UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANA
DEPARTAMENTO ACADÊMICO DE ELETRÔNICA
CURSO DE ESPECIALIZACÃO EM CONFIGURAÇÃO E GERENCIAMENTO DE SERVIDORES E EQUIPAMENTOS DE REDES

FERNANDO RADECK

CONFIGURAÇÃO DE POLÍTICAS DE SEGURANÇA NO WINDOWS SERVER 2008 – ACTIVE DIRECTORY

MONOGRAFIA

CURITIBA
2012

FERNANDO RADECK

CONFIGURAÇÃO DE POLÍTICAS DE SEGURANÇA NO WIDOWS SERVER 2008 – ACTIVE DIRECTORY

Monografia apresentada como requisito parcial para obtenção do grau de especialista em Configuração e Gerenciamento de Servidores e Equipamentos de Redes, do Departamento Acadêmico de Eletrônica da Universidade Tecnológica Federal do Paraná.
Orientador: Prof. Dr. Augusto Foronda.

CURITIBA

2012

Dedico esta monografia a minha querida e amada esposa, responsável pela minha felicidade e dedicação de aprendizado maior a cada dia que passa.

RESUMO

RADECK, Fernando. **Configuração de políticas de segurança no Windows server 2008 – Active Directory**. 2012. 31 f. Monografia (Especialização em Gerenciamento de Redes) – Universidade Tecnológica Federal do Paraná. Curitiba, 2012.

O estudo desta monografia, baseia-se num estudo teórico e prático de aplicações de políticas de segurança que podem ser implementadas em empresas utilizando os recursos que o Windows Server 2008 disponibiliza. Tais políticas visam demonstrar que as informações/recursos da empresa não estão sendo utilizadas de maneira errônea e/ou de maneira não permitida pelas políticas de segurança do setor de TI.

Palavras-chave: Políticas de Segurança, GPO, Windows Server, TI.

ABSTRACT

RADECK, Fernando. **Setting up security policies in Windows Server 2008 – Active Directory.** 2012. 31 f. Essay (Graduate Certificate in Networking and Systems Administration) - Federal Technological University of Paraná. Curitiba, 2012.

The study of this monograph, based on a theoretical study and practical application of security policies that can be implemented in companies using the features that *Windows Server* 2008 provides. Such policies aim to guarantee that the information / resources of the company are not being used erroneously and / or in a manner not allowed by the security policies of the IT industry.

Keywords: Security Policy, GPO, *Windows Server*, IT.

LISTA DE SIGLAS

TI - Tecnologia da Informação

GPO - *Group Policy*

USB - *Universal Serial Bus*

LAN - *Local Area Network*

AD - *Active Directory*

ISS - *Internet Information Services*

CPU - Unidade Central de Processamento

DC - Controlador de Domínio

DNS - *Domain Name System*

DHCP - *Dynamic Host Configuration Protocol*

DVD - *Digital Versatile Disc*

CMD - *Command*

SUMÁRIO

1 INTRODUÇÃO

Com a facilidade de adquirir novos equipamentos eletrônicos, a segurança dos dados das grandes e pequenas empresas encontra-se mais facilitada para ações de usuários tentando burlar as regras impostas pelas políticas do setor de Tecnologia da Informação (TI). Com recursos disponibilizados pela Microsoft nos seus sistemas operacionais para servidor, como o *Windows Server* 2008, utilizado nesta pesquisa, a segurança da informação passa a ser regulada e controlada, utilizando os Objetos de Diretiva de Grupos (GPO).

1.1 DELIMITAÇÃO DA PESQUISA

Serão utilizados os recursos disponíveis na versão disponibilizada pela empresa Microsoft chamada *Windows Server* 2008, utilizando as GPOs inseridas no contexto disponibilizado pela versão do sistema. Para esta pesquisa, as GPOs implementadas serão: acesso a *Universal Serial Bus* (USB), acesso ao painel de controle, configurações da internet, papel de parede padrão para todas as estações de trabalho, desabilitar o acesso ao *Command* (cmd), bloqueio para execução de alteração no registro do *Windows* (*Regedit*) e alterações das propriedades de LAN desativadas.

1.2 PROBLEMA

Atualmente, não podemos mais considerar os usuários apenas como usuários “bobos”, que irão irá chegar ao seu local de trabalho, sentar e ficar restritos ao uso necessário para o seu bom desempenho durante o dia de trabalho. A disponibilidade da internet em casa faz-se com que eles busquem soluções para quebrar as regras impostas pelas empresas, realizando tentativas fortuitas de burlar o sistema.

1.3 OBJETIVOS

A seguir, os objetivos esperados para este trabalho serão descritos.

1.3.1 Objetivo Geral

Realizar um estudo de algumas GPOs para utilização no controle de utilização dos recursos de TI disponibilizada na empresa para seus colaboradores.

1.3.2 Objetivos Específicos

Os objetivos específicos são:

- Descrever as GPOs utilizadas neste trabalho;
- Implementar algumas GPOs para garantir a segurança da informação para as empresas.

1.4 JUSTIFICATIVA

Ao término desta pesquisa, visando o entendimento e compreensão de que a segurança de TI deve ser cada vez mais necessária nas empresas, veremos como os recursos das GPOs podem auxiliar na resolução de velhos problemas que enfrentamos todos os dias no nosso ambiente de trabalho. A segurança torna-se primordial com a capacidade simples e prática que usuários “comuns” encontram disponibilizadas diariamente na internet para tentativas de quebrar a segurança. O principal método é o diálogo e a conscientização de nossos usuários referente à segurança de informação, porém, sabemos que tentativas de burlar o sistema serão praticamente diárias. Explicar os motivos, mostrar exemplos e ensinar uma cultura de uso consciente para os usuários, pode fazer com que muitas das regras que temos que implementar atualmente, sejam facilmente desnecessárias. A utilização recursos, como as GPOs, tem um custo que poderia ser reduzido drasticamente com esta cultura, porém, infelizmente, ainda necessitamos desses recursos para auxiliar no dia-a-dia da empresa.

1.5 PROCEDIMENTOS METODOLÓGICOS

No desenvolvimento deste trabalho, são utilizados conceitos encontrados em referências bibliográficas específicas e oficiais Microsoft, disponibilizadas em cursos oficiais nos quais participei, como o curso oficial 6419B cujos conteúdos encontram-se disponíveis em Microsoft (2011).

É realizada a apresentação e explicação de algumas GPOs disponibilizadas pelo sistema operacional utilizado, como conceitos, funcionalidade e aplicação.

A implementação das GPOs escolhidas é realizada em uma máquina virtual, utilizando testes e mostrando os resultados encontrados com a prática e aplicação de GPOs em uma unidade organizacional.

1.6 FUNDAMENTAÇÃO TEÓRICA

Os conceitos técnicos em que foram baseados os estudos deste trabalho estão descritos em Microsoft (2011) em sites oficiais *Microsof* como www.technet.microsoft.com e microsoft.com e em Torres (2001).

Com estas bibliografias, os conceitos abordados estão fundamentados em documentos oficiais disponibilizados pela empresa *Microsoft*, com garantias que os mesmos funcionem no ambiente de teste gerado para conseguir utilizar alguns recursos disponibilizados.

Foram utilizados conceitos para implementação da segurança em um ambiente com uma versão recente do sistema operacional e com base nas estações de trabalhos utilizando o sistema operacional *Windows Seven Professional*.

1.7 ESTRUTURA

A estrutura desta monografia está descrita em 4 (quatro) capítulos. O primeiro especifica principalmente os objetivos do trabalho justificando em quesitos funcionais quais as necessidades de implementação do conceito de AD nas empresas, sendo todo ele fundamentado em conceitos escritos e desenvolvidos pelo fabricante da solução, ou seja, a Microsoft.

No segundo capítulo, são apresentados os conceitos sobre o sistema operacional responsável por gerir os recursos implementados da ferramenta AD. Na tentativa de uma abordagem clara, objetiva e com detalhes de possíveis versões que possam ser implementadas no ambiente corporativo.

No terceiro capítulo, os conceitos da ferramenta AD e suas funcionalidades são mostrados, assim como os seus recursos de como podem ser implementados, dando uma base para o próximo capítulo.

No quarto capítulo, são apresentados exemplos práticos simulados em ambiente virtual da aplicação e utilidade de alguns exemplos de GPOs, demonstrando através de figuras as configurações das GPOs no servidor e a aplicação real em possíveis estações de trabalhos de usuários.

2 CONHECENDO O WINDOWS SERVER 2008

Esta versão do *Windows Server* foi lançada em 27 de Fevereiro de 2008. Porém o nome pelo qual era conhecido no meio profissional até meados de maio de 2007 era *Server Longhorn*. O intuito da empresa que desenvolveu o *software*, no caso a Microsoft, foi de procurar alcançar o máximo dos recursos disponíveis para a época e pensando em novos recursos que estavam sendo desenvolvidos, ou seja, um planejamento estratégico da tecnologia que poderia permanecer por vários anos. Utilizando o *Windows Server* 2008, as opções de tecnologias disponíveis aumentam a eficiência e principalmente a segurança.

Um item diferencial do desenvolvimento do *Windows Server* 2008, a programação para a internet, um recurso chamado *Internet Information Services 7.0 (ISS 7)* foi adicionado ao seu escopo, na qual possui uma arquitetura mais segura e simples para desenvolver e hospedar com confiança aplicativos e serviços. O desenvolvimento de aplicativos utilizando tal recurso agrega mais integridade dos aplicativos que conectam usuários e dados, permitindo visualizar e compartilhar as informações mais pertinentes da aplicação.

Outro destaque importante nessa versão de sistema operacional para servidores foi a tecnologia de virtualização chamada *Hyper-V*, um sistema baseado em uma estrutura na qual permite que os recursos de *hardware* possam ser compartilhados com vários Sistemas Operacionais chamado *Hypervisor* (MICROSOFT, 2011).

2.1 VERSÕES DO WINDOWS SERVER 2008

Foram desenvolvidas pela Microsoft nove versões desse Sistema Operacional de servidores, buscando suprir a necessidade de recursos de rede e custos, desde uma empresa pequena com pouco potencial financeiro até grandes corporações dispostas a pagar por um produto teoricamente completo.

2.1.1 WINDOWS SERVER 2008 STANDARD

Segundo Lima (2012), o *Windows Server 2008 Standard* é um sistema com algumas limitações, dando suporte a multiprocessamento simétrico, aceitando até 4 gigabytes de memória em sistemas de 32 bits e 32 gigabytes em sistemas de 64 bits. Recomendado para pequenas e médias empresas, pois suporta os principais serviços de regras disponíveis nessa versão.

2.1.2 WINDOWS SERVER 2008 ENTERPRISE

O *Windows Server 2008 Enterprise* Estende os recursos oferecidos pela versão *Standard*, proporcionando um nível corporativo para aplicação de aplicações consideradas críticas. O gerenciamento de identidades está mais seguros e consolidados nessa versão. Uma das ideias primordiais dessa versão é a de redução de custos na infraestrutura com os direitos de licença para utilizar a virtualização, fornecendo recursos extremamente confiáveis e dinâmicos. Na questão de *hardware*, essa versão reconhece em servidores de 32 bits até 32 gigabytes de memória Ram e em sistemas que trabalham em 64 bits, 2 terabytes de memória Ram e 8 CPUs. (LIMA, 2012).

2.1.3 WINDOWS SERVER 2008 DATACENTER

O *Windows Server 2008 Datacenter* é utilizado em âmbito corporativo, a virtualização é utilizada em grandes escalas nas empresas, virtualizando desde os seus pequenos servidores até os servidores maiores. Com essa tecnologia, os custos para a empresa na implementação de servidores tornam-se menores além de contar com uma disponibilidade de *cluster* e disponibilidade de particionamento dinâmico de *hardware*. Na esfera corporativa, essa versão busca a solução em uma escala vertical e virtualização de nível corporativo.

Em quesitos de *hardware*, permite o escalonamento de 2 a 64 processadores, aceita a utilização de 64 gigabytes de memória RAM em sistemas de 32 bits e até 2 terabytes em sistemas de 64 bits (LIMA, 2012).

2.1.4 WINDOWS WEB SERVER 2008

Segundo Lima (2012), o *Windows Web Server 2008* é dedicada a fornecer serviços Web, possui recursos de infraestrutura *Web* que permitem organizar, implantar páginas, *sites*, aplicações e serviços *Web*. Possui uma integração que facilita toda esse gerenciamento *Web* com aplicações como IIS 7.0, ASP.NET e Microsoft . NET *framework*. Sendo um servidor exclusivamente, recursos como *Active Directory* não estão disponíveis nessa versão, sendo necessário a instalação do *server core* para obter uma funcionalidade padrão.

Em *hardware*, em sistemas de 32 bits oferece recurso para 32 gigabytes de memória Ram e 4 CPUs.

2.1.5 WINDOWS SERVER 2008 FOR ITANIUM-BASED SYSTEMS

Desenvolvido para conseguir suprir as necessidades de clientes de grande porte, suportando até 64 processadores. Foi otimizado para aplicativos de bancos de dados de grande porte e gestão de negócios, fornecendo para os seus clientes alta disponibilidade e escalabilidade, atendendo o alto nível de desempenho esperado para aplicações de banco de dados (LIMA , 2012).

2.1.5 WINDOWS SERVER 2008 FOUNDATION

Um produto desenvolvido de baixo custo, sendo um grande atrativo para pequenas empresas que buscam uma solução prática e com recursos que lhe atendam no seu dia-a-dia. Voltada para uma rede com até 15 usuários, possui serviços primordiais como *Active Directory*, compartilhamento de arquivos e impressoras, acesso remoto e segurança (LIMA, 2012).

3 AD (ACTIVE DIRECTORY)

Neste capítulo, serão abordadas as funcionalidades encontradas na solução Microsoft para acesso dos usuários na rede, o chamado *Active Directory*.

3.1 CONCEITOS

Surgiu juntamente com o *Windows Server* 2000. Seu desenvolvimento trouxe várias vantagens para os administradores de rede. Antes de a solução ser apresentada, os usuários nas empresas tinham um sério problema relacionado a sistemas, o esquecimento de suas inúmeras senhas para diversas aplicações diferentes.

Com a implementação do *AD*, os usuários passaram a ter apenas uma senha sincronizada com as mais diversas aplicações utilizadas na empresa. A ideia de centralização de recursos funciona no AD com um banco de dados que possui as principais informações, como usuários, grupos, membro dos grupos, senhas, etc. Assim, o acesso à informação fica viável e

de simples conferência, tanto para manutenção dos recursos quanto para administração do AD. (TORRES, 2001).

3.2 DOMÍNIO

Em uma empresa, possuímos servidores e máquinas as quais os usuários utilizam para suas atividades variadas durante o dia. Todos esses itens, além das informações dos diretórios, são definidos no conceito de AD como domínio, sendo considerado um agrupamento lógico de contas e recursos compartilhando políticas de seguranças impostas pelo setor de TI da empresa, todos os servidores que contém uma cópia da base de dados do AD fazem parte do domínio. Um domínio que seja baseado em *Active Directory* pode ter dois tipos de servidores: Controladores de Domínio (DC) e Servidores Membros.

Os DC utilizam o AD para armazenar cópias de leituras e gravação do banco de dados do domínio utilizado pela empresa, aplicando as replicações necessárias das informações autenticando os usuários, garantindo a consistência das informações.

Os servidores membros não processa *logons* de contas, não armazena informações de diretivas de segurança de um domínio. Normalmente são utilizados na função de servidor de arquivo, aplicativos, banco de dados, servidor *Web*, servidor de certificados, *firewalls* ou servidores de acesso remoto.

Quaisquer alterações que sejam feitas em um DC, automaticamente serão replicadas para todos os outros DC. Em servidores membros, a criação de uma lista de usuários e grupos não seria ideal pela dificuldade.

A segurança com a qual o AD trabalha, baseia-se na autenticação dos usuários através do *login* e senha, digitados pelo usuário. O AD verifica os dados inseridos, faz uma busca em sua base de dados e autentica o usuário liberando acessos a ele permitido. O serviço de nomeação de servidores e recursos de soluções de nomes utilizados pelo AD é o DNS (*Domain Name System*), (VIDAL, 2006).

3.2 UNIDADES ORGANIZACIONAIS

São itens encontrados no AD onde o administrador pode adicionar usuários, grupos, computadores e criar novas unidades organizacionais, sendo que, uma unidade organizacional não pode conter objetos que se encontram em outros domínios. Cada domínio possui a sua

própria estrutura de unidade organizacional, não é preciso, necessariamente, que todos possuam a mesma estrutura. (WINDOWS, 200-).

3.3 OBJETOS DO ACTIVE DIRECTORY

Contas de usuários: é um objeto do AD, as principais informações que encontramos nesse objeto são o primeiro nome, último nome, descrição, usuário, senha entre outros.

Contas de Computador: todo o computador que faz parte da rede, assim que é adicionado no domínio, automaticamente é criado a sua conta no AD, não importa se é um computador de um colaborador ou um servidor da empresa.

Grupos de usuários: sua principal função é facilitar o gerenciamento e as atribuições de permissões de acesso a recursos (VIDAL, 2007).

3.4 FUNÇÕES DO AD

No *Windows Server 2008* as principais funções que encontramos são:

- Função Serviços de Domínio no AD: mantem em seu banco de dados informações dos usuários, computadores e outros serviços que podemos encontrar na rede. A facilidade de gerenciamento auxilia o responsável pela rede a verificar e manter a integridade das informações nele cadastradas, entre elas, o compartilhamento de recursos e a colaboração entre os usuários. Para um correto funcionamento dessa função, faz-se necessária a sua instalação na rede para que outros aplicativos possam sincronizar os seus recursos de dependência do AD.
- Função AD *Rights Managenebte Services*: sua principal função é a proteção da informação. Os aplicativos que possuam esse recurso terão sua garantia de que apenas os usuários com as respectivas permissões irão ter acesso a eles, deixando a informação persistente e segura.
- Função Serviços AD *Lightweight Directory Services*: serviço utilizado para aplicativos que estão habilitados em um diretório. Fornece armazenamento de recuperação de dados, sendo otimizados para leitura.
- Função Serviços de Federação do AD: pode ser utilizado em diversas plataformas diferentes e ser utilizado via web.

- Função Serviços de Certificado do AD: o gerenciamento de segurança presente nessa função baseia-se em certificados de chaves públicas, que podem ser vinculados a uma chave privada aos aplicativos correspondentes.

4 GPO (*Group Police)*

As principais funções das GPOs são facilitar o trabalho do administrador da rede, oferecendo recursos que podem ser implementados tanto em *sites*, domínio ou até mesmos em OUs específicas, oferecendo uma segurança e tranquilidade no gerenciamento da rede. Seus principais recursos podem ser designados somente para os usuários que fazem parte do domínio na estação de trabalho quanto para qualquer usuário, que esteja no domínio, localmente na estação de trabalho.

As GPOs disponíveis no *Windows Server 2008* permitem que as definições configuradas sejam efetivadas tanto em estações de trabalho com *Windows XP* ou com *Windows 7* instalado. As configurações padrão para as GPOs são delimitadas em *enable, disable* e *Not Configured*, sendo a primeira função explicitando que a GPO escolhida será ativada e as configurações dela replicadas para a situação escolhida, a segunda função informa que a GPO estará desabilitada, não sendo configurada e a terceira função, sem alterações, ou seja, não ativa nem desativa o item escolhido.

Para realizar a configuração de uma GPO, um item importante deve ser analisado com cautela, a hierarquia das GPOs. Possui três níveis diferentes: *sites*, domínios e OUs. Qualquer GPO que seja adicionada ao *site*, será replicado para todos os domínios que fazem parte do site, GPOs adicionadas ao domínio, será replicado para todos os usuários e grupos que fazem parte deste domínio e as GPOs adicionadas nas OU será aplicado exclusivamente aos usuários que façam parte dela.

A partir dos próximos itens, serão descritos a implementação de algumas GPOs já citadas. Tais GPOs foram testadas em um ambiente virtual utilizando o programa Oracle Virtual Box, onde foi criada três máquinas virtuais, uma com *Windows Server 2008*, a segunda com *Windows 7* e a terceira com *Windows XP*.

As GPOs implementadas utilizadas para teste são: acesso a USB (*Universal Serial Bus*), acesso ao painel de controle, configurações da internet, papel de parede padrão para todas as estações de trabalho, desabilitar o acesso ao *Command* (cmd), bloqueio para execução de alteração no registro do *Windows* (*Regedit*) e alterações das propriedades de LAN desativadas (Microsoft, 2011).

4.1 GPO - DESABILITAR PAINEL DE CONTROLE

Uma das principais funções para realizar o bloqueio de acesso ao conteúdo do painel de controle das versões do *Windows* se dá ao fato de que, vários de seus recursos permitem alterações que não são autorizados para que os usuários locais realizem, por exemplo, alteração das configurações de data e hora, podendo ocasionar falhas de comunicação entre *softwares* instalados no servidor que dependem do sincronismo dos horários. A figura 1 demonstra que a GPO foi habilitada, ou seja, a ação de desabilitar a GPO está ativa e os usuários do domínio não podem realizar o acesso conforme mostra a figura 2.

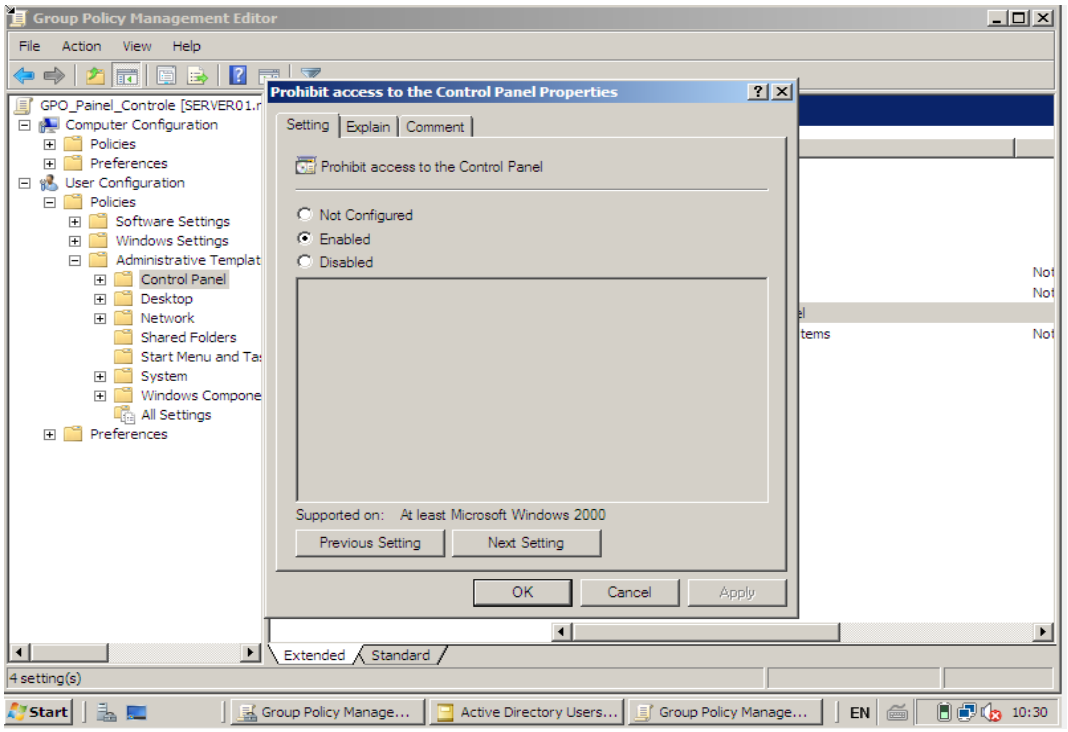

Figura 1: GPO – Proibir acesso ao Painel de Controle
Fonte: autor, utilizado no Windows Server.

Figura 2 – Usuário do domínio sem acesso ao Painel de Controle.
Fonte: autor, utilizado no Windows XP.

4.2 GPO - DESABILITAR PROPRIEDADE DE LAN (ETHERNET)

A figura 3 demonstra a ativação da GPO para desabilitar as propriedades do adaptador de rede. Sua principal função estar desabilitada impõe uma regra para que os usuários do domínio em hipótese nenhuma tenham acesso às alterações das configurações e IPs configuradas pelo servidor DHCP, não dando margem para que haja uma tentativa de acesso na rede com algum número de IP diferente da permitida e programado pelos servidores da empresa. A figura 4 demonstra a opção desabilitada para um usuário do domínio na sua estação de trabalho.

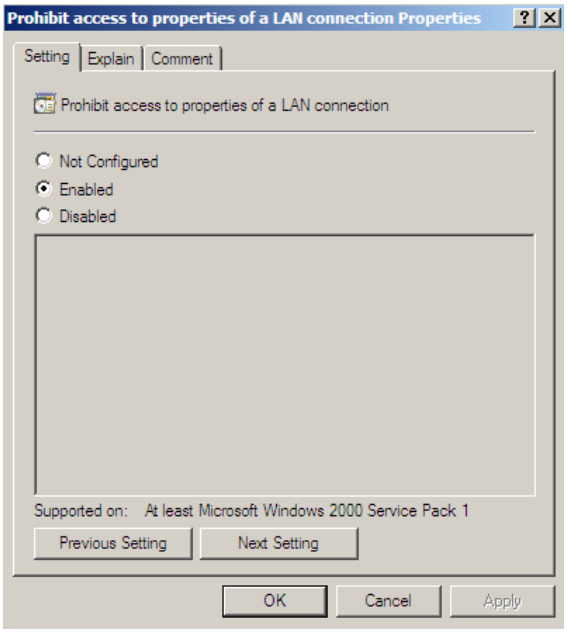

Figura 3 – GPO Configuração de LAN.
Fonte: autor, utilizado no Windows Server.

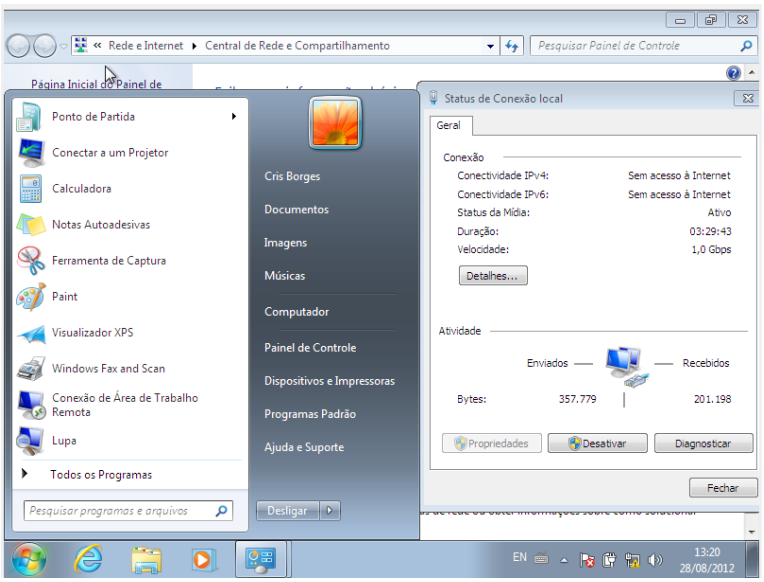

Figura 4 – Usuário do domínio com opção de propriedades da LAN desabilitado.
Fonte: autor, utilizado no Windows.

4.3 GPO – BLOQUEIO CD/DVD/USB

Com a facilidade de acesso à dispositivos de armazenamento, o bloqueio nas máquinas dos usuários do domínio fica evidente pela facilidade de conseguir tirar da empresa as informações através desses dispositivos. Com essa GPO, o acesso fica restrito nas portas

USB somente para mouse e teclado que utilizem esse tipo de conexão. A figura 5 demonstra as GPOs ativas para bloqueio do CD-Rom, Dvd-Rom e Unidades de armazenamento (USB). O exemplo na prática de um usuário do domínio pode ser visualizado na figura 6, negando o acesso ao drive de DVD-ROM, por exemplo.

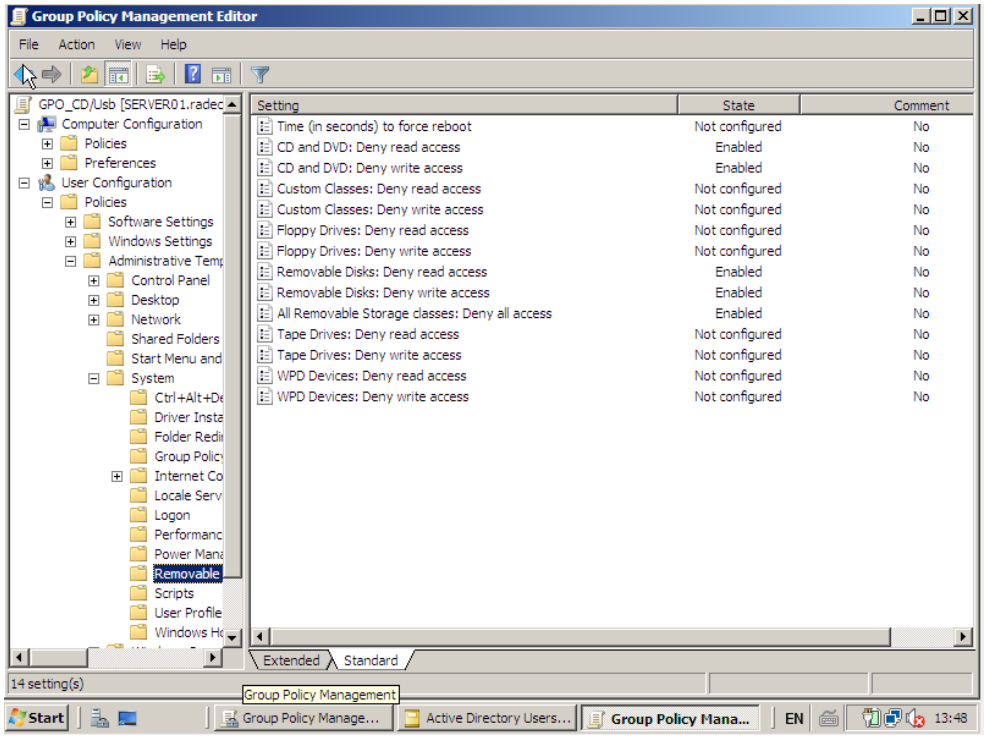

Figura 5 – GPOs Configuração ativas.
Fonte: autor, utilizado no Windows.

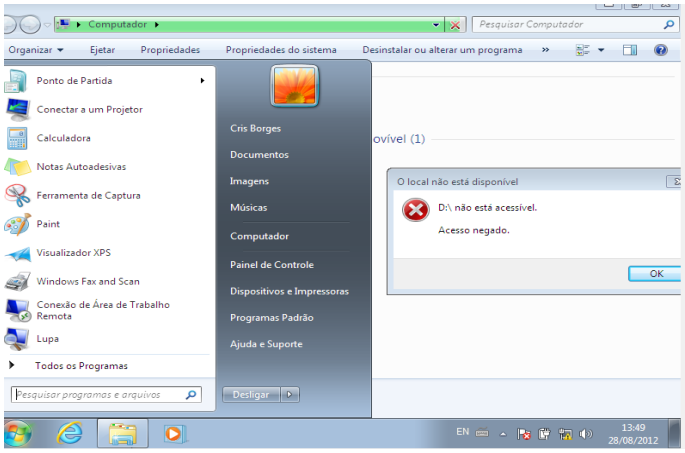

Figura 6 – Acesso negado ao driver de DVD-ROM.
Fonte: autor, utilizado no Windows.

4.3 GPO – CONFIGURAÇÕES DO INTERNET EXPLORER

As opções que os usuários do domínio possuem de acesso às configurações do *Internet Explorer* podem facilitar o acesso a configurações que possam burlar as regras de segurança imposta pelo setor de TI da empresa, como por exemplo, adicionando um número de *proxy* que libere determinadas portas no firewall e consiga acesso total a internet. A figura 7 mostra todos os itens que estarão ativos nas GPOs para que sejam implementadas nos usuários do domínio. A figura 8, mostra o exemplo na prática de um usuário do domínio sem acesso as principais funções do *Internet Explorer*.

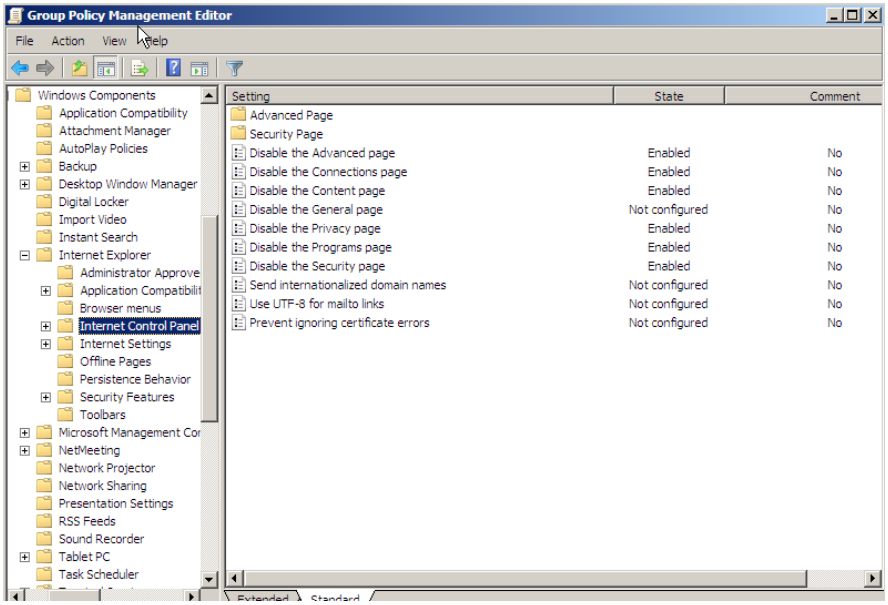

Figura 7 – GPO Configurações Internet Explorer
Fonte: autor, utilizado no Windows.

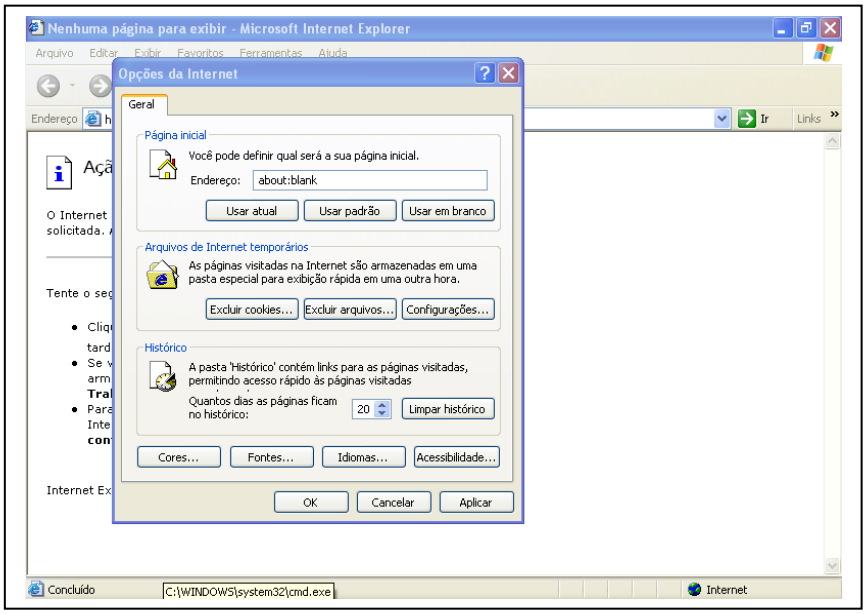

Figura 8 – GPO Configurações Internet Explorer.
Fonte: autor, utilizado no Windows.

4.4 GPO – PAPEL DE PAREDE PADRÃO

Com esta GPO habilitada, a empresa pode padronizar todos os papéis de parede nas estações dos usuários que realizem o *login* na rede. Bloqueando também o acesso a alteração dessa opção, a padronização e facilidade de comunicação com os usuários ficam explícitas, sendo fácil alteração pelo servidor do padrão de imagens impostas pelas políticas internas da empresa. A figura 9 exemplifica a configuração da GPO para esta função e na figura 10 o padrão de papel de parede na estação do usuário do domínio.

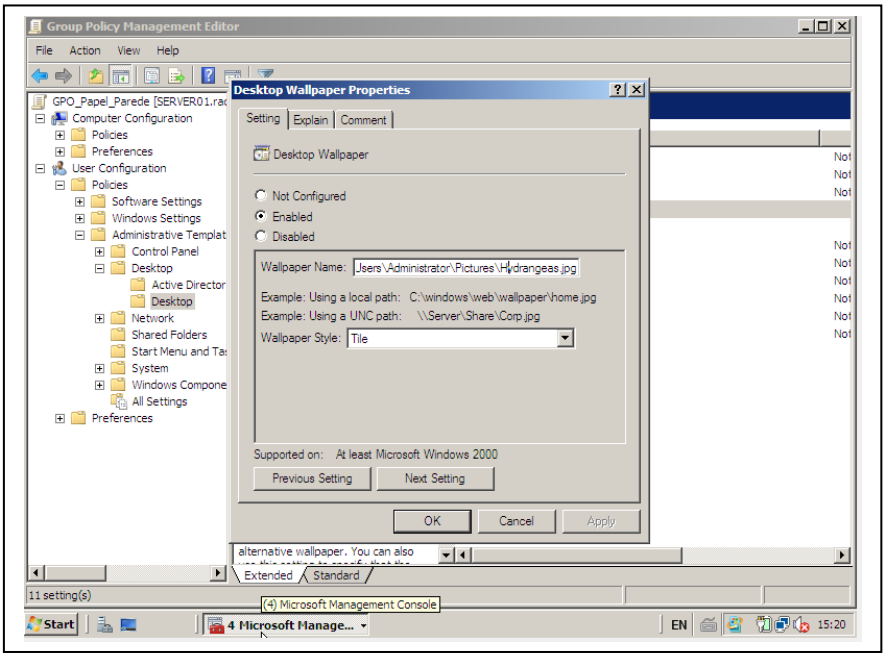

Figura 9 – GPO Configurações Papel de Parede.
Fonte: autor, utilizado no Windows.

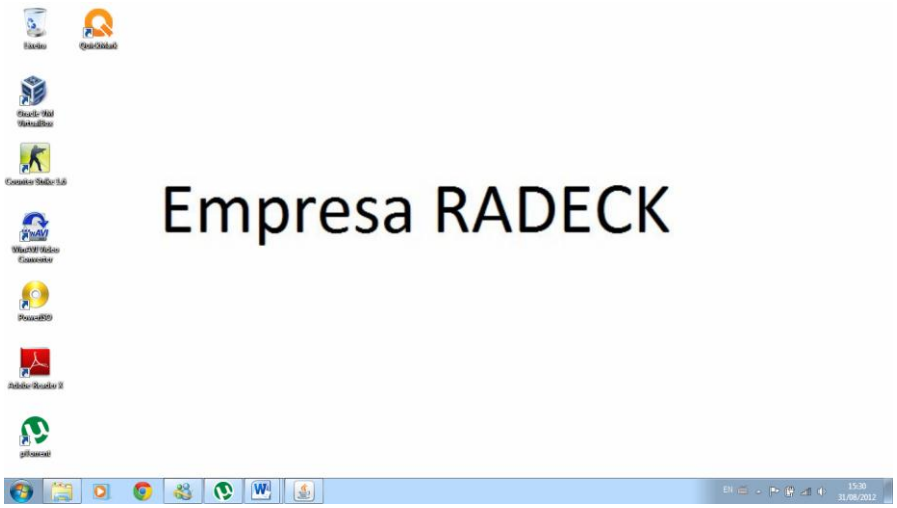

Figura 10 – Configuração do papel de parede usuário do Domínio.
Fonte: autor, utilizado no Windows.

4.5 GPO – DESABILITAR *COMMAND*

Esta GPO tem como principal função desabilitar a função do *Command* do *Windows*, a figura 11 demonstra a mesma ativa. Sem esse recurso ativo, os usuários do domínio não conseguem utilizar recursos que poderiam ser executados via linha de comando. A figura 12 exemplifica a restrição de acesso do usuário do domínio ao *command.*

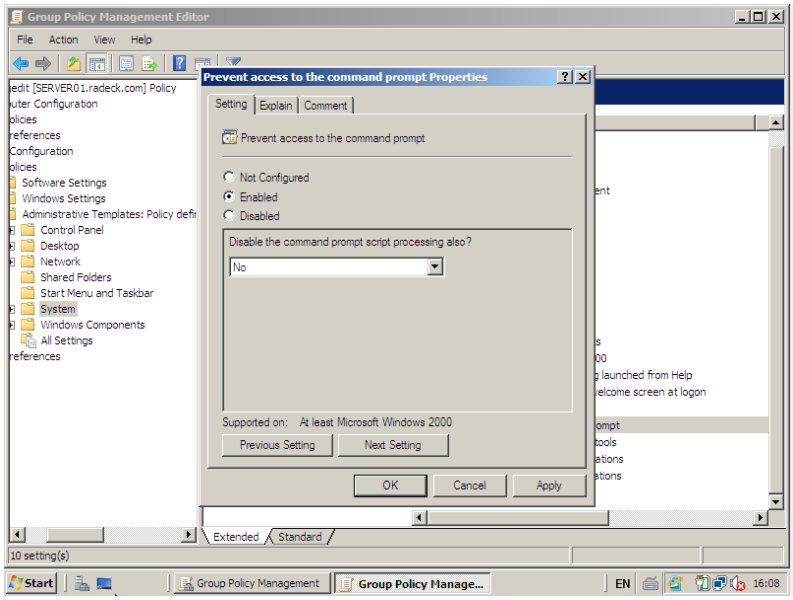

Figura 11 –GPO Desabilitar *Command*.
Fonte: autor, utilizado no Windows.

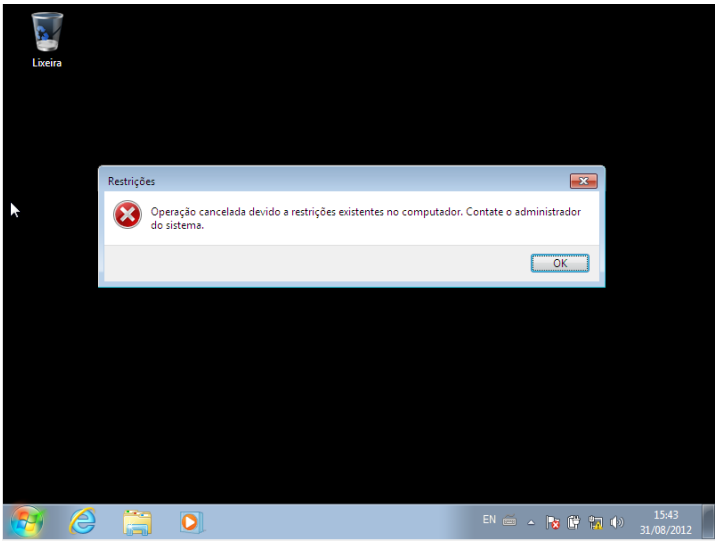

Figura 12 – GPO Desabilitar *Command*
Fonte: autor, utilizado no Windows.

4.5 GPO – DESABILITAR *REGEDIT*

Desabilitando o acesso ao registro para os usuários do domínio, a segurança dos programas instalados, como exemplo *Sped* Fiscal, está garantida, pois sem acesso a este item, o usuário fica impossibilitado de tentar qualquer ação que interfira no correto funcionamento da aplicação no sistema operacional. A figura 13 demonstra a ativação da GPO e a figura 14

demonstra na prática a mensagem de alerta informada ao usuário do domínio a negação de acesso ao *regedit.*

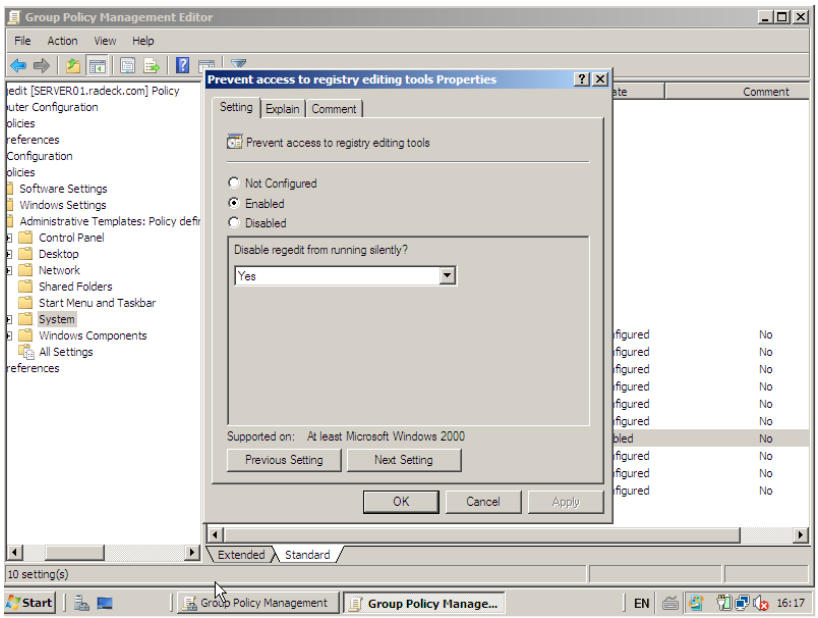

Figura 13 –GPO Desabilitar *regedit*.
Fonte: autor, utilizado no Windows.

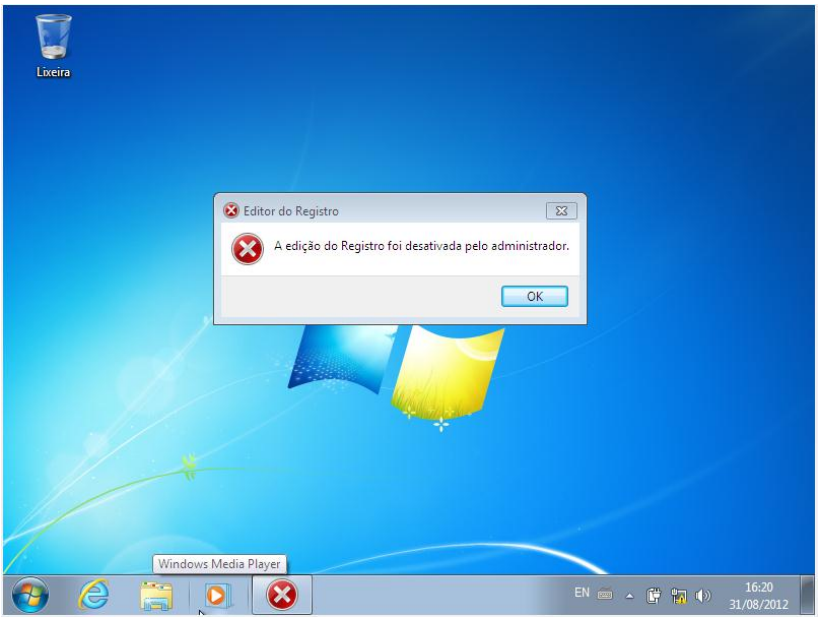

Figura 14 –*Regedit* desativado para o usuário.
Fonte: autor, utilizado no Windows.

5 CONCLUSÃO

A cada dia que passa, a facilidade de comunicação entre funcionários nas empresas causa um tremor gigante para a área de TI. Com as inúmeros facilidades de acessos a equipamentos que comunicam-se com a *internet*, facilitando a possibilidade de tráfego das informações para fora da rede interna, a garantia de segurança deve-se ao fato de utilizarmos recursos pagos para a maior proteção possível dessas informações e controle de acesso.

Sabendo que, atualmente é impossível proteger uma rede 100%, quanto maior a quantidade de recursos oferecidos pelo mercado para tentativa de deixar seguro, melhor. Com isso, recursos da empresa Microsoft foram utilizados para demonstração de pequenas, porém usuais regras para tentar ao máximo coibir o acesso indevido pelos funcionários na empresa.

Com esses recursos disponibilizados, ficou provado que em um ambiente corporativo onde se utiliza sistema que estejam em comunicação ideal, à segurança torna-se melhor e mais fácil de controlar, auxiliando os responsáveis pela TI a esse gerenciamento.

REFERÊNCIAS

LIMA, Raphael. **O que é isto? (AD DS, AD RMS, AD LDS, AD FS, AD CS).** Disponível em: <http://www.raphaell.info/?p=1306>. Acesso em: 12 de agosto de 2012.

MICROSOFT. **Configuring, Managing, and Maintaining Windows Server 2008 – based Servers.** v.1, Cargraphics Gráfica e Editora Ltda, 2011.

MICROSOFT. Disponível em: <microsoft.com>. Acesso em: 10 de junho de 2012.

TORRES, Gabriel. **Redes de computadores:** curso completo. Rio de Janeiro: Axel Books do Brasil Editora Ltda, 2001.

VIDAL, Josue. **Redes e Servidores:** Entendendo Active Directory. 2006. Disponível em: <http://imasters.com.br/artigo/4735/servidores_windows/entendendo_active_directory> Acesso em: 10 agosto de 2012.

_____. **Redes e Servidores:** Objetos do Active Directory. 2007. Disponível em: <http://imasters.com.br/artigo/6058/redes-e-servidores/objetos-do-active-directory>. Aceso em 10 de agosto de 2012.

WINDOWS Server. Disponível em: <http://technet.microsoft.com/pt-br/library/cc758565(v=ws.10).aspx>. Acesso em: 15 de julho de 2012.