

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

DJONES CARLOS JUTTEL

IMPLEMENTAÇÃO DO WINDOWS 2008 SERVER

MONOGRAFIA

CURITIBA

2012

DJONES CARLOS JUTTEL

IMPLEMENTAÇÃO DO WINDOWS 2008 SERVER

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

RESUMO

JUTTEL, DJones. **Implementação do *Windows 2008 Server***. 2012. 40 f. Monografia (Especialização em Gerenciamento de Redes) – Universidade Tecnológica Federal do Paraná. Curitiba, 2012.

O propósito desta monografia está apresenta a segurança da informação em servidores que disponibilizam informações voltadas para rede interna do Escritório Contábil São Bento. Primeiramente, são apresentados os conceitos de vários tópicos abordados no trabalho, como redes de computadores, sistema operacional *Windows 2008 Server*, *GPO*, *OU*, políticas de segurança, restrições. A ênfase do trabalho foi a aplicação de um conjunto de regras e restrições para administrar de uma maneira eficaz todas as movimentações no domínio da rede interna, gerando maior confiabilidade, segurança e monitoramento.

Palavras-chave: *Windows 2008 Server*. *GPO*. Políticas de Segurança. Redes.

ABSTRACT

JUTTEL, Djones. **Implementing a Windows 2008 Server**. 2012. 40 f. Essay (Graduate Certificate in Networking and Systems Administration) - Federal Technological University of Paraná. Curitiba, 2012.

The purpose of this monograph is to present information security on servers that provide information focused on the internal network of the Accounting Office St. Benedict. First, we present the concepts of several topics covered at work, as computer networks, operating system Windows Server 2008, GPO, OU, security policies, restrictions. The emphasis of this study was to apply a set of rules and restrictions for administering an effective way all drives in the domain of internal network, resulting in greater reliability, security and monitoring.

Keywords: Windows 2008 Server. GPO. Security Policy. Network.

LISTA DE FIGURAS

Figura 1 – Serviços instalados no Windows 2008 Server [Autoria Própria].....	16
Figura 2 – Criando uma OU [Autoria Própria].....	17
Figura 3 – Organização das OUs [Autoria Própria].....	18
Figura 4 – Inclusão de uma conta de usuário no AD [Autoria Própria].....	19
Figura 5 – Dados do usuário e conta [Autoria Própria].....	20
Figura 6 – Criação de Grupo na OU [Autoria Própria].....	21
Figura 7 – Nomeando o grupo [Autoria Própria].....	22
Figura 8 – Alocando usuários dentro de um grupo [Autoria Própria].....	22
Figura 9 – Documentos compartilhados para OU [Autoria Própria].....	24
Figura 10 – Permissão para o grupo DL_CONTABIL [Autoria Própria].....	25
Figura 11 – Gerenciamento de Diretiva de Grupo [Autoria Própria].....	26
Figura 12 – Diretiva redirecionamento de pasta [Autoria Própria].....	27
Figura 13 – Definindo o local de redirecionamento [Autoria Própria].....	28
Figura 14 – Local de armazenamento [Autoria Própria].....	29
Figura 15 – Usuário final redirecionamento [Autoria Própria].....	30
Figura 16 – Ocultado unidade de disco [Autoria Própria].....	32
Figura 17 – Impedir acesso as unidades de disco. [Autoria Própria].....	32
Figura 18 – Unidades ocultas para o usuário remoto [Autoria Própria].....	33
Figura 19 – Programas liberados para o usuário remoto [Autoria Própria].....	34
Figura 20 – Negando acesso a um aplicativo fora da lista [Autoria Própria].....	34

SUMÁRIO

1 INTRODUÇÃO.....	7
1.1 DELIMITAÇÃO DA PESQUISA	8
1.2 PROBLEMA.....	8
1.3 OBJETIVOS	9
1.6 JUSTIFICATIVA.....	9
2 WINDOWS 2008 SERVER.....	10
REFERÊNCIAS.....	36
4 CONCLUSÃO.....	35
REFERÊNCIAS.....	36

1 INTRODUÇÃO

Redes internas são de extrema importância para qualquer tipo de empresa, seja ela privada como pública. Esse tipo de rede facilita muito para quem está lidando com programas que são compartilhados.

A rede interna do Escritório Contábil São Bento vem atravessando uma série de problemas com relação a sua rede interna não possui um servidor no qual aplica diretivas de segurança e restrições a certos usuários ou grupo de usuários.

Os conceitos de *active directory*, unidade organizacional e *group policy* serão explicados, pois serão as principais ferramentas a serem utilizadas no processo de implementação.

Buscando um melhor desempenho da rede para os usuários e garantir a segurança das informações, a implementação do *Windows 2008 Server*, irá buscar benefícios e monitoramento nas atividades que são geradas através da rede.

O Escritório Contábil São Bento, fundado em 02 de abril de 1991, atualmente com 19 anos de serviços prestados aos clientes, com abertura de empresas, assessoria empresarial, contabilidade, escrita fiscal, recursos humanos, totalmente informatizados e integrados através de um planejamento de recursos empresariais contábil, possui 15 colaboradores, tem em sua carteira mais de clientes 170 clientes, distribuídos nas atividades de indústria, comércio, prestadoras de serviços e associações, classificadas em grandes, médias e microempresas. Desde 18 de Junho de 2003, possui o certificado de aprovação do Selo Catarinense de Qualidade para empresas de serviços contábeis.

1.1 DELIMITAÇÃO DA PESQUISA

Será demonstrado uma implementação do *Windows 2008 Server*, com algumas de suas funcionalidades.

Na parte de fundamentação teórica abordará conceitos sobre o *Windows 2008 Server*, *Active Directory*, *Group Policy* e unidade organizacional demonstrando alguns recursos dessas ferramentas citadas.

O foco principal será demonstrar de uma maneira geral funcionalidades e vantagens que o *Windows 2008 Server* pode oferecer ao administrador da rede, para que o mesmo garanta a segurança e de maneira preventiva evitar que aconteça possíveis aberturas na rede interna que comprometa arquivos ou até mesmo o banco de dados da contabilidade.

1.2 PROBLEMA

Com o decorrer das atividades empregadas no Escritório Contábil São Bento, o gerenciamento se tornou necessário devido ao aumento de colaboradores e como em qualquer ambiente corporativo, alguns contra tempos podem ocorrer ou até mesmo abusos de políticas de segurança cometidos por alguns usuários.

Os arquivos armazenados no servidor de arquivos nenhum deles possui um apontamento ou uma *GPO* que faça o redirecionamento da pasta “Meus Documentos” para uma pasta em específico no servidor. E também a falta de políticas de segurança para estar restringindo alguns tipos de acesso.

Para resolver os problemas em questão será abordado como proceder na criação do redirecionamento de pastas e também como criar políticas restritivas para que o servidor de domínio atenda as necessidades que a empresa pretende alcançar com essas implementações.

1.3 OBJETIVOS

1.4 Objetivo Geral

Fazer uma implementação de políticas de segurança utilizando o sistema operacional *Windows 2008 Server* e utilizar suas ferramentas para criação de *OU* e *GPOS*.

1.5 Objetivos Específicos

Os objetivos específicos são:

- Instalando o *Windows 2008 Server*;
- Configurações de recursos do *Windows 2008 Server*;
- Criação de *OU*, *GPOS*;
- Demonstrar as vantagens e diferenças do servidor configurado devidamente.

1.6 JUSTIFICATIVA

No termino desta implementação poderá ser observado como a rede interna do escritório se encontra melhor organizada e principalmente com diretivas e políticas de segurança.

As mesmas irão ser criadas com o intuito de que cada estação tenha a pasta de “Meus Documentos” apontada para o servidor e algumas restrições para um determinado usuário ou até mesmo um grupo inteiro.

2 WINDOWS 2008 SERVER

O *Windows Server 2008* é a plataforma ideal para construção de uma infraestrutura de aplicações conectadas, redes e *Web Services*, do grupo de trabalho ao *datacenter*. Esse sistema operacional pode fornecer inúmeros benefícios para o administrador de rede. Através do mesmo pode gerenciar, monitorar, usuários, grupos, estações de trabalho e aplicar permissões ou restrições de acordo com a política de segurança implantada pela empresa (*Microsoft TechNet, 2012*).

É o sistema operativo mais robusto desenvolvido pela Microsoft. Projetado para aumentar a confiabilidade e a flexibilidade da sua infraestrutura, altamente dinâmica e escalável, ajuda, simultaneamente, a poupar tempo e a reduzir custos.

Além de fornecer toda a parte gerencial de usuários e estações de trabalho, o mesmo ainda também disponibiliza vários recursos de rede. No caso serviço de *DNS (Domain Name System)*, *DHCP (Dynamic Host Configuration Protocol)*, agendamento de *backup*. Enfim várias ferramentas que facilitam o gerenciamento e monitoramento de uma rede (TORRES, 2001).

É disponibilizado um serviço de monitoramento de sites, onde o administrador pode estar definindo regras de acesso a internet para da cada usuário ou *OU*. No caso do Escritório Contábil São Bento essa ferramenta não foi utilizado pois já possui um *firewall* a parte no qual faz todo o monitoramento, permissões e bloqueios na parte de acessos a Internet (*Microsoft TechNet, 2012*).

2.1 ACTIVE DIRECTORY

O *Active Directory (AD)* é um serviço de diretório nas redes Windows 2008. É um conjunto de atributos sobre recursos e serviços existentes na rede, isso significa que é uma maneira de organizar e simplificar o acesso aos recursos de sua rede centralizando-os; Bem como, reforçar a segurança e dar proteção aos objetos da *database* contra intrusos, ou controlar acessos dos usuários internos da rede

O *Active Directory* mantém dados como contas de usuários, impressoras, grupos, computadores, servidores, recursos de rede, etc. O *AD* pode ser escalonável e hierárquico, ele

dá as opções que certos usuários se tornem administrador do grupo, delegando a esse administrador algumas funções (TORRES, 2001).

O *Active Directory* também inclui (Microsoft TechNet, 2012):

- Um conjunto de regras, o esquema, que define as classes de objetos e atributos contidos no diretório, as restrições e os limites das ocorrências desses objetos e o formato de seus nomes. Para obter mais informações sobre o esquema.

- Um catálogo global que contém informações sobre cada objeto no diretório. Permite aos usuários e administradores encontrarem informações de diretório independentemente de qual domínio do diretório realmente contenha os dados. Para obter mais informações sobre o catálogo global.

- Um mecanismo de consulta e índice para que os objetos e suas propriedades possam ser publicados e encontrados por usuários ou aplicativos da rede.

- Um serviço de replicação que distribui dados de diretório em uma rede. Todos os controladores de domínio em um domínio participam da replicação e contêm uma cópia completa de todas as informações de diretório referentes a seu respectivo domínio. Qualquer alteração nos dados de diretório é replicada para todos os controladores de domínio no domínio.

- Suporte para software cliente do *Active Directory*, que disponibiliza vários recursos do *Microsoft Windows 2000 Professional* ou do *Windows XP Professional* para computadores que executem *Windows 95*, *Windows 98* e *Windows NT Server 4.0*. Para os computadores cliente que não estiverem executando o software cliente do *Active Directory*, o diretório será exibido somente como um diretório do *Windows NT*.

2.2 DOMINIO

O domínio do *Windows 2008* é uma estrutura lógica onde compartilha uma central de serviços e diretórios. A base de dados do diretório contém contas de usuários e segurança da informação do domínio. No Domínio compõe computadores configurados com uma única conta, os usuários podem validar-se no domínio a partir de qualquer máquina (onde se tenha autorização), a partir daí, usufruir dos recursos da rede para os quais o administrador do domínio lhes der permissões (*Microsoft TechNet, 2012*).

O domínio pode conter um grupo local, conta de usuários, computadores para uma melhor organização e administração (6419A *Configuring, Managing and Maintaining Windows Server 2008, 2011*).

Um domínio apresenta várias vantagens:

- Organização de objetos. O uso de unidades organizacionais simplifica a maneira que o domínio é organizado. Através desse recurso é possível estar dividindo o domínio em segmentos ou setores, facilitando assim o gerenciamento e as regras de políticas de segurança implementada.
- A aplicação de um objeto de diretiva de grupo ao domínio consolida o gerenciamento de recursos e segurança. Uma diretiva de segurança (*GPO*) agrega junto a esse volume de recursos necessários para o monitoramento da rede onde o domínio se encontra (6419A *Configuring, Managing and Maintaining Windows Server 2008, 2011*).
- Em cada *OU* pode haver a existência de um administrador daquele grupo, fazendo assim uma descentralização e preocupações por parte do administrador da rede. Esse administrador de grupo pode se ater na organização do grupo em que se encontra e passar para o administrador global algumas sugestões de diretivas.
- Se por ventura a empresa achar necessário dentro da sua empresa a criação de mais um domínio, dentro do mesmo. O administrador terá que elaborar novos usuários, grupos, políticas de segurança. Ou seja, não existe a possibilidade de replicar dados do domínio já criado (*Microsoft TechNet, 2012*).

- Cada domínio armazena somente as informações sobre os objetos nele localizados. Se você fizer a partição do diretório dessa forma, o *Active Directory* poderá ser dimensionado para um grande número de objetos (TORRES, 2001).

2.3 UNIDADES ORGANIZACIONAIS (OU)

Unidades Organizacionais é uma ferramenta que funciona juntamente com o domínio, facilita a organização de usuários, podendo distribuir os mesmos por setor ou como o administrador achar melhor a distribuição das *OUs*. Podem conter usuários, computadores, grupos e até mesmo outras *OUs*.

Cria limites administrativos dentro do domínio atribuindo autoridade, recipientes de modelos de estrutura lógica. Facilita a aplicação de diretivas de segurança. Ou seja, em cada *OU* pode se aplicar diferentes diretivas de segurança, conforme a necessidade que o administrador de rede achar conveniente e de acordo com as políticas de segurança necessárias (6419A *Configuring, Managing and Maintaining Windows Server 2008, 2011*).

2.4 GPO (GROUP POLICY)

Group Policy(GPO), é capaz de mudar configurações, restringir ações ou até mesmo distribuir aplicações em seu ambiente de rede. As vantagens são muitas, e podem ser aplicadas em sites, domínios e *organizational units(OUs)*. Uma vez criada uma *OU* para um determinado setor poderá estar sendo configurada uma *GPO* exclusiva para aquele setor. Ou seja, pode ter várias *OUs* para cada setor e uma *GPO* que irá atender as necessidades, permissões ou restrições. Deixando várias opções para o administrador de rede definir que tipo de política de segurança ele vai tomar com cada setor em questão (*Microsoft TechNet, 2012*).

Grande parte dos itens de uma *GPO* tem 3 diferentes opções:

Habilitado: Especifica que aquele item será ativado.

Desabilitado: Especifica que aquele item será desativado.

Não Configurado: Deixa a opção neutra, nem ativa e nem desativa o item, ou seja, fica como está agora. Esta é a configuração padrão.

Segue um exemplo:

Para desabilitar o gerenciador de tarefas de todos os desktops da rede. Para isso existe um item chamado Remover Gerenciador de Tarefas, a configuração default para esse item é Não Configurado.

Caso configurado como Habilitado, o Gerenciador de Tarefas será desativado e configurado como Desabilitado, será ativado explicitamente.

Pode parecer estranho o Habilitado remover uma função, mas pode ser observado que a opção é “Remover o Gerenciador de Tarefas”, ou seja, o Habilitado está ativando a opção “Remover o Gerenciador de Tarefas”.

As configurações das *GPOs* podem ser aplicadas em dois tipos de objetos do *Active Directory*: Usuários e Computadores, desde que estejam em uma *OU*. Se houver algum conflito entre as configurações dos computadores e dos usuários, as configurações dos usuários vão prevalecer. (*Microsoft TechNet*, 2012)

Os tipos de configurações que podem ser feitas estão descritas abaixo:

Configuração do Computador: O administrador pode definir que tipo de acesso o usuário terá acesso, ou seja, se ele poderá ou não ter acesso a USB ou drive de CD.

Configuração do *Windows*: O administrador define qual é a maneira que o usuário final irá utilizar a estação de trabalho. Definindo que tipo de acesso ele terá ao sistema operacional.

Exemplificando: Nos computadores, pode criar uma rotina que ao fazer o *logon* no *Windows* automaticamente já inicialize a calculadora e o bloco de notas. Nos usuários pode bloquear o *download* no *Internet Explorer*.

Modelos Administrativos: Também são diferentes as opções para computadores e usuários.

Por exemplo: Customizar o que pode ser usado ou não no painel de controle, que tipos de programas vão estar presente no menu iniciar (6419A *Configuring, Managing and Maintaining Windows Server 2008, 2011*).

3 IMPLEMENTAÇÃO

3.1 INSTALANDO O *WINDOWS 2008 SERVER*

Com o sistema operacional *Windows 2008 Server* instalado e o mesmo operacional, o administrador da rede logo ao iniciar terá um menu no qual poderá inserir as funcionalidades que melhor irá atender a sua rede.

Nesse menu irá conter diversas funções que o servidor pode vir a exercer na rede, contendo algumas funcionalidades que na hora da primeira execução do sistema operacional já é possível deixar configurado. No caso do servidor do Escritório Contábil São Bento foi optado por instalar o servidor de *DNS (Domain Name System)*. A função de *DHCP (Dynamic Host Configuration Protocol)* ficou desabilitada devido ao fato do administrador ter optado por configurar as estações com *IP (Internet Protocol)* estático). Essa opção partiu da idéia para um melhor controle por parte do administrador que esses *IPs* fossem estáticos, fazendo com que o mesmo na hora de algum tipo de problema com a estação com determinado *IP* saiba de forma eficaz e rápida de qual estação está com algum tipo de problema.

A figura 1 ilustra quais os serviços que o mesmo já possui instalado.

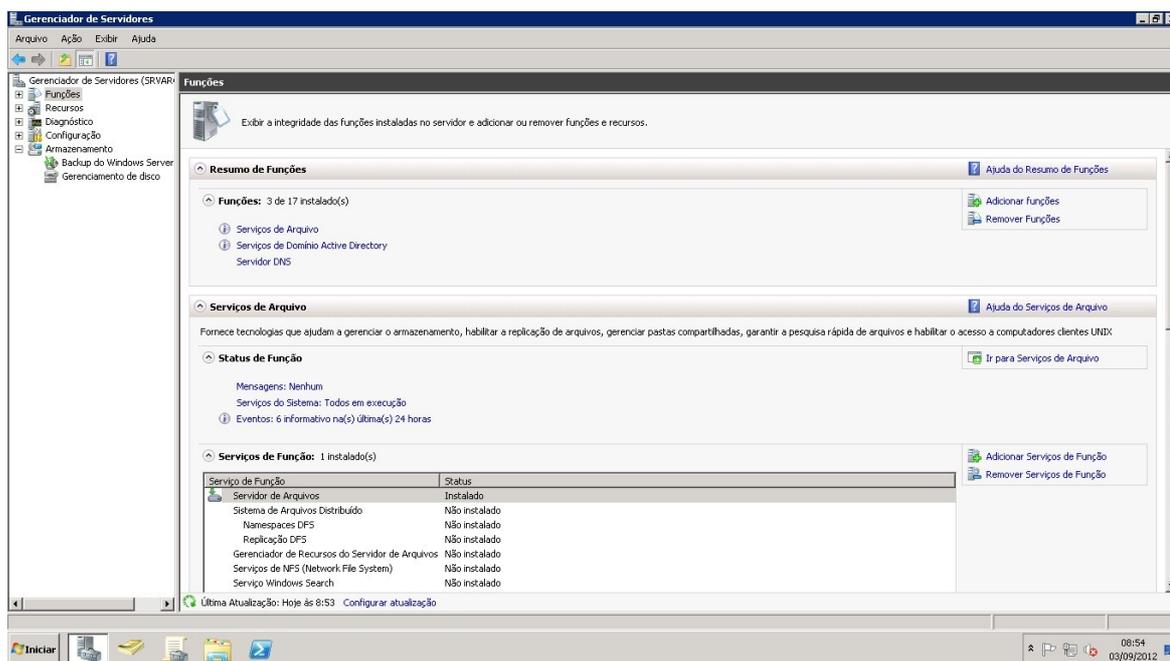


Figura 1: Serviços instalados no *Windows 2008 Server* [Autoria Própria]

Pode ser observado que o servidor possui os seguintes serviços/funções instalados: Serviços de Arquivo, Serviços de Domínio *Active Directory* e Servidor *DNS*.

O Servidor de Arquivo trabalha junto com a *GPO*, no qual é possível fazer que as pastas de cada usuário sejam redirecionadas para o servidor e como o mesmo já possui rotina de *backup* esse procedimento garante integridade total dos arquivos armazenados dentro dessa pasta com redirecionamento.

Consta o serviço de domínio do *Active Directory*, que é através do mesmo onde irão ser criados todos os usuários do domínio (esse mesmo já foi criado na hora da ativação do *active directory*), juntamente com as *OUs* de cada setor dentro da empresa.

3.2 CRIANDO UMA *OU* NO *ACTIVE DIRECTORY*

De acordo com o livro *Configuring, Managing and Maintaining Windows 2008 Server 2008* Volume 1, as *OUs* tem objetivo simples organizar o *AD*. Uma vez criado poderá conter dentro dela: usuários, grupos, computadores e outras *OUs*. A partir do momento em que a mesma está criada, em cada *OU* poderá conter uma determinada *GPO* para um usuário, grupo ou computador. Isso facilita a administração e manutenção das diretivas de segurança aplicadas.

Diante dos fatos pode aplicar uma diretiva para um único usuário, ou se for o caso aplicar a diretiva para todo um grupo, fazendo assim que todos os usuários dentro daquele grupo já estejam submetidos à diretiva aplicada naquela *OU*.

Para a criação de uma *OU*, utilizar a ferramenta administrativa Usuários e Computadores do *Active Directory*. A figura 2 retrata como é feito o procedimento de criação.

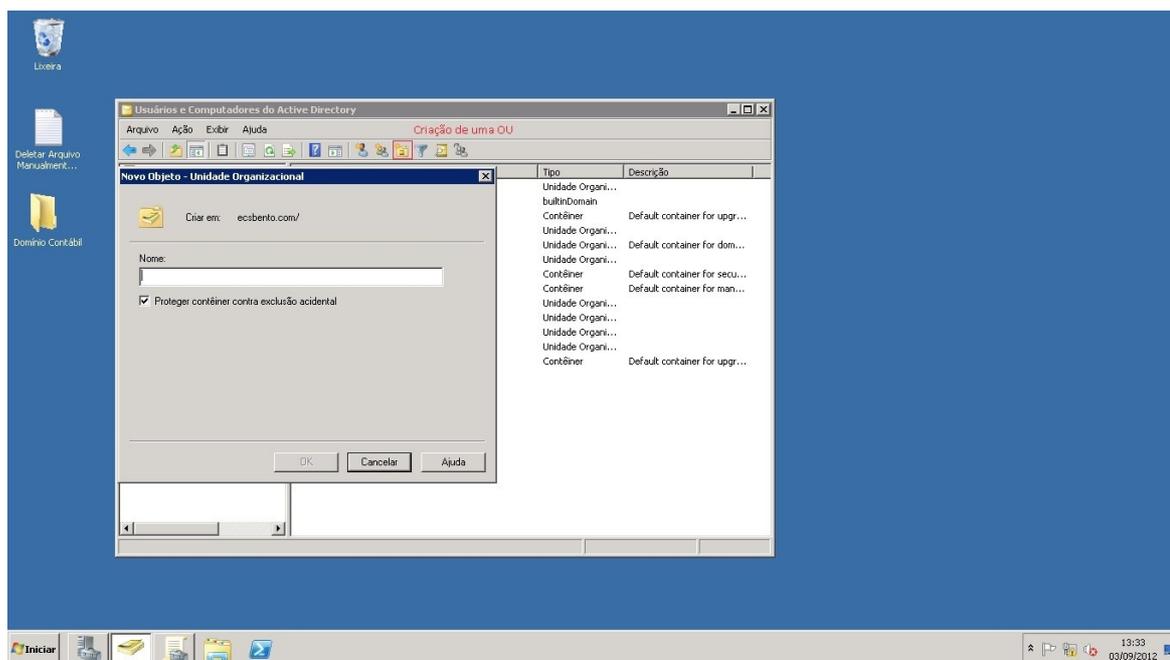


Figura 2: Criando uma *OU* [Autoria Própria]

Clicando no ícone grifado na figura 2, irá surgir uma caixa de mensagem onde deverá definir o nome da *OU*

No Escritório Contábil São Bento foram adotadas seis *OUs* separadas por setor e uma para o acesso remoto, distribuído da seguinte maneira:

- Administração;
- Contábil;
- Fiscal;
- Recepção;
- Remoto;
- RH;
- TI.

A figura 3 demonstra como é organizado as *OUs*.

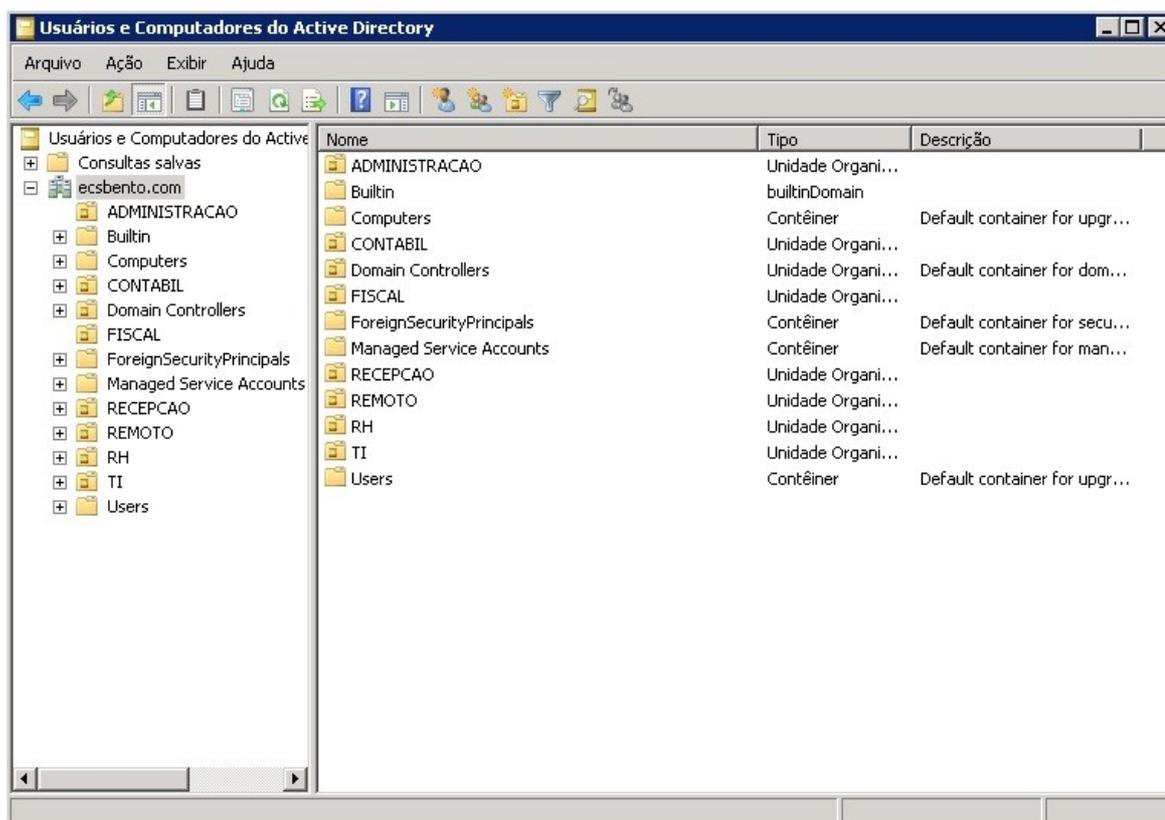


Figura 3: Organização das OUs [Autoria Própria]

Uma vez pronta, cabe ao administrador criar os usuários e grupos para determinada OU e que posteriormente seja alocada as diretivas de segurança de acordo com a necessidade de cada situação.

3.3 CRIANDO UM USUÁRIO NO ACTIVE DIRECTORY

Segundo o *site Microsoft TechNet*, o Console de Gerenciamento Microsoft contém ferramentas para administrar redes, computadores, serviços e outros componentes do sistemas. Utiliza-se da interface gráfica GUI – Interface Gráfica do Usuário.

Conforme figura 4 demonstra como incluir um usuário no AD utilizando o Console de Gerenciamento.

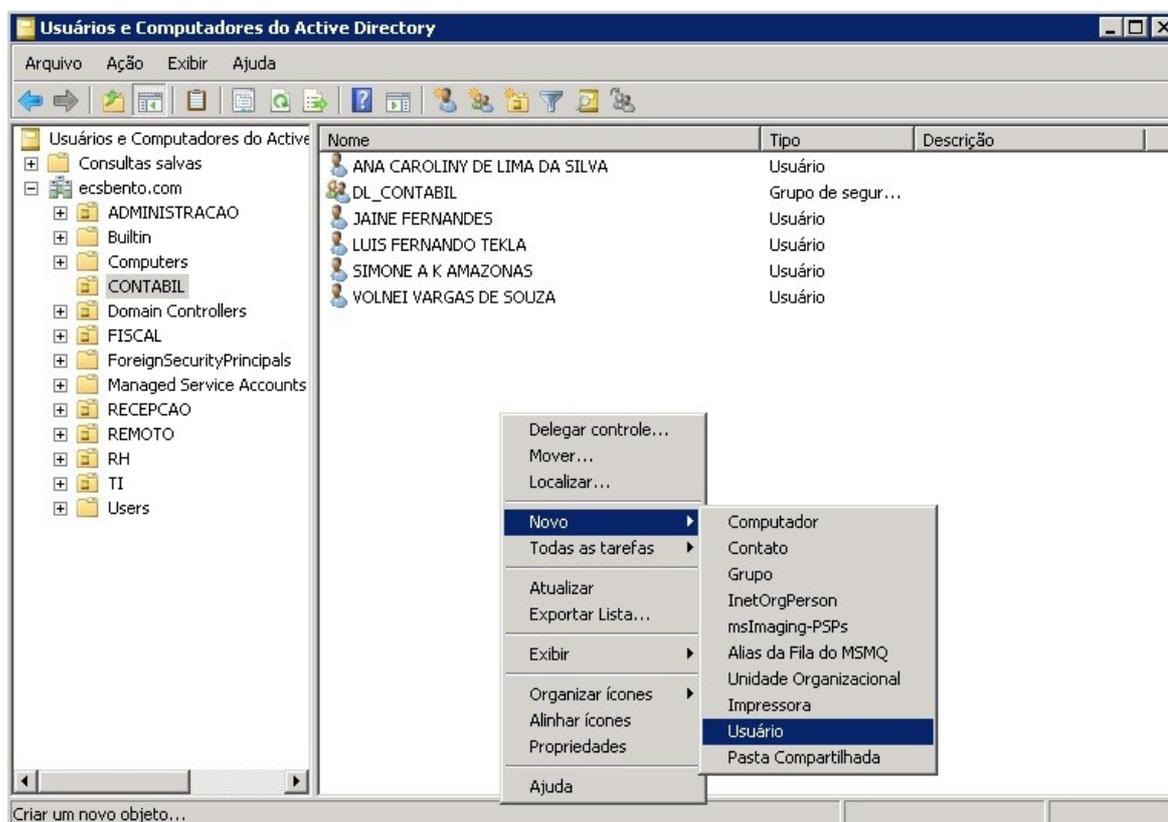


Figura 4: Inclusão de uma conta de usuário no AD [Autoria Própria]

Para efetuar a inclusão de novos usuários o administrador de rede deve seguir os seguintes passos:

- Abrir o Usuarios e Computadores do *Active Directory*;
- Localizar a *OU* no qual irá adicionar o novo usuário;
- Clicar com o botão direito do mouse, em novo, usuário;
- Definir conta do usuário.

A figura 5 demonstra a continuidade da criação do usuário.

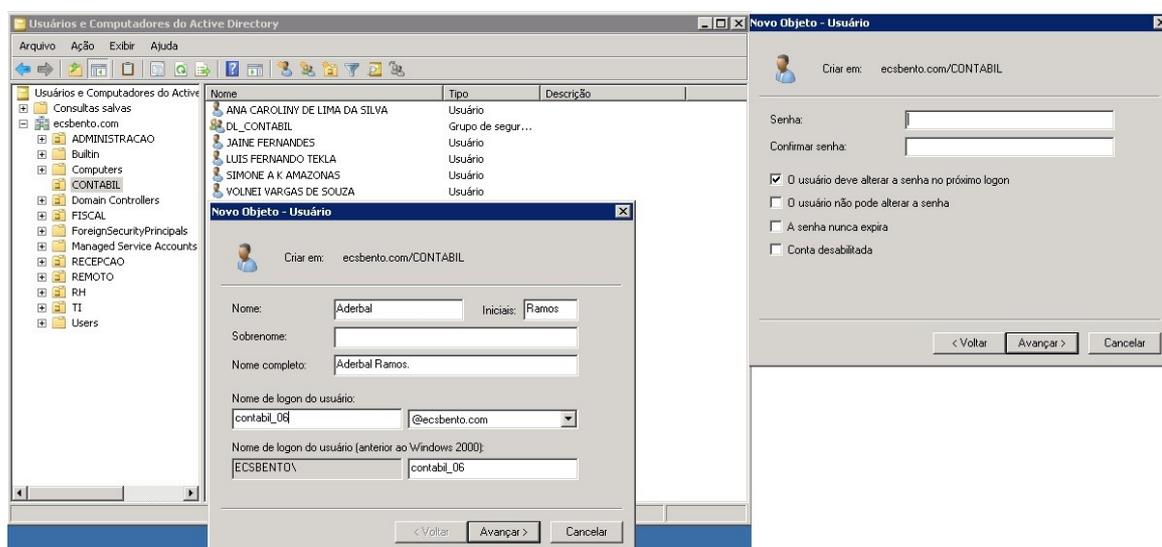


Figura 5: Dados do usuário e conta [Autoria Própria]

Pode ser observado na figura 5 Nome, Sobrenome. O campo Nome Completo é preenchido automaticamente. Outro campo a ser completado é o Nome de *logon* de usuário. Muitos preferem nessa parte inserir o nome do usuário para o *logon*.

No Escritório Contábil São Bento foi optado em inserir o Nome de *Logon* o nome da estação de trabalho, isso foi decidido pensando em uma possível rotatividade de colaboradores ou até mesmo o remanejamento de um colaborador para outro setor, ou seja, caso tenha alguma mudança o administrador irá se preocupar apenas em mudar o nome da pessoa que assumiu aquela estação de trabalho, não havendo assim a necessidade da criação de mais um usuário no *AD*.

Na parte final o administrador opta se vai definir algum tipo de senha padrão tratado diretamente com o usuário da estação. Existe mais umas opções que o administrador vai habilitar ou não, que são elas:

- O usuário deve alterar a senha no próximo *logon*. Ou seja, o administrador definiu uma senha padrão o usuário por segurança muda a senha que lhe convém.
- O usuário não pode alterar a senha. Nesse caso o administrador define que a senha padrão não poderá ser alterada.
- A senha nunca expira. A senha por padrão tem um prazo 42 dias, habilitando essa opção a senha definida nunca irá expirar

- Conta Desabilitada. Utilizada no caso se algum colaborador vier a se afastar da empresa por um período e o administrador por motivo de organização e segurança desabilita a conta até o retorno da mesma.

Feito esses procedimentos a criação do usuário dentro do *active directory* estará concluída e o mesmo já poderá ser enquadrado dentro de grupo na própria *OU*.

3.4 CRIANDO UM GRUPO NO ACTIVE DIRECTORY

Para a criação de um grupo deverá acessar a ferramenta Usuários e Computadores do Active Directory, acessar uma *OU* e criar o grupo conforme a figura 6.

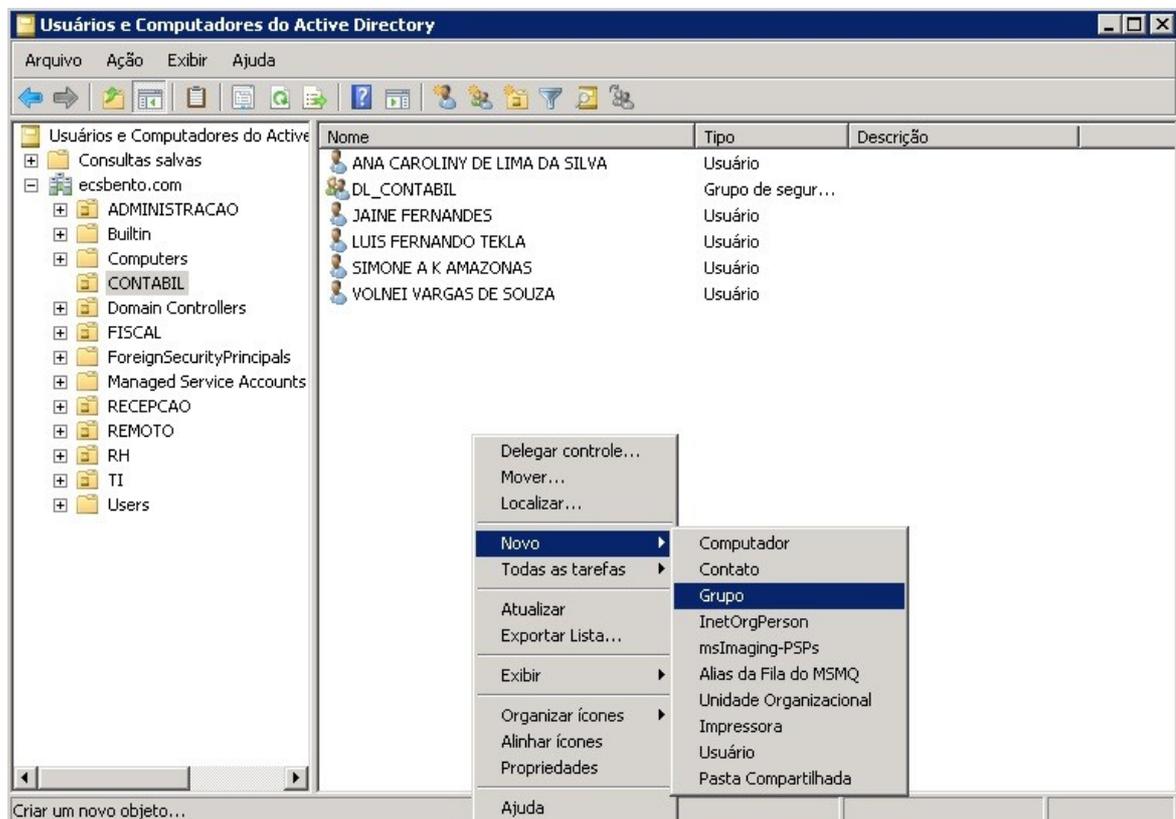


Figura 6: Criação de Grupo na OU [Autoria Própria]

Após esses passos conforme a figura 7 irá pedir para confirmar o nome do grupo e por padrão definir que aquele grupo vai ser Global, para estar participando do domínio em um todo.

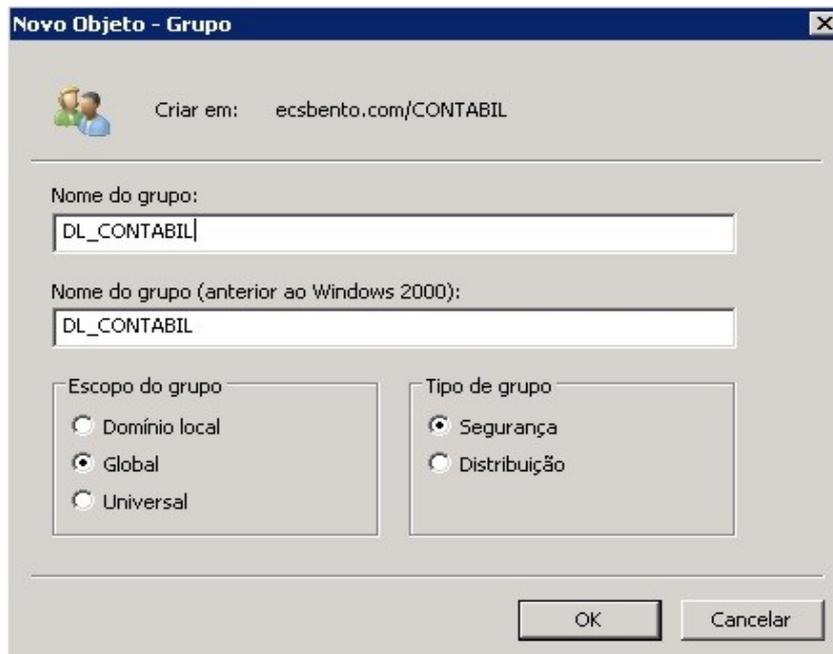


Figura 7: Nomeando o grupo [Autoria Própria]

O grupo ele trará o benefício de poder aplicar uma diretiva de segurança para todos aqueles que estejam usuários estejam alocados dentro desse grupo. A figura 8 demonstra como fazer tal procedimento.

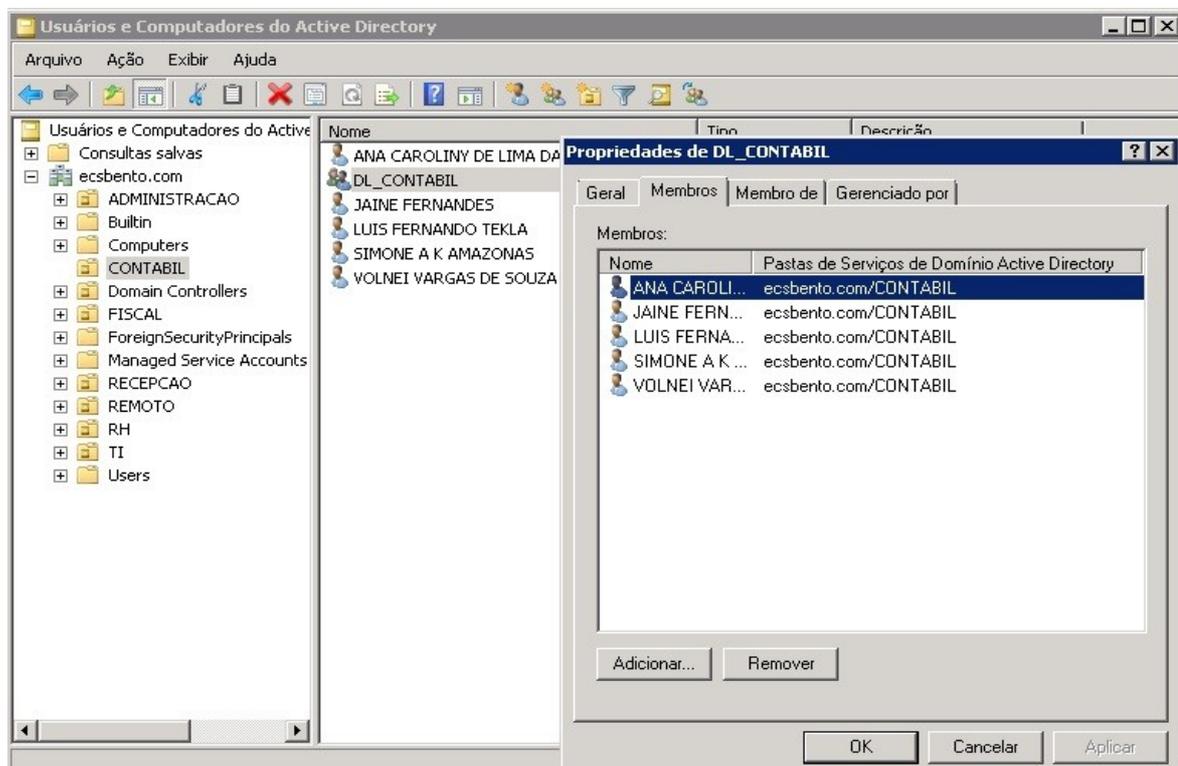


Figura 8: Alocando usuários dentro de um grupo [Autoria Própria]

Para efetuar a alocação dos usuários criados dentro da *OU* no grupo, no caso do DL_CONTABIL. Executar os seguintes passos:

- Duplo clique no DL_CONTABIL;
- Acessar a guia Membros;
- Clicar na opção Adicionar;
- Adicionar os usuários da respectiva *OU*.

Com essas etapas concluídas cada setor já tem sua *OU* criada com seus respectivos usuários e grupos criados. Sendo assim o próximo passo é criar *GPOS* e definir para cada grupo ou usuário qual diretiva de segurança será aplicada de acordo com a necessidade de cada um.

3.5 CRIAÇÃO DE *GPO*

Com todos os procedimentos já explicados, o *AD* já tem os recursos necessários para que as *GPOS* sejam criadas de acordo com cada *OU*. Com essas diretivas de segurança segundo o *site TechNet* podem ser definidas varias situações para os usuários finais. Permissões, bloqueios, acessos a unidades de *CD*, *pen drive*, unidades de disco. Enfim cabe ao administrador analisar cada setor e definir quais os bloqueios e permissões que cada *OU* deve conter.

3.5.1 *GPO* REDIRECIONAMENTO DE PASTA

Uma *GPO* que foi implementada no Escritório Contábil São Bento é a redirecionamento de pasta. A função dela é muito simples e extremamente funcional para a organização dos documentos de todas as estações ligadas ao domínio. Essa *GPO* permite que a centralização dos arquivos no servidor de arquivos, ainda podendo separar as pastas por *OU* e também restringir quem pode ter acesso aquelas pastas ou não. Facilitando também a cópia de segurança dessas pastas, pois todas vão estar em um único lugar.

O primeiro passo é criar uma pasta onde irá ser armazenada as pastas de cada *OU* que no caso foi a pasta “Documentos” dentro dessa mesma pasta foi criada outras com o nome de cada *OU* que tenho cadastrada dentro do *AD* como pode ser observado na figura 9.

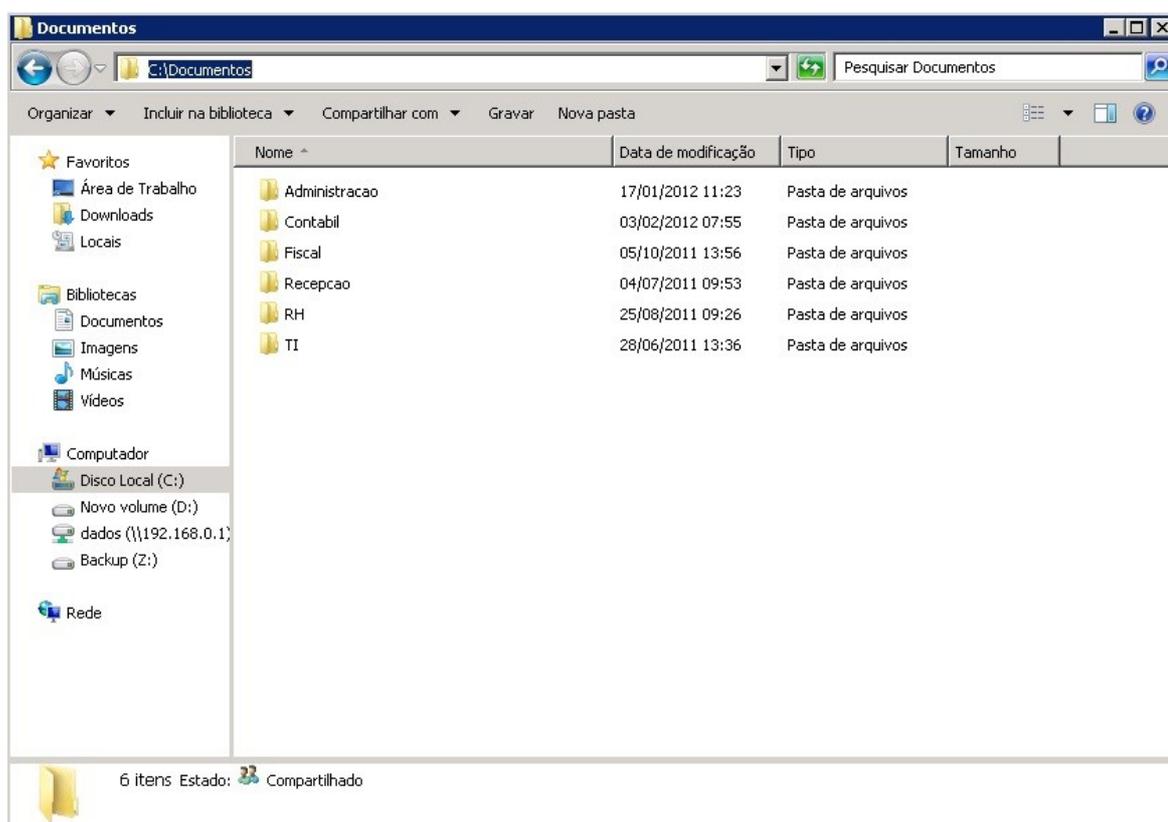


Figura 9: Documentos compartilhados para *OU* [Autoria Própria]

Após a criação das pastas para cada *OU*, deverá entrar em cada pasta e definir nela a permissão que cada *OU* terá permissão para acessar a pasta do setor que cada usuário pertence. Por exemplo, os usuários cadastrados na *OU* contábil, terão acesso apenas na pasta contabil, fazendo assim que apenas o setor consiga ter acesso aos arquivos de cada usuário do grupo, ou ainda se o administrador achar necessário restringir o acesso apenas para o usuário não dando permissão para os demais do grupo (que não será o caso demonstrado).

Conforme a figura 10 demonstra como é feita a liberação de acesso da pasta de cada usuário ao grupo que pertence.

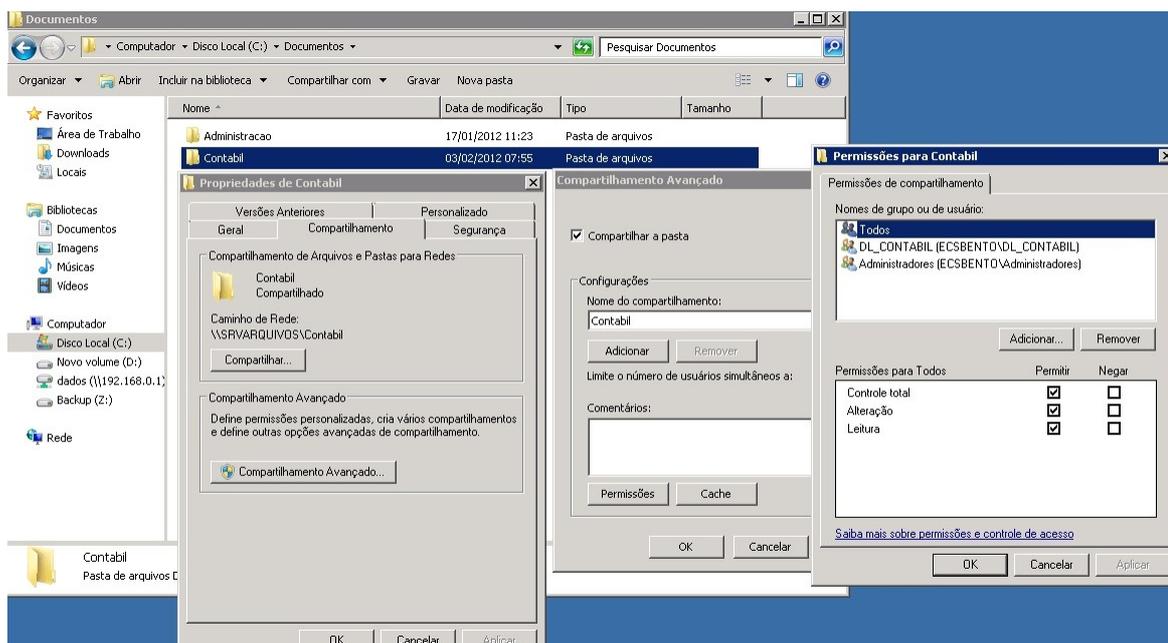


Figura 10: Permissão para o grupo DL_CONTABIL [Autoria Própria]

Para a fazer o compartilhamento para o grupo DL_CONTABIL deve seguir os seguintes passos:

- Localizar a pasta Documentos, posteriormente a pasta Contabil;
- Clicar com o botão direito do mouse na opção Propriedades;
- Acessar a opção Compartilhar, para que essa pasta seja compartilhada;
- Acessar a guia Compartilhamento e por sua vez Compartilhamento Avançado;
- Na tela seguinte acessar a opção Permissões;
- E na ultima tela acessar a opção Adicionar... e posteriormente conceder a permissão de compartilhamento para o grupo DL_CONTABIL, como pode ser observado na figura 10.

Feito esse procedimento irá ser feito a *GPO* na qual irá fazer o redirecionamento da pasta Meus Documentos da estação de trabalho aponte para essa pasta que foi criada no servidor de arquivos.

O próximo passo é abrir a ferramenta administrativa Gerenciamento da Diretiva do Grupo, onde lá estará todas as *OU* criadas e uma por uma vou definir essa diretiva de redirecionamento de pasta. A figura 11 demonstra como é a tela dessa ferramenta.

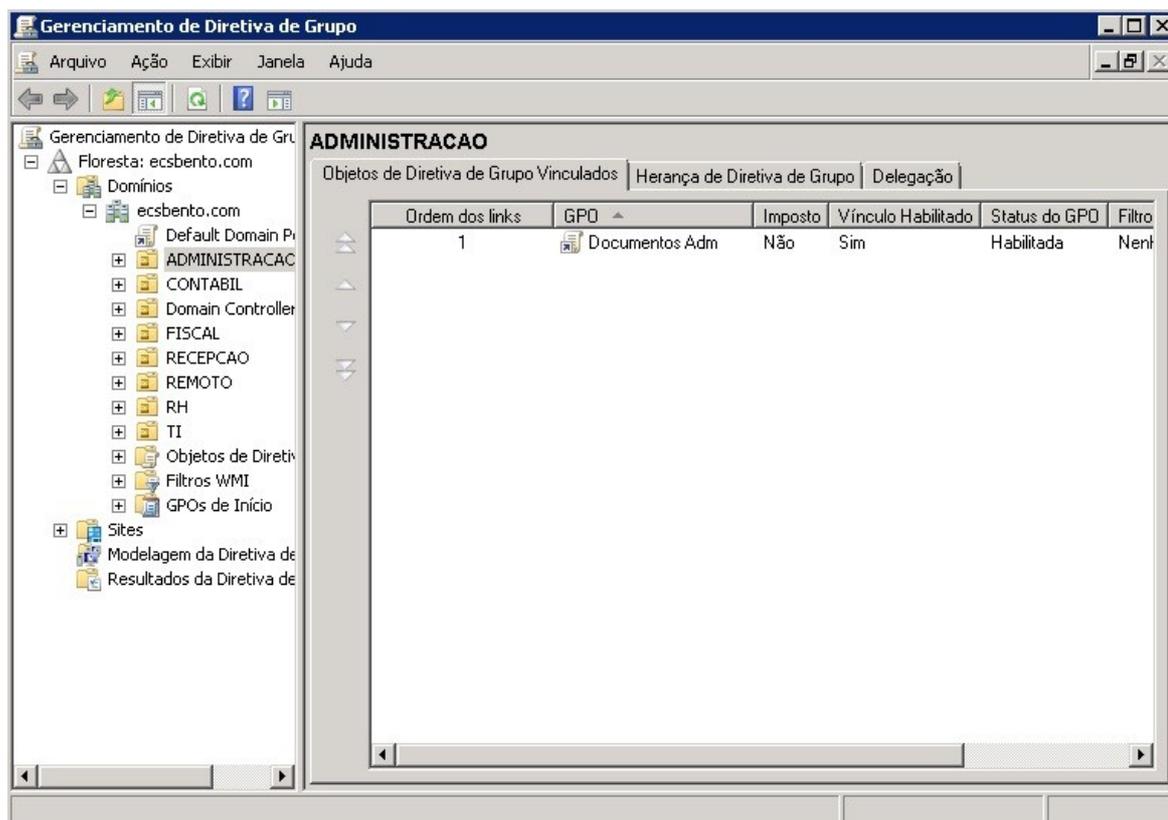


Figura 11: Gerenciamento de Diretiva de Grupo [Autoria Própria]

Com o conhecimento da ferramenta deverá seguir os passos para a criação da diretiva:

- Clicar com o direito do mouse na *OU* desejada selecionar a opção Criar um *GPO* nesse domínio e fornecer um *link* para ele aqui...;
- Nomear a *GPO*, no caso Documentos Adm (observar a figura 9);
- Clicar com o direito do mouse em Documentos Adm, na opção Editar.

Depois de concluído esse procedimento uma nova tela surgirá onde serão fornecidas as informações necessárias para o redirecionamento. A figura 12 demonstra o caminho a ser seguido até onde irá ser configurado o redirecionamento de pasta para a *OU* deseje.

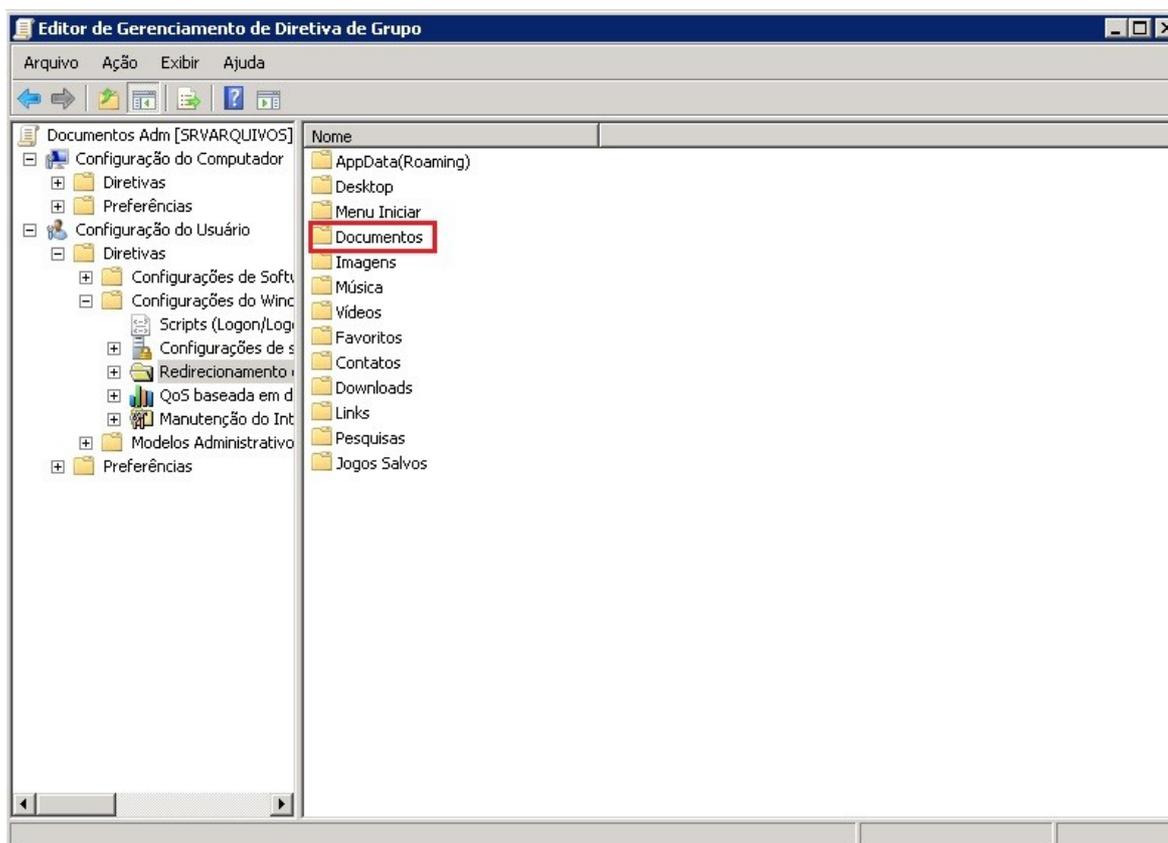


Figura 12: Diretiva redirecionamento de pasta [Autoria Própria]

Para chegar na configuração dessa diretiva deverá seguir os seguintes passos:

- Configuração de usuário;
- Diretivas;
- Configurações do Windows;
- Redirecionamento de Pasta;
- Documentos;
- Clicar com o botão direito do mouse em Documentos e ir à opção propriedades;

Nas propriedades é possível fazer o redirecionamento em questão, mas para que isso aconteça deverá observar a figura 13.

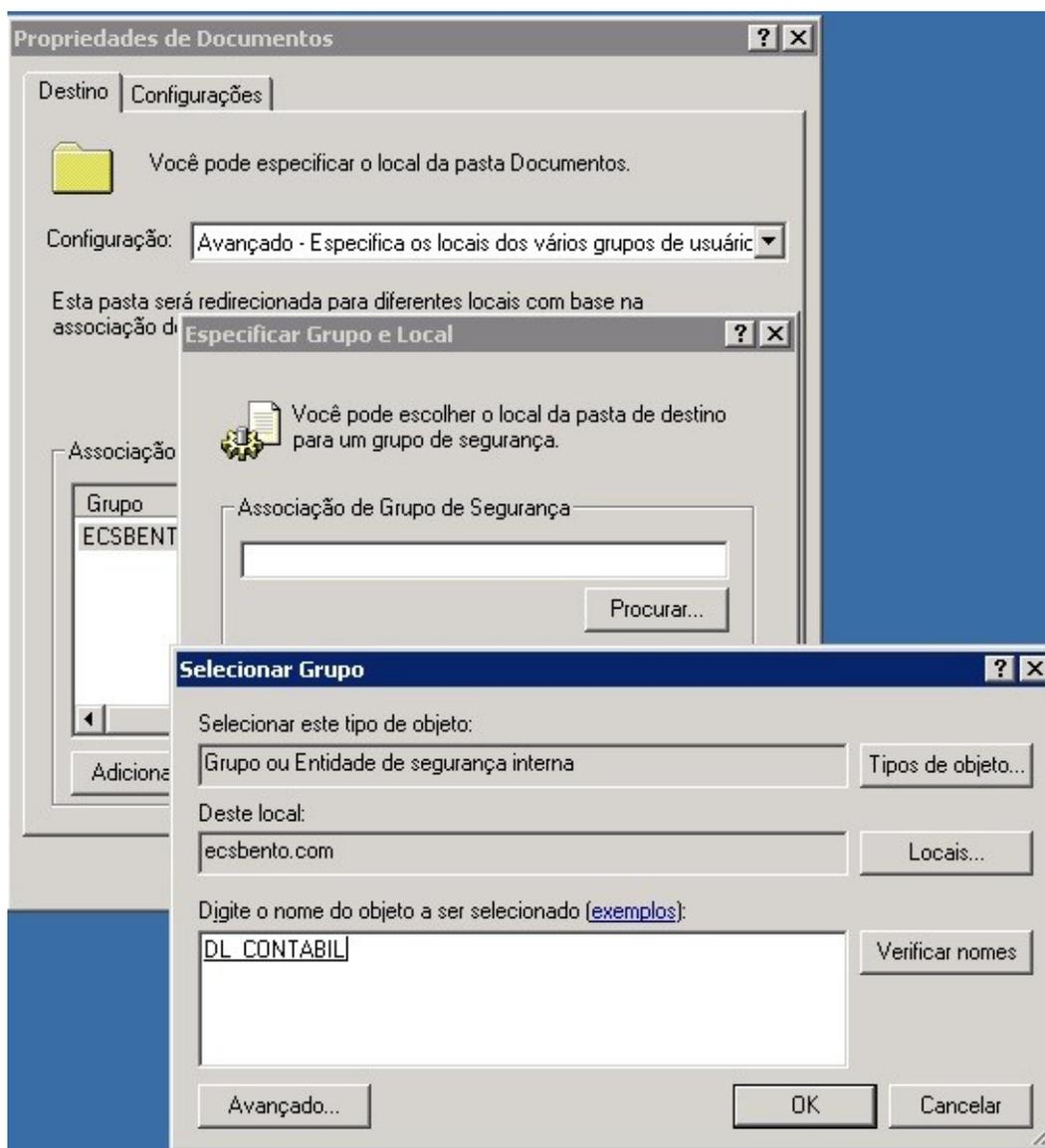


Figura 13: Definindo o local de redirecionamento [Autoria Própria]

Os procedimentos para o redirecionamento da pasta de armazenamento são os seguintes:

- Configuração;
- Selecionar a opção: Avançado – Especifica os locais dos vários grupos de usuários;
- Clicar no botão Adicionar;
- Na próxima tela no campo Associação de Grupo de Segurança, clicar na opção procurar;
- Deverá agora selecionar a qual *OU* em questão terá o redirecionamento de pasta, conforme figura 11 o setor selecionado foi o contábil.

Uma vez definido a *OU* no qual teve o redirecionamento feito através da diretiva, na tela de configuração poderá ver que o mesmo já definiu o caminho que a pasta Documentos irá ter quando o usuário fizer o *logon* no domínio. A figura 12 mostra o caminho em questão.

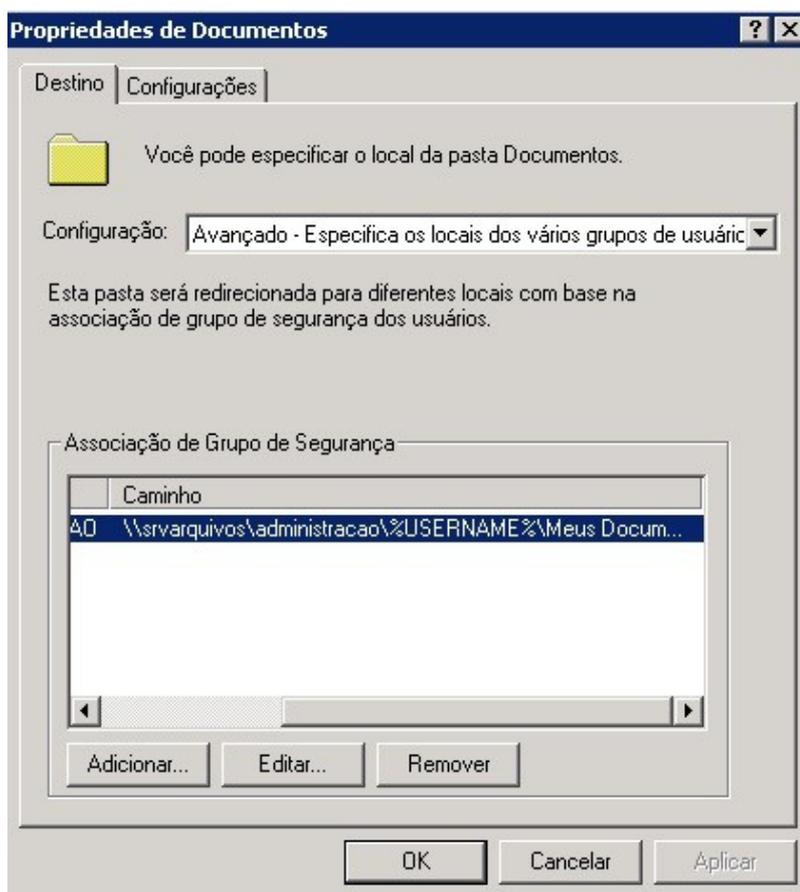


Figura 14: Local de armazenamento [Autoria Própria]

O caminho definido em questão como pode ser observado na figura 12 ficou da seguinte maneira `\\srvarquivos\administracao\%username%\Meus Documentos`. O termo `%USERNAME%` referencia o usuário que a diretiva irá apontar. Por exemplo, o usuário `administracao` logou no domínio pela primeira vez com a diretiva de redirecionamento de pasta ativa, a mesma irá configurar o caminho que será `\\srvarquivos\administracao\administracao\Meus Documentos`. Então para cada usuário configurado dentro de uma determinada *OU* a expressão citada será o nome do usuário logado no domínio.

Para concluir a parte de redirecionamento fica o exemplo do caminho configurado na estação do usuário que tem essa diretiva ativa e funcional conforme figura 14.

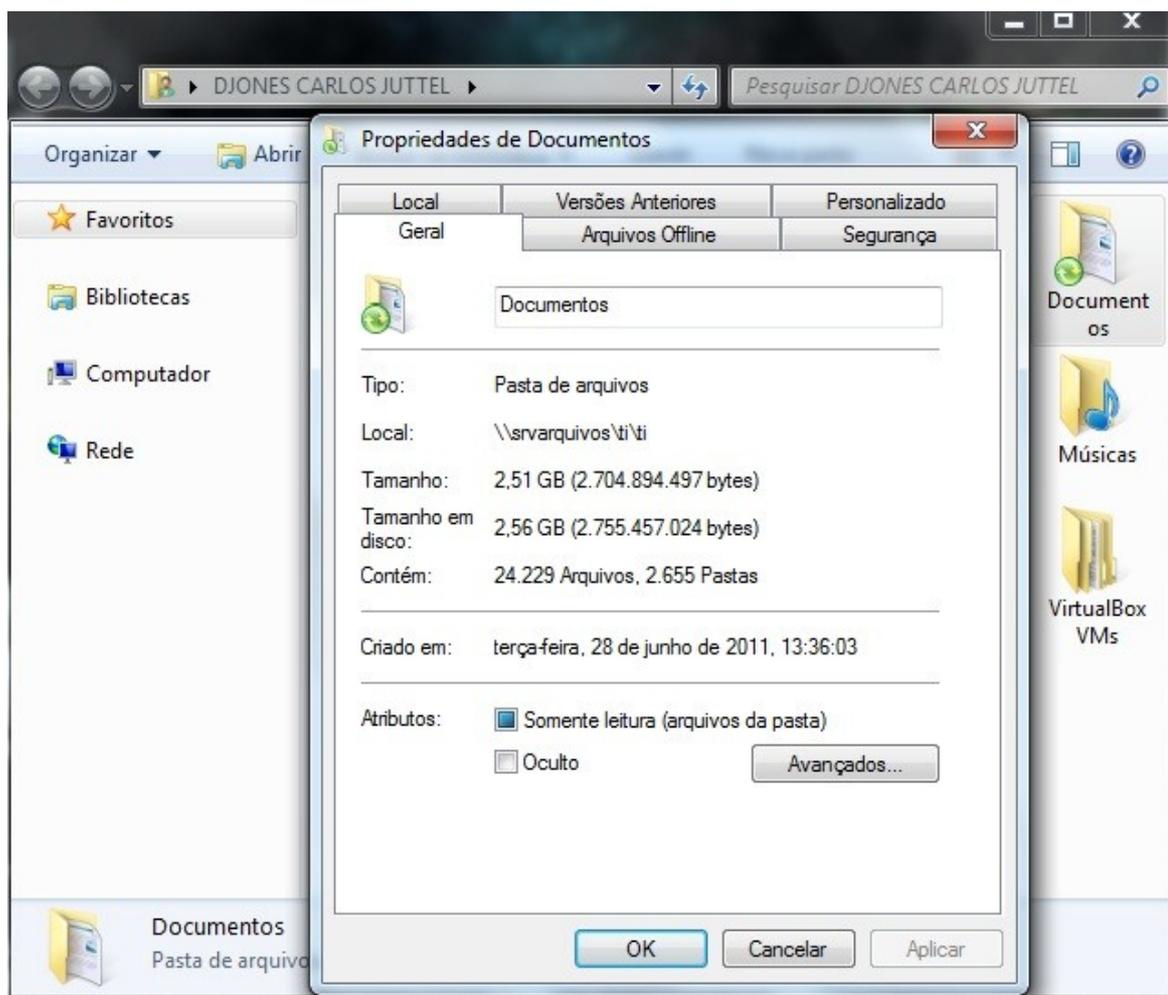


Figura 15: Usuário final redirecionamento [Autoria Própria]

A figura 15 mostra como fica o redirecionamento da pasta Meus Documentos, onde pode se observar que o local aponta para o servidor e para a pasta do usuário.

Com essa diretiva de redirecionamento de pasta o administrador passa a ter um maior controle do conteúdo que cada usuário aloca dentro do seu servidor de arquivos e também facilitando muito o processo de *backup*, que uma vez armazenado da forma correta utilizando a ferramenta que o *Windows 2008 Server* disponibiliza todos os documentos contidos na pasta raiz estarão devidamente seguros.

3.5.2 GPO PARA RESTRIÇÕES

As diretivas de segurança trazem vários tipos de restrições que podem ser aplicadas a um usuário do domínio. Determinadas restrições tem o intuito de fazer com o que o usuário não tenha acesso a alguns recursos ou componentes do *Windows*.

No Escritório Contábil São Bento foi criada uma diretiva de segurança para o usuário remoto. É através desse usuário que será feita possíveis conexões remotas. Foi decidido que esse usuário só teria acesso a dois programas. Qualquer outro tipo de recurso do *Windows* desabilitado para garantir a integridade do e das informações.

Então o primeiro passo dado foi criar uma *OU* com nome de remoto e também a criação do usuário remoto. A partir disso foi iniciado o processo de criação da *GPO* aplicativos, onde nela será configurado permissões e restrições que esse usuário irá ter.

3.5.3 GPO PARA OCULTAR UNIDADES DE DISCO

Para garantir a integridade das informações ou que o usuário que for fazer o acesso remoto não tenha acesso a nenhum tipo de arquivo das unidades de disco, essa diretiva ela é de grande valia. Ela dá a opção de ocultar as unidades de disco existente no computador e se o usuário for do tipo mais avançado, mesmo que ele tente utilizar o executar do *Windows* outra diretiva impede que o mesmo tenha acesso à unidade que alguém venha tentar ter acesso.

O administrador deve utilizar o editor de diretivas de grupo, selecionar a *OU* vincular a ela a *GPO* aplicativos, clicar com o direito do mouse na opção editar e seguir os seguintes passos:

- Configurações do Usuário;
- Diretivas;
- Modelos Administrativos;
- Componentes do Windows;
- Windows Explorer;
- Oculta essas unidades especificadas em Meu Computador.

A figura 16 demonstra como é determinada a execução dessa diretiva, que por opção restringiu todas as unidades de disco.

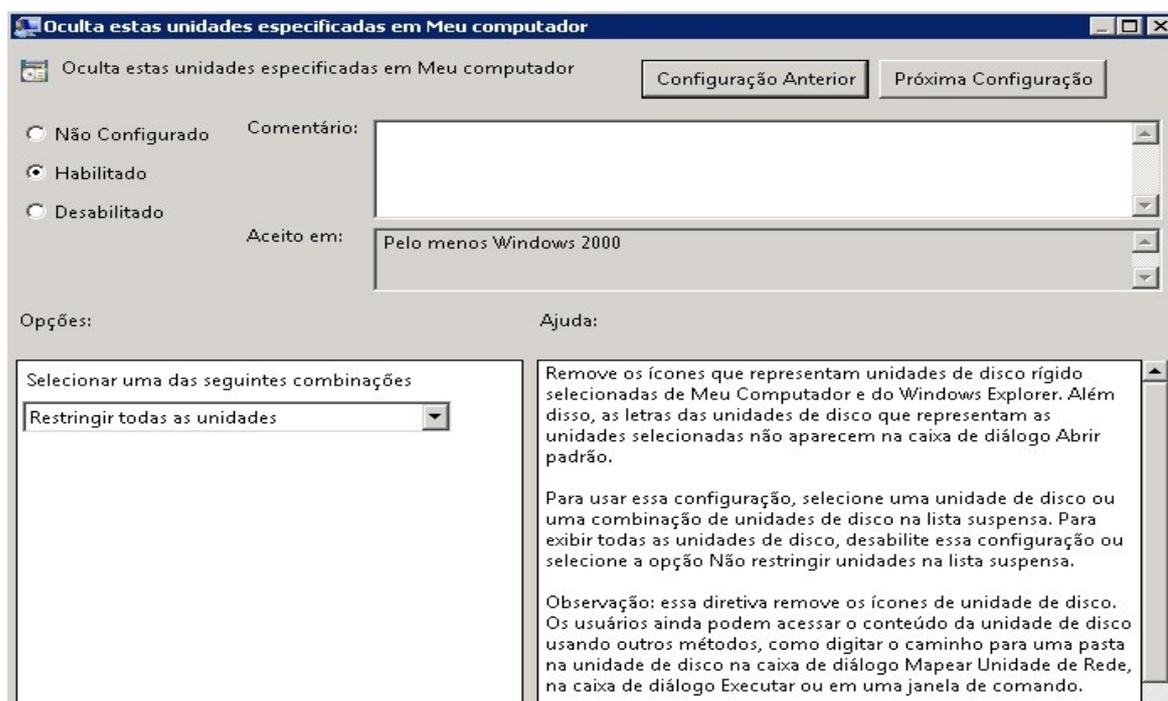


Figura 16: Ocultado unidade de disco [Autoria Própria]

E para complementar essa diretiva, para impedir o acesso a unidades de rede, o procedimento é o mesmo para ocultar a unidade de disco, porém acessando a opção impedir o acesso a unidades do Meu Computador, de acordo com a figura 17.

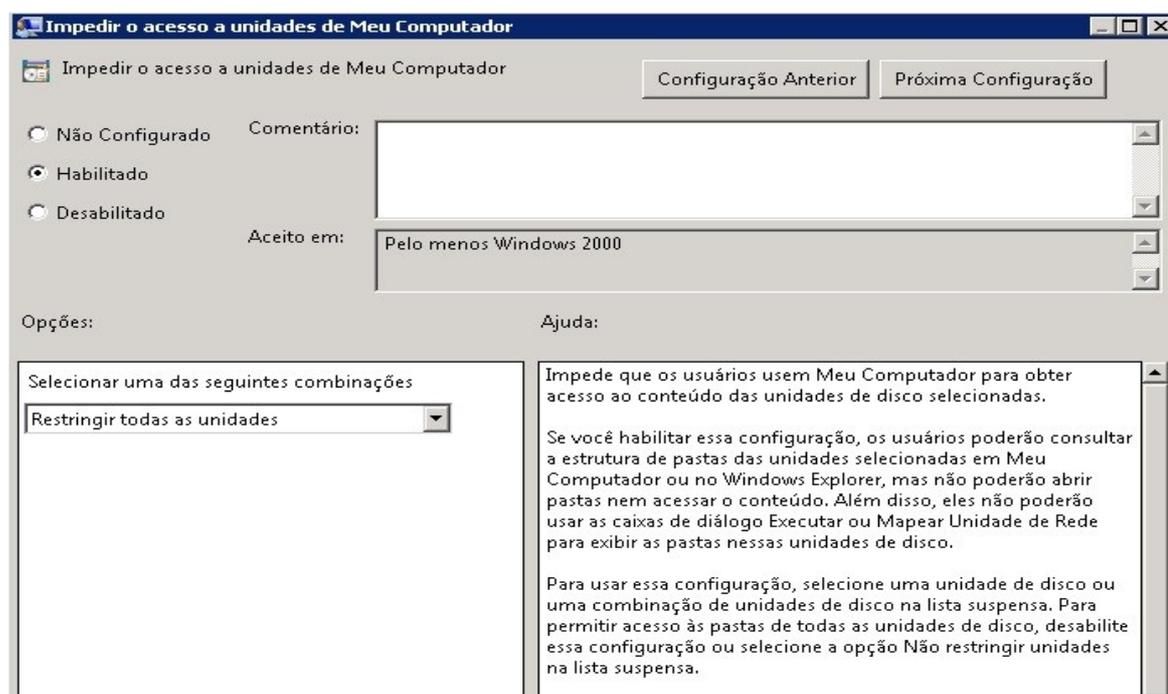


Figura 17: Impedir acesso as unidades de disco. [Autoria Própria]

Feito essas duas diretivas o usuário remoto quando for tentar acessar através do Meu Computador não conseguirá visualizar e muito menos acessar as unidades de disco daquele computador. A figura 18 demonstra a tela que surge para o usuário remoto no momento do acesso.

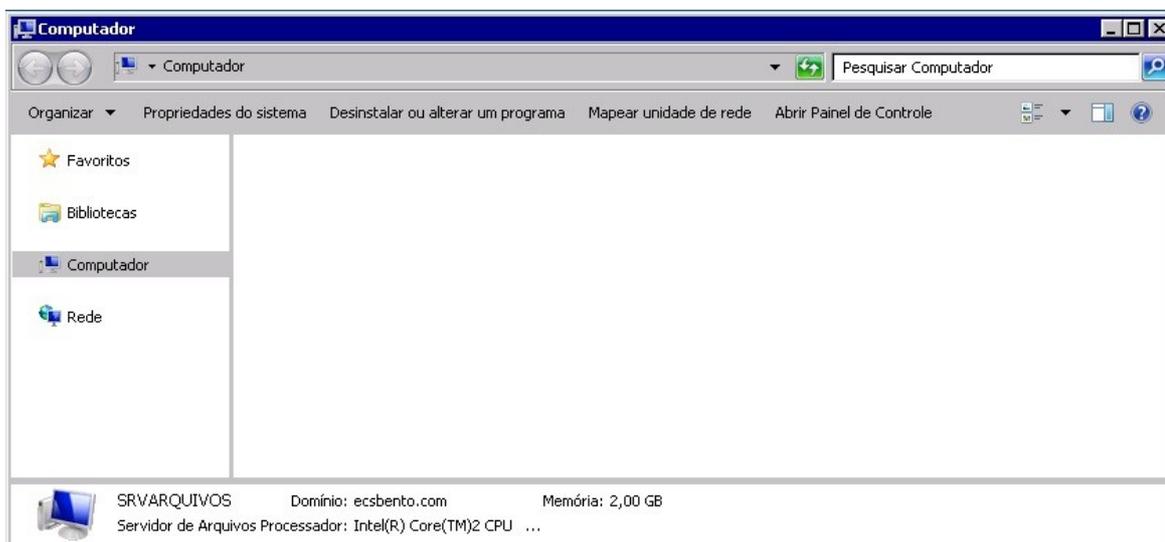


Figura 18: Unidades ocultas para o usuário remoto [Autoria Própria]

3.5.4 GPO PARA EXECUTAR APENAS ARQUIVOS ESPECIFICOS

Uma maneira de restringir ainda mais os acessos do usuário remoto, é criar uma diretiva na qual ele apenas irá conseguir utilizar programas que o administrador permite na hora da configuração da mesma.

Para que a criação dessa diretiva, deverá utilizar a ferramenta administrativa gerenciamento de diretivas de grupo, selecionar a *OU* remota e nela clicar com o direito do mouse e ir na opção editar e seguir os seguintes passos:

- Configuração do Usuário;
- Diretivas;
- Modelos Administrativos;
- Sistema;
- Executar apenas aplicativos do *Windows* especificados.

Na tela que irá surgir quando selecionar a opção habilitado na parte de opções irá aparecer um campo lista de aplicativos permitidos. Clicando nessa opção será disponível estar adicionando os programas que o usuário remoto poderá utilizar. A figura 19 demonstra a lista

de programas permitidos. No caso os aplicativos bloco de notas, *winword*, calculadora e os programas contábeis.

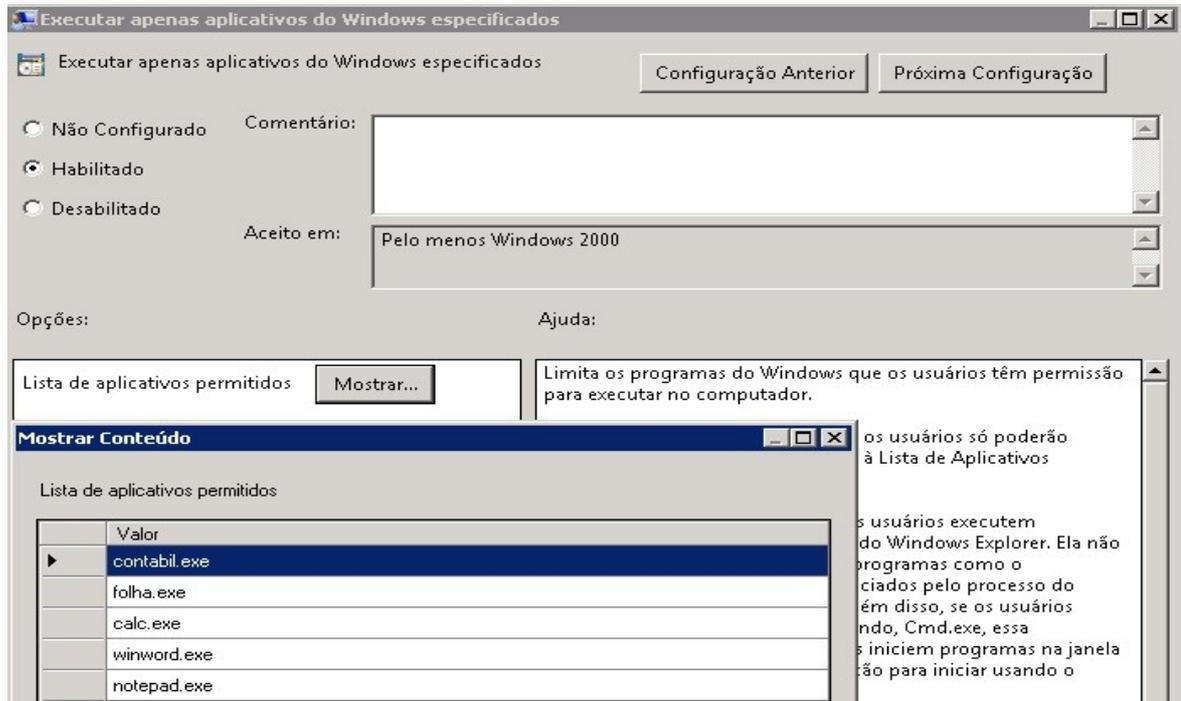


Figura 19: Programas liberados para o usuário remoto [Autoria Própria]

Enfim, a figura 20 mostra a tentativa do usuário em tentar utilizar algum outro aplicativo que não esteja na lista de programas permitidos na diretiva. No caso o usuário irá tentar acessar o *prompt* de comando.

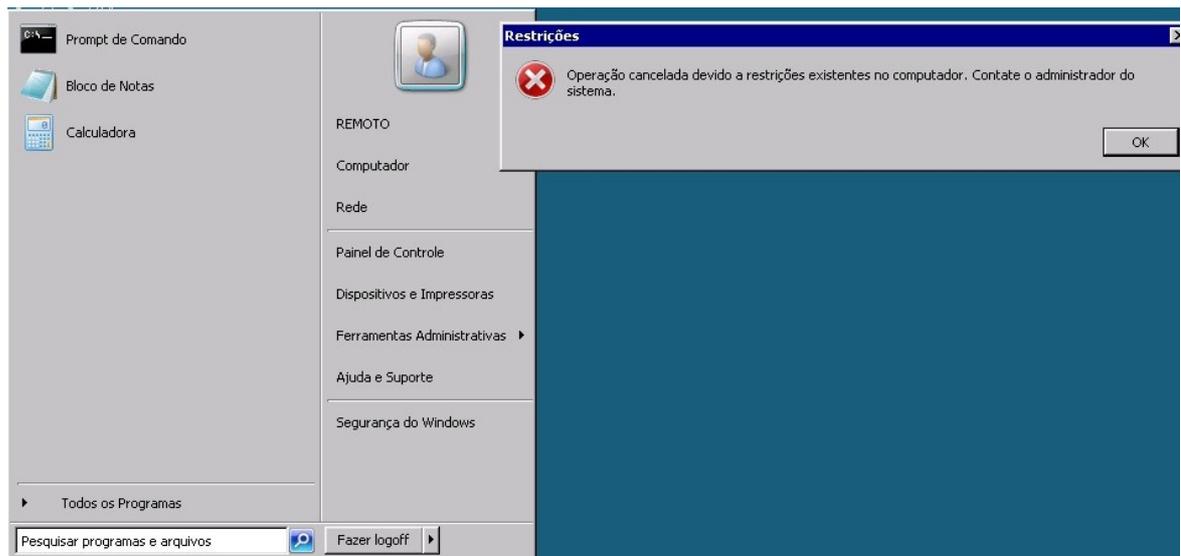


Figura 20: Negando acesso a um aplicativo fora da lista [Autoria Própria]

4 CONCLUSÃO

O processo de implementação do *Windows 2008 Server*, não é complicado como muitos acham que é. O trabalho demonstrou a parte básica e prática de como fazer a configuração de alguns recursos básicos que esse sistema operacional pode oferecer.

Em um primeiro momento foi comentado a respeito dos conceitos envolvidos no processo de implementação como, *Windows 2008 Server*, *active directory*, domínio, unidade organizacional e diretivas de segurança.

De acordo com o problema relatado na conclusão de todo o processo, os usuários finais notaram a centralização dos arquivos em um servidor e também a existência de uma cópia de segurança todo dia dos seus arquivos contido na pasta Meus Documentos, a segurança de ter seus ambientes de trabalhos (*desktop*) salvos da maneira que lhe convêm melhor.

Existem muitas possibilidades de criação de diretivas de segurança, as que foram apresentadas, eram as que tinham real necessidade para fazer com que a rede interna do Escritório Contábil São Bento chegasse a um nível de organização pretendido pelo administrador da rede. Como o sistema de diretivas de segurança é totalmente dinâmico fica aberto a novas inclusões de diretivas conforme a necessidade de restrição ou permissão a meios do *Windows*, *hardware* e *software*.

Então diante dessas afirmações fica aberto para um próximo projeto estar elaborando novas diretivas de segurança, estreitando ainda mais permissões ou bloqueios ao usuário e máquina. Uma sugestão seria uma diretiva para instalação sistematizada a partir do servidor, onde o programa é instalado no servidor e assim as máquinas que pertencem ao domínio ao fazerem o *logon* na rede esse programa em questão seja instalado automaticamente na estação, sem o administrador precisar estar se deslocando para efetuar o procedimento.

REFERÊNCIAS

MICROSOFT, TECHNET. *ACTIVE DIRECTORY*. Disponível em: <<http://technet.microsoft.com/pt-br/library/dd871105.aspx>> 01 set. 2012

MICROSOFT, TECHNET. **Dominio**. Disponível em: <<http://technet.microsoft.com/pt-br/library/cc771294.aspx>>. Acesso em: 01 set. 2012

MICROSOFT, TECHNET. *Windows 2008 Server*. Disponível em: <<http://technet.microsoft.com/pt-br/windowsserver/bb310558.aspx>> Acesso em 15 ago. 2012.

MICROSOFT, Official Learning Product. **6419 A Configuring, Managing and Maintaining Windows Server 2008**, v.1

TORRES, Gabriel. **Rede de Computadores Curso Completo**. 1ª ed. Rio de Janeiro: Axcel Books do Brasil Editora, 2001. 644p.