

## Um guia para a proteção do IIS 5.0

### Resumo

Este documento fornece um plano gráfico aos administradores e arquitetos do sistema para a proteção de um servidor Web do Microsoft® Internet Information Server (IIS) 5.0. Este documento o ajuda a preparar a estrutura para projetar e implementar um servidor Web seguro com a tecnologia Microsoft. É importante que você analise com atenção estas sugestões e as utilize para definir suas próprias configurações e diretivas corporativas.

### Introdução

Os servidores podem estar vulneráveis a um grande número de ataques. Como um administrador ou arquiteto de servidores, você quer ter certeza de que todas as áreas de segurança são consideradas ao configurar servidores Web. As informações a seguir servem como uma lista de verificação para ajudá-lo a certificar-se de que todas as áreas necessárias foram abrangidas.

### Ambiente de servidores Web

Os cenários neste documento assumem que o servidor Web que está sendo protegido atende a estas especificações.

- Execução do Microsoft Windows® 2000 Server ou posterior
- Sistema de arquivos NTFS
- Execução do Internet Information Server 5.0 ou posterior
- Incorporado ao Active Directory.

### Considerações específicas de segurança

#### Sistema de arquivos

Listas de controle de acesso (ACLs) devem ser definidas em pastas que façam parte do sistema operacional. Além disso, existem configurações separadas para os arquivos especificamente utilizados pelo IIS. Ao proteger um servidor Web, uma consideração-chave é limitar a habilidade de navegar por diretórios. Isso impede que prováveis intrusos naveguem pelos diretórios que lhes ofereçam as ferramentas para causar danos. Outro item importante é não permitir que qualquer diretório tenha os privilégios de gravação e execução para o grupo **todos**. Em geral, isso é esquecido ao proteger um servidor Web.

Dois diretórios precisam de atenção extra, devido a como são facilmente comprometidos sem ACLs corretas. Os diretórios-padrão para FTP `c:\inetpub\ftproot` e para SMTP `c:\inetpub\mailroot` têm privilégios totais para o grupo **todos**, por padrão. Eles devem ser alterados, dependendo da funcionalidade necessária. Isso é possível utilizando o comando `Xcacls.exe`. O exemplo a seguir dá a

**todos** o privilégio de execução, bem como o controle total aos administradores e contas de logon do sistema.

```
xcaccls c:\inetpub\ftproot /e /c /p everyone:x administrators:f system:f /y
```

Teste o exemplo em um servidor que não seja de produção, antes de implementá-lo aos servidores Web, para verificar se essas são as ACLs a serem incorporadas. Para obter mais informações sobre Xcaccls.exe, consulte a ajuda on-line do IIS e o Windows 2000 Resource Kit.

Ao configurar um servidor Web, você precisa da capacidade de validar as ações do servidor em qualquer período específico. Isso pode ser realizado ao ativar logs do servidor Web. Do ponto de vista de segurança, isso lhe permite determinar o que aconteceu se o servidor foi violado ou reinicializado. Para impedir que intrusos violem essas informações, é preciso certificar-se de que as ACLs corretas sejam aplicadas. Ao aplicar as permissões corretas, você mesmo poderá impedir que o arquivo de log seja excluído.

### Para ativar logs

1. Inicie a ferramenta Internet Information Services.
2. Clique com o botão direito do mouse no site em questão e escolha **Propriedades**.
3. Clique na guia **Site da Web**.
4. Escolha **Ativar logs**.
5. Escolha **Formato de arquivo de log estendido W3C** na lista suspensa **Formato de log ativo**.
6. Clique em **Propriedades**.

Clique na guia **Propriedades estendidas** e defina as propriedades a seguir:

- Endereço IP do cliente
- Nome do usuário
- Método
- Tronco URI
- Status do HTTP
- Status do Win32
- Agente do usuário
- Endereço IP do servidor
- Porta do servidor

A tabela a seguir lhe dá uma idéia das ACLs que você deve ter para cada tipo de arquivo. Se você estiver configurando um site da Web, poderá tornar mais fácil a aplicação de novas ACLs criando diretórios separados para cada tipo de arquivo. No entanto, em um ambiente de hospedagem, isso se torna difícil de gerenciar para clientes. Certifique-se de considerar o seu ambiente à medida que estrutura como aplicar ACLs.

Tipo de arquivo	Listas de controle de acesso
CGI (exe, dll, cmd, pl)	Todos (execução) Administradores (controle total) Sistema (controle total)
Arquivos de script (asp)	Todos (execução) Administradores (controle total) Sistema (controle total)
Arquivos de inclusão (inc, shtm, shtml)	Todos (execução) Administradores (controle total) Sistema (controle total)
Conteúdo estático (txt, gif, jpg, html)	Todos (somente leitura) Administradores (controle total) Sistema (controle total)

## Active Directory

O Active Directory fornece administração centralizada juntamente com o suporte administrativo em camadas—dois motivos pelos quais ele é essencial ao desenvolver uma solução para hospedagem da Web. A autenticação e o controle de acesso, ambos totalmente integrados ao Active Directory, são recursos-chave de segurança no sistema operacional Windows 2000.

A administração baseada em diretivas é outro benefício ao analisar a segurança no Active Directory. A Diretiva de grupo armazena definições de configuração aplicadas a computadores ou usuários. Um objeto de diretiva de grupo contém todas as configurações da Diretiva de grupo e as aplica aos sites, domínios ou unidades organizacionais do Active Directory. Com objetos de diretiva de grupo, você pode determinar os aplicativos que usuários ou computadores específicos podem utilizar. Objetos de diretiva de grupo também podem determinar o acesso aos recursos da rede para o usuário ou computador. O tempo gasto para garantir que sua diretiva de grupo esteja correta e é exatamente o que deseja é essencial para toda a segurança básica por você configurada.

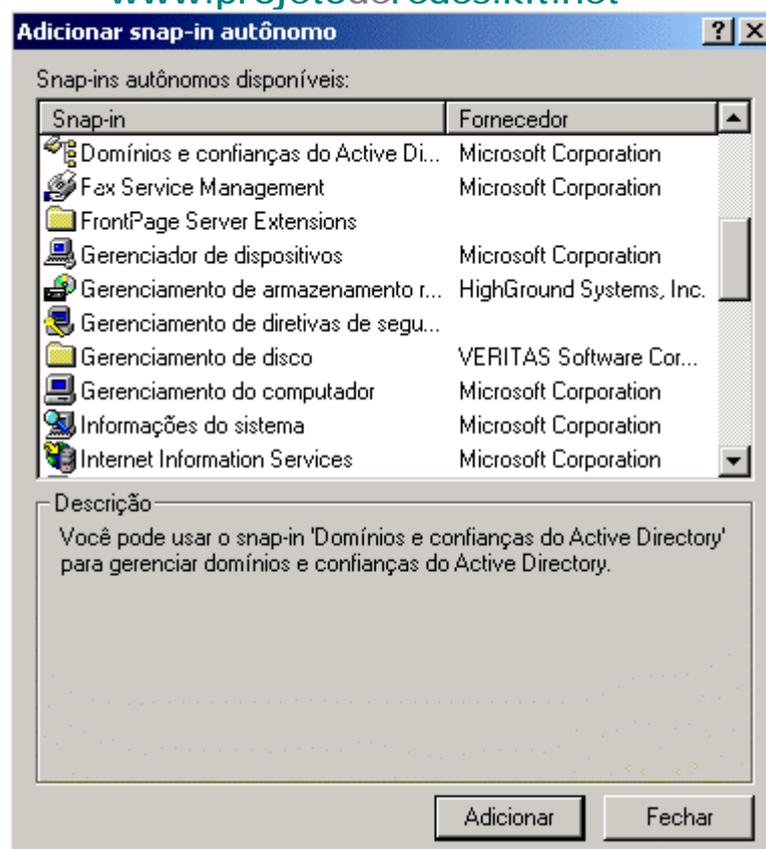
## Security Configuration Manager

O Security Configuration Manager é um snap-in do Microsoft Management Console (MMC) usado para definir atributos de segurança de áreas, tais como diretivas de contas, diretivas locais, log de eventos, grupos restritos, serviços do sistema, Registro e sistema de arquivos.

O Windows 2000 Server é fornecido com vários modelos que são criados com base na função do Windows 2000 Server. O Security Configuration Manager foi desenvolvido para permitir que você edite as opções de modelo. Você pode fazer o download do Security Configuration Manager em <http://download.microsoft.com/download/win2000srv/SCM/1.0/NT5/EN-US/hisecweb.exe>. Após o download desse modelo, copie-o para %SYSTEMROOT%\Security\Templates

### Para usar o Security Configuration Manager

1. Clique em **Iniciar** e escolha **Executar**. Na caixa de texto, digite *MMC*.
2. Após iniciado o MMC, expanda a janela e escolha **Adicionar/remover snap-in**.
3. Adicione **Security Configuration and Analysis** e **Security Templates** da lista de snap-ins, como mostra a tela a seguir.

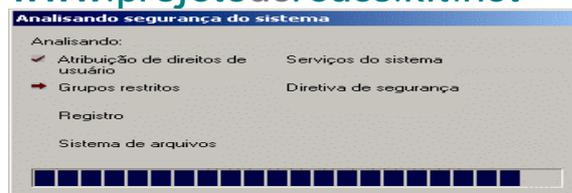


4. No MMC, procure na pasta Security Templates, o modelo hisecweb. Aqui, você pode exibir as configurações expandindo cada subcategoria, como mostra a tela a seguir.
5. Faça alterações nas configurações, conforme apropriado. Uma vez revistas as configurações, clique com o botão direito do mouse no modelo hisecweb no painel esquerdo do MMC. Escolha **Save As** e dê um nome ao modelo. Para o objetivo deste documento, denomine-o *meu-hisecweb*.

Você desenvolveu um modelo de servidor Web padrão para as implantações do seu servidor Web. A próxima etapa é aplicar esse modelo. Para isso, você deve usar o plug-in Security Configuration and Analysis do MMC.

#### Para aplicar o seu modelo

1. No MMC, clique com o botão direito do mouse em **Security configuration and analysis** e escolha **Open Database**.
2. Na janela de abertura da seleção de banco de dados, digite *meu-hisecweb* e clique em **OK**.
3. Quando for solicitado que você selecione o modelo a ser importado, selecione *meu-hisecweb.inf*.
4. Clique com o botão direito do mouse em **Security Configuration and Analysis** e escolha **Analyze Computer Now**.
5. Clique em **OK** para aceitar as configurações padrão para os locais dos arquivos de log. A análise de segurança do servidor é iniciada e o indicador de progresso a seguir é exibido.



- Quando a análise for concluída, faça uma nova verificação expandindo cada categoria. Como mostra a tela a seguir, o painel direito do MMC contém colunas para a configuração do banco de dados e para a configuração do computador. Isso lhe permite comparar as configurações de linha de base do servidor e as configurações definidas no modelo.
- Em seguida, configure o servidor com o modelo. Clique com o botão direito do mouse em **Security Configuration and Analysis** e selecione **Configure Computer Now**. Clique em **OK** para aceitar o local padrão para o arquivo de log.
- Feche o MMC sem salvar as configurações do console.
- Finalmente, você deve verificar se as configurações definidas são realmente aplicadas ao servidor. Clique em **Iniciar** e selecione **Executar**. Na caixa de texto, digite *gpedit.msc*. Isso inicia o editor de diretivas de grupo, mostrado na tela a seguir.
- No editor de diretivas de grupo, você pode procurar as configurações definidas para confirmar se foram aplicadas.

## Hotfixes e service packs

Você pode impedir muitos ataques ao garantir que correções de segurança e service packs estejam atualizados. Isso pode ser realizado utilizando a ferramenta de Verificação de hotfixes (HFCheck) do IIS 5.0 no Windows 2000, a qual garante que qualquer servidor Web que esteja executando a ferramenta está atualizado com todas as correções de segurança. A ferramenta HFCheck é extremamente funcional; você não precisa conectar todos os servidores Web ao site da Microsoft na Web para atualizações. Se um único servidor Web estiver conectado e atualizado, os outros servidores poderão ser conectados a ele para atualizações. Essa ferramenta é especificamente projetada para o IIS 5.0 e sua segurança. Você pode fazer o download da ferramenta HFCheck em <http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24168>.

Outra maneira de certificar-se de que você tem correções de segurança e service packs atualizados é pelo Microsoft Windows Update, que acompanha todas as máquinas. Esse programa verifica se você está executando todas as correções do sistema operacional disponíveis para o servidor.

A notificação de segurança do produto é uma terceira maneira de verificar se os service packs estão atualizados. Esse é um serviço baseado em assinatura. O procedimento a seguir descreve como assiná-lo.

### Para assinar o serviço de notificação de segurança do produto

1. Redija um email para [microsoft\\_security-subscribe-request@announce.microsoft.com](mailto:microsoft_security-subscribe-request@announce.microsoft.com). A linha de assunto e o corpo da mensagem não são utilizados para processar a solicitação de assinatura; você pode deixá-los em branco.
2. Envie o email.
3. Você receberá uma resposta que solicitará para que confirme o que deseja assinar. Redija um email de resposta com **OK** como o corpo da mensagem. Envie-o.
4. Você receberá dois e-mails, um confirmando que foi adicionado à lista de assinantes e outro com informações sobre o serviço de notificação. Após a assinatura, você receberá notificações de segurança via e-mail.

Esse é um serviço gratuito de notificação de e-mails que a Microsoft utiliza para enviar informações aos assinantes sobre a segurança dos produtos da Microsoft. O objetivo desse serviço é fornecer informações precisas que os clientes possam utilizar para se protegerem de ataques mal-intencionados. A equipe de segurança da Microsoft investiga os problemas relatados diretamente para a Microsoft, bem como os problemas discutidos em determinados grupos de notícias de segurança populares. Os quadros de avisos contêm informações que descrevem o problema, quais produtos são afetados pelo problema, como se proteger, quais correções de segurança estão disponíveis e links para outras informações sobre o problema.

Esse serviço suplementa os procedimentos para o relatório de segurança existente da Microsoft. Você pode continuar lendo os quadros de avisos de segurança e outras informações sobre a segurança dos produtos Microsoft em <http://www.microsoft.com/technet/security>.

A Microsoft assina digitalmente todos os quadros de avisos de segurança. Para verificar a assinatura, faça o download da chave PGP em <http://www.microsoft.com/technet/security/MSRC.asc>. A identificação da chave é 5E39 0633 D6B3 9788 F776 D980 AB7A 9432.

### Hotfixes específicos

### Removendo exemplos

O IIS 5.0 é instalado com exemplos que demonstram como configurar a tecnologia. Esses exemplos deixam o servidor vulnerável a ataques, já que hackers sabem onde estão e como utilizá-los. Antes de colocar um servidor em produção na Internet, você deve sempre excluir os exemplos. A maioria desses exemplos é canalizada pelo <http://localhost> ou [127.0.0.1](http://127.0.0.1), mas não é necessária e deve ser removida dos servidores de produção. A tabela a seguir lista os exemplos que você deve remover do servidor antes que fique ativo e operacional.

Exemplo	Diretório virtual	Local
Exemplos do IIS	\IISamples	c:\inetpub\iissamples
Documentação do IIS	\IISHelp	c:\winnt\help\iishelp
Acesso a dados	\MSADC	c:\arquivos e programas\arquivos comuns\system\msadc

Juntamente com esses exemplos, você também precisa considerar outros diretórios virtuais que devem ser removidos. Você deve remover o diretório virtual IISADMPWD, se presente, e não deve instalá-lo a menos que absolutamente necessário como um requisito de gerenciamento. Esse diretório é projetado para permitir a capacidade de redefinir senhas em intranets. Por padrão, não está instalado no IIS 5.0, mas se você atualizar a partir do IIS 4.0, deverá certificar-se de que não esteja presente.

## Ferramentas

### AuditPol.exe

AuditPol.exe é uma ferramenta de linha de comandos utilizada para modificar as diretivas de auditoria a partir da linha de comandos.

Sintaxe:

```
auditpol [\\computador] [/enable | /disable] [/help | /?] [/category: tipo] [/category: tipo]
```

Exemplo:

```
C:\>auditpol
```

```
Running ...
```

```
(X) Audit Enabled
```

```
System = Success and Failure
```

```
Logon = Success and Failure
```

```
Object Access = No
```

```
Privilege Use = No
```

```
Process Tracking = No
```

```
Policy Change = Success and Failure
```

```
Account Management = Success and Failure
```

```
Directory Service Access = No
```

```
Account Logon = Success and Failure
```

Para obter mais informações, consulte o Windows 2000 Server Resource Kit

## XcAcls

XcAcls é uma poderosa ferramenta de linha de comandos. Você pode utilizá-la para definir a segurança do sistema de arquivos pelo Windows Explorer. Também tem funcionalidade adicional, como **Editar ACLs**, que não é possível pelo Windows Explorer.

Sintaxe:

```
xcacls nome do arquivo [/T] [/E] [/C] [/G usuário:permissão;especif] [/R usuário] [/P usuário:permissão;especif [...]] [/D usuário [...]] [/Y]
```

Para obter mais informações, consulte o Windows 2000 Server Resource Kit

## SecEdit

SecEdit é uma ferramenta de linha de comandos que lhe permite manipular os modelos de segurança em um sistema. As operações suportadas por essa ferramenta são **Criar modelo**, **Aplicar modelo** e **Analisar**.

Sintaxe:

```
secedit /refreshpolicy {diretiva_da_máquina | diretiva_do_usuario} [/enforce]
secedit /refreshpolicy
secedit /export [/mergedPolicy] [/DB nome_do_arquivo ] [/CFG nome_do_arquivo ] [/areas área1
área2...] [/log caminho_do_log] [/verbose] [/quiet]
```

Para obter mais informações, consulte o Windows 2000 Server Resource Kit

## IISPerms

IISPERMS é uma ferramenta do tipo "E se..." projetada para auxiliá-lo na solução de problemas de segurança do IIS. Você pode fazer o download dessa ferramenta e de informações sobre ela em <http://support.microsoft.com/support/kb/articles/Q229/6/94.ASP>.

## IISLock

IISLock permite bloquear o IIS 5 no Windows 2000 sem definir configurações do Registro, diretivas de segurança ou outros detalhes individuais associados ao IIS. Você pode fazer o download da ferramenta em <http://www.microsoft.com/Downloads/Release.asp?ReleaseID=19889>

## QChain.exe

QChain.exe é uma ferramenta de linha de comandos que lhe permite aplicar vários hotfixes sem reinicializar o servidor.

Sintaxe:

```
qchain [Nome_do_arquivo_de_log]
```

Você pode fazer o download dessa ferramenta em

<http://www.microsoft.com/downloads/release.asp?ReleaseID=29821>

## Fortalecimento do Registro

Na proteção do IIS, você deve modificar algumas entradas do Registro. Teste as entradas a seguir em um laboratório antes de modificar os Registros do servidor, já que muitos aplicativos podem não funcionar após as modificações no Registro. Essas entradas são informativas e devem ser utilizadas conscientemente.

## Proteção contra o ataque SYN Flood

Os ataques básicos na Internet podem consistir em negação de serviço distribuída (DDOS) e SYN.Flood A DDOS não pode ser parada, mas pode ser reduzida por uma entrada do Registro que ajuda o servidor Web. Para proteção contra SYN Flood, edite a chave do Registro a seguir.

HKLM\System\CurrentControlSet\Services\Tcpip\Parameters

Nome do valor	SynAttackProtect
Tipo de valor	REG_DWORD
Dados do valor	altere para 2  0=padrão; proteção normal contra ataques SYN  1=conexão termina mais rapidamente  2=tempo limite adicional de 1; também limita determinadas opções de soquete

## Desativando a impressão na Internet

O Windows 2000 fornece a capacidade de imprimir a partir da Internet; essa funcionalidade deve ser desativada. As impressoras estão conectadas ao servidor por meio de uma página da Web; a administração dessas impressoras também é acessada em uma página da Web. Isso cria um grande orifício pelo qual o servidor pode ser atacado. Muitas vezes, a impressão na Internet é desativada no Gerenciador de serviços de Internet, mas após a reinicialização ou logoff, o objeto de Diretiva de

grupo que ativa a impressão na Internet irá reiniciar essa funcionalidade. Certifique-se de que ela não esteja no objeto de Diretiva de grupo antes de implantar o servidor.

Para desativar a impressão na Internet, edite a chave do Registro a seguir.

HKLM\Software\Policies\Microsoft\Windows NT\Printers\DisableWebPrinting

Nome do valor	DisableWebPrinting
Tipo de valor	REG_DWORD
Dados do valor	o padrão é nada altere para 0x1

### Restringindo logon anônimo

Com um servidor conectado à Internet, você deve desativar o logon anônimo já que ele permite que qualquer intruso provável obtenha informações sobre o servidor a partir de nomes de contas locais e, além disso, obtenha acesso a quem está atualmente conectado ao servidor. Para obter mais informações, consulte "How to Use the RestrictAnonymous Registry Value in Windows 2000" (Como usar o valor do Registro RestrictAnonymous no Windows 2000) em <http://support.microsoft.com/directory/article.asp?id=KB;EN-US;Q246261>

Para restringir o logon anônimo, edite a chave do Registro a seguir.

HKLM \System\CurrentControlSet\Control\LSA

Nome do valor	RestrictAnonymous
Tipo de valor	REG_DWORD
Dados do valor	altere para 2  0=sem restrições; utilizar permissões padrão  1=não permitir a enumeração de contas e nomes SAM  2=nenhum acesso sem permissões

	anônimas explícitas
--	---------------------

### Removendo compartilhamentos administrativos

Qualquer servidor executando o Windows 2000 tem compartilhamentos de administração padrão que devem ser removidos. Ao remover essa entrada do Registro, certifique-se de que a diretiva de grupo não a restaure após ela ter sido definida. Os compartilhamentos ocultos são designados por nomes de unidade lógica que você possui no servidor; por exemplo, a unidade C:\ é C\$.

Para remover os compartilhamentos administrativos, edite a chave do Registro a seguir.

HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters

Nome do valor	AutoShareServer
Tipo de valor	REG_DWORD
Dados do valor	O padrão é 1, altere para 0

### Desativando a compatibilidade com o formato de arquivo 8.3

Os administradores geralmente desejam a compatibilidade com versões anteriores; no entanto, um formato de compatibilidade não é desejável. A compatibilidade para nome de arquivo com o formato 8.3 está ativada por padrão; ela deve ser desativada para que o servidor não tenha que considerar os dois tipos de nomes de arquivo.

Para restringir a desativação da compatibilidade com 8.3, edite a chave do Registro a seguir.

HKLM\SYSTEM\CurrentControlSet\Control\FileSystem

Nome do valor	NtfsDisable8dot3NameCreation
Tipo de valor	REG_DWORD
Dados do valor	O padrão é 0 altere para 1

### Restringindo o acesso de sessão nula

Sessões nulas são o ponto fraco que pode ser explorado pelos vários compartilhamentos existentes no sistema. Você deve considerar modificar o acesso de sessão nula a compartilhamentos no sistema. Para isso adicione RestrictNullSessAccess, um valor do Registro que ativa e desativa os compartilhamentos de sessão nula.

Para restringir o acesso a sessão nula, adicione a chave do Registro a seguir.

HKLM\System\CurrentControlSet\Services\LanManServer\Parameters

Nome do valor	RestrictNullSessAccess
Tipo de valor	REG_DWORD
Dados do valor	Defina para 1

## Referências

### Sites de segurança na Web

- Segurança da Microsoft: <http://www.microsoft.com/security>
- Segurança do Microsoft TechNet: <http://www.microsoft.com/technet/security/default.asp>
- Lista de verificação de segurança do Microsoft Internet Information Server 4.0:  
<http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/columns/questions/iischeck.asp>
- Informe oficial de segurança do Microsoft SQL Server 7.0:  
<http://www.microsoft.com/sql/techinfo/administration/70/securityWP.asp>
- Números de portas conhecidos pela Autoridade de números atribuídos da Internet (IANA):  
<http://www.iana.org/assignments/port-numbers>
- Lista de vulnerabilidades e exposições comuns: <http://www.cve.mitre.org>
- Lista de correio NTBugtraq (discussão de façanhas de segurança e erros de segurança no Windows NT e em aplicativos associados): <http://ntbugtraq.ntadvice.com>
- Lista de correio NTSecurity (discussão dos Problemas de segurança no Windows NT):  
<http://ntsecurity.ntadvice.com/>
- Centro de coordenação CERT (assistência técnica 24 horas para incidentes de segurança do computador): <http://www.cert.org>
- Instituto SANS: <http://www.sans.org>
- Biblioteca de diretivas de segurança de informações PentaSafe: <http://www.baselinesoft.com/>
- Trusted System Services, Inc., Diretrizes de segurança do Windows NT:  
<http://www.trustedsystems.com/NSAGuide.htm>

### Artigos da Knowledge Base

- Internet Server indisponível devido a ataques mal-intencionados de SYN:  
<http://support.microsoft.com/support/kb/articles/Q142/6/41.asp>
- Recomendações práticas para a proteção de sistemas Windows NT conectados à Internet:  
<http://support.microsoft.com/support/kb/articles/Q164/8/82.ASP>
- Serviços padrão requeridos para o Internet Information Server:  
<http://support.microsoft.com/support/kb/articles/Q164/8/85.asp>
- Implicações de segurança de RDS 1.5, IIS 3.0 ou 4.0, e ODBC:  
<http://support.microsoft.com/support/kb/articles/Q184/3/75.ASP>

## [www.projetoederedes.kit.net](http://www.projetoederedes.kit.net)

- Como solucionar problemas de permissões no Internet Information Server 4.0:  
<http://support.microsoft.com/support/kb/articles/Q185/8/74.ASP>
- Como utilizar a ferramenta de segurança do IIS "What If":  
<http://support.microsoft.com/support/kb/articles/Q229/6/94.asp>
- Como alterar as senhas de contas do Windows NT utilizando o Internet Information Server (IIS) 4.0:  
<http://support.microsoft.com/support/kb/articles/q184/6/19.asp>
- O Internet Information Server retorna o endereço IP no cabeçalho de HTTP (Localização de conteúdo): <http://support.microsoft.com/support/kb/articles/q218/1/80.asp>
- Como adicionar configurações do Registro personalizadas ao Editor de configuração de segurança:  
<http://support.microsoft.com/support/kb/articles/Q214/7/52.ASP>
- Download e utilização da ferramenta Security Configuration Manager:  
<http://support.microsoft.com/support/kb/articles/Q245/2/16.ASP>
- Distinção dos registros de eventos de auditoria do Windows NT:  
<http://support.microsoft.com/support/kb/articles/Q140/7/14.asp>

### Revisões passo a passo do Microsoft Windows 2000

A lista completa de revisões passo a passo está localizada em

<http://www.microsoft.com/windows2000/techinfo/planning/default.asp>.

- Revisão passo a passo da configuração de diretivas de segurança empresarial:  
<http://www.microsoft.com/windows2000/techinfo/planning/security/entsecsteps.asp>
- Revisão passo a passo da utilização do conjunto de ferramentas de configuração de segurança:  
<http://www.microsoft.com/windows2000/techinfo/planning/security/secconfsteps.asp>
- Revisão passo a passo da segurança de ponta a ponta: uma introdução à segurança do protocolo Internet: <http://www.microsoft.com/WINDOWS2000/techinfo/planning/security/ipsecsteps.asp>
- Revisão passo a passo do mapeamento de certificados para contas de usuário:  
<http://www.microsoft.com/windows2000/techinfo/planning/security/mappingcerts.asp>