

A close-up, front-facing view of a red Ferrari Formula 1 car. The car features several prominent sponsor logos: 'KASPERSKY lab' in white on the front wing, the 'PIRELLI' logo in white on a yellow background, and the 'FIAT' logo in white. The car's aerodynamic components, including the front wing and sidepods, are visible. The background is blurred, showing other parts of the race track environment.

Rexcon Consultoria
www.rexcon.com.br

Boas práticas para proteção de endpoints

Boas práticas para proteção de endpoints

- Planejando as instalações do KSC e KES
- Selecionando o Banco de Dados para o KSC
- Configurando as políticas de proteção / políticas do agente de rede
- Tarefas de Varredura / Atualização / Inventário
- Realocação de computadores / Instalação automática

Boas práticas para proteção de endpoints

Planejando a instalação do KSC e KES

- Número total de endpoints
- Definir o Hardware do servidor KSC
- Unidades (Escritórios locais / filiais)
- Tarefas de Atualização / Varredura / Inventário
- Filiais com links de comunicação reduzidos

Boas práticas para proteção de endpoints

Planejando as instalações do KSC e KES

Número total de endpoints

- Informação importante para planejar a implementação, tarefas, etc
- < 1.000 Ep, o HW do KSC 2 CPUs – 4 Gb RAM , 150 Gb HD
- 1.000 até 5.000 Ep, o HW do KSC 4 CPUs – 8 Gb RAM , 200 Gb HD
- > 5.000 Ep, o HW do KSC 8 CPUs – 16 Gb RAM , 250 Gb HD
- > 2.000 Ep. recomenda-se SQL SERVER corporativo
- > 5.000 Ep. é obrigatório o uso de SQL SERVER corporativo

Boas práticas para proteção de endpoints

Planejando as instalações do KSC e KES

Unidades (Escritórios locais / filiais)

- Empresas com somente um escritório central, utilizar um servidor KSC + update agents selecionados pelo próprio KSC
- Empresas com filiais, podem ser utilizados dois cenários:
 - Filiais com grande número de computadores e suporte local - Servidor KSC Slave
 - Filiais com pequeno número de computadores e sem suporte local - Update agents

Boas práticas para proteção de endpoints

Planejando as instalações do KSC e KES

Update Agents / Agentes de Atualização

- Podem ser atribuídos de forma automática em empresas sem filiais. Ao utilizar de forma manual, a recomendação é um update agent a cada 100 computadores na mesma rede local
- A configuração é realizada nas propriedades do servidor KSC

Seções

Geral

Notificação de eventos

Chaves

Servidor proxy do KSN

Configurações

Ataque de vírus

Tráfego

Armazenamento de eventos

Servidor da Web

Segurança

Funções de usuário

Agentes de atualização

Regras de identificação

Configurações de entrega da notificação

Avançado

Agentes de atualização

☐ Atribuir automaticamente os agentes de atualização

Computador

Adicionar o agente de atualização

Computador para agir como o agente de atualização:

Selecionar

Conjunto de computadores associados com este agente de atualização:

Selecionar

OK Cancelar

Adicionar computadores

Computadores gerenciados

Leonardo

Secure Mail Gateway

LENOVO-LEANDRO

WIN-XI035VM2Q0C

OK Cancelar

Adicionar

Propriedades

As subredes NLA são usadas para definir o escopo dos agentes de atualização. Você também pode ativar a atribuição automática de agentes de atualização para subredes NLA selecionadas.

[Configurar subredes NLA](#)

Ajuda

OK

Cancelar

Aplicar

Start

Kaspersky Security C...

PT

7:44 PM

Boas práticas para proteção de endpoints

Planejando as instalações do KSC e KES

Connection Gateways

Ao configurar um update agent como connection gateway, você garante que todos os computadores daquele grupo não irão se comunicar com o KSC diretamente

A configuração é realizada nas propriedades da política do agente de rede

<https://support.kaspersky.com/10601>

Boas práticas para proteção de endpoints

Selecionando o Banco de Dados para o KSC

Até 2.000 Ep. recomenda-se seguir com a instalação SQL SERVER EXPRESS (nativo do instalador KSC)

> 2.000 e < 5.000 Ep. recomenda-se SQL SERVER EXPRESS pode crescer até o limite de 10 Gb, e ser necessária uma migração para a versão corporativa

> 5.000 Ep. é obrigatório o uso de SQL SERVER corporativo

Hardware recomendado para o servidor SQL corporativo

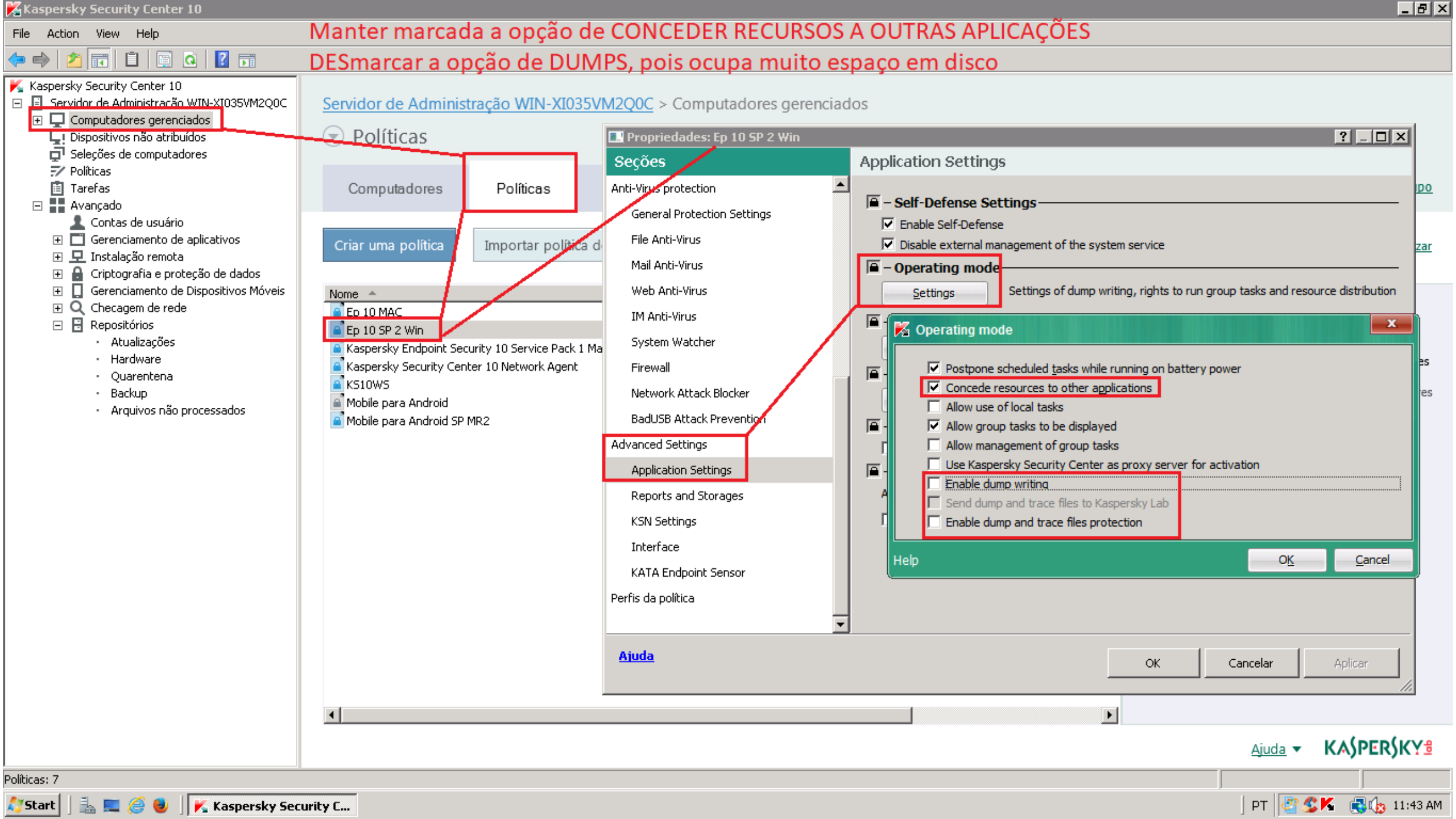
De 2.000 até 5.000 Ep. - 1 a 4 CPUs, 8 Gb de RAM

Acima de 5.000 Ep. - 6 a 8 CPUs, 16 Gb de RAM

Boas práticas para proteção de endpoints

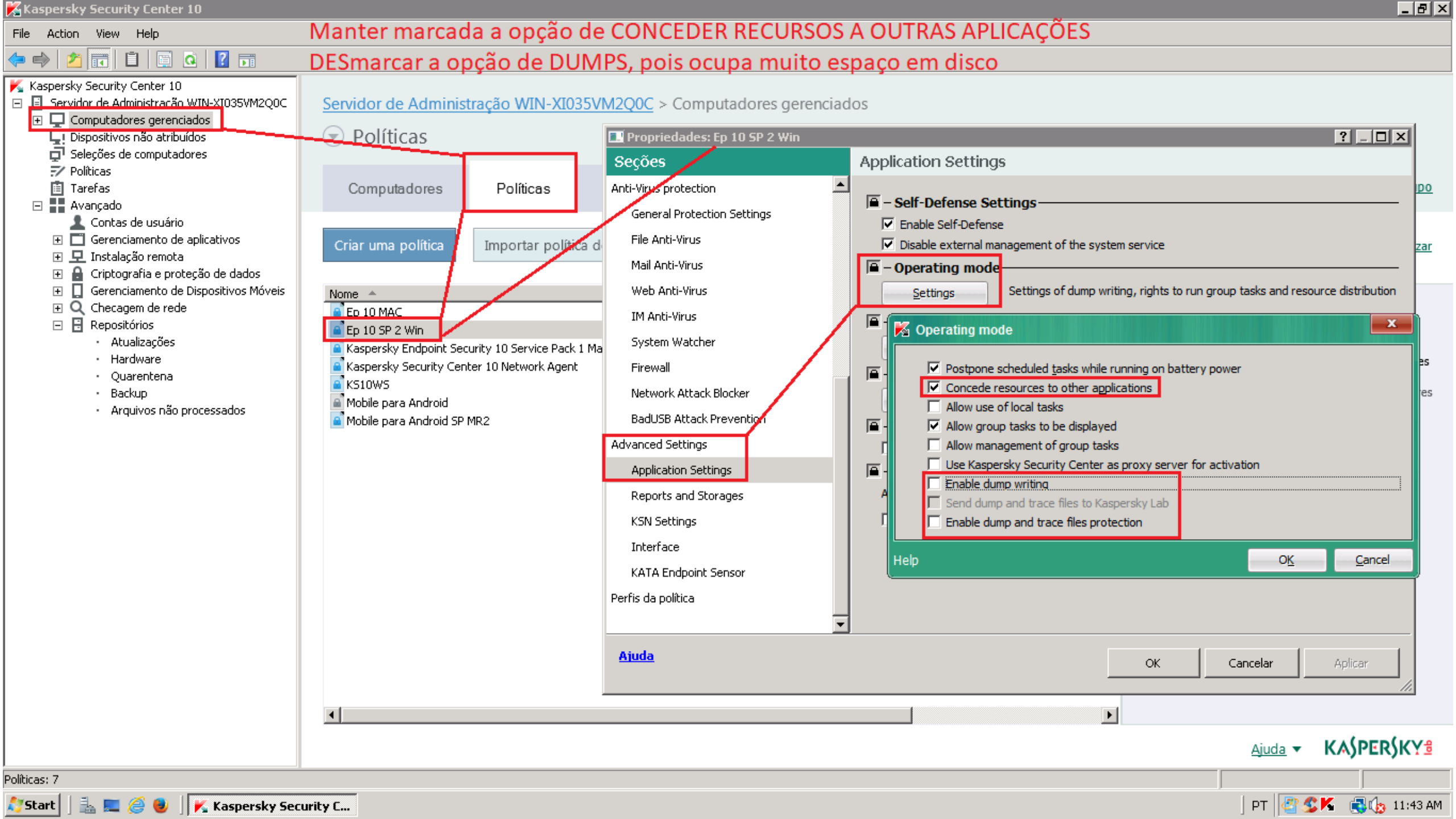
Configurando as políticas de proteção / políticas do agente de rede

- Application Startup Control - Bloqueio de execução de determinados aplicativos, baseando-se em nome do software, executável, ou categoria
- Application Privilege Control - Monitora o funcionamento de aplicativos usando categorias e assinatura digital dos arquivos
- Device Control - Bloquear o acesso a dispositivos tais como pendrives / HDs externos, unidades DVDs, etc
- Web Control - Bloquear o acesso a sites por categoria ou lista inserida



Manter marcada a opção de CONCEDER RECURSOS A OUTRAS APLICAÇÕES

DESmarcar a opção de DUMPS, pois ocupa muito espaço em disco



Manter marcadas as opções de Self-Defense***** Importantíssimo *** Manter pelo menos o Quick Scan para dispositivos removíveis**

- Kaspersky Security Center 10
- Servidor de Administração WIN-XI035VM2Q0C
 - Computadores gerenciados
 - Dispositivos não atribuídos
 - Seleções de computadores
 - Políticas
 - Tarefas
 - Avançado
 - Contas de usuário
 - Gerenciamento de aplicativos
 - Instalação remota
 - Criptografia e proteção de dados
 - Gerenciamento de Dispositivos Móveis
 - Checagem de rede
 - Repositórios
 - Atualizações
 - Hardware
 - Quarentena
 - Backup
 - Arquivos não processados

Servidor de Administração WIN-XI035VM2Q0C > Computadores gerenciados

Políticas

Computadores

Políticas

Criar uma política

Importar política d

Nome

- Ep 10 MAC
- Ep 10 SP 2 Win
- Kaspersky Endpoint Security 10 Service Pack 1 Ma
- Kaspersky Security Center 10 Network Agent
- KS10WS
- Mobile para Android
- Mobile para Android SP MR2

Propriedades: Ep 10 SP 2 Win

Seções

Anti-Virus protection

General Protection Settings

File Anti-Virus

Mail Anti-Virus

Web Anti-Virus

IM Anti-Virus

System Watcher

Firewall

Network Attack Blocker

BadUSB Attack Prevention

Advanced Settings

Application Settings

Reports and Storages

KSN Settings

Interface

KATA Endpoint Sensor

Perfis da política

[Ajuda](#)

Application Settings

Self-Defense Settings

- ☒ Enable Self-Defense
- ☒ Disable external management of the system service

Operating mode

Settings

Settings of dump writing, rights to run group tasks and resource distribution

Proxy Server Settings

Settings

Address is defined automatically, port 80

Password protection

Settings

Password protection: Enabled

Background scan

- ☐ Perform Idle Scan

Scan removable drives on connection

Action on removable drive connection:

Quick Scan

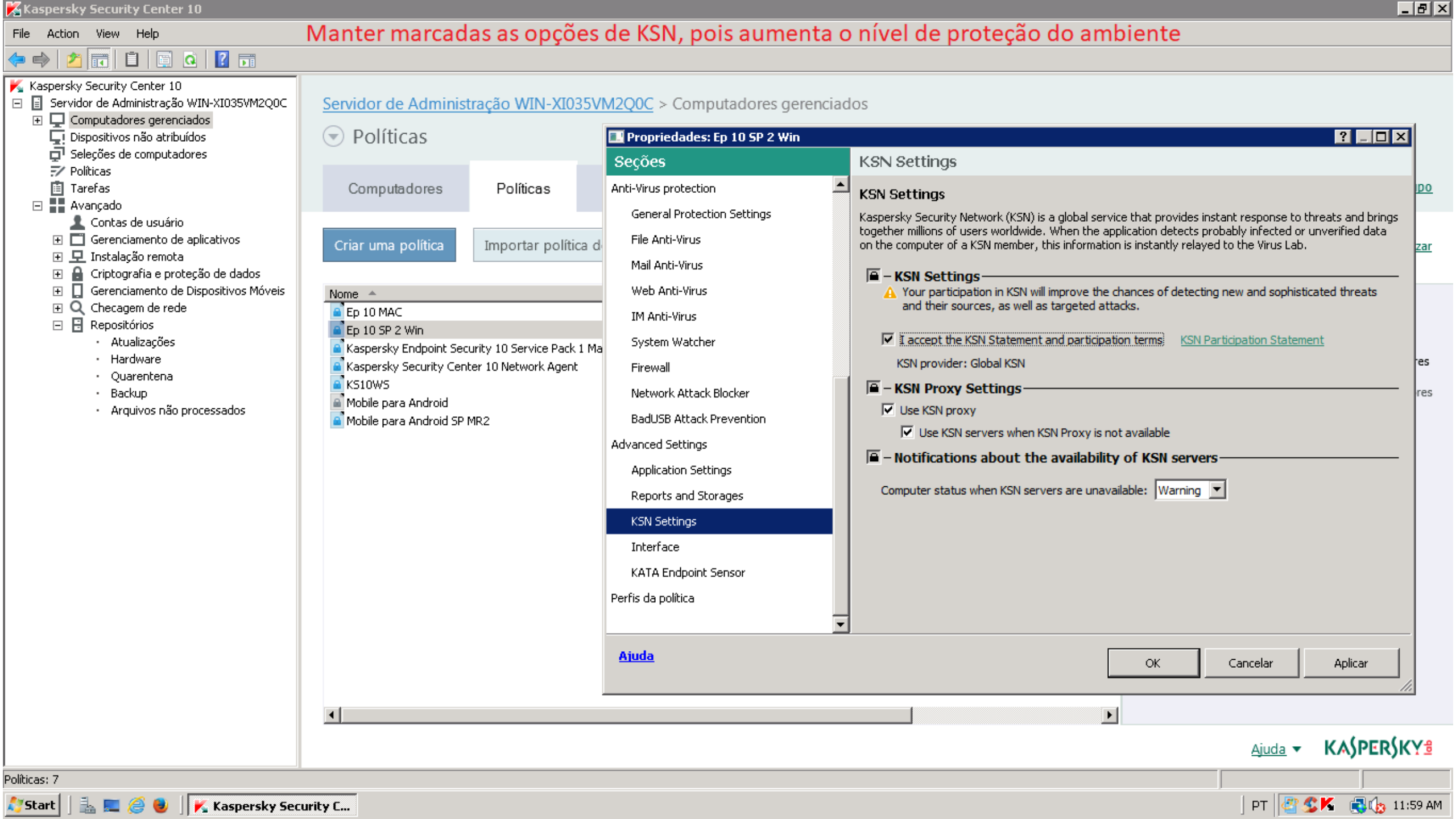
☐ Maximum removable drive size:

4096 MB

OK

Cancelar

Aplicar



Manter marcadas as opções de KSN, pois aumenta o nível de proteção do ambiente

Servidor de Administração WIN-XI035VM2Q0C > Computadores gerenciados

Políticas

Computadores

Políticas

Criar uma política

Importar política d

Nome

Ep 10 MAC

Ep 10 SP 2 Win

Kaspersky Endpoint Security 10 Service Pack 1 Ma

Kaspersky Security Center 10 Network Agent

KS10WS

Mobile para Android

Mobile para Android SP MR2

Propriedades: Ep 10 SP 2 Win

Seções

Anti-Virus protection

General Protection Settings

File Anti-Virus

Mail Anti-Virus

Web Anti-Virus

IM Anti-Virus

System Watcher

Firewall

Network Attack Blocker

BadUSB Attack Prevention

Advanced Settings

Application Settings

Reports and Storages

KSN Settings

Interface

KATA Endpoint Sensor

Perfis da política

[Ajuda](#)

KSN Settings

KSN Settings

Kaspersky Security Network (KSN) is a global service that provides instant response to threats and brings together millions of users worldwide. When the application detects probably infected or unverified data on the computer of a KSN member, this information is instantly relayed to the Virus Lab.

KSN Settings

⚠ Your participation in KSN will improve the chances of detecting new and sophisticated threats and their sources, as well as targeted attacks.

☒ I accept the KSN Statement and participation terms [KSN Participation Statement](#)

KSN provider: Global KSN

KSN Proxy Settings

☒ Use KSN proxy

☒ Use KSN servers when KSN Proxy is not available

Notifications about the availability of KSN servers

Computer status when KSN servers are unavailable: Warning

OK

Cancelar

Aplicar

[Ajuda](#)

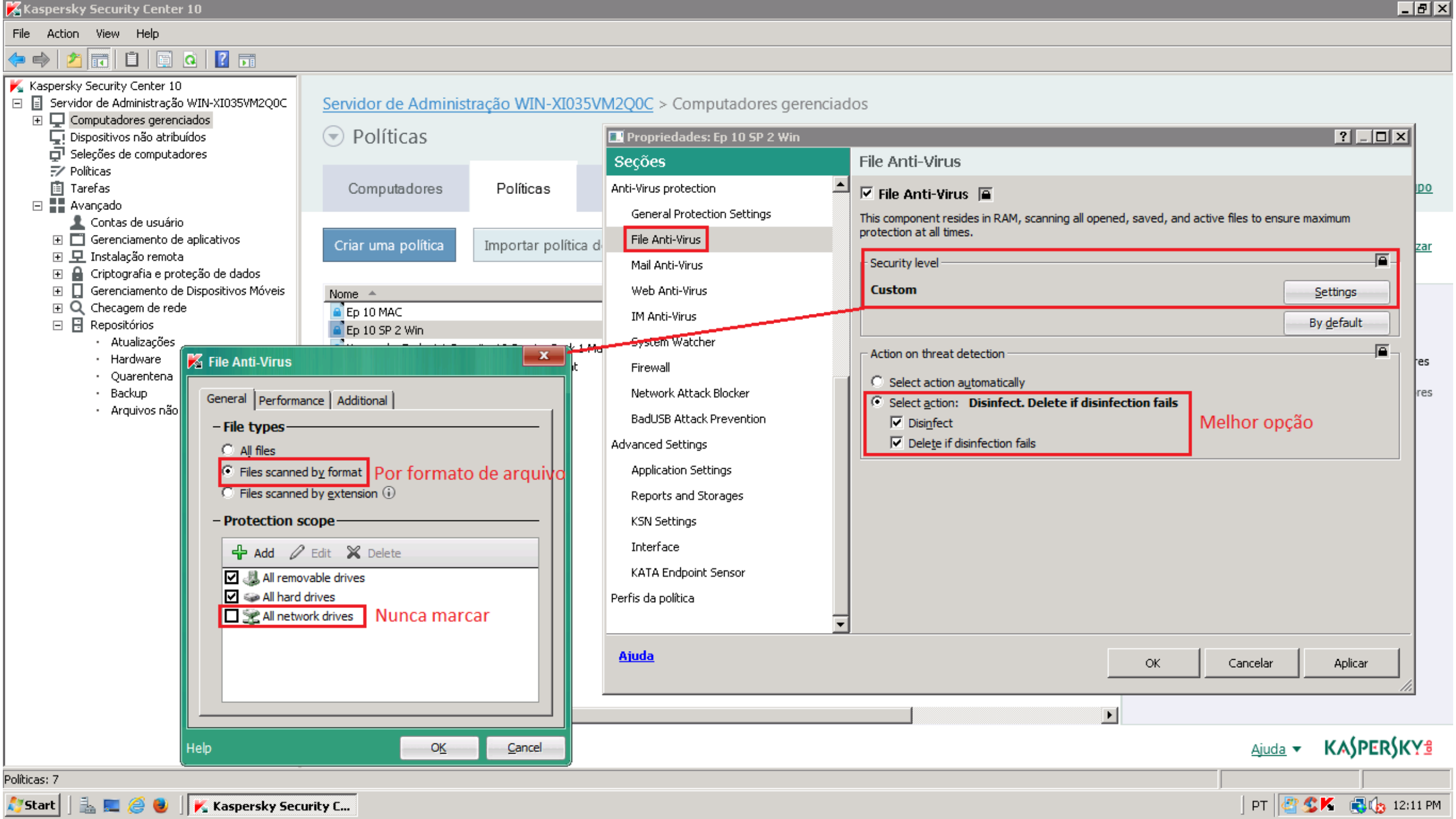
KASPERSKY

Políticas: 7

Start Kaspersky Security C...

PT 11:59 AM





Servidor de Administração WIN-XI035VM2Q0C > Computadores gerenciados

Políticas

Computadores

Políticas

Criar uma política

Importar política d

Nome

Ep 10 MAC

Ep 10 SP 2 Win

Propriedades: Ep 10 SP 2 Win

Seções

Anti-Virus protection

General Protection Settings

File Anti-Virus

Mail Anti-Virus

Web Anti-Virus

IM Anti-Virus

System Watcher

Firewall

Network Attack Blocker

BadUSB Attack Prevention

Advanced Settings

Application Settings

Reports and Storages

KSN Settings

Interface

KATA Endpoint Sensor

Perfis da política

Ajuda

File Anti-Virus

☒ File Anti-Virus

This component resides in RAM, scanning all opened, saved, and active files to ensure maximum protection at all times.

Security level

Custom

Settings

By default

Action on threat detection

☐ Select action automatically

☒ Select action: **Disinfect. Delete if disinfection fails**

☒ Disinfect

☒ Delete if disinfection fails

Melhor opção

File Anti-Virus

General

Performance

Additional

File types

☐ All files

☒ Files scanned by format

☐ Files scanned by extension

Protection scope



Add



Edit



Delete



☒ All removable drives



☒ All hard drives



☐ All network drives

Nunca marcar

Help

OK

Cancel

Ajuda

KASPERSKY

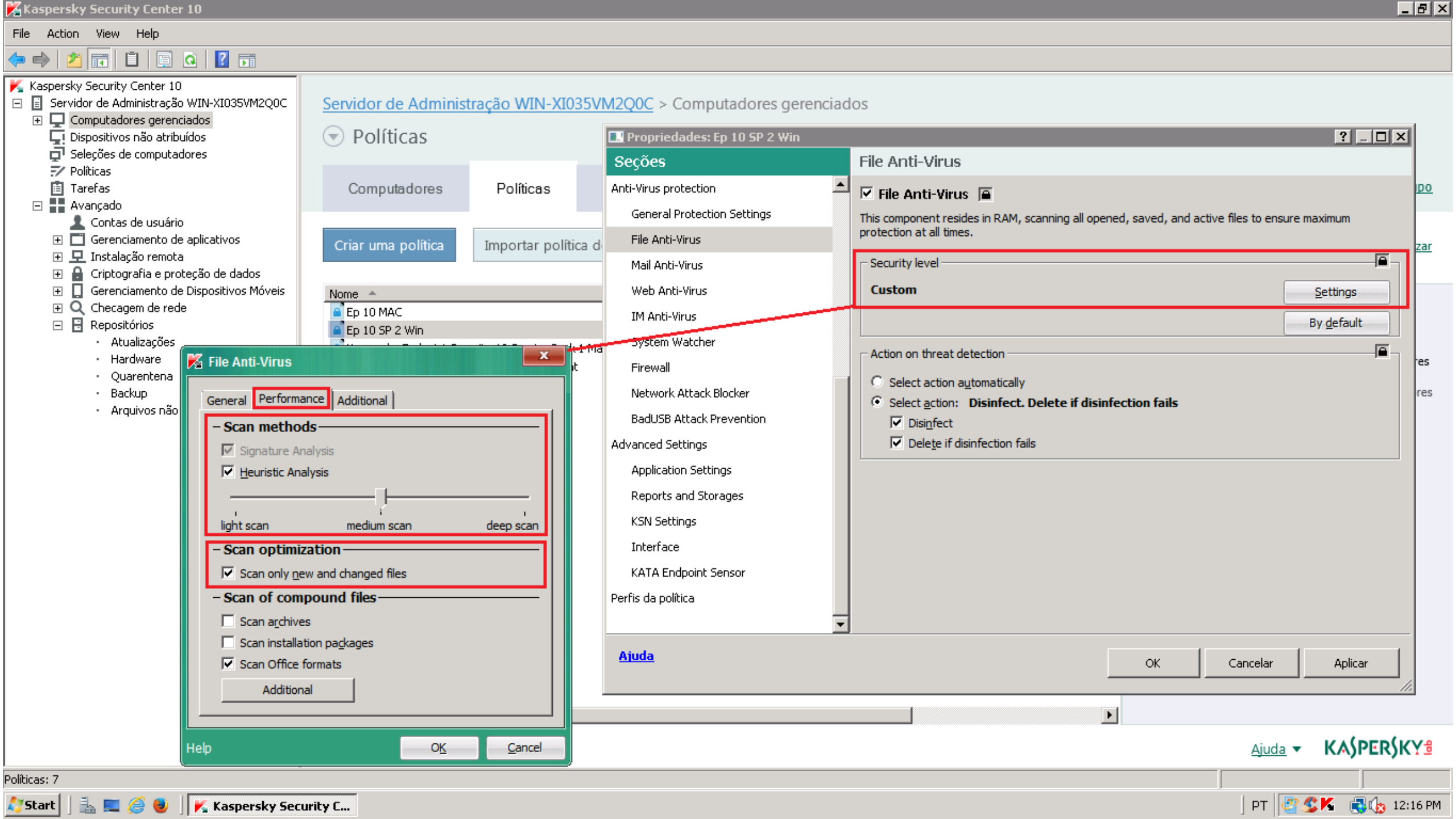
Políticas: 7

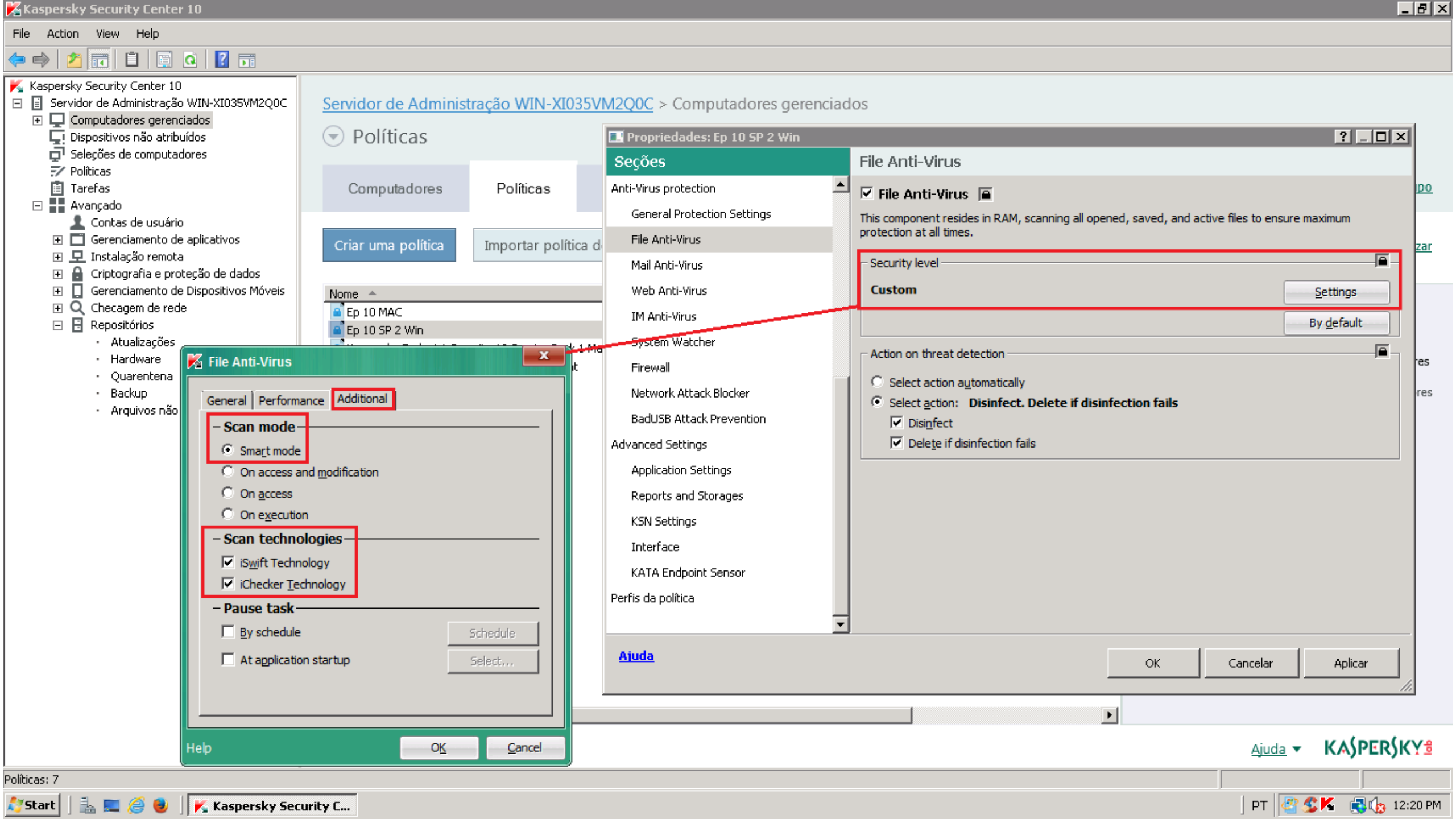
Start

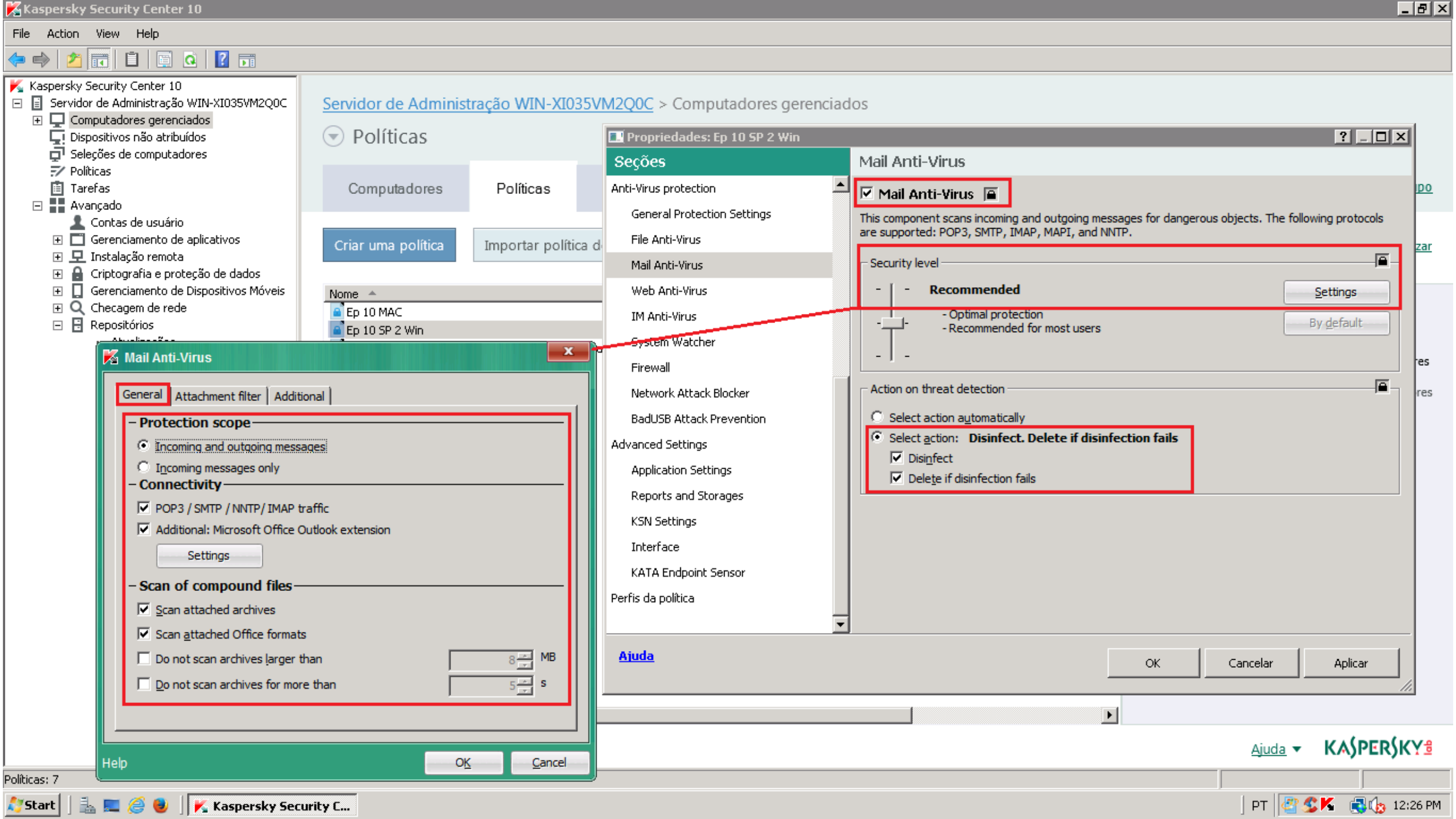
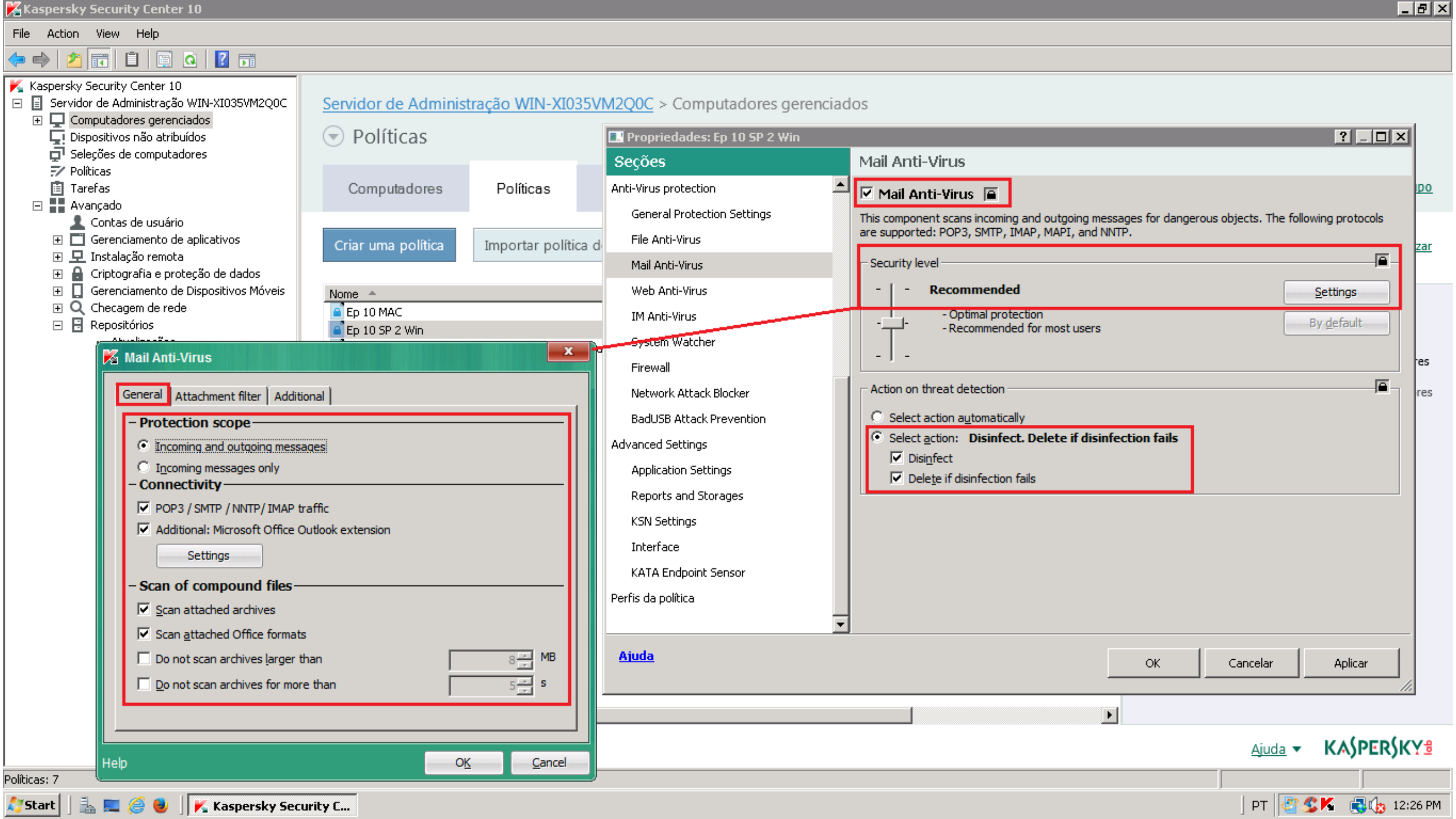
Kaspersky Security C...

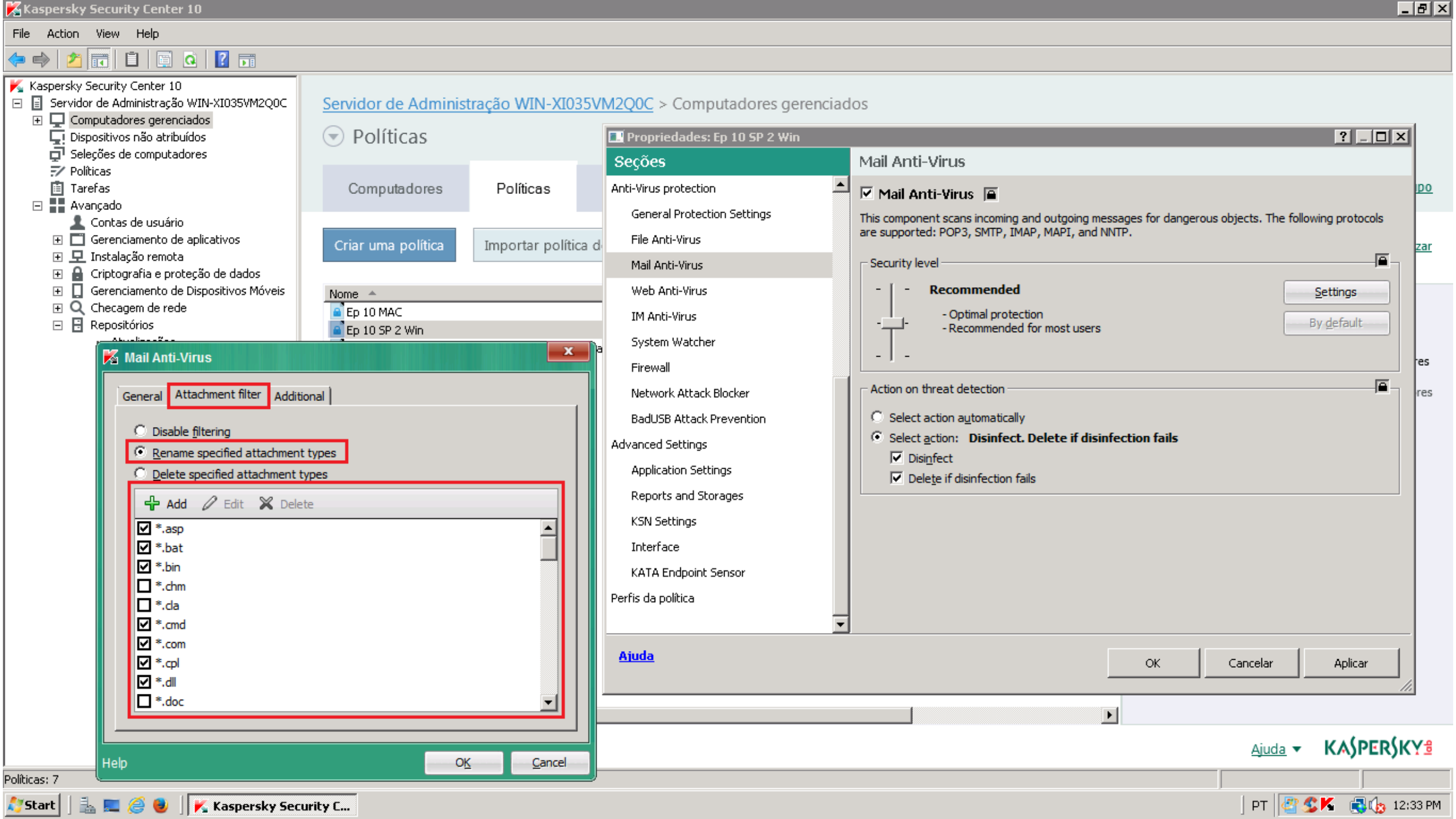
PT

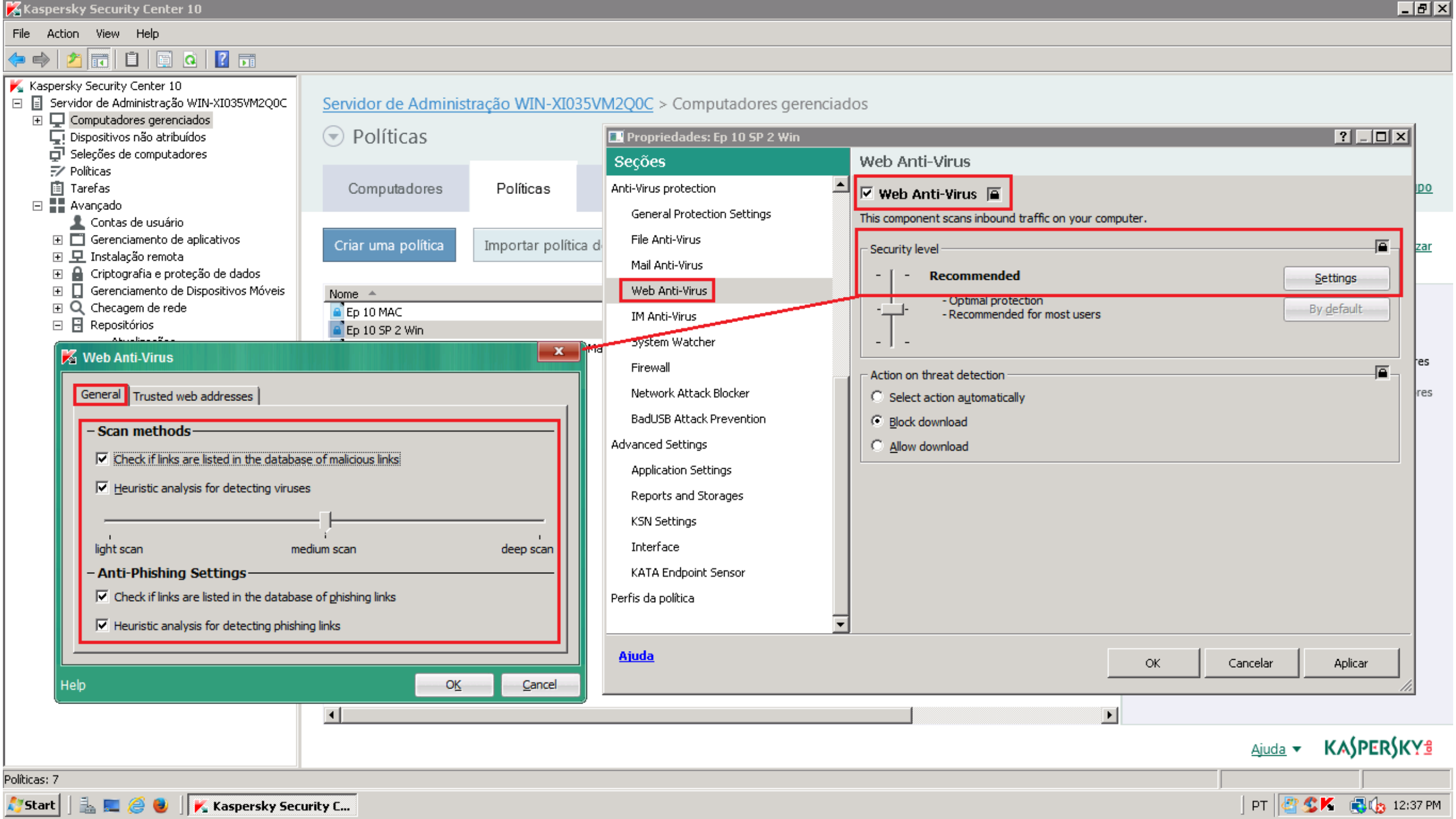
12:11 PM













Kaspersky Security Center 10

Servidor de Administração WIN-XI035VM2Q0C

Computadores gerenciados

Dispositivos não atribuídos

Seleções de computadores

Políticas

Tarefas

Avançado

Contas de usuário

Gerenciamento de aplicativos

Instalação remota

Criptografia e proteção de dados

Gerenciamento de Dispositivos Móveis

Checagem de rede

Repositórios

Servidor de Administração WIN-XI035VM2Q0C > Computadores gerenciados

Políticas

Computadores

Políticas

Criar uma política

Importar política d

Nome

Ep 10 MAC

Ep 10 SP 2 Win

Propriedades: Ep 10 SP 2 Win

Seções

Anti-Virus protection

General Protection Settings

File Anti-Virus

Mail Anti-Virus

Web Anti-Virus

IM Anti-Virus

System Watcher

Firewall

Network Attack Blocker

BadUSB Attack Prevention

Advanced Settings

Application Settings

Reports and Storages

KSN Settings

Interface

KATA Endpoint Sensor

Perfis da política

Ajuda

Web Anti-Virus

☒ Web Anti-Virus

This component scans inbound traffic on your computer.

Security level

Recommended

Settings

- Optimal protection

- Recommended for most users

By default

Action on threat detection

☐ Select action automatically☒ Block download☐ Allow download

OK

Cancelar

Aplicar

Web Anti-Virus

General Trusted web addresses

Web Anti-Virus does not scan web traffic from trusted web addresses.

☒ Do not scan web traffic from trusted web addresses:

+ Add Edit X Delete

☒ *.adventistas.org/*☒ *.iatec.com/*☒ *.hasilvestre.org.br/*

Help

OK

Cancel

Ajuda

KASPERSKY



Kaspersky Security Center 10

Servidor de Administração WIN-XI035VM2Q0C

- Computadores gerenciados
- Dispositivos não atribuídos
- Seleções de computadores
- Políticas
- Tarefas
- Avançado
 - Contas de usuário
 - Gerenciamento de aplicativos
 - Instalação remota
 - Criptografia e proteção de dados
 - Gerenciamento de Dispositivos Móveis
 - Checagem de rede
 - Repositórios
 - Atualizações
 - Hardware
 - Quarentena
 - Backup
 - Arquivos não processados

Servidor de Administração WIN-XI035VM2Q0C > Computadores gerenciados

Políticas

Computadores

Políticas

Criar uma política

Importar política d

Nome

- Ep 10 MAC
- Ep 10 SP 2 Win
- Kaspersky Endpoint Security 10 Service Pack 1 Ma
- Kaspersky Security Center 10 Network Agent
- KS10WS
- Mobile para Android
- Mobile para Android SP MR2

Propriedades: Ep 10 SP 2 Win

Seções

Anti-Virus protection

General Protection Settings

File Anti-Virus

Mail Anti-Virus

Web Anti-Virus

IM Anti-Virus

System Watcher

Firewall

Network Attack Blocker

BadUSB Attack Prevention

Advanced Settings

Application Settings

Reports and Storages

KSN Settings

Interface

KATA Endpoint Sensor

Perfis da política

Ajuda

IM Anti-Virus

☐ IM Anti-Virus

This component protects traffic for the following IM clients: ICQ, MSN, AIM (version 6.9.1.16 or earlier) and Mail.Ru Agent.

Protection scope

☒ Incoming and outgoing messages☐ Incoming messages only

Scan methods

☒ Check if links are listed in the database of malicious links☒ Check if links are listed in the database of phishing links

OK

Cancelar

Aplicar

Ajuda

KASPERSKY

Políticas: 7



Kaspersky Security C...

PT



12:58 PM

Kaspersky Security Center 10

Servidor de Administração WIN-XI035VM2Q0C

- Computadores gerenciados
- Dispositivos não atribuídos
- Seleções de computadores
- Políticas
- Tarefas
- Avançado
 - Contas de usuário
 - Gerenciamento de aplicativos
 - Instalação remota
 - Criptografia e proteção de dados
 - Gerenciamento de Dispositivos Móveis
 - Checagem de rede
 - Repositórios
 - Atualizações
 - Hardware
 - Quarentena
 - Backup
 - Arquivos não processados

Servidor de Administração WIN-XI035VM2Q0C > Computadores gerenciados

Políticas

Computadores

Políticas

Criar uma política

Importar política d

Nome

- Ep 10 MAC
- Ep 10 SP 2 Win
- Kaspersky Endpoint Security 10 Service Pack 1 Ma
- Kaspersky Security Center 10 Network Agent
- KS10WS
- Mobile para Android
- Mobile para Android SP MR2

Propriedades: Ep 10 SP 2 Win

Seções

Anti-Virus protection

General Protection Settings

File Anti-Virus

Mail Anti-Virus

Web Anti-Virus

IM Anti-Virus

System Watcher

Firewall

Network Attack Blocker

BadUSB Attack Prevention

Advanced Settings

Application Settings

Reports and Storages

KSN Settings

Interface

KATA Endpoint Sensor

Perfis da política

Ajuda

System Watcher

☒ System Watcher

System Watcher receives information about application activity in the operating system and searches for threats that may be missing from anti-virus databases of the application.

☒ Enable Exploit Prevention

Operating mode

☒ Do not monitor the activity of applications that have a digital signature

Action on threat detection

On detecting malware activity:

Select action automatically

Rollback of malware actions

☒ Roll back malware actions during disinfection

OK

Cancelar

Aplicar

Ajuda

KASPERSKY

*** Importantíssimo *** O módulo de Firewall é outro utilizado na contração contra RANSOMWARE
No Firewall são liberados ou bloqueados os pacotes para RDP, PING, TELNET, etc; e cadastradas as REDES



- Kaspersky Security Center 10
- Servidor de Administração WIN-XI035VM2Q0C
 - Computadores gerenciados
 - Dispositivos não atribuídos
 - Seleções de computadores
 - Políticas
 - Tarefas
 - Avançado
 - Contas de usuário
 - Gerenciamento de aplicativos
 - Instalação remota
 - Criptografia e proteção de dados
 - Gerenciamento de Dispositivos Móveis
 - Checagem de rede
 - Repositórios
 - Atualizações
 - Hardware
 - Quarentena
 - Backup
 - Arquivos não processados

Servidor de Administração WIN-XI035VM2Q0C > Computadores gerenciados

Políticas

Computadores

Políticas

Criar uma política

Importar política d

Nome

- Ep 10 MAC
- Ep 10 SP 2 Win
- Kaspersky Endpoint Security 10 Service Pack 1 Ma
- Kaspersky Security Center 10 Network Agent
- KS10WS
- Mobile para Android
- Mobile para Android SP MR2

Propriedades: Ep 10 SP 2 Win

Seções

Anti-Virus protection

General Protection Settings

File Anti-Virus

Mail Anti-Virus

Web Anti-Virus

IM Anti-Virus

System Watcher

Firewall

Network Attack Blocker

BadUSB Attack Prevention

Advanced Settings

Application Settings

Reports and Storages

KSN Settings

Interface

KATA Endpoint Sensor

Perfis da política

Ajuda

Firewall

☒ Firewall

This component filters all network activity according to the specified rules.

Firewall rules

Settings

Configure rules for Application Privilege Control in the operating system.

Settings

Configure rules for network packets and data streams.

Available networks

Settings

Configure settings for network connections.

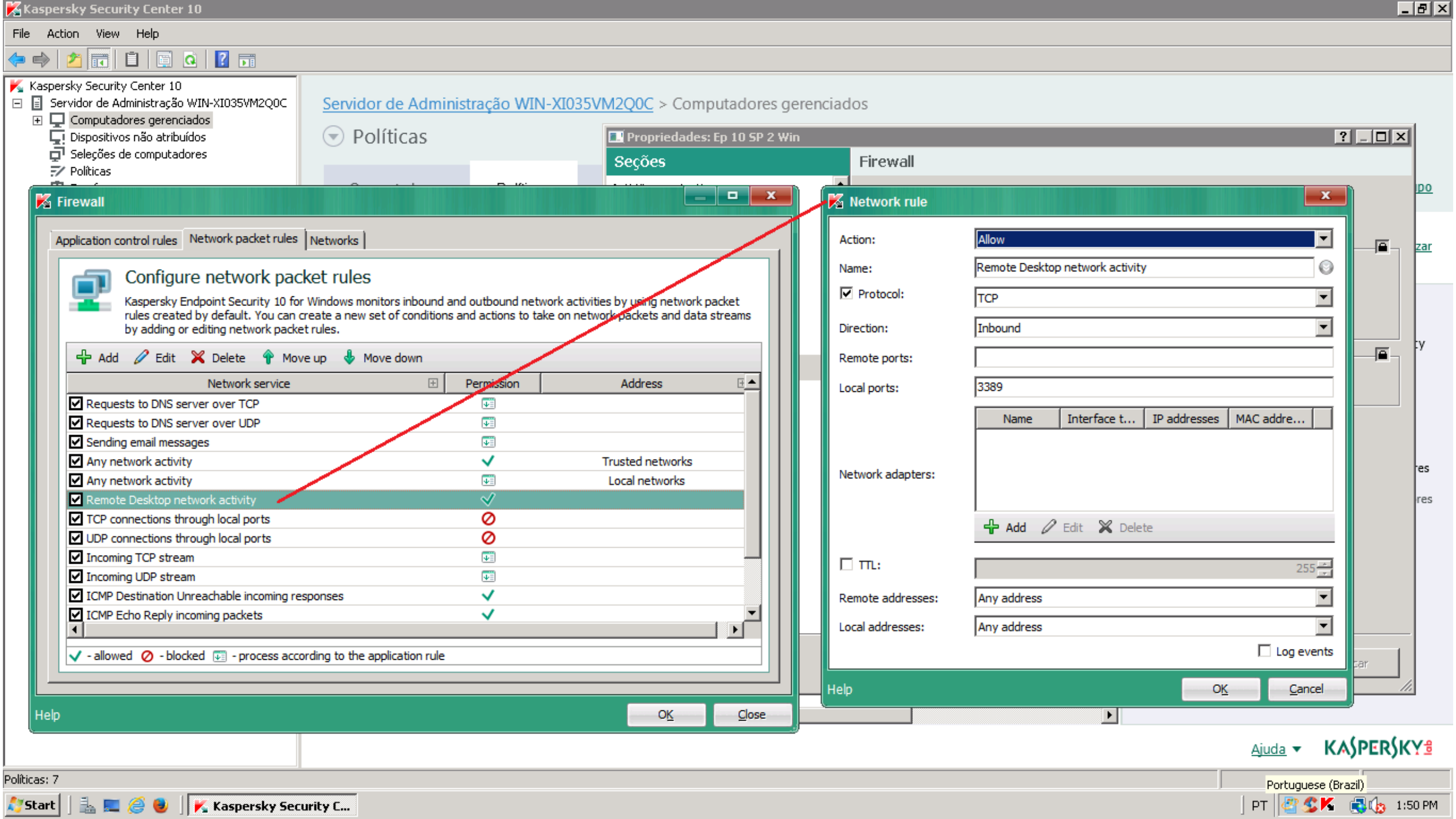
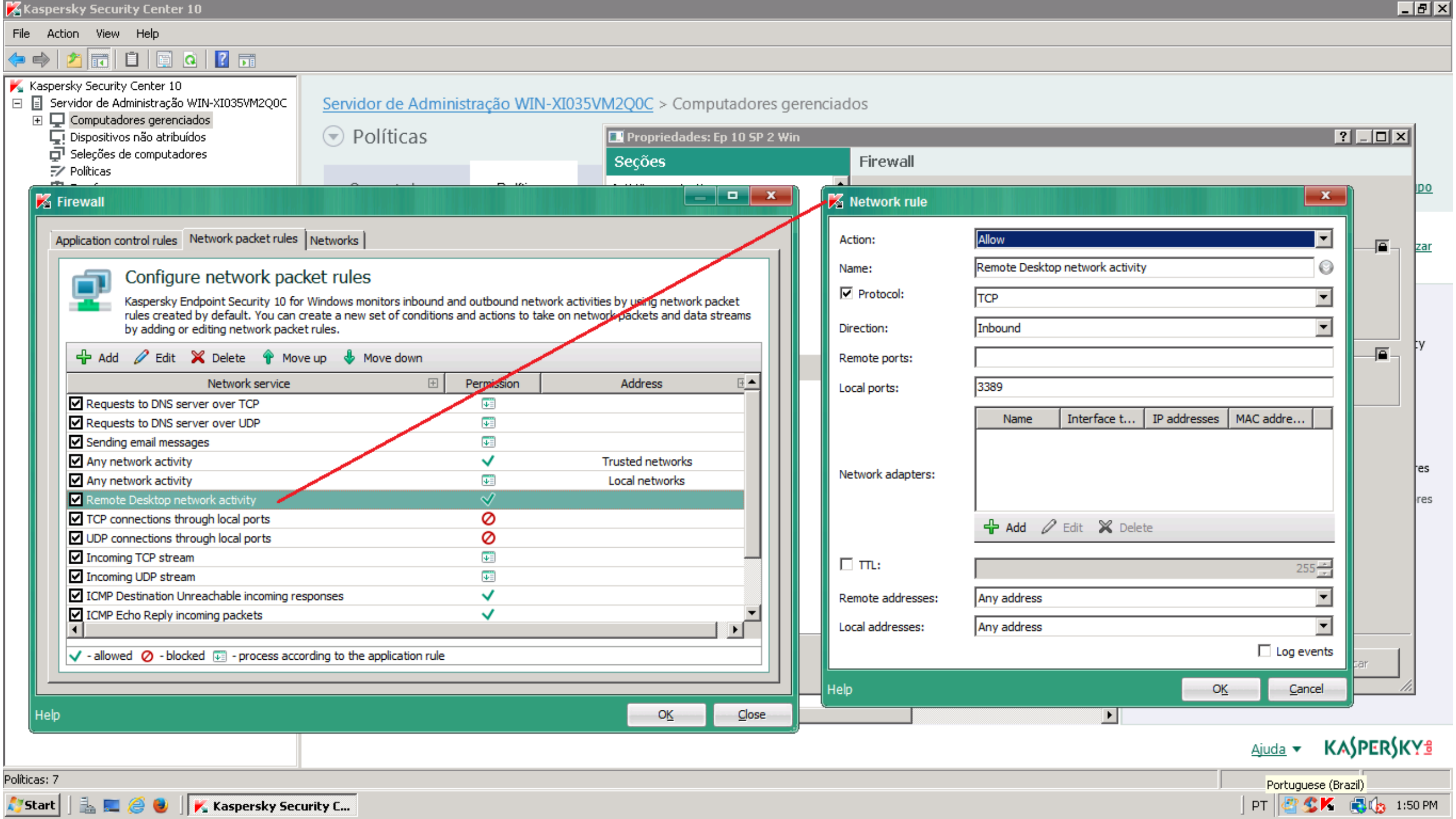
OK

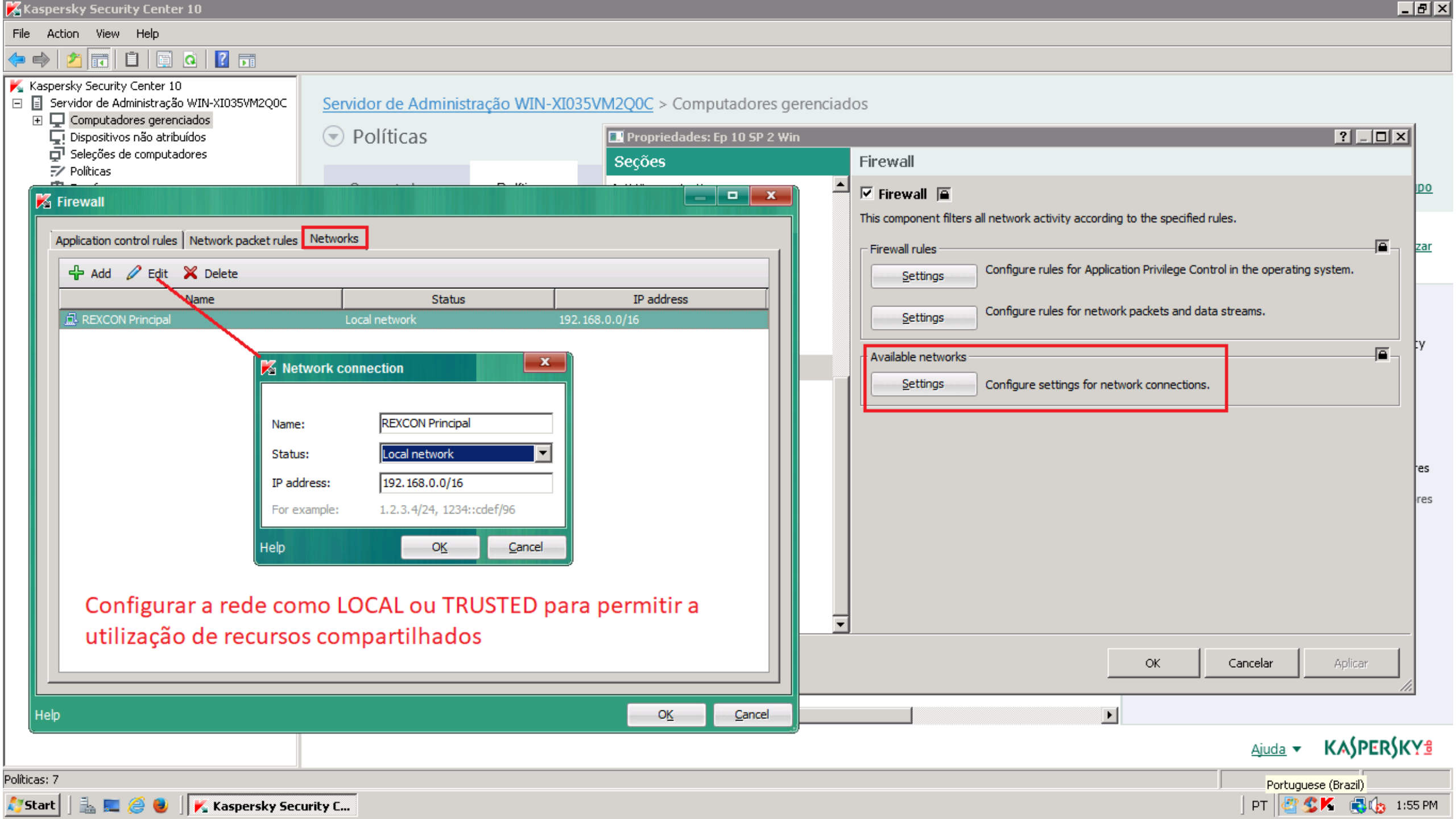
Cancelar

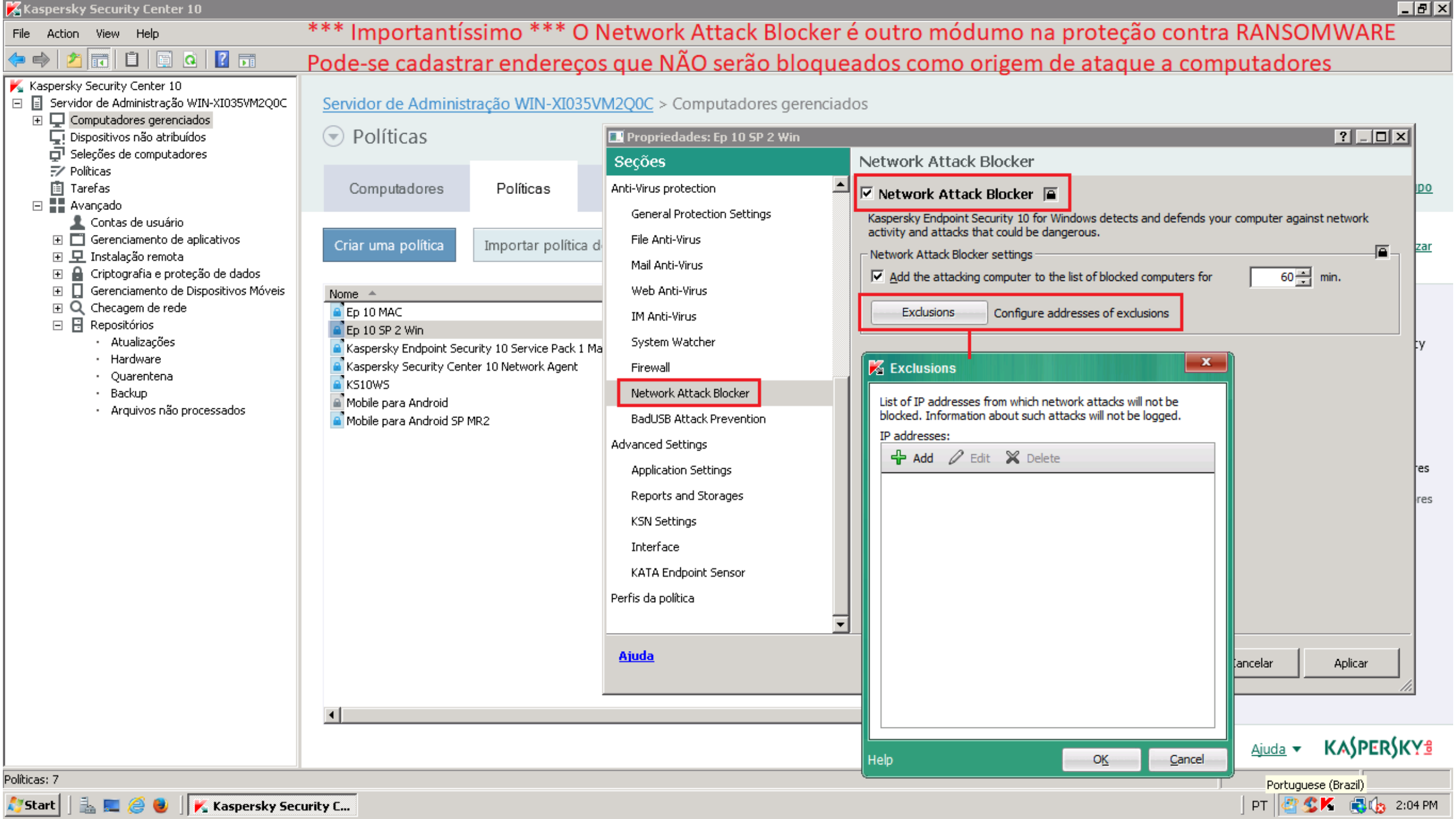
Aplicar

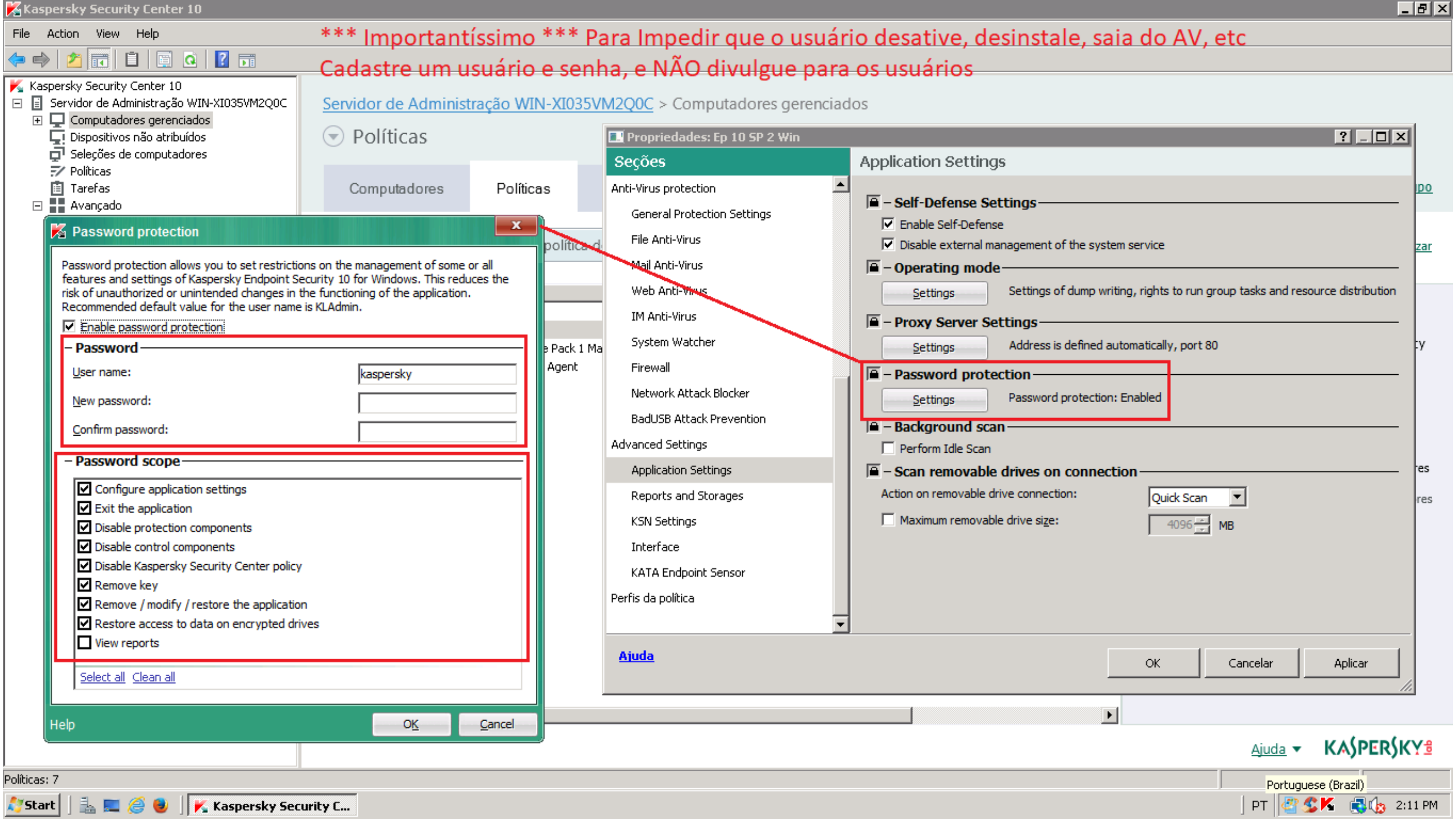
Ajuda

KASPERSKY









Boas práticas para proteção de endpoints

Tarefas de Atualização / Varredura / Inventário

Para Tarefas de Atualização de Base de Dados:

- Até 10.000 o KSC deve buscar de um em uma hora, e entregar aos Endpoints quando encontrar atualizações
- A partir de 10.000 o KSC deve buscar de um em uma hora, e entregar aos Endpoints de seis em seis horas, ou uma vez ao dia



- Kaspersky Security Center 10
 - Servidor de Administração WIN-XI035VM2Q0C
 - Computadores gerenciados
 - Dispositivos não atribuídos
 - Seleções de computadores
 - Políticas
 - Tarefas
 - Avançado
 - Contas de usuário
 - Gerenciamento de aplicativos
 - Instalação remota
 - Criptografia e proteção de dados
 - Gerenciamento de Dispositivos Móveis
 - Checagem de rede
 - Repositórios**
 - Atualizações**
 - Hardware
 - Quarentena
 - Backup
 - Arquivos não processados

Aqui vemos a configuração do repositório de atualizações do KSC; O KSC busca dos servidores da Kaspersky Lab, para depois entregar aos Endpoints (por outra tarefa de atualização)

[Servidor de Administração WIN-XI035VM2Q0C](#) > [Avançado](#) > [Repositórios](#) > Atualizações

Atualizações

Atualizações do banco de dados e módulos de software.

Baixar atualizações

Relatório de uso do banco de dados

Ações adicionais ▼

Modificar configurações de atualização do repositório

Configurar a atualização em estações de trabalho

[Atualizar](#)

Versão de banco de dados:

- Os bancos de dados estão atualizados: 2
- Atualizado nas últimas 24 horas: 0
- Atualizado nos últimos 3 dias: 0
- Atualizado durante os últimos 7 dias: 0
- Atualizado há mais de uma semana: 0

[Adicionar/Remover colunas](#)

Nome	Descrição	Criado ▲	Recebido	Tamanho	
• Rootkit scan databases	Data for the rootkit detection module	7/10/2017 1:28:00 AM	7/3/2017 9:02:12 PM	2569 KB	
• Autorun objects scanner	Updates for autorun objects scanner that uses Anti-Root...	7/10/2017 1:29:00 AM	7/4/2017 6:00:08 AM	3399 KB	
• Anti-Banner databases	URL masks for the Anti-Banner component (for version 6...	8/21/2017 4:49:00 AM	8/21/2017 6:04:19 AM	213 KB	
• Startup objects scan and advanced disinfect...	Updates required for startup objects scan and advanced ...	8/21/2017 6:18:00 AM	7/3/2017 9:22:25 PM	399 KB	
• Firewall databases	Description of typical network attacks	8/21/2017 7:37:00 AM	8/21/2017 9:03:13 AM	1179 KB	
• Security Analyzer	AVZ utility databases	8/29/2017 5:08:00 AM	8/29/2017 1:17:53 PM	266 KB	
• Vulnerability Scan	Updates for Vulnerability Scan task of Kaspersky Security...	9/7/2017 9:44:00 AM	9/7/2017 10:11:33 AM	4827 KB	
• Kaspersky Security Center patches	Kaspersky Security Center patches	9/7/2017 10:46:00 AM	8/14/2017 6:00:44 AM	41599 KB	
• Proactive Defense databases	Descriptions of dangerous and suspicious activity types	9/8/2017 4:46:00 AM	9/8/2017 6:13:01 AM	280 KB	
• Web Control databases	Databases for streamlined scanning (for versions 6.0 MP...	9/8/2017 5:30:00 AM	9/8/2017 7:11:04 AM	3 KB	
• Databases of phishing URLs	Updates for databases of phishing URLs	9/8/2017 7:58:00 AM	9/8/2017 10:07:11 AM	1877 KB	
• System Watcher	Updates for System Watcher	9/8/2017 9:32:00 AM	9/8/2017 12:59:23 PM	11927 KB	
• Proactive Defense databases	Data for the heuristic analyzer	9/8/2017 10:04:00 AM	9/8/2017 1:59:24 PM	37157 KB	
• Anti-virus databases	Description of viruses and other dangerous programs (for...	9/8/2017 10:04:00 AM	9/8/2017 1:59:25 PM	317488 KB	
• KSN service	Updates for KSN	9/8/2017 10:06:00 AM	9/8/2017 11:59:52 AM	1658 KB	
• Urgent Detection System	Updates for Urgent Detection System	9/8/2017 10:06:00 AM	5/26/2017 4:13:16 AM	438 KB	
• Databases of malicious and phishing URLs	List of malicious and phishing URLs	9/8/2017 10:11:00 AM	9/8/2017 12:59:23 PM	1239 KB	

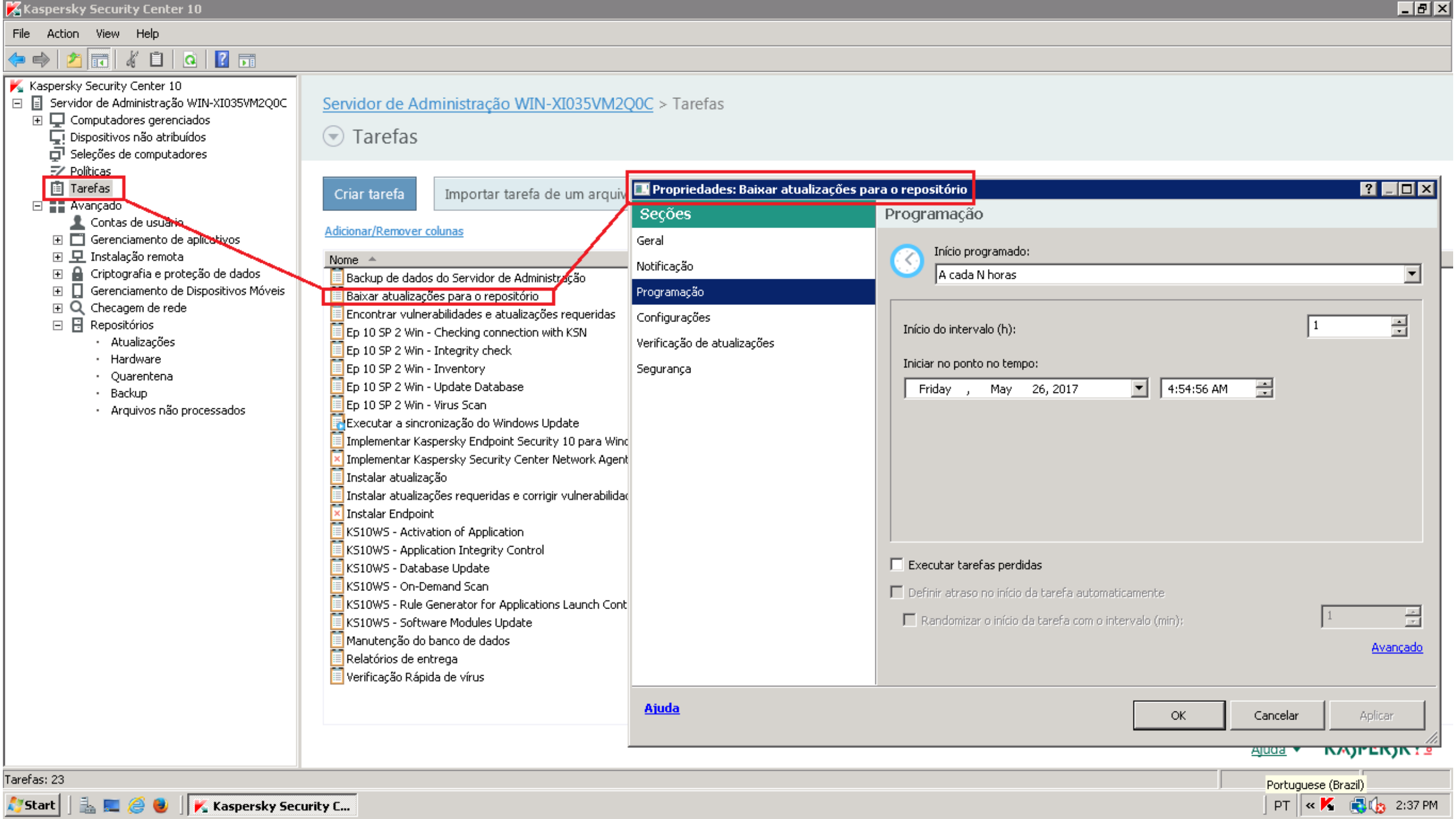
[Ajuda](#) ▼ **KASPERSKY**

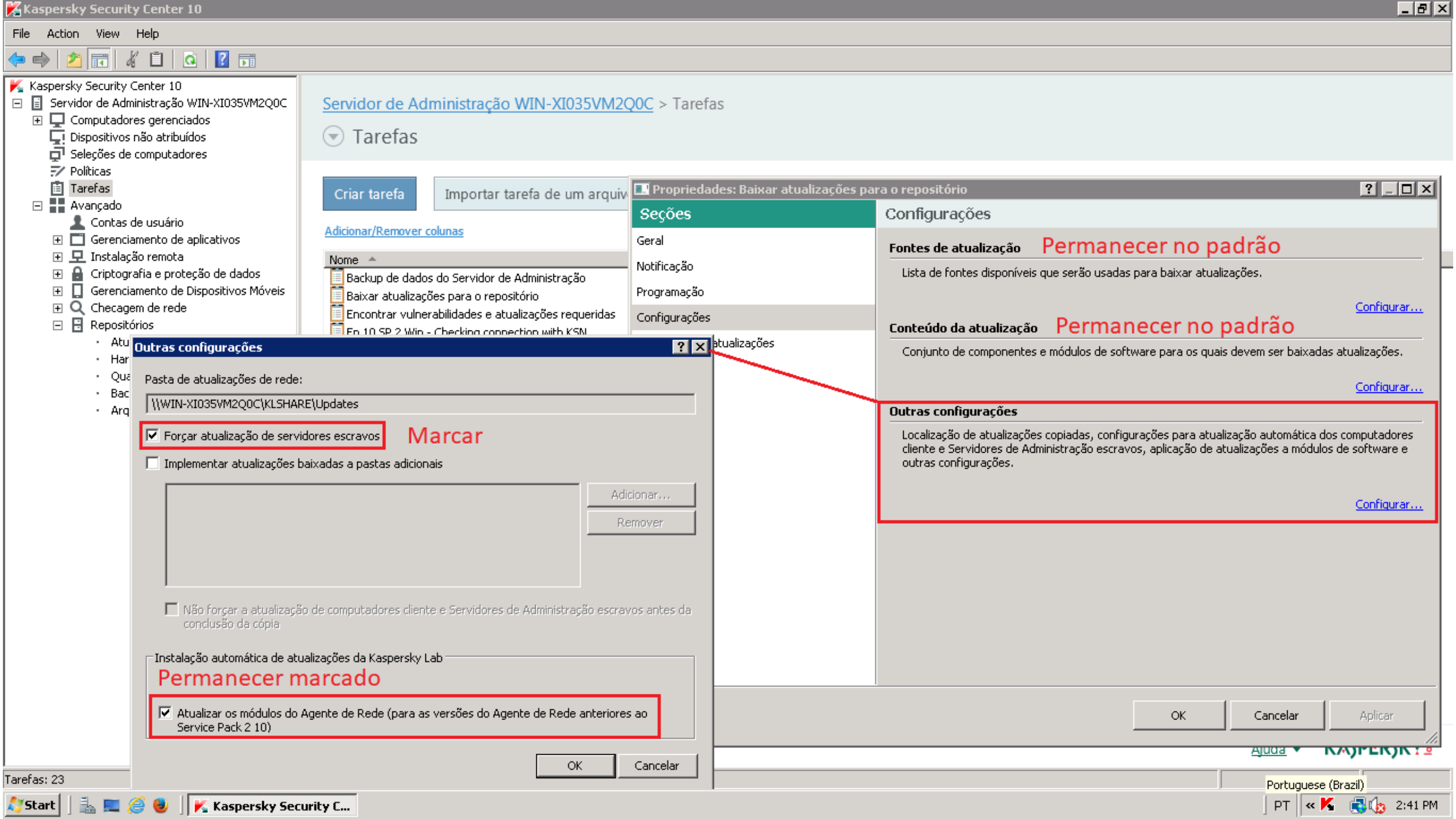
Atualizações: 20

Portuguese (Brazil)

PT

2:29 PM





File

Action

View

Help

←

→

Kaspersky Security Center 10

Servidor de Administração WIN-XI035VM2Q0C

Computadores gerenciados

Dispositivos não atribuídos

Seleções de computadores

Políticas

Tarefas

Avançado

Contas de usuário

Gerenciamento de aplicativos

Instalação remota

Criptografia e proteção de dados

Gerenciamento de Dispositivos Móveis

Checagem de rede

Repositórios

Atualizações

Hardware

Quarentena

Backup

Arquivos não processados

Aqui vemos a tarefa de atualização dos Endpoints

A base de dados do KSC, atualizada previamente, é replicada nos Endpoints

Servidor de Administração WIN-XI035VM2Q0C > Computadores gerenciados

Tarefas de grupo

Computadores

Políticas

Tarefas

Criar tarefa

Importar tarefa de um arquivo

Nome

Verificação Rápida de vírus

KS10WS - Software Modules Update

KS10WS - Rule Generator for Applications Launch Cont

KS10WS - On-Demand Scan

KS10WS - Database Update

KS10WS - Application Integrity Control

KS10WS - Activation of Application

Instalar atualizações requeridas e corrigir vulnerabilidac

Instalar atualização

Ep 10 SP 2 Win - Virus Scan

Ep 10 SP 2 Win - Update Database

Ep 10 SP 2 Win - Inventory

Seções

Geral

Notificação

Programação

Properties

Conta

Exclusões do escopo da tarefa

Programação

Manter este padrão

Início programado:

Quando novas atualizações são baixadas no repositório

Executar tarefas perdidas

Definir atraso no início da tarefa automaticamente

Randomizar o início da tarefa com o intervalo (min):

1

OK

Cancelar

Aplicar

Avançado

Ativar computador antes do início da tarefa pela função Wake On LAN (min.):

5

Desligar computador depois de concluir a tarefa

Parar se a tarefa levar mais que (min):

120

OK

Cancelar

Tarefas: 15

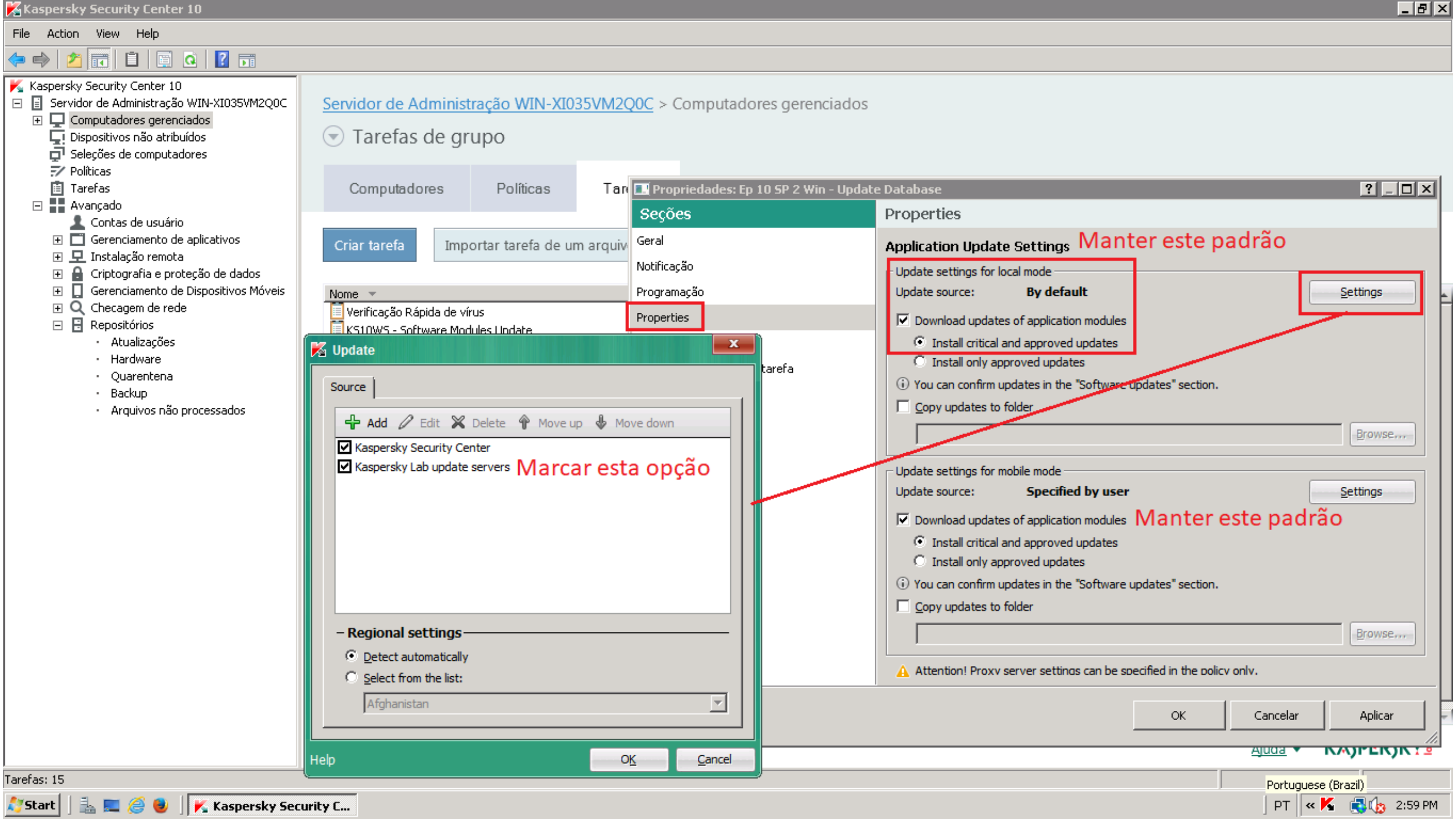
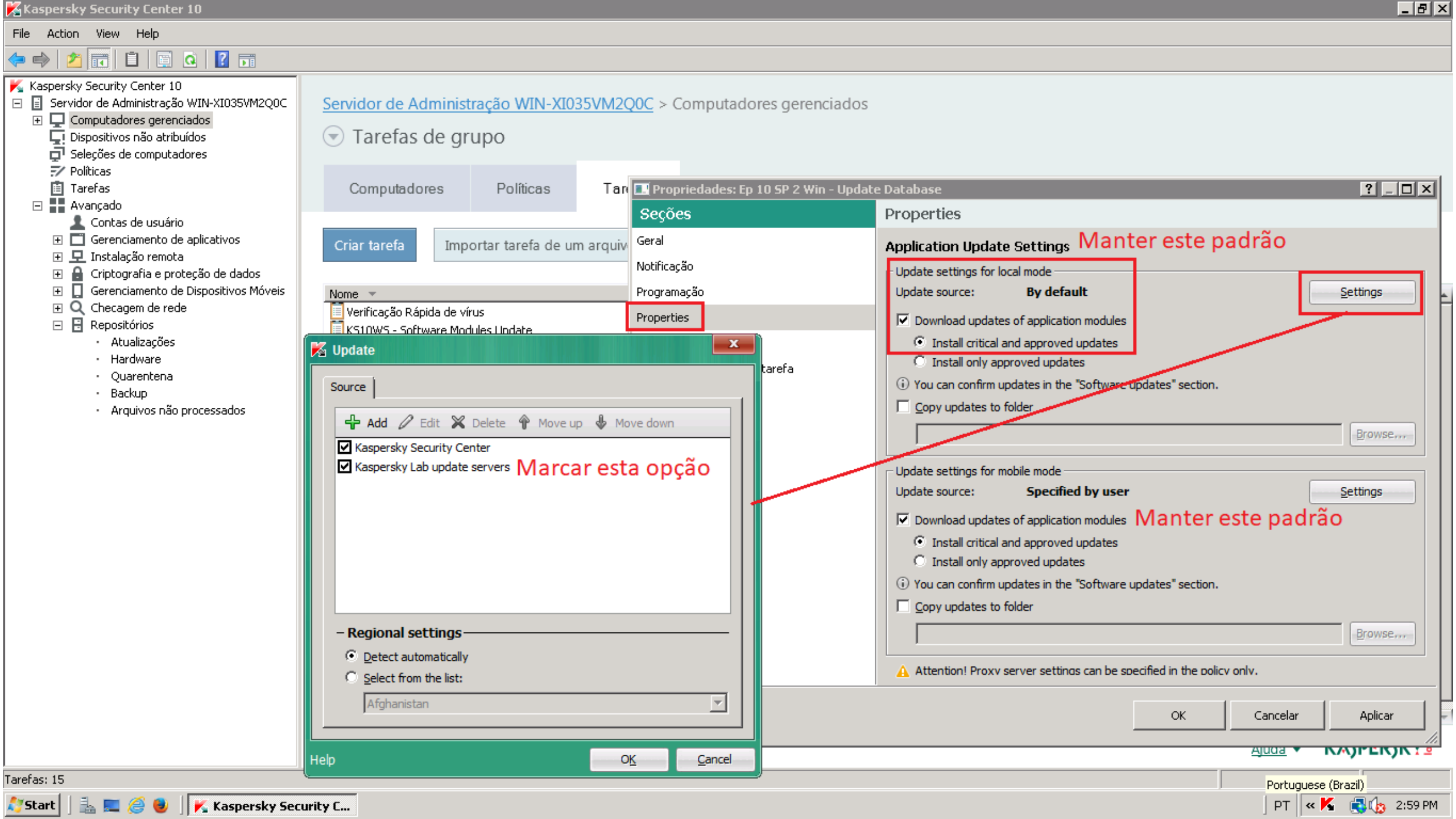
Start

Kaspersky Security C...

Portuguese (Brazil)

PT

2:50 PM



File

Action

View

Help

Kaspersky Security Center 10

Servidor de Administração WIN-XI035VM2Q0C

Computadores gerenciados

Dispositivos não atribuídos

Seleções de computadores

Políticas

Tarefas

Avançado

Contas de usuário

Gerenciamento de aplicativos

Instalação remota

Criptografia e proteção de dados

Gerenciamento de Dispositivos Móveis

Checkagem de rede

Repositórios

Atualizações

Hardware

Quarentena

Backup

Arquivos não processados

Programe a tarefa de Varredura / Virus Scan , semanalmente em um horário próximo ao almoço

Servidor de Administração WIN-XI035VM2Q0C > Computadores gerenciados

Tarefas de grupo

Computadores

Políticas

Tarefas

Criar tarefa

Importar tarefa de um arquivo

Nome

Verificação Rápida de vírus

KS10WS - Software Modules Update

KS10WS - Rule Generator for Applications Launch Cont

KS10WS - On-Demand Scan

KS10WS - Database Update

KS10WS - Application Integrity Control

KS10WS - Activation of Application

Instalar atualizações requeridas e corrigir vulnerabilidac

Instalar atualização

Ep 10 SP 2 Win - Virus Scan

Ep 10 SP 2 Win - Update Database

Ep 10 SP 2 Win - Inventory

Ep 10 SP 2 Win - Integrity check

Ep 10 SP 2 Win - Checking connection with KSN

Encontrar vulnerabilidades e atualizações requeridas

Seções

Geral

Notificação

Programação

Properties

Conta

Exclusões do escopo da tarefa

Programação

Início programado:

Semanalmente

Dia da semana:

Monday

Hora de início:

11:59:00 AM

☒ Executar tarefas perdidas

☒ Definir atraso no início da tarefa automaticamente

☐ Randomizar o início da tarefa com o intervalo (min):

1

Avançado

Ajuda

OK

Cancelar

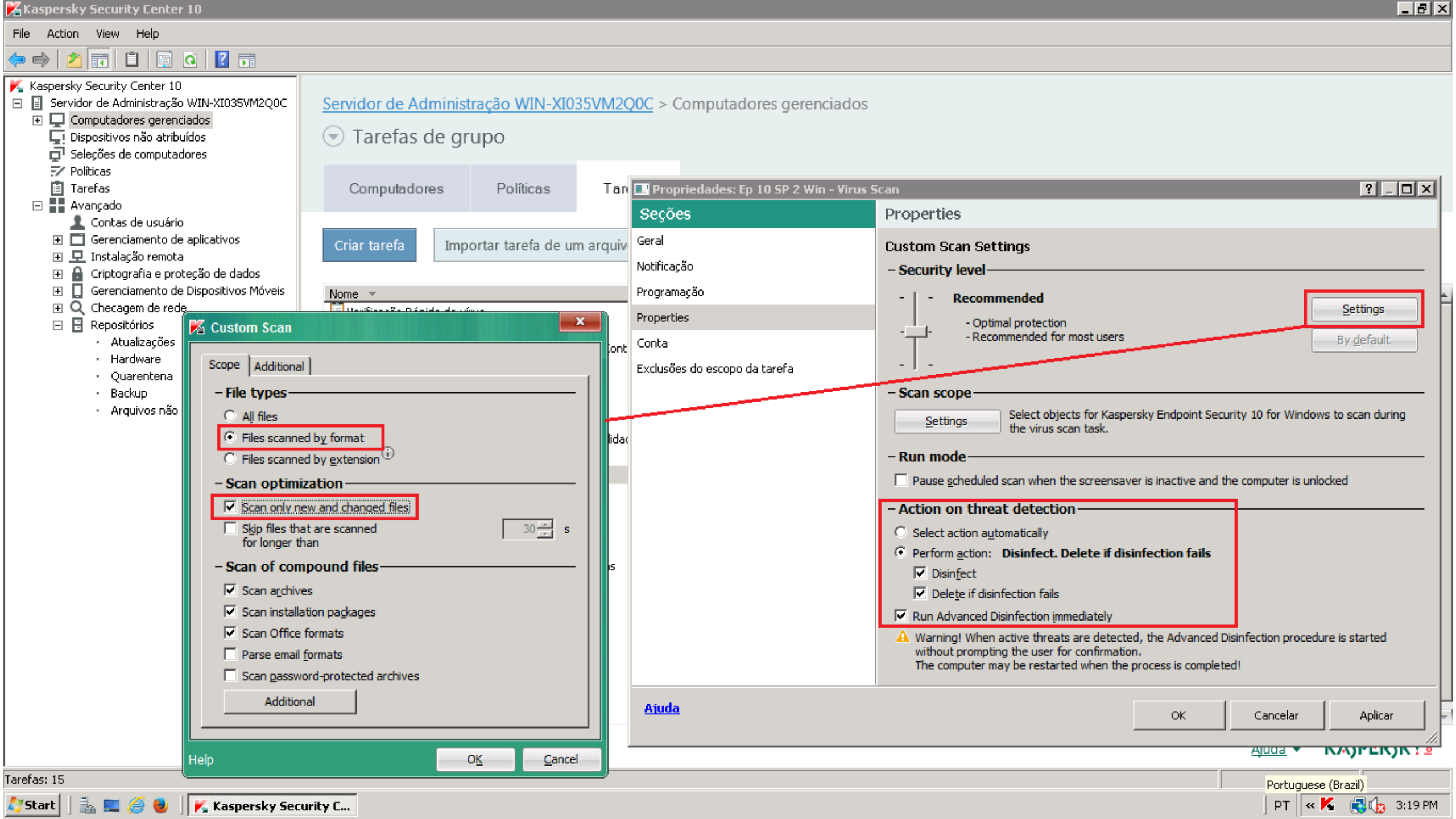
Aplicar

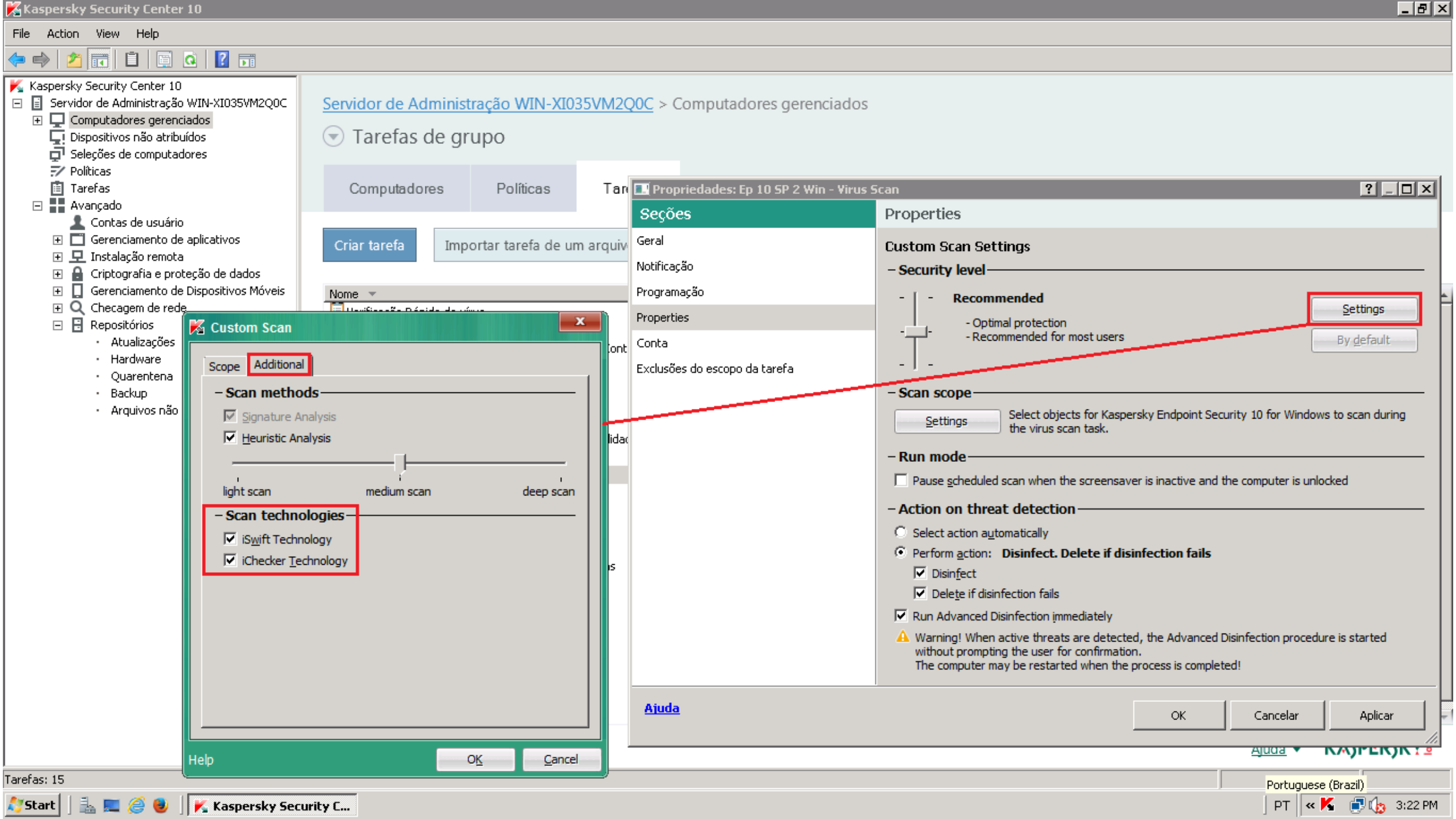
Tarefas: 15

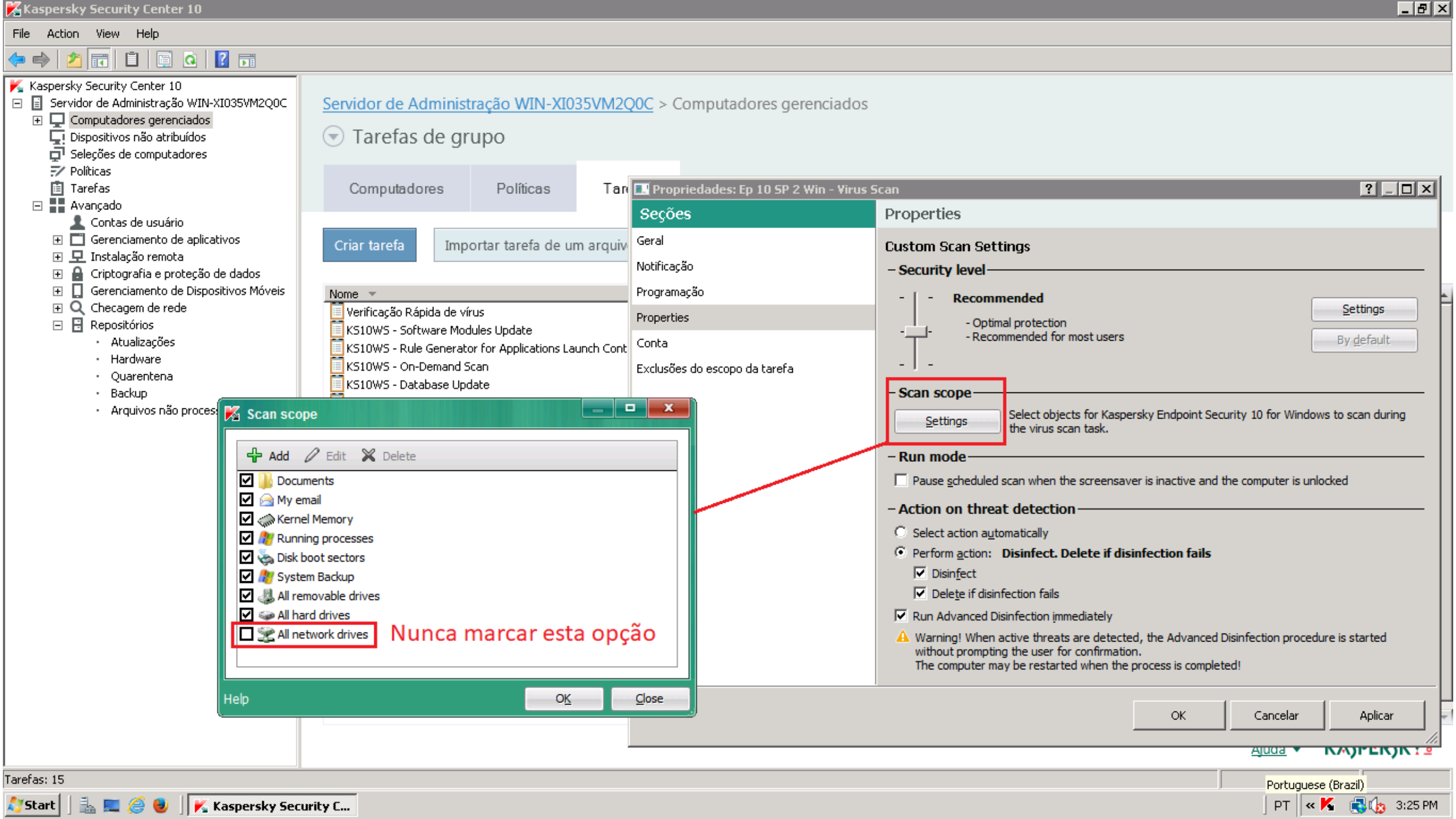
Portuguese (Brazil)

PT

3:14 PM







Servidor de Administração WIN-XI035VM2Q0C > Computadores gerenciados

Tarefas de grupo

Computadores

Políticas

Criar tarefa

Importar tarefa de um arquivo

Nome

- Verificação Rápida de vírus
- KS10WS - Software Modules Update
- KS10WS - Rule Generator for Applications Launch Cont
- KS10WS - On-Demand Scan
- KS10WS - Database Update

Propriedades: Ep 10 SP 2 Win - Virus Scan

Seções

Geral

Notificação

Programação

Properties

Conta

Exclusões do escopo da tarefa

Properties

Custom Scan Settings

Security level

Recommended
- Optimal protection
- Recommended for most users

Settings

By default

Scan scope

Settings

Select objects for Kaspersky Endpoint Security 10 for Windows to scan during the virus scan task.

Run mode

☐ Pause scheduled scan when the screensaver is inactive and the computer is unlocked

Action on threat detection

- ☐ Select action automatically
- ☒ Perform action: **Disinfect. Delete if disinfection fails**
 - ☒ Disinfect
 - ☒ Delete if disinfection fails
- ☒ Run Advanced Disinfection immediately

Warning! When active threats are detected, the Advanced Disinfection procedure is started without prompting the user for confirmation. The computer may be restarted when the process is completed!

OK

Cancelar

Aplicar

Scan scope

+ Add Edit Delete

- ☒ Documents
- ☒ My email
- ☒ Kernel Memory
- ☒ Running processes
- ☒ Disk boot sectors
- ☒ System Backup
- ☒ All removable drives
- ☒ All hard drives
- ☐ All network drives

Nunca marcar esta opção

Help

OK

Close

Tarefas: 15

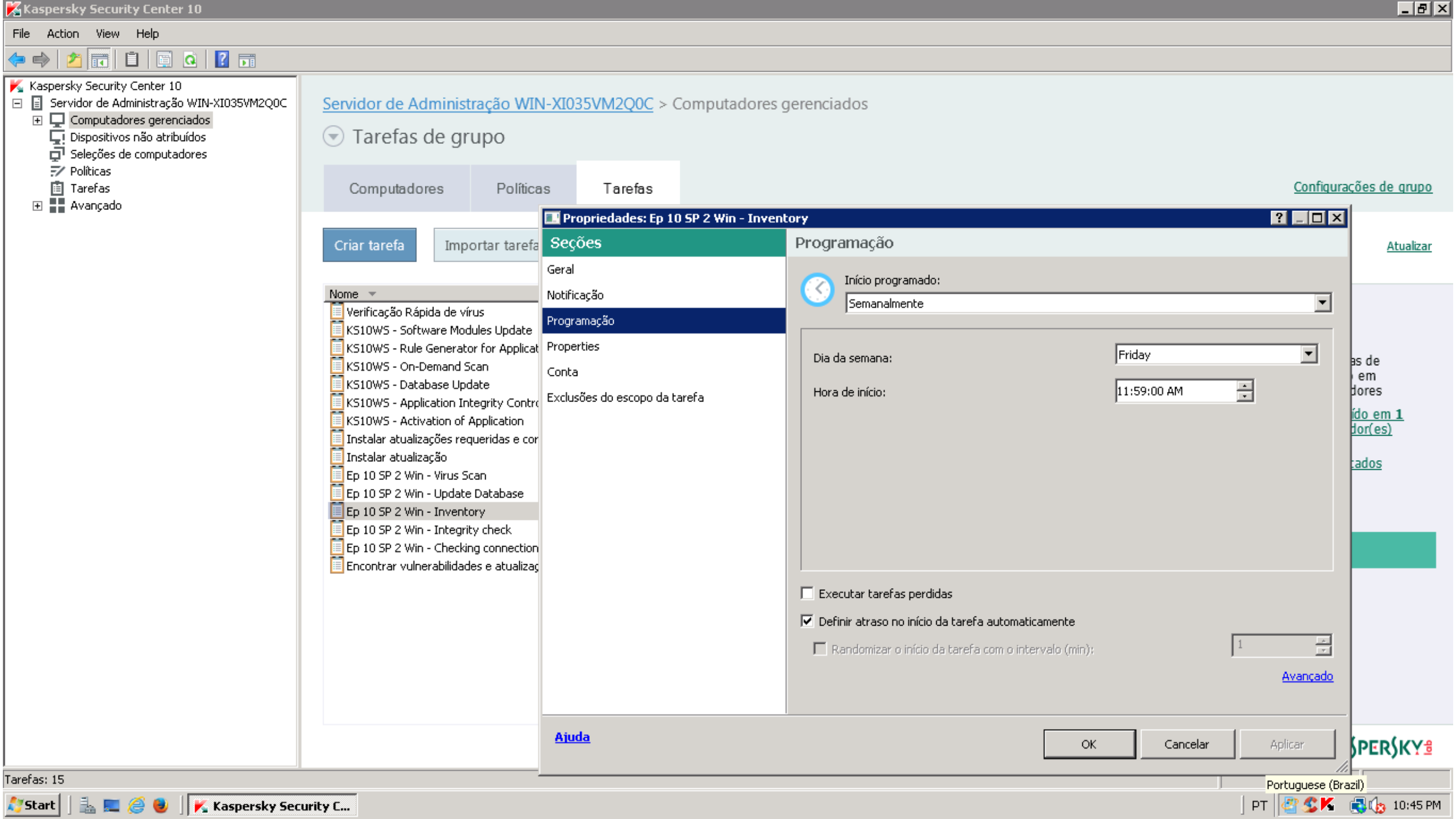
Start

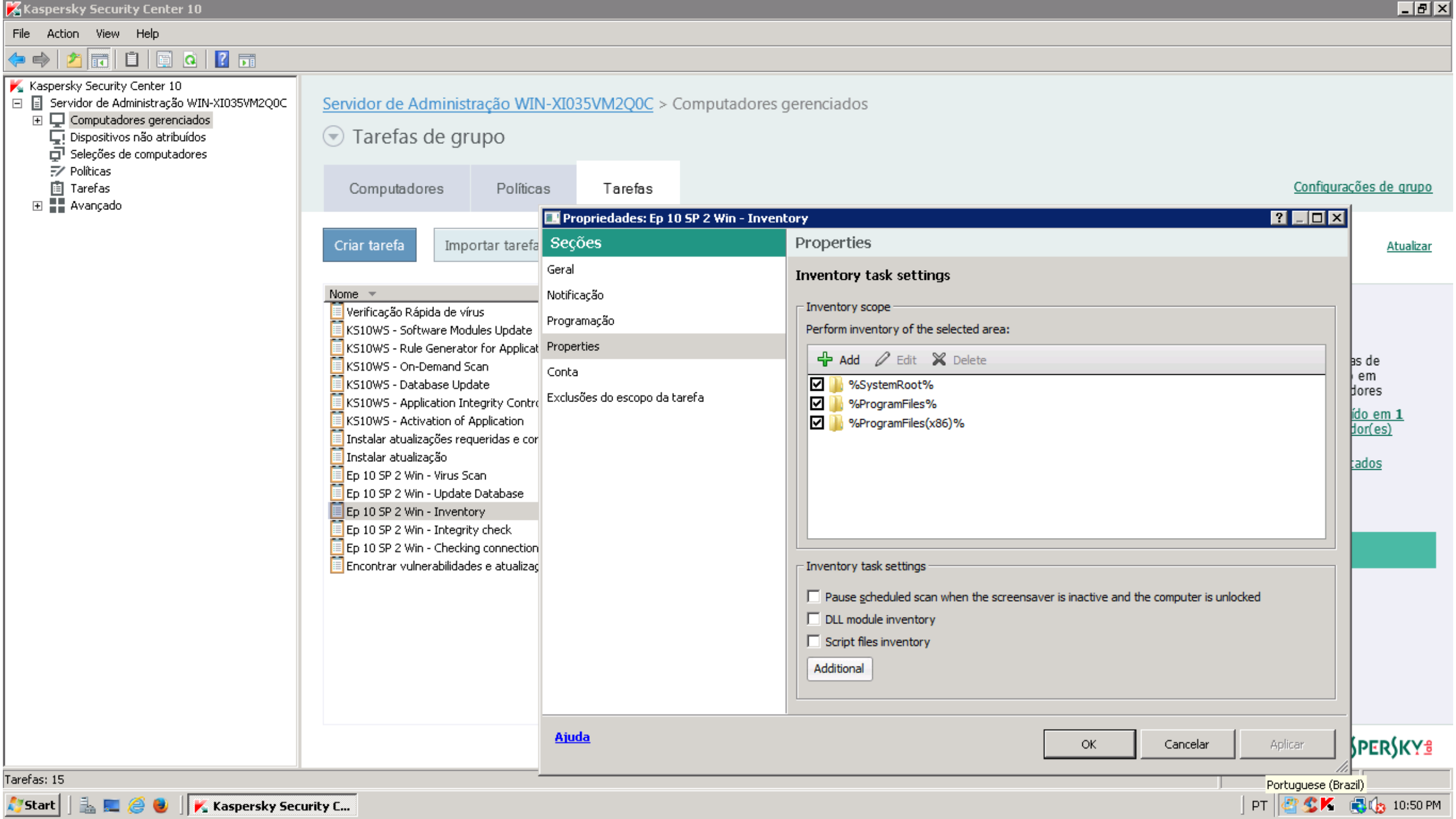
Kaspersky Security C...

Portuguese (Brazil)

PT

3:25 PM





Boas práticas para proteção de endpoints

Atenção ao painel do servidor

Atender as indicações em vermelho:

- Atualizações de produtos que necessitam de aprovação
- Atualizações do KSC
- Vulnerabilidades encontradas



Kaspersky Security Center 10

Servidor de Administração WIN-XI035VM2Q0C

- Computadores gerenciados
- Dispositivos não atribuídos
- Seleções de computadores
- Políticas
- Tarefas
- Avançado

Servidor de Administração WIN-XI035VM2Q0C (WIN-XI035VM2Q0C\Administrator)

Monitorar

Estatísticas

Relatórios

Eventos

[Configurações do servidor](#)

▼ Implementação

Versões mais recentes de aplicativos da Kaspersky Lab.

- [Instalar o Kaspersky Anti-Virus](#)
- [Gerenciar chaves](#)
- [Relatório de implementação da proteção](#)

▼ Gerenciamento de computador

- [Visualizar estrutura de computadores gerenciados](#)
- [Configurar a colocação automática de computadores em grupos de administração](#)
- [Ver dispositivos não atribuídos](#)

▼ Proteção do computador e verificação de vírus

Foi detectada uma vulnerabilidade de software em computadores cliente.

- [Editar política de proteção para estações de trabalho](#)
- [Editar tarefa de verificação de vírus para estações de trabalho](#)
- [Gerenciar aplicativos em computadores cliente](#)

▼ Atualizar

Atualizações de produtos da Kaspersky Lab não aprovadas

- [Ir para a pasta de Atualizações](#)
- [Reportar sobre os bancos de dados de antivírus em uso](#)

▼ Monitorar

Eventos críticos registrados no Servidor de Administração.
Eventos de erro registrados no Servidor de Administração.

- [Visualizar status da proteção](#)
- [Ver pedidos de usuário](#)
- [Editar configurações de notificação](#)

▼ Servidor de Administração

A atualização "patch_10_3_407_server_SF1.exe" está disponível para o Servidor de Administração e requer uma aprovação de instalação do administrador.

- [Propriedades do Servidor de Administração](#)
- [Ver informações sobre a chave do Servidor de Administração](#)
- [Configurar funcionalidade exibida na interface do usuário](#)

[Ajuda](#)

Portuguese (Brazil)

PT

10:43 PM

A close-up, front-facing view of a red Ferrari Formula 1 car. The car's nose features the Kaspersky Lab logo, which includes a yellow sunburst emblem above the text "KASPERSKY lab". The front wings and tires are visible, with "P ZERO" written on the left tire. The background is a blurred red wall.

Rexcon Consultoria
www.rexcon.com.br

REXCON parceiro Kaspersky Lab

Leandro Ferreira (21) 3046-5880 / 98088-5538 Tim / 96702-6698 Vivo
Leandro.ferreira@rexcon.com.br