

Arquitetura de Computadores e Sistemas Operacionais

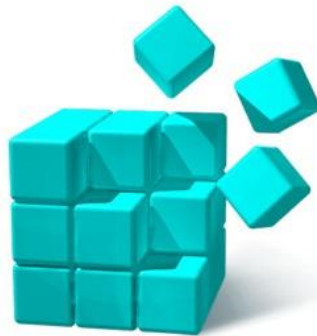
FABIANO GISBERT

Etapa 06

Operações Windows

Registro do Windows

Presente desde o Microsoft Windows 3.1, o "Registro do Sistema" ainda é visto como uma funcionalidade bastante misteriosa (e até perigosa) para a maioria das pessoas. Poucos sabem o que ele é e muito menos qual a sua real função, e uma simples alteração mal planejada pode comprometer todo o sistema.



Registro do Windows

O registro é um banco de dados do sistema que armazena todas as configurações dos aplicativos e drivers de dispositivos que instalamos.

Sempre que trocamos uma configuração de vídeo, instalamos um aplicativo ou trocamos o nosso navegador padrão de internet, efetuamos modificações nesse banco de dados para que o Windows as salve e saiba como queremos que ele funcione.

O registro fica armazenado na pasta principal do Windows:

PATH: \\Windows\\system32\\config

Registro do Windows

Para acessar as chaves de registro do Windows usamos o Editor de Registro do Windows (digitando "regedit" no campo de busca do Menu Iniciar)



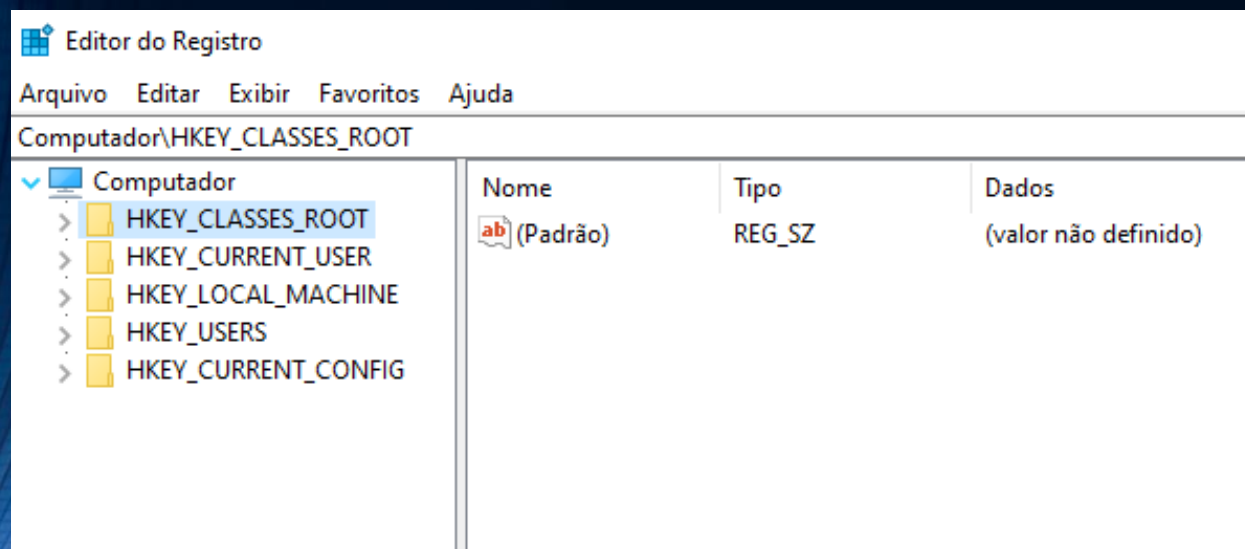
DEFAULT	27/03/2012 17:18	Arquivo	256 KB
default.LOG1	27/03/2012 17:18	Arquivo LOG1	165 KB
default.LOG2	14/02/2012 14:40	Arquivo LOG2	0 KB
SAM	27/03/2012 17:02	Arquivo	256 KB
SAM.LOG1	27/03/2012 17:02	Arquivo LOG1	25 KB
SAM.LOG2	14/02/2012 14:40	Arquivo LOG2	0 KB
SECURITY	27/03/2012 17:17	Arquivo	256 KB
SECURITY.LOG1	27/03/2012 17:17	Arquivo LOG1	21 KB
SECURITY.LOG2	14/02/2012 14:40	Arquivo LOG2	0 KB
SOFTWARE	27/03/2012 17:22	Arquivo	19.200 KB
SOFTWARE.LOG1	27/03/2012 17:22	Arquivo LOG1	256 KB
SOFTWARE.LOG2	14/02/2012 14:40	Arquivo LOG2	0 KB
SYSTEM	27/03/2012 17:17	Arquivo	14.336 KB

Quando abrimos o Editor de Registro do estamos na verdade abrindo uma interface que reúne cinco arquivos localizados na pasta , que juntos armazenam todas as configurações do sistema:

Default, SAM, Security. Software e System. Todos protegidos pelo sistema e não liberados para alterações diretamente a eles.

Registro do Windows

Editor de Registros



Todas as configurações do Windows poderão ser editadas através de chaves, também conhecidas como Hives, que são a unidade padrão de informação do registro.

Registro do Windows

Chave de Registros

Por padrão, o Windows utiliza de 5 chaves principais que se subdividem em várias outras de uma forma semelhante às pastas que estamos acostumados no Windows Explorer, cada uma referente à configuração de uma parte do sistema acompanhado de uma chave. Cada uma dessas sub-chaves possui um valor, e a mudança aqui é o que efetivamente realiza uma alteração. No Windows 7 temos cinco chaves principais:

HKEY_CLASSES_ROOT (HKCR): presente nas versões atuais do Windows apenas para manter a compatibilidade com programas mais antigos, da geração 16 bits (dos tempos do DOS), HKEY_LOCAL_MACHINE\SOFTWARE\Classes.

HKEY_CURRENT_USER (HKCU): é uma sub-chave de HKEY_USERS, contendo todas as configurações do usuário logado no sistema.

HKEY_LOCAL_MACHINE (HKLM): chave mais importante do registro, guarda todas as informações que o sistema operacional precisa para funcionar e de sua interface gráfica. Utiliza o arquivo SYSTEM para armazenar essas configurações.

HKEY_USERS (HKU): guarda as configurações de aparência do Windows e as configurações efetuadas pelos usuários, como papel de parede, protetor de tela, temas e outros, utilizando o arquivo USER para armazenar essas informações.

HKEY_CURRENT_CONFIG (HKCC): salva os perfis de hardware utilizados pelo usuário. Como normalmente só é utilizado um perfil, o valor da chave é HKEY_LOCAL_MACHINE\CONFIG.

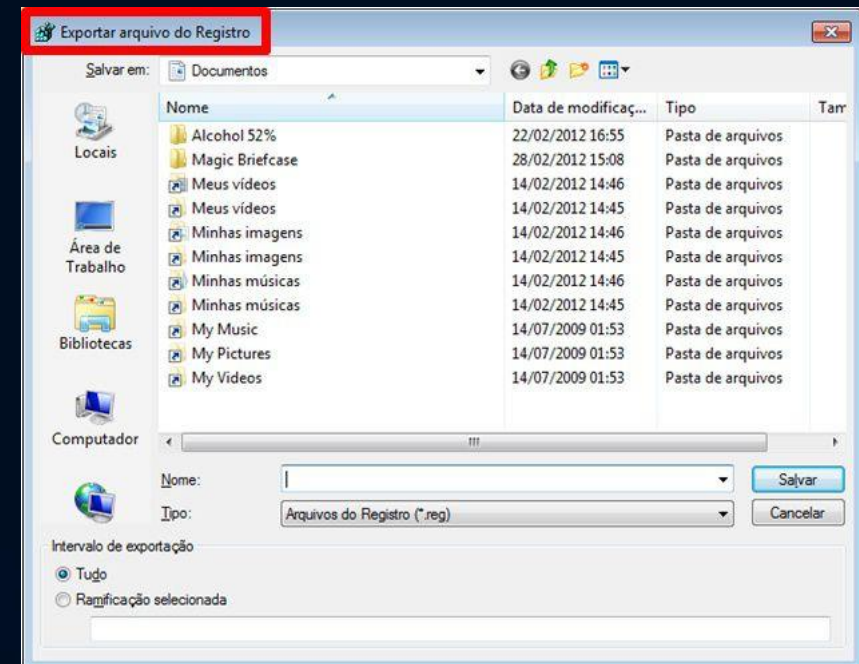
Registro do Windows

Backup de Registros

É possível guardar uma cópia dos arquivos de registros através do Editor de Registro. É um procedimento importante de se realizar antes de fazer qualquer operação em registro.

Procedimento: Ir em "Arquivo" e depois em "Exportar" para salvar uma cópia do estado atual do registro.

Se precisar futuramente, basta restaurar esse arquivo clicando em "Arquivo" e "Importar"..



Exemplos de Operação de Registro

Remover entradas inválidas da ferramenta Adicionar/remover programas

Ocasionalmente, um programa pode não ser desinstalado completamente e uma referência ao programa pode permanecer na caixa de diálogo programas instalados no momento . Alterar ou remover um programa pode resultar em várias mensagens sobre arquivos que não podem ser localizados, mas são necessárias para concluir a alteração ou desinstalação.

1. Localize a seguinte chave:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall`

2. Localize a chave a ser excluída, localizando o nome da chave criado pelo programa. Se o nome da chave não estiver visível, navegue em cada chave e observe o valor de DisplayName. Esta é a cadeia de caracteres exibível na ferramenta Adicionar/remover programas

3. Exclua a chave do registro selecionada e seus valores. Não exclua toda a chave de desinstalação.

Exemplos de Operação de Registro

Desinstalar Driver Completamente do Windows

Por alguma falha no processo de desinstalação de um driver de um dispositivo, ele não é retirado do registro do Windows, e com isso um novo driver não pode ser instalado. Para corrigir o problema, basta retirar a entrada deste driver, localizando-a no registro pelo nome que consta no Gerenciador de Dispositivos.

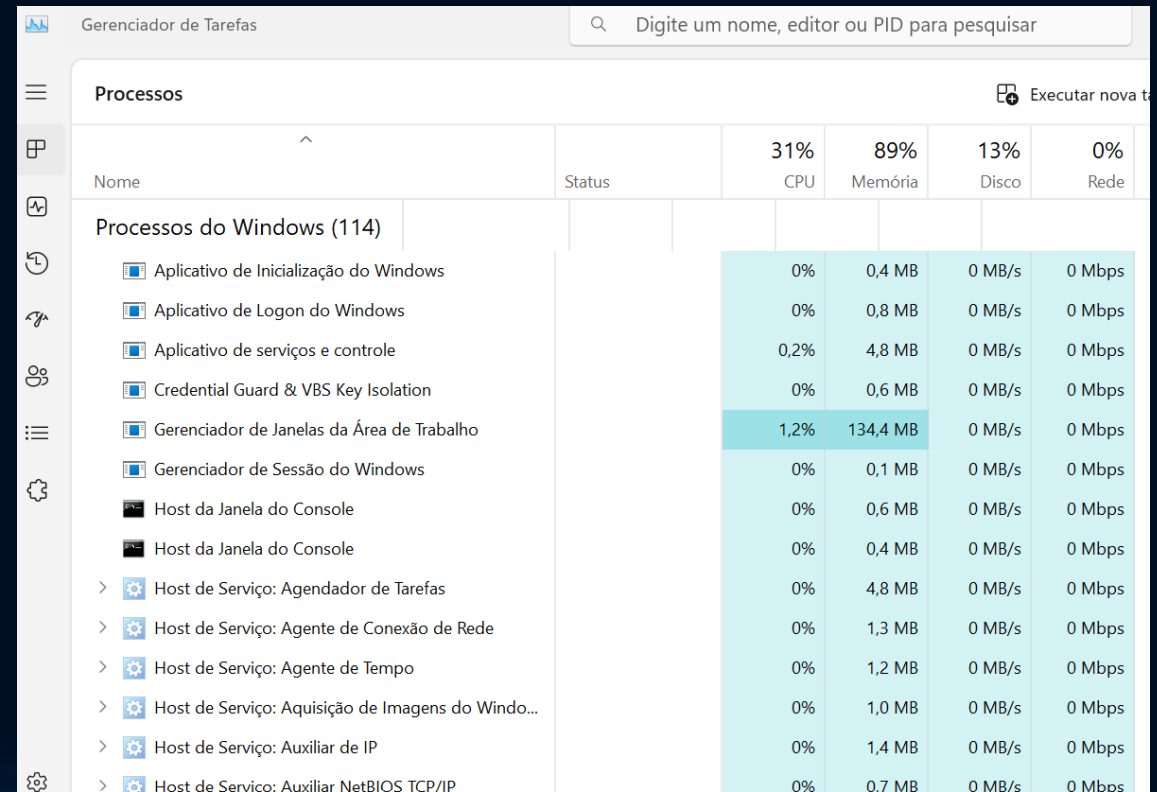
1. Uma vez dentro do Editor de registro do Windows, devemos localizar a seguinte chave:
`HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services`
2. Localizamos o objeto (driver ou serviço), selecionamos e apagamos.

Outras ferramentas de Diagnóstico

Gerenciador de Tarefas

O Gerenciador de Tarefas (Windows) permite que um usuário visualize o desempenho do sistema.

Ele contém exibições que mostram o desempenho geral e o desempenho por Pacote/Processo. Ele também mostra os Usuários e Serviços atualmente conectados do computador. Eles podem ser controlados por um administrador..



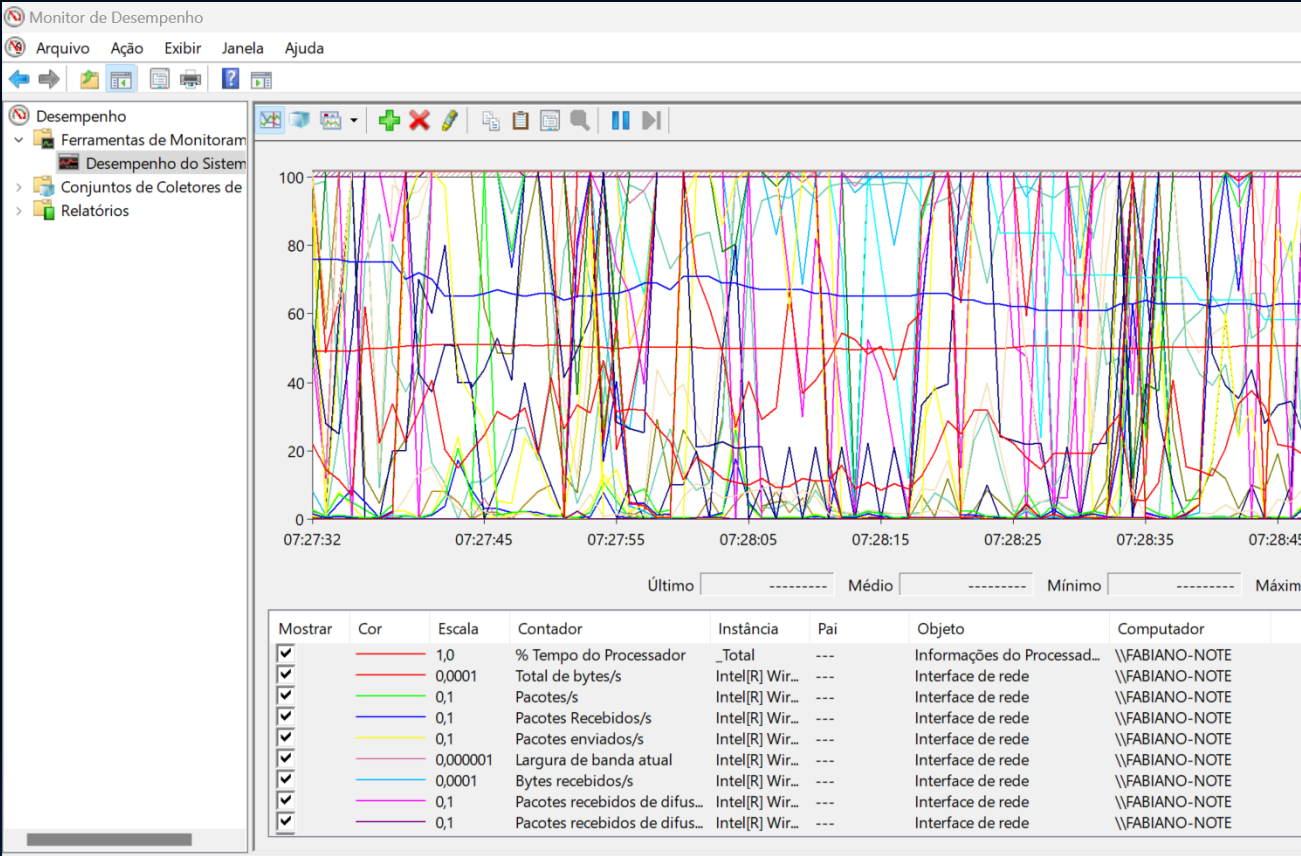
The screenshot shows the Windows Task Manager interface with the 'Processes' tab selected. At the top, there is a search bar with the placeholder text 'Digite um nome, editor ou PID para pesquisar'. Below the search bar, the 'Processos' section displays a table of running processes. The table has columns for 'Nome', 'Status', 'CPU', 'Memória', 'Disco', and 'Rede'. The overall system performance is shown at the top right: CPU 31%, Memória 89%, Disco 13%, and Rede 0%. The table lists 114 Windows processes, with the 'Gerenciador de Janelas da Área de Trabalho' process highlighted in blue, showing 1,2% CPU usage and 134,4 MB of memory.

Nome	Status	31% CPU	89% Memória	13% Disco	0% Rede
Processos do Windows (114)					
Aplicativo de Inicialização do Windows		0%	0,4 MB	0 MB/s	0 Mbps
Aplicativo de Logon do Windows		0%	0,8 MB	0 MB/s	0 Mbps
Aplicativo de serviços e controle		0,2%	4,8 MB	0 MB/s	0 Mbps
Credential Guard & VBS Key Isolation		0%	0,6 MB	0 MB/s	0 Mbps
Gerenciador de Janelas da Área de Trabalho		1,2%	134,4 MB	0 MB/s	0 Mbps
Gerenciador de Sessão do Windows		0%	0,1 MB	0 MB/s	0 Mbps
Host da Janela do Console		0%	0,6 MB	0 MB/s	0 Mbps
Host da Janela do Console		0%	0,4 MB	0 MB/s	0 Mbps
Host de Serviço: Agendador de Tarefas		0%	4,8 MB	0 MB/s	0 Mbps
Host de Serviço: Agente de Conexão de Rede		0%	1,3 MB	0 MB/s	0 Mbps
Host de Serviço: Agente de Tempo		0%	1,2 MB	0 MB/s	0 Mbps
Host de Serviço: Aquisição de Imagens do Windo...		0%	1,0 MB	0 MB/s	0 Mbps
Host de Serviço: Auxiliar de IP		0%	1,4 MB	0 MB/s	0 Mbps
Host de Serviço: Auxiliar NetBIOS TCP/IP		0%	0,7 MB	0 MB/s	0 Mbps

Outras ferramentas de Diganóstico

Monitor de Desempenho

Monitor de Desempenho analisa a utilização de recursos do sistema. Coleta e exibe dados de desempenho em tempo real na forma de contadores. Você pode usar os contadores para recursos de servidor, como uso de processador e de memória.



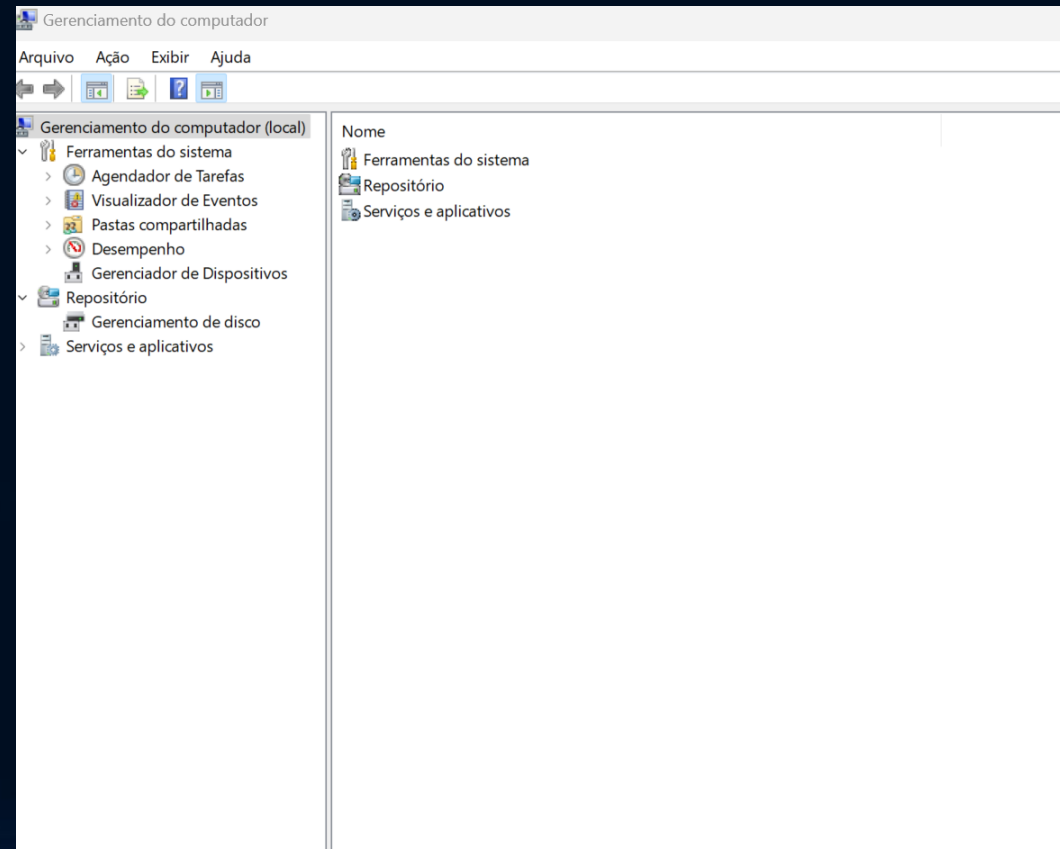
Outras ferramentas de Diagnóstico

Gerenciamento do Computador

Conjunto de Ferramentas para gerenciamento dos recursos do computador onde o Windows está instalado.

Inclui as ferramentas:

- Agendador de Tarefas
- Visualizador de Eventos
- Gerenciador de Dispositivos
- Gerenciador de Discos
- Visualizador de Serviços

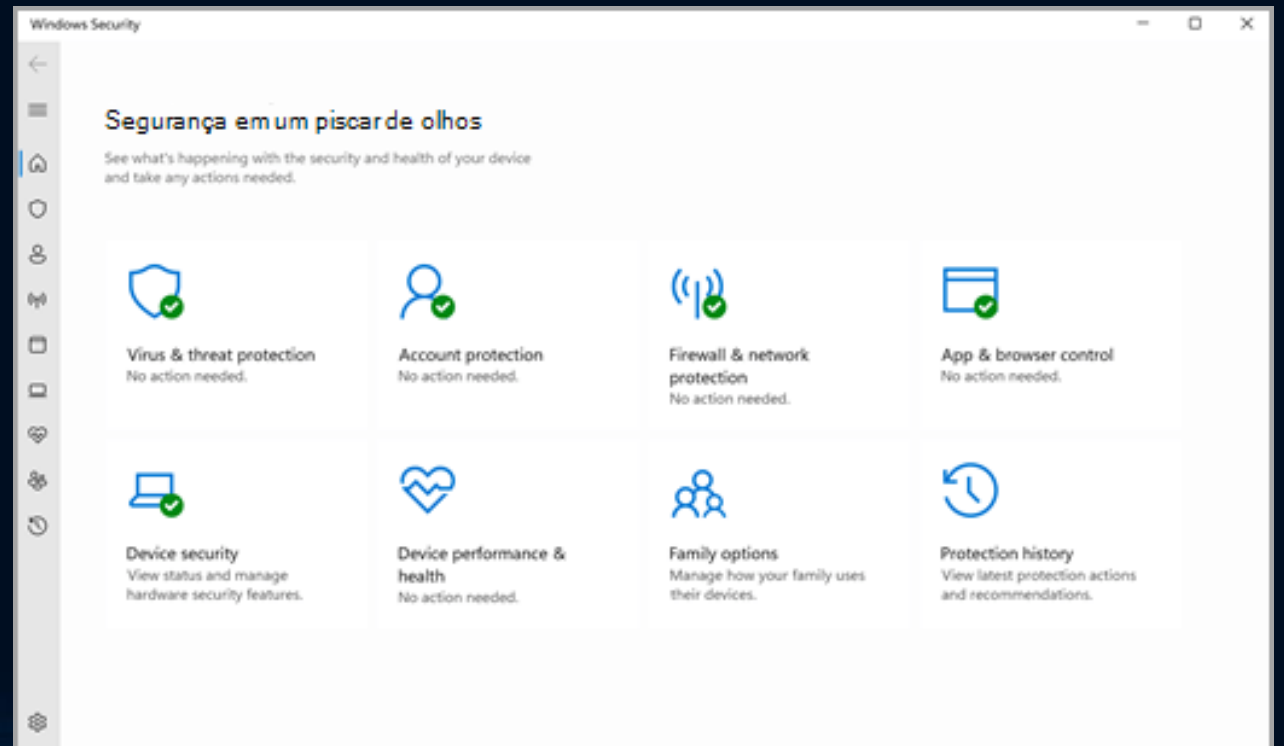


Outras ferramentas de Diagnóstico

Windows Security

O Windows 10 e 11 incluem o Windows Security, que fornece um conjunto de ferramentas de proteção para o sistema operacional. Entre elas incluem:

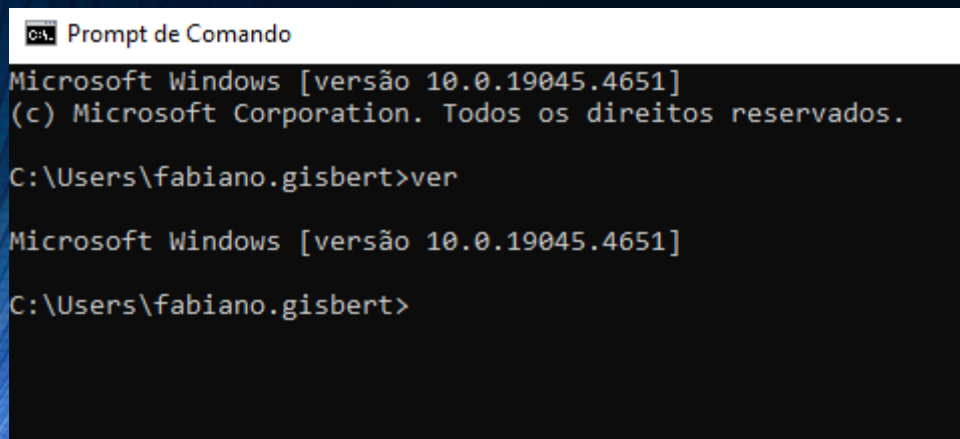
- Proteção contra vírus e ameaças;
- Proteção de contas;
- Firewall e proteção de redes;
- Controle de Aplicativos;
- Proteção do dispositivo.



Outras ferramentas de Diagnóstico

Verificar versão de Kernel

Algumas situações, principalmente de segurança, demandam o conhecimento da versão exata do Kernel do Windows. Para isso basta usar o comando `ver` no Prompt de Comando.

A screenshot of a Windows Command Prompt window. The title bar is white with a black icon and the text 'Prompt de Comando'. The background is black with white text. The text in the window shows the Windows version information: 'Microsoft Windows [versão 10.0.19045.4651]' and '(c) Microsoft Corporation. Todos os direitos reservados.' followed by the command 'C:\Users\fabiano.gisbert>ver' and the output 'Microsoft Windows [versão 10.0.19045.4651]' and 'C:\Users\fabiano.gisbert>'.

```
CA Prompt de Comando
Microsoft Windows [versão 10.0.19045.4651]
(c) Microsoft Corporation. Todos os direitos reservados.

C:\Users\fabiano.gisbert>ver

Microsoft Windows [versão 10.0.19045.4651]

C:\Users\fabiano.gisbert>
```

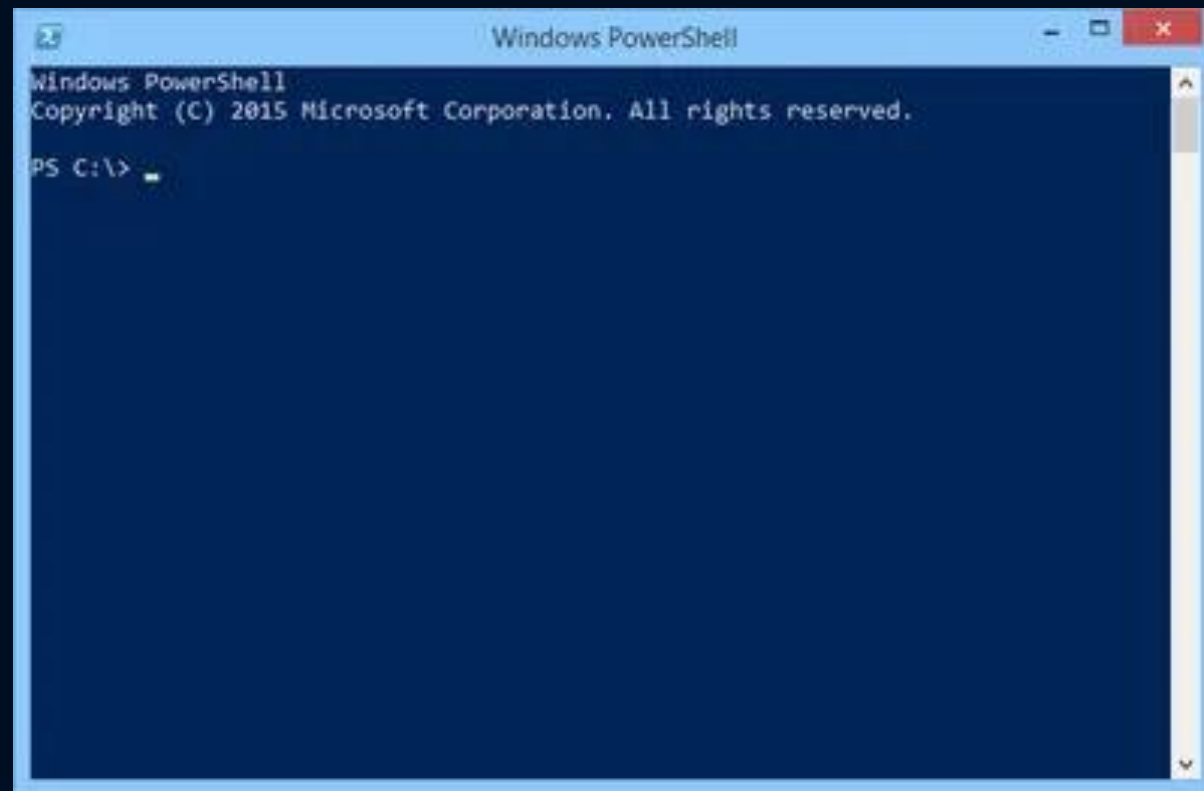
Outras ferramentas de Diagnóstico

Power Shell

PowerShell é um shell de linha de comando baseado em tarefas e linguagem de script desenvolvido no .NET. Inicialmente, apenas um componente do Windows, o PowerShell tornou-se de código aberto e multiplataforma em 18 de agosto de 2016 com a introdução do PowerShell Core.

Mais utilizado para execução de scripts para automatizar tarefas.

Exemplo de uso do powershell: winget (instalar aplicações por linha de comando)



Fim