.

  Se a caixa estiver marcada, você poderá especificar o tempo máximo de uso da Internet permitido a cada 24 horas. O tempo de uso total é inserido no formato hh:mm.

  Se a caixa estiver desmarcada, o tempo total de uso da Internet a cada 24 horas não será limitado.

5.4.1.5 Navegação na Web*:*



Na seção “Controlar a Navegação na Web” é possível restringir o acesso a sites de acordo com seu conteúdo:

- Ativar a pesquisa segura: Esta caixa de seleção ativa/desativa o modo de pesquisa segura, que é aplicado quando você utiliza mecanismos de pesquisa.

- Ativar controle: Esta caixa ativa/desativa o controle de sites visitados para a conta selecionada.

  Se a caixa estiver marcada, as informações sobre os sites visitados para a conta selecionada serão exibidas no Relatório de Navegação na Web. Você também pode bloquear/permitir o acesso a sites de uma categoria específica ou configurar uma lista de exceções.

Na seção Bloquear sites, é possível selecionar categorias de sites aos quais o acesso deve ser bloqueado e criar uma lista de exclusões:

- Bloquear sites das seguintes categorias:

✓ Selecionar tudo: Ao clicar neste link, são marcadas as caixas correspondentes a todas as categorias de sites aos quais o acesso deve ser bloqueado.

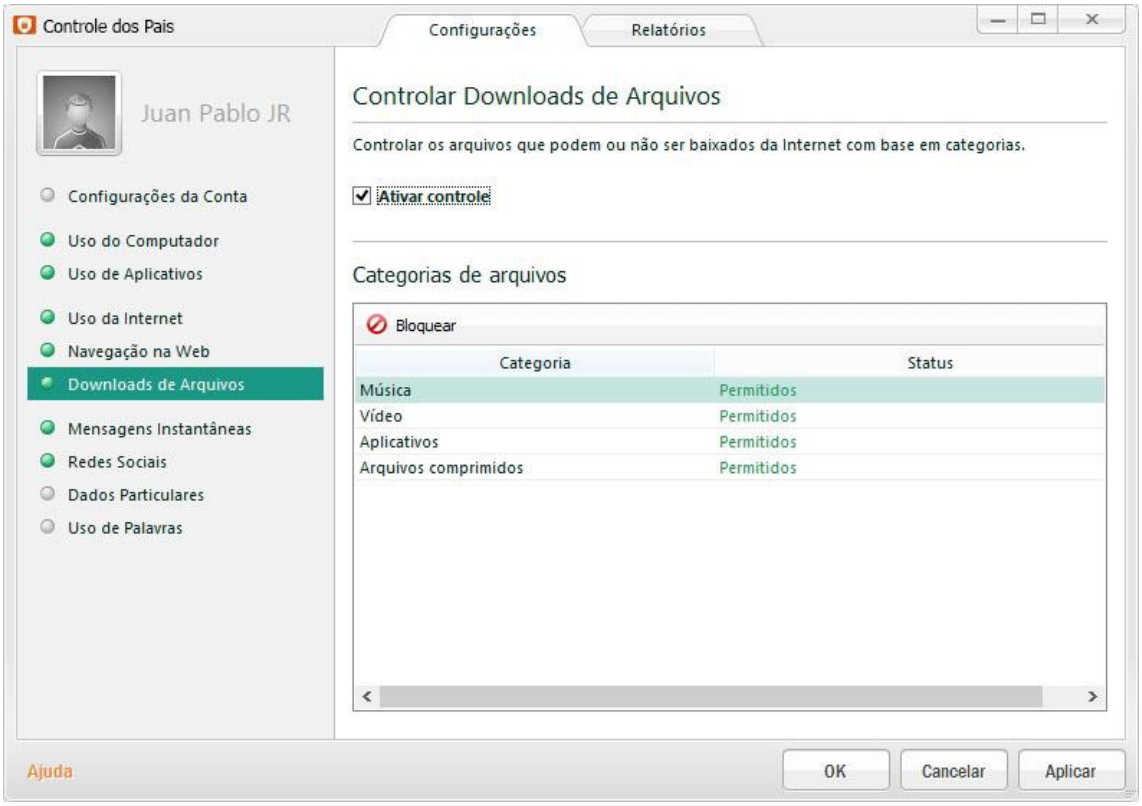
✓ Limpar tudo: Ao clicar neste link, são marcadas as caixas correspondentes a todas as categorias de sites aos quais o acesso deve ser bloqueado.

✓ Seleção manual: Marque manualmente apenas as caixas dos itens de interesse.

- Bloqueia o acesso a todos os sites, exceto aqueles permitidos na lista de exclusões:

✓ Exclusões: Ao clicar neste botão, a janela Bloquear sites: exclusões é aberta. Nesta janela, é possível criar e editar uma listas de sites com acesso permitido/bloqueado, independente das configurações atuais especificadas para o controle de conteúdo da Web:

5.4.1.6 Downloads de Arquivos



Na seção “Controlar Downloads de Arquivos” é possível limitar o download de arquivos da Internet:

- Ativar controle: Esta caixa ativa/desativa o controle de downloads de arquivos da Internet para a conta selecionada.

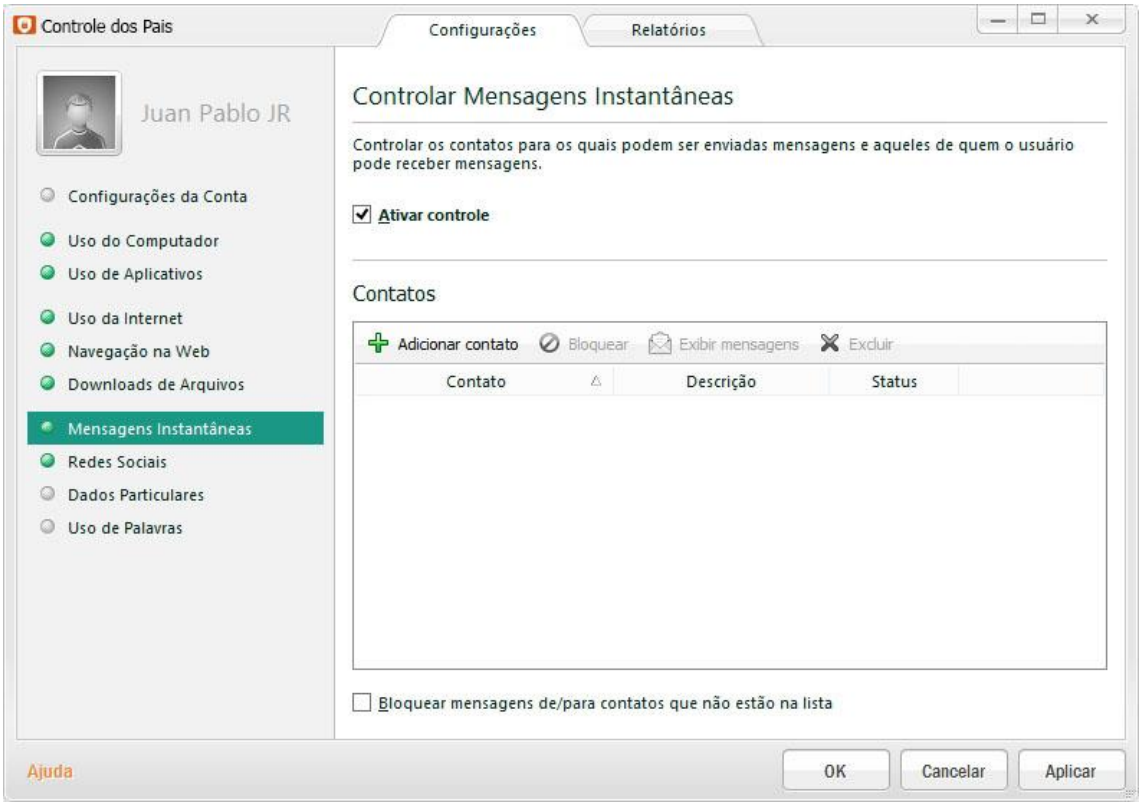
  Se a caixa estiver marcada, as informações sobre os arquivos bloqueados ou baixados da Internet serão exibidas no Relatório de Downloads de Arquivos para a conta selecionada. Você também pode permitir ou bloquear o download de arquivos da Web de acordo com as categorias às quais eles pertencem.

  Se a caixa estiver desmarcada, as estatísticas de download de arquivos não serão mantidas, de forma que o usuário poderá baixar arquivos da Internet sem limites.

- Categorias de arquivos: A lista contém as seguintes categorias de arquivos cujo download da Internet é permitido/bloqueado pelo Controle para Pais:

  - Música;
  - Vídeo;
  - Aplicativos;
  - Arquivos comprimidos.

5.4.1.7 Mensagens Instantâneas



Na seção Controlar Mensagens Instantâneas, é possível restringir as mensagens do usuário em programas de mensagens instantâneas (IM).

- Ativar controle: Esta caixa ativa/desativa o controle de mensagens instantâneas para a conta selecionada.

  Se a caixa estiver marcada, informações sobre todas as mensagens enviadas e recebidas serão exibidas no Relatório de Mensagens Instantâneas para a conta selecionada. Além disso, você pode criar listas de contatos permitidos e bloqueados.

  Se a caixa estiver desmarcada, as estatísticas de mensagens bloqueadas não serão mantidas e o usuário estará liberado para trocar mensagens instantâneas com todos os contatos.

- Adicionar contato: Este botão permite abrir a janela Novo contato para adicionar um novo contato.

- Bloquear/Permitir: Este botão permite/bloqueia a troca de mensagens com um contato. Por padrão, o aplicativo permite as mensagens com todos os contatos. Por padrão, a comunicação entre contatos que são adicionados à lista é bloqueada.

- Exibir mensagens: Este botão permite abrir a janela Mensagens para exibir o texto das mensagens com o contato selecionado.

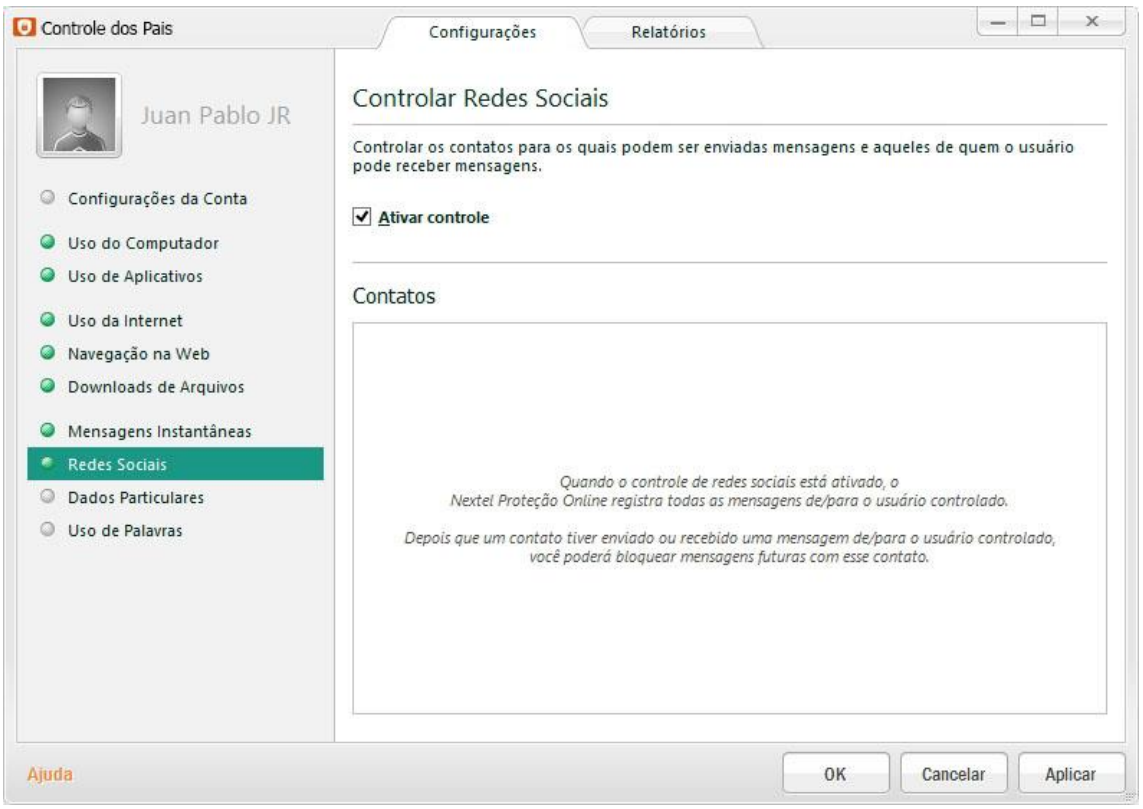
- Excluir: Este botão permite remover o contato selecionado da lista.

- Bloquear mensagens de/para contatos que não estão na lista: Esta caixa ativa/desativa o bloqueio das mensagens com todos os contatos, exceto os permitidos.

  Se esta caixa estiver marcada, o usuário poderá trocar mensagens apenas com os contatos permitidos.

  Se esta caixa estiver desmarcada, o usuário poderá trocar mensagens apenas com os contatos que não foram bloqueados.

5.4.1.8 Redes sociais



Na seção Controlar Redes Sociais, é possível restringir as mensagens do usuário em redes sociais.

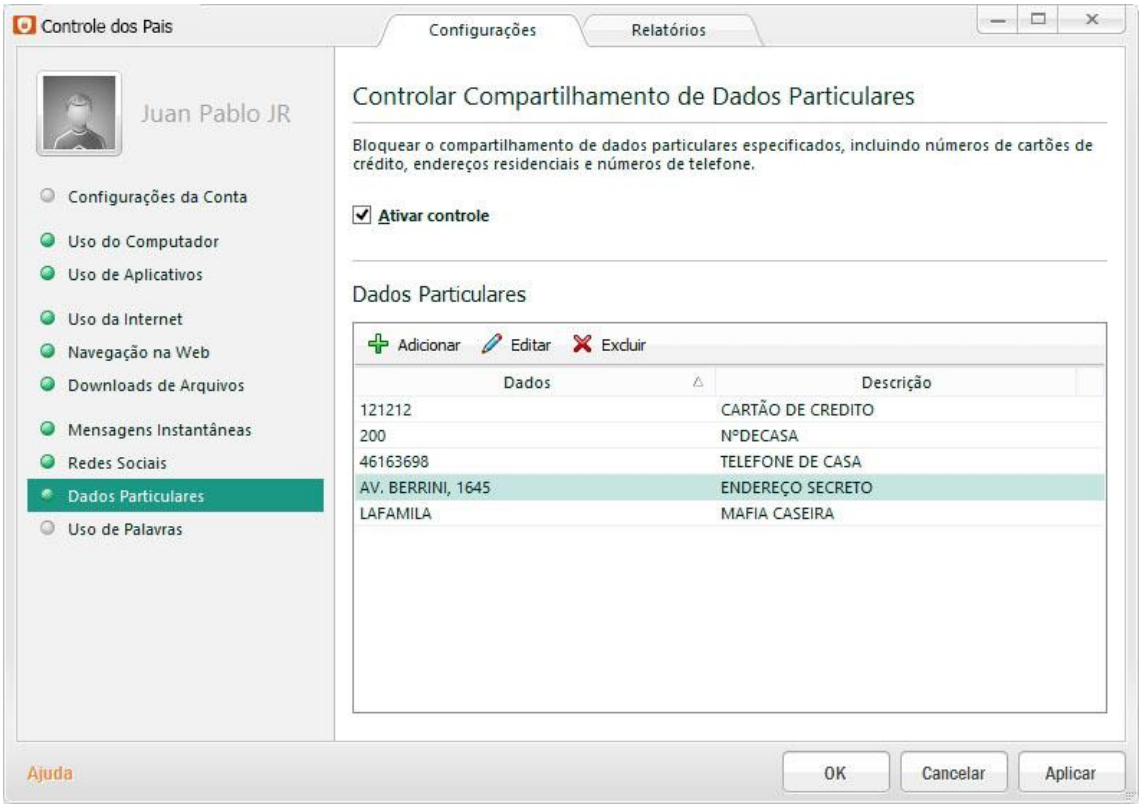
- Ativar controle: Esta caixa ativa/desativa o controle da correspondência em redes sociais para a conta selecionada.

  Se a caixa estiver marcada, as informações sobre todas as mensagens enviadas e recebidas em redes sociais serão exibidas no Relatório de Redes Sociais. Se a caixa estiver marcada, você também poderá criar e editar listas de contatos de redes sociais permitidos e bloqueados.

  Se a caixa estiver desmarcada, as estatísticas de mensagens bloqueadas não serão mantidas e o usuário estará liberado para trocar mensagens com todos os contatos de redes sociais. Esta caixa está desmarcada por padrão.

Contatos: Permite criar uma lista dos contatos do usuário em redes sociais com os quais a troca de mensagens será permitida/bloqueada.

5.4.1.9 Dados Particulares



Na seção Controlar Compartilhamento de Dados Particulares, é possível restringir a transferência de dados pessoais pelo usuário através de programas de IM, redes sociais e ao enviar dados a sites:

- Ativar controle: Esta caixa ativa/desativa o controle de transferências de dados pessoais para a conta selecionada.

  Se a caixa estiver marcada, as informações sobre todas as mensagens com dados pessoais enviadas e recebidas serão exibidas no Relatório de Compartilhamento de Dados Particulares. Você também pode criar uma lista de registros que contêm dados confidenciais, como endereços físicos e números de telefone.

  Se a caixa estiver desmarcada, as estatísticas sobre tentativas de transferência de dados pessoais não serão mantidas e o usuário poderá enviar dados pessoais sem restrições.

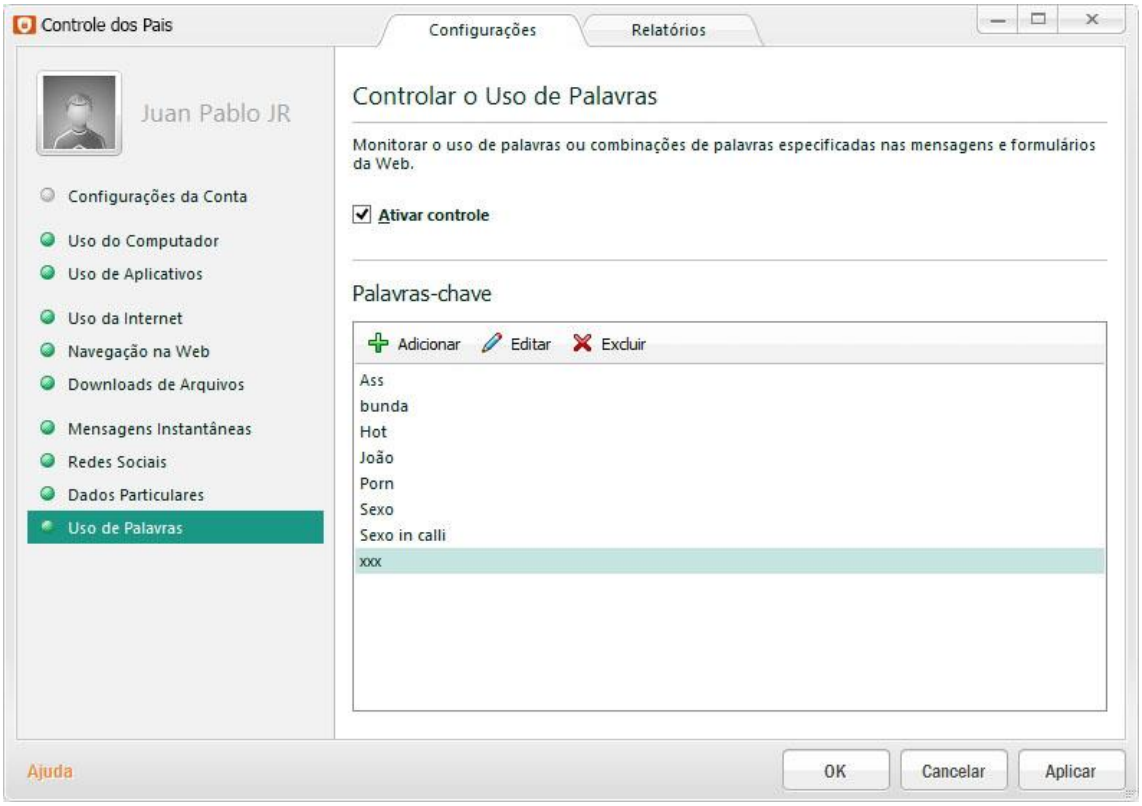
- Dados Particulares: A lista contém registros com informações que não podem ser encaminhados. Você pode editar os registros da lista.

  - Adicionar: Ao clicar no botão, é aberta a janela Dados particulares, na qual é possível adicionar um novo registro com dados pessoais à lista.

  - Editar: Ao clicar no botão, é aberta a janela Dados particulares, na qual é possível editar um registro com dados pessoais.

  - Excluir: Ao clicar neste botão, é possível remover o registro de dados particulares selecionado da lista.

5.4.1.10 Uso de Palavras



Na seção Controlar o Uso de Palavras, é possível monitorar o uso de determinadas palavras e combinações de palavras nas mensagens do usuário em programas de IM, redes sociais e ao enviar dados a sites.

- Ativar controle: Esta caixa ativa/desativa o controle de palavras-chave para a conta selecionada.

  Se a caixa estiver marcada, informações sobre as palavras-chave detectadas nas mensagens serão exibidas no Relatório de Uso de Palavras para a conta selecionada. Além disso, você pode criar uma lista de palavras-chave e combinações de palavras que devem ser rastreadas nas mensagens do usuário.

  Se a caixa estiver desmarcada, as estatísticas sobre palavras-chave detectadas em mensagens não serão mantidas para a conta selecionada.

- Palavras-chave: A lista contém palavras-chave e combinações de palavras que devem ser rastreadas nas mensagens. Você pode editar palavras e combinações de palavras incluídas na lista.

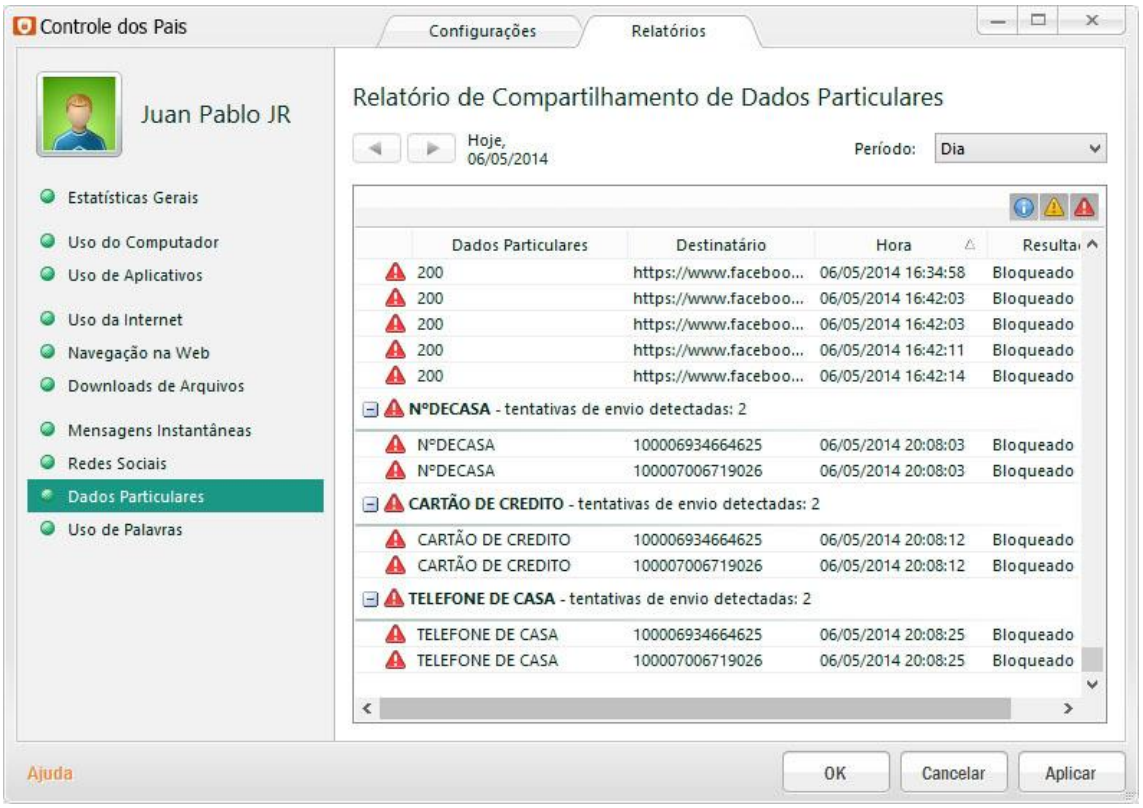
- Adicionar: Este botão permite abrir a janela Palavra-chave para adicionar uma nova palavra-chave ou combinação de palavras.

- Editar: Este botão permite abrir a janela Palavra-chave para editar uma palavra-chave ou combinação de palavras selecionada na lista.

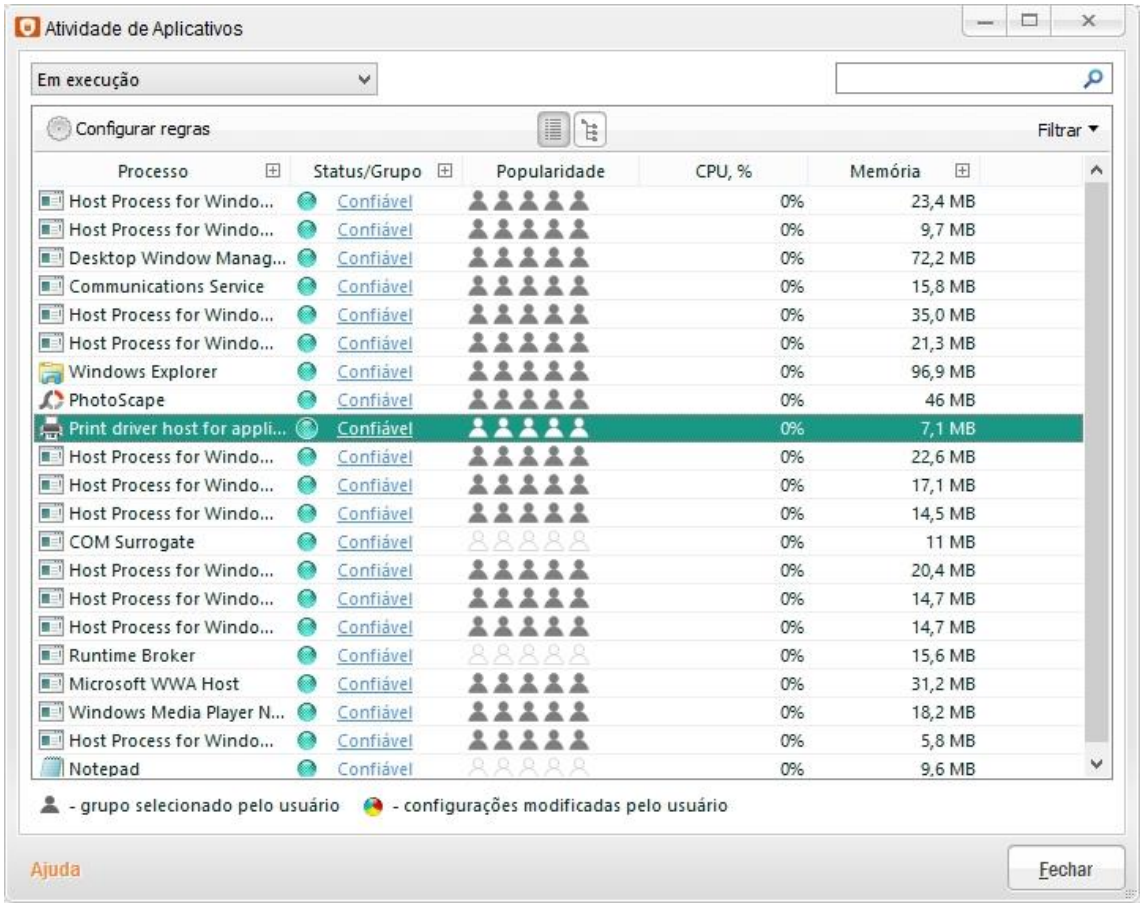
- Excluir: Este botão permite remover a palavra ou a combinação de palavras selecionada da lista.

Obs. Na Janela “Controle dos Pais” Na parte superior, temos a Pasta “Relatórios”.

É possível exibir o relatório geral de operação do Controle para Pais em todas as Seções de Componentes. Conforme podemos observar na tela abaixo:



5.5 Atividade de Aplicativos

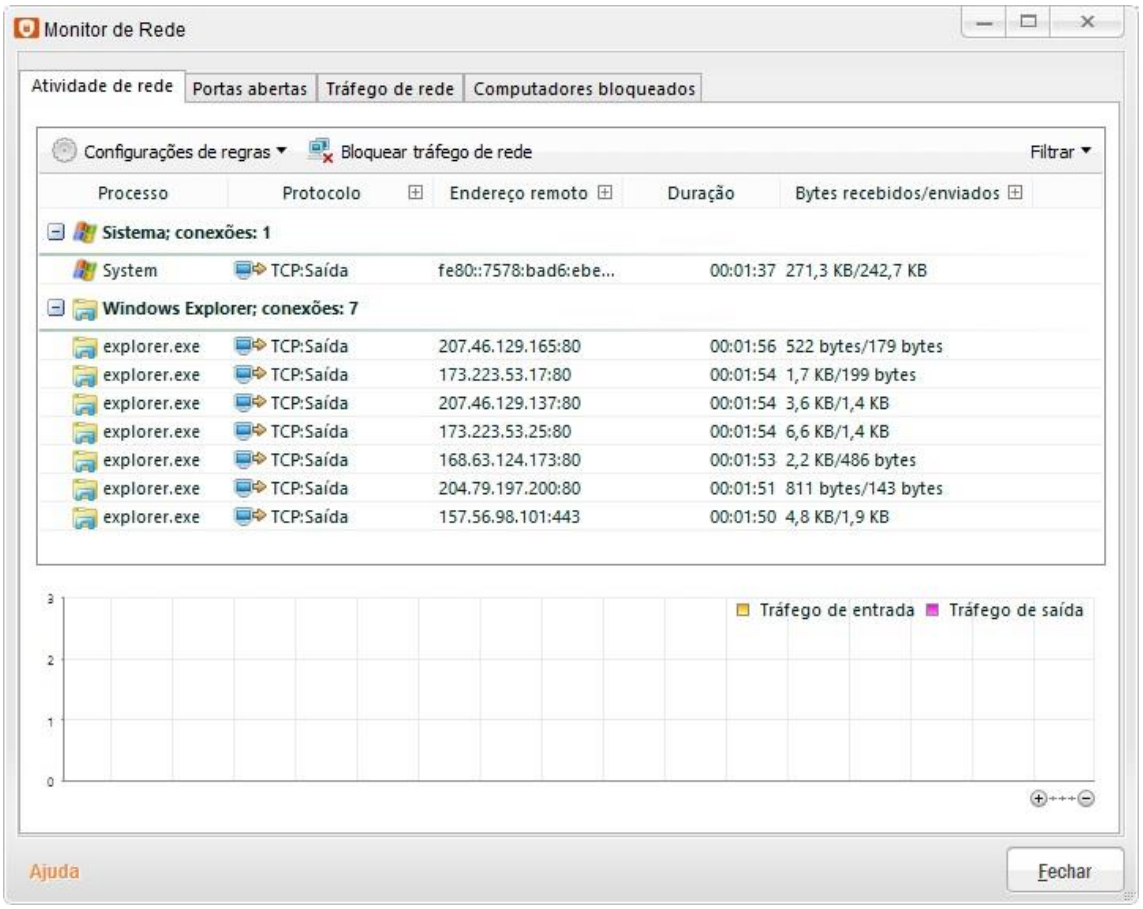


Exibe a lista atividade de aplicativos em atividade no computador.

O usuário pode filtrar a visualização por:

- Aplicativo
- Status/Grupo
- Popularidade
- Última execução

5.6 Monitor de rede

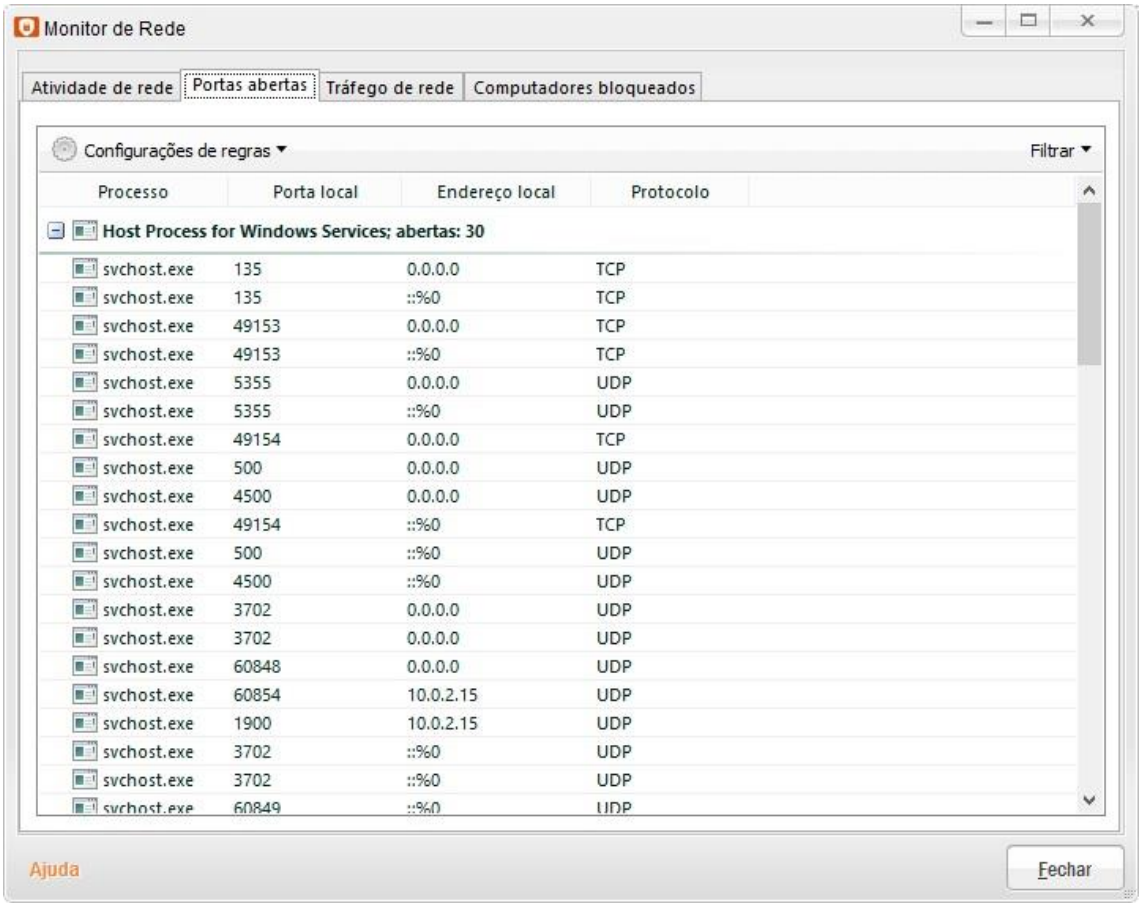


"Atividade de rede": Esta lista contém todas as conexões de rede ativas estabelecidas no computador no momento.

São exibidas as seguintes informações para cada conexão:

- Nome do processo (programa, serviço, servidor) que iniciou a conexão
- O protocolo da conexão
- Configurações de conexão (portas local e remota e endereços IP)
- Duração da conexão
- Volume de dados transferidos/recebidos (bytes).

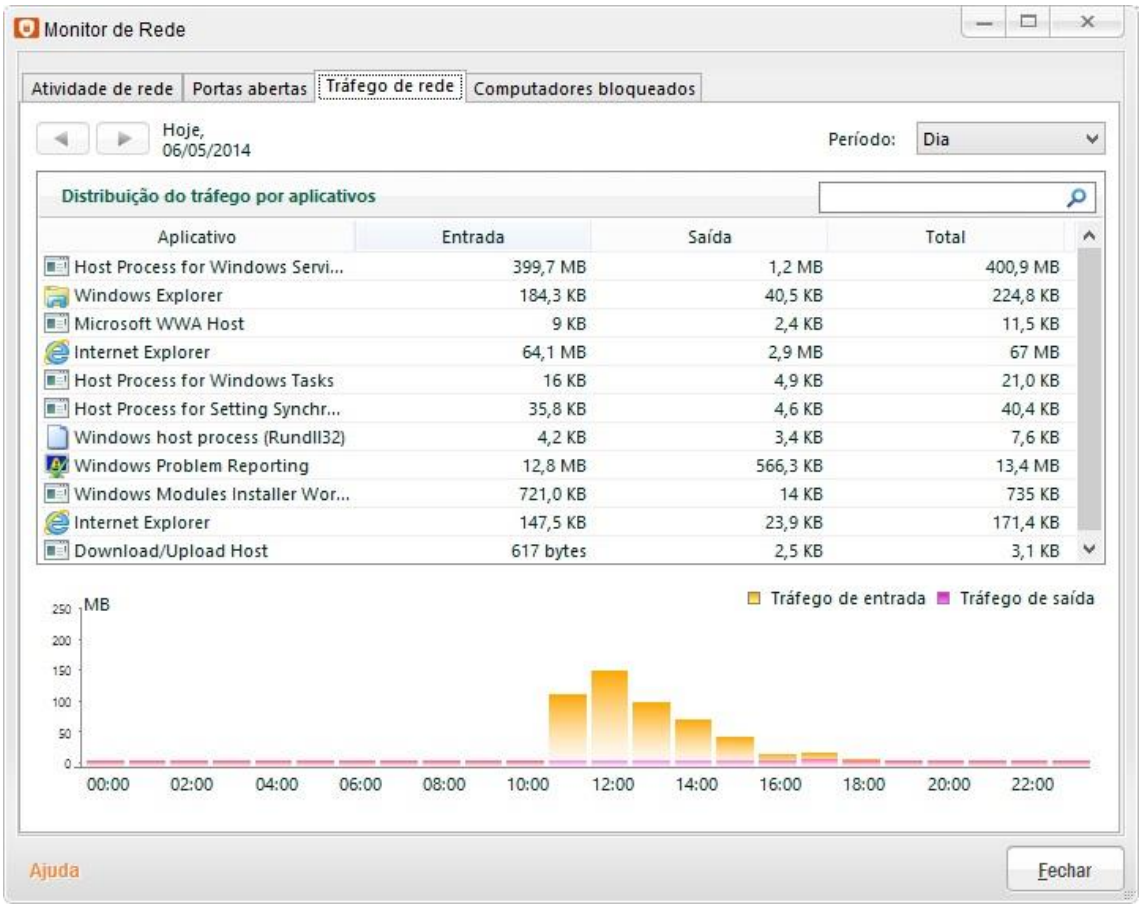
“Portas abertas”: Contém informações sobre todas as portas abertas para cada processo.



São exibidas as seguintes informações de cada porta:

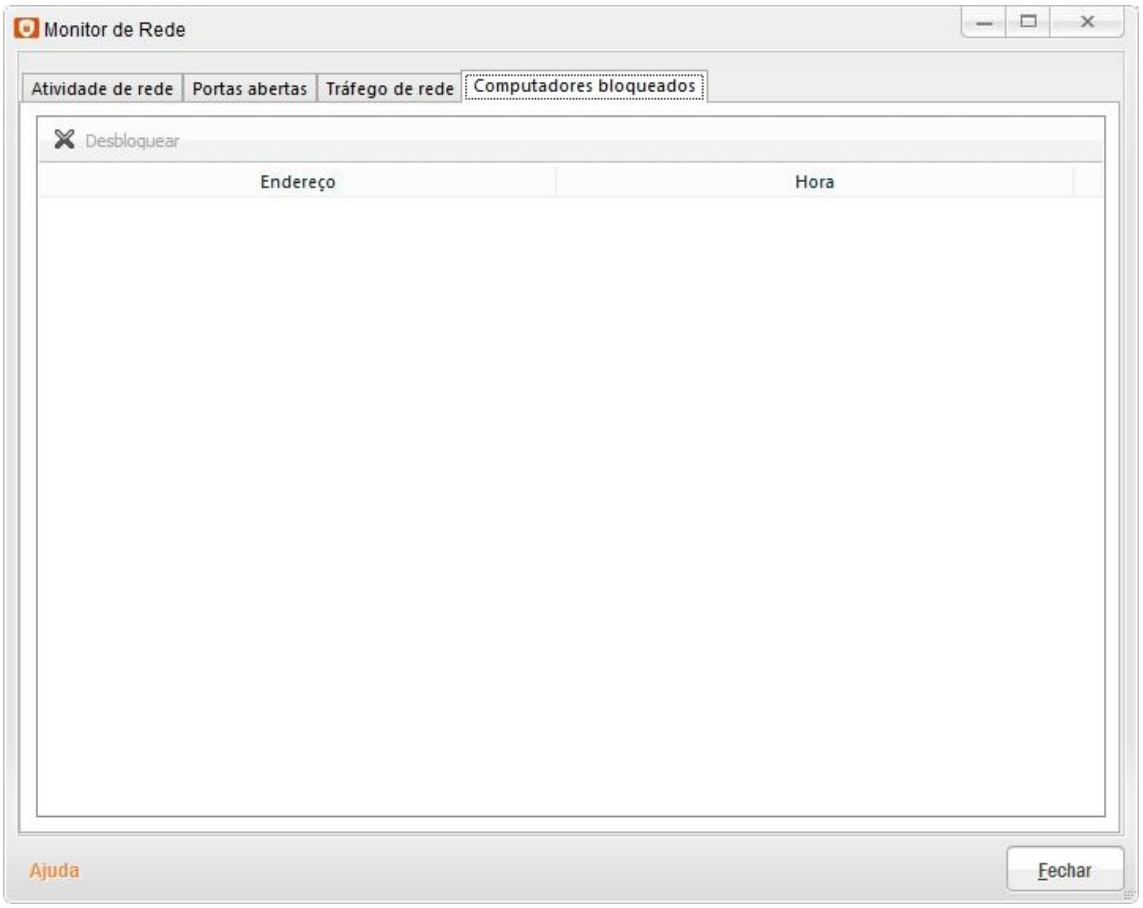
- Nome do processo (aplicativo, serviço, servidor, executor) que usa a porta.
- Número da porta, endereço IP local do processo.
- Endereço Local
- Protocolo de dados.

“Tráfego de rede”: Contém informações sobre todas as conexões de entrada e de saída estabelecidas entre o seu computador e outros computadores.



O volume de tráfego de entrada e de saída é exibido para cada programa (computador, serviço, servidor, processo). O volume de tráfego é exibido em quilobytes e megabytes.

“Computadores bloqueados”: A lista Computadores bloqueados contém informações sobre os hosts para os quais o Bloqueador de Ataques de Rede proibiu todas as atividades de rede direcionadas ao seu computador.



Endereço: Coluna exibindo o endereço IP de um host bloqueado.

5.7 Teclado Virtual

"Teclado Virtual": O Teclado Virtual exibe um teclado visual com todas as teclas padrão. Você pode selecionar as teclas usando o mouse ou outro dispositivo apontador.

5.8 Quarentena

Contém uma lista de arquivos movidos para a Quarentena. A Quarentena foi criada para armazenar cópias de backup de arquivos que foram excluídos ou modificados durante o processo de desinfecção.

"Restaurar": Ao clicar neste botão, o Nextel Proteção Online retorna um arquivo selecionado na lista para a pasta na qual ele foi armazenado antes de ser movido para a Quarentena.

"Excluir": Ao clicar neste botão, o Nextel Proteção Online exclui um arquivo selecionado da lista.

"Limpar a Quarentena": Clicar nesse botão faz com que o Nextel Proteção Online exclua todos os arquivos da Quarentena.

5.9 Ferramentas

"Disco de Recuperação Nextel Proteção Online"; Criar: Este botão inicia o Assistente para Criação do Nextel Proteção Online Rescue Disk. Você pode usar o Nextel Proteção Online Rescue Disk para restaurar a funcionalidade do sistema operacional após um ataque de vírus, caso os arquivos do sistema operacional estejam corrompidos ou se a inicialização falhar.

"Solução de problemas do Microsoft Windows"; Iniciar: Clicar neste botão inicia o Assistente para Instalação de Certificados. Esse assistente verifica alterações no sistema, analisa as informações coletadas e sugere ações para remover rastros de objetos maliciosos do sistema.

"Limpeza de Dados Particulares"; Iniciar: Clicar nesse botão inicia o Assistente de Limpeza de Dados Particulares, o qual encontra e excluir rastros da atividade do usuário no sistema (por exemplo, o histórico de sites visitados ou dos aplicativos iniciados, os arquivos temporários criados, entre outros).

"Configuração do Navegador"; Iniciar: Este botão inicia o Assistente de Configuração do Navegador, que analisa as configurações do Microsoft® Internet Explorer® da perspectiva da segurança.