PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

SISTEMAS DE INFORMAÇÃO – NÚCLEO UNIV. BETIM

Implementação do Login Individual, como Política de Segurança, na rede acadêmica da PUC Minas utilizando o Active Directory

Cristiano Batista Veronez

Betim, Novembro de 2004.

Cristiano Batista Veronez

Implementação do Login Individual, como Política de Segurança, na rede acadêmica da PUC Minas utilizando o Active Directory

Trabalho de Monografia apresentado na Pontifícia Universidade Católica de Minas Gerais, Núcleo Universitário de Betim.

Orientador: Prof. Nesley Daher

Betim

Agradecimentos

Agradeço a Deus onde encontrei forças para fazer este projeto.

À minha mãe, meu irmão e meus avós pelo amor, carinho e força na minha formação acadêmica.

Ao coordenador de Sistemas de Informação da PUC Minas Contagem José Wilson, que me deu oportunidade de desenvolver este projeto na PUC.

Aos meus colegas de trabalho que me ajudaram na correção desta monografia e ao técnico Leonardo que me ajudou no desenvolvimento do projeto.

Ao Prof. Nesley Daher por sua orientação e total apoio no desenvolvimento deste projeto ficam meus sinceros agradecimentos.

Cristiano Batista Veronez

Implementação do Login Individual como Política de Segurança, na rede acadêmica da PUC Minas, utilizando Active Directory

Trabalho de Monografia apresentado na Pontifícia Universidade Católica de Minas Gerais, Núcleo Universitário de Betim.

_____

Nesley Daher (Orientador) – PUC Minas

_____

João Medrado – PUC Minas

_____

Márcio Campos – PUC Minas

Resumo

O objetivo do presente trabalho é apontar a ferramenta desenvolvida para implantar o Login Individual na PUC Minas utilizando como base o Active Directory do Windows Server 2003 e demonstração das tecnologias utilizadas. Este sistema será implantado na rede acadêmica da PUC Minas e a justificativa para a utilização desta ferramenta, é, principalmente, a segurança da rede e acesso de pessoas que não são do meio acadêmico da PUC. Serão abordadas questões sobre segurança da rede acadêmica e como o Login se aplicará à mesma. O sistema desenvolvido tem uma interação direta com Active Directory utilizando API do Windows Server 2003 através de linhas de comando. Será apresentado também como o sistema foi desenvolvido até o momento da instalação, detalhando todas as funcionalidades do mesmo.

Abstract

The purpose of that work is to present the tool developed to implant Individual Login in the Catholic University of Minas Gerais using the Active Directory of Windows Server 2003. This system will be implanted in PUC Minas academic net and the justification for the use of this tool is, mainly, to protect the academic net for unauthorized users. It also gives the opportunity of controlling what users do in the net, allowing the administrator to know if it is being used in an inappropriate way. The developed system has a direct interaction with Active Directory using the API of Windows Server 2003 through command lines. We will also show how the system was developed until the moment of the installation, detailing all the functionalities of the same.

Lista de figuras

Abreviaturas

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name Services

IIS – Internet Information Services

WAN – World Area Network

UML – Unified Modeling Language

GPMC – Group Policy Manager Console

ADMT – Active Directory Migration Tools

Sumário

1 – Introdução

A proposta deste trabalho é abordar o sistema de login individual, que está em implantação, como política de segurança, para gerar um nível melhor de controle na rede acadêmica da PUC Minas. Para a implementação deste sistema será utilizado a linguagem Delphi e o banco de dados MySQL. Ele será desenvolvido para funcionar sobre plataforma Windows Server 2003 podendo ser executado em outras plataformas Windows, apesar de não apresentar todas funcionalidades ativas.

Existe a necessidade do desenvolvimento deste sistema porque será necessário criar usuário no domínio[1] para cada aluno da PUC Minas, o que é praticamente impossível criar cada um manualmente. A partir dos recursos do Windows Server 2003, foi desenvolvida a ferramenta de login individual que a partir de uma base de dados de alunos, propícia a criação de todos os usuários no Active Directory.

Serão abordadas no capítulo 2, questões sobre Tecnologia NT e plataformas Windows 2000 Server e Windows Server 2003. Também no capítulo 2 serão abordadas questões sobre Active Directory envolvendo aplicação de diretivas de segurança, definição de sites e replicação. No capítulo 3 serão abordadas questões sobre a Rede Acadêmica da PUC Minas, de que forma o sistema de Login Individual será aplicado nela e as políticas de segurança da rede. No capítulo 4 será apresentado o sistema de Login Individual, da forma que o mesmo foi implementado, as características de sua instalação e explicação de suas funcionalidades. Por fim, na conclusão do projeto abordando os benefícios do sistema Login Individual na política de segurança da Rede Acadêmica da PUC Minas.

[1] Organização lógica de usuários e máquinas de uma rede

2 – Revisão Bibliográfica

2.1 - Tecnologia Windows NT

A proposta de utilização da Tecnologia NT está alinhada com o trabalho, haja visto que, o mesmo foi implementado a partir da base dos sistemas operacionais, Windows Server 2003 e Windows 2000 Server.

Segundo a Microsoft [Microsoft, 1999], a tecnologia utilizada no sistema operacional Windows NT possui excelentes funcionalidades de segurança para uma rede corporativa. Um único acesso ao domínio Windows NT permite acesso a recursos em qualquer lugar da rede corporativa. O Windows NT possui ferramentas administrativas de fácil uso tanto para política de segurança quanto gerenciamento de usuários, isto faz com que sua implantação tenha um custo reduzido.

O NT possui um modelo de segurança que proporciona um plataforma sólida para implantação de sistemas cliente/servidor para a rede corporativa. Esta tecnologia em questões de segurança corporativa foi levada para a família Windows 2000 e Windows Server 2003. No entanto, nas novas versões servidoras de Windows, esta tecnologia teve melhoras em questão de gerenciamento e segurança. As novidades que vieram com o Windows 2000 simplificaram a administração de domínios onde gerenciam os usuários e computadores além de aumentar a segurança de autenticação baseada em criptografia de chave pública. Uma das novidades é a inclusão do Active Directory em substituição ao gerenciamento de usuários e computadores que o Windows NT trás. Também veio junto o protocolo de autenticação Kérberos[2] na versão 5.

[2] Protocolo de autenticação de rede que é um padrão de segurança internet

2.2 - Windows 2000

O sistema operacional Windows 2000, é baseado na tecnologia NT. Porém, foi lançado no mercado com várias novidades em relação ao Windows NT, seu precursor de 1993. Segundo Campos [Campos, 2003] o Windows 2000 chegou de fato ao ambiente corporativo e com ele seria possível suprir todas as necessidades das redes dos clientes. Como família, o Windows 2000 foi apresentado nas seguintes edições:

- Microsoft Windows 2000 Server Family
- Microsoft Windows 2000 Advanced Server
- Microsoft Windows 2000 DataCenter Server
- Microsoft Windows 2000 Professional.

Segundo a Microsoft [Microsoft, 1999], a segurança do Windows 2000 foi implementado para adaptar as diversas situações com o objetivo de suportar empresas que tenham seus serviços baseados em internet. Algumas dessas mudanças refletem avanços no suporte a grandes organizações, através do uso do Active Directory hierárquico do Windows 2000. Com o Windows 2000, teve também alterações no gerenciamento dos serviços de DHCP[3] e DNS[4], estas alterações facilitaram muito o serviço do administrador de Rede uma vez que ficou mais fácil configurar e gerenciar estes serviços.

[3] Serviço de distribuição automático de IP configurados em servidores de domínio.
[4] Serviço de resolução de nomes da rede em endereços IP.

2.3 - Windows Server 2003

O Windows Server 2003 lançado no final de Abril de 2003, segundo Hara, [Hara, 2003], surge no mercado com a promessa de oferecer melhorias e suporte para futuras tecnologias. O Windows Server 2003 chega com quatro versões: Standard Edition, Datacenter Edition, Enterprise Edition e Web Server Edition. Uma nova versão Web Server Edition é novidade no mercado. Ela atende apenas para aplicações Web utilizando o IIS[5] 6.0 com suporte a ASP.NET. Com ela não é possível utiliza-la para controlador de domínio. Esta versão dá suporte a servidores de até 2 processadores e 2 GB de memória RAM. Existem também as versões para servidores de 64Bits, elas são: Datacenter Edition e a Enterprise Edition.

Segundo Hara [Hara, 2003], controladores de domínio[6] Windows Server 2003 vem habilitado por padrão requerimentos de assinatura SMB[7]. Isto impede estações que tenham sistema operacional Windows 95 e DOS de se autenticar na rede. Com isto, para a implantação de um Domain Controller Windows Server 2003 em nossa rede, deve ser revisto o parque de máquinas da empresa. Estações com sistema operacional Windows 98, NT, 2000 e XP conseguem autenticação no Windows Server 2003 sem problemas.

As novidades que o Windows Server 2003 trouxe em seu pacote, segundo Hara [Hara, 2003] é um novo Active Directory, novas políticas de segurança, novos serviços de Cluster e Rede. Alguns destes serviços já vieram no Windows XP e estão nas versões de Windows Server 2003.

[5] Ferramentas de gerenciamento de informações para serviço de rede Intranet e Internet
[6] São servidores responsáveis par ao gerenciamento do domínio da rede
[7] Protocolo de compartilhamento de recursos suportado pela maioria dos Sistemas operacionais Microsoft

O Active Directory trouxe novidades no gerenciamento, uma das novidades está no processo de replicação entre Domains Controllers que no Windows 2000 consumia muita CPU e memória pelo fato dos pacotes que seriam trafegados na replicação eram comprimidos. Na nova versão de Active Directory é possível desabilitar esta funcionalidade liberando CPU e memória para outros processos.

Outras novidades referentes ao Active Directory serão tratadas no próximo tópico. Mais uma novidade do Windows Server 2003 segundo Hara, [Hara, 2003], são 100 novas políticas de segurança no Group Policy. Group Policy é a ferramenta onde são definidas as políticas de grupo que serão aplicadas a um parque de máquinas da rede. Uma outra ferramenta que pode ser instalada no Windows Server 2003 após a instalação do sistema operacional é a GPMC (Group Policy Management Console). Ela permite um gerenciamento mais fácil de políticas aplicadas no Active Directory. Ao executa-la, a ferramenta traz a estrutura do Active Directory para que o administrador possa visualizar onde as políticas são aplicadas. Pode-se criar novas políticas ou criar um vínculo de uma política já existente para uma unidade organizacional do Active Directory.

As novidades que o Windows Server 2003 trás em relação à rede são alguns serviços e ferramentas que no Windows 2000 não existia. Uma das novidades é a inclusão de um Firewall[8] no adaptador de rede permite que seu servidor esteja protegido de ataques. Esta ferramenta pode ser uma solução para pequenas empresas que tenham poucos computadores. Uma restrição que o Windows Server 2003 trás, em relação à rede, é não deixar que o administrador da rede exclua o protocolo TCP/IP,

[8] Serviço de filtro de pacotes de rede

pois ele é indispensável para o funcionamento de vários serviços do Windows Server 2003 como por exemplo o DHCP e DNS que trabalham utilizando este protocolo.

Segundo Hara [Hara, 2004], o Windows Server 2003 também trás novas ferramentas que permitem facilitar tarefas que antes eram consideradas trabalhosas pelos administradores de rede. Além de todas serem de fácil execução, elas possuem textos explicativos e fáceis de entender. Estas ferramentas são executadas no prompt de comando e que podem automatizar algumas tarefas. Entre elas tem vários comandos que trabalham diretamente com o Active Directory e estes comandos nos permitem fazer criação, alteração, exclusão, movimentação e busca de objetos dentro do Active Directory. Ainda é possível fazer operações com usuários, grupos, computadores e unidades organizacionais[9]. É possível a criação de scripts e ou aplicações externas para trabalhar com o Active Directory. É com estes comandos que está sendo desenvolvido o sistema que gerencia o Login Individual implantado na PUC Minas.

[9] Unidades Organizacionais são pastas ou containers do Active Directory para possibilitar a organização de usuários, grupos e computadores.

2.4 - Active Directory

Segundo a Microsoft [Microsoft, 1999], o serviço Active Directory fornece recursos de logon único e um repositório central para informações de toda a infra-estrutura, simplificando o gerenciamento de usuários e de computadores e garantindo o acesso aos recursos em rede, ou seja, é um banco de dados que é responsável por armazenar, gerenciar e organizar os objetos da rede. Nele é possível gerenciar as contas dos usuários, grupos de usuários, computadores e controladores de domínio.

Segundo Battisti [Battisti, 2003], o Active Directory foi sem dúvida a grande novidade do Windows 2000 em relação ao Windows NT 4.0. No Windows Server 2003, o Active Directory também é o elemento central e fundamental para uma infra-estrutura de rede planejada, ou seja, o Active Directory chegou no Windows 2000 tomando lugar do Gerenciador de Usuários e Gerenciador de Computadores existente no Windows NT, melhorando todo gerenciamento em uma só ferramenta.

O Active Directory é instalado em computadores que serão controladores de domínio. Promovendo um servidor a controlador de domínio, todas as máquinas da rede deverão se ingressar neste domínio através de configuração local em cada estação da rede. Em uma rede você pode ter vários controladores de domínio interligados, permitindo que sua rede tenha um balanceamento de carga na autenticação dos usuários. Depois do domínio já criado os próximos servidores que entrarem na rede, terão que ingressar ao domínio já existente. No momento que o novo servidor tiver entrando no domínio, automaticamente o Active Directory já irá replicar todas as informações para o segundo servidor. Quando existe mais de um servidor controlador de domínio na rede, eles replicarão informações do Active

Directory em um tempo configurado de acordo com a necessidade do administrador da rede. Isto possibilita que os servidores estejam sempre iguais para o bom funcionamento da rede.

Para que o Active Directory funcione perfeitamente é necessário à instalação de um servidor DNS na rede, de preferência que seja em ambiente Windows. O DNS é necessário porque o domínio do Active Directory utiliza a nomenclatura DNS na rede. Quando uma máquina da rede quer fazer qualquer tipo de acesso ao Active Directory, ele consulta o DNS para obter o endereço da máquina que contém o serviço procurado. Para que isto funcione, todas as máquinas da rede deverão ter configurado em seu adaptador de rede, o endereço DNS correspondente ao DNS utilizado pelo Active Directory.

O Active Directory trabalha com uma estrutura hierárquica muito parecida com estrutura de um disco rígido. Os diretórios que o Active Directory possui são chamados de “Organizational Units” (OU), traduzindo, Unidades Organizacionais. Estas OUs são utilizadas para organizar os objetos dentro do Active Directory. Ao instalar, o Active Directory terá apenas a OU Domain Controllers criada. As outras pastas não são OU e já vem por padrão. Elas são: Users, Computers, Builtin dentre outras.

Para Battisti [Battisti, 2003], o projeto do Active Directory é bem mais ambicioso do que ser simplesmente um diretório para conter informações dos elementos de uma rede baseada em Windows Server 2003. Ele foi projetado para tornar-se, com o tempo, o único diretório necessário na rede da empresa com a idéia de criar o tão sonhado logon único. Ou seja, a idéia é utilizar o Active Directory para ser o servidor de usuários para todas as aplicações utilizadas nas empresas

integradas esta ferramenta. Se não tivermos uma base única, toda alteração deverá ser feita em cada base individualmente.

Segundo Battisti [Battisti, 2003], árvore de domínio é um agrupamento de vários domínios do Windows Server 2003, os quais compartilham um espaço de nome. Compartilhar um espaço de nome quer dizer que, quando se tem uma árvore de domínios, e o nome inicial do domínio que no caso da PUC, é pucmg.net, cada domínio da árvore irá compartilhar um espaço de nome deste domínio. No caso da PUC, a rede acadêmica, que irei falar sobre ela no próximo capítulo, terá uma árvore de domínio e cada unidade será um membro desta árvore com uma nomenclatura de domínio utilizando o pucmg.net. Na unidade de Contagem, quando tiver na árvore de domínio terá o nome contagem.pucmg.net. Árvore de domínio é utilizada para melhor organização do mesmo, separando a rede por localidades o que facilita o gerenciamento.

Quando fala-se de segurança da rede implementando o Active Directory não se pode esquecer de mencionar as relações de confiança. Segundo Battisti [Battisti, 2003], é através do uso de relações de confiança entre domínios que é possível que um usuário de um domínio possa fazer o logon com sua conta de usuário e senha, mesmo utilizando um computador de outro domínio. Esta relação de confiança funciona da seguinte forma: os servidores controladores de domínio serão configurados para que os domínios se comuniquem. Quando um usuário do domínio A, por exemplo, tentar se autenticar no domínio B, o domínio A, tendo uma relação de confiança com o domínio B, pergunta ao domínio B se aquele usuário é pertencente ao domínio dele e se a senha e usuários estão corretos. Segundo Battisti [Battisti, 2003] na época do Windows NT 4.0 as relações de confiança no NT Server eram definidas por três características: são unilaterais, ou seja, se o domínio

A confia no domínio B não quer dizer que o B também confia no A. Para isto teria que fazer a relação de B para A também; não são transitivas, ou seja, se o domínio A confia no domínio B e o domínio B confia no domínio C, não quer dizer que o domínio A confie também no domínio C, para que isto seja possível deveria ser criado uma relação de confiança entre os domínios A e C e que devem ser criadas manualmente pelo administrador que é um processo muito trabalhoso. Segundo Battisti [Battisti, 2003], no Windows Server 2003 as relações de confiança são criadas automaticamente entre os domínios de uma árvore de domínios. Ou seja, todos os domínios que estiverem na árvore do domínio terá relação de confiança entre eles. As relações no Windows 2003 são bidirecionais, todos os domínios confiam entre si nesta árvore de domínios.

Um outro conceito a ser tratado é o de Global Catalog. Segundo Battisti [Battisti, 2003]; Global Catalog é uma base de dados que o Active Directory mantém com algumas informações sobre objetos de todos os domínios da rede. Esta base está centrada nos controladores de domínio que são configurados para atuar como servidores de Global Catalog. Numa rede onde se tem mais de um controlador de domínio, não é necessário que tenha mais de um Global Catalog mas, em domínios de apenas um controlador de domínio é obrigatório que este seja também um servidor de Global Catalog. Quando um domínio é instalado na rede, automaticamente aquele primeiro servidor passa a ser também um servidor Global Catalog e os próximos controladores de domínio não terão esta função. Mas se for de interesse do administrador, isto pode ser configurado após a instalação. A função dele é armazenar informações de todos os objetos do Active Directory proporcionando uma melhor performance na pesquisa de objetos. Quando o usuário solicita uma pesquisa de objetos para o Active Directory, esta pesquisa é feita no

servidor Global Catalog mais próximo do usuário e a pesquisa podem englobar todos os domínios de uma floresta.

2.4.1 - Group Policy e Active Directory

O Group Policy é uma console[10] onde se configura todas as políticas de segurança de estações, usuários e servidores. Para Battisti [Battisti, 2003], este recurso é de "enorme" utilidade para o administrador de rede uma vez que ela permite que configure até a página inicial do navegador da estação, por exemplo. Podem-se criar políticas de Group Policy para a rede local através dos servidores de domínio, para isso os mesmo devem ser Windows 2000 Server ou Server 2003 com o Active Directory configurado. Cria-se políticas para o domínio e as máquinas ligadas à ele sendo estações com sistema operacional Windows 2000/XP/2003, receberão estas políticas do domínio. Para criação destas políticas pode-se utilizar a ferramenta GPMC, já mencionada anteriormente e que será detalhada no tópico 2.5 deste capítulo, para facilitar a criação e aplicação destas políticas na árvore do Active Directory.

2.4.2 - Sites e Replicação do Active Directory

Para Battisti [Battisti, 2003], o conceito de site no ambiente do Active Directory é uma ferramenta para o qual é utilizado, representar a divisão física da rede e é muito importante para a implementação de um sistema de replicação das informações do Active Directory entre Domains Controllers.

[10] Janela que é usada para abrir ferramentas de configurações do Windows

Em um domínio onde existem vários Domains Controllers que se replicam, é necessário a configuração dos sites para que a rede não tenha problemas com a replicação. Cada site criado no Active Directory irá representar uma estrutura física da rede e através destes sites criados, podem-se criar os vínculos de replicação. Este vínculo diz, por exemplo, que o Domain Controller A terá uma conexão com o Domain Controller B.

Mas os sites não são apenas para replicação. São utilizados também para autenticação de usuários. Como que isto funciona? Quando um usuário de um determinado site irá se autenticar na rede, ele procura os Domains Controllers pertencentes àquele site. Isto evita tráfego desnecessário numa rede onde elas são ligadas utilizando um link WAN. Na console de configuração de sites, pode-se colocar um Domain Controller interligados a vários outros Domains Controllers. Por exemplo, olhando para o Ambiente da Rede acadêmica da PUC Minas, as unidades são interligadas utilizando um link WAN para cada uma. Quando tivermos os controladores de domínio interligados com relação de confiança configurada, pode-se criar vínculos entre os controladores de localidades diferentes. Estes vínculos que definirão com qual outro controlador de domínio serão feitos a replicação. Utilizamos estes vínculos para ligar um controlador onde o link WAN é lento com um controlador onde o link WAN é rápido. Com isto conseguimos um desempenho melhor na replicação.

2.5 - Comparando Windows 2000 Server e Windows Server 2003

Segundo Campos [Campos, 2003], o Windows 2000 já entrou no mercado com muitas facilidades que antes eram exclusivas do Unix. Mas agora com o

lançamento do Windows Server 2003 a Microsoft atacam um ponto muito criticado pelos usuários, ou seja, a questão de segurança que para a Microsoft virou prioridade.

Campos [Campos, 2003] ainda fala que este tema de segurança esteve presente até na revisão do desempenho das linhas de código e isto tem sido um diferencial do Windows Server 2003. A Microsoft lançou também junto com o Windows Server 2003 a ferramenta chamada SUS[11]. Esta ferramenta não vem instalada no Windows Server 2003, mas pode ser baixada gratuitamente no site da Microsoft. O SUS é uma ferramenta que atualiza as estações que possuam SO Windows 2000 Service Pack 3 e Windows XP. Após instalada e configurada o SUS faz uma sincronização com Windows Update da Microsoft fazendo com que todas as atualizações de um idioma definido nas configurações, estejam em sua rede fazendo com que suas estações não tenham que sair para a internet e atualizar o Windows. Para que as estações atualizem automaticamente pelo SUS é necessário a configuração na estação. Esta configuração pode ser feita localmente em cada máquina ou definida pelas diretivas de grupo do Windows. Nestas configurações informa-se para a estação qual será o servidor que tem o SUS instalado, qual (is) o(s) dia(s) e horário que a estação irá procurar por atualização.

Na configuração do SUS é possível informar o idioma das atualizações que serão baixadas, qual o intervalo de tempo que o SUS irá sincronizar com o Windows Update, se a sincronização será feita a partir do Windows Update ou de um outro SUS já existente na rede, qual o nome do servidor na rede que as máquinas irão enxergar e outras configurações básicas do funcionamento do SUS.

[11] Software Update Services

Agora com a chegada do Windows Server 2003, existem duas versões de Active directory. Segundo Allen [Allen, 2003], esta nova versão que o chega com o Windows Server 2003 traz um grande numero de atualizações e novas características que o Active Directory do Windows 2000 não tinha. Ou seja, melhorias para ganhar o mercado. Segundo a Microsoft, o Active Directory do Windows Server 2003 trouxe os seguintes aperfeiçoamentos:

- Mais segurança;
- Implantação e gerenciamento fáceis;
- Melhoria do desempenho e confiabilidade.

A Microsoft melhorou o gerenciamento das relações de confiança entre florestas no Active Directory permitindo maior facilidade de configuração para o administrador. Foram criadas novas políticas que, configuradas pelo administrador, restringe a instalação de softwares não autorizados nos computadores. Com estas regras de restrição de software é possível bloquear instalação de softwares não confiáveis e devem ser criadas as regras para os softwares específicos. Dentro do pacote de segurança existe agora a autenticação entre florestas. Esta autenticação é utilizada no caso de um usuário da floresta A acessar o computador da floresta B, neste caso acontece à autenticação entre florestas para permitir o acesso do usuário àquele computador.

Em questão de implantação e gerenciamento fácil, a Microsoft traz uma nova versão para a ferramenta de migração do Active Directory que se chama ADMT[12], versão 2.0. Ela permite a migração de usuários e senhas que estejam no Windows NT 4.0 para Windows Server 2003 ou Windows 2000 Server para Windows Server 2003. Uma outra novidade que veio em questão de flexibilidade do Active Directory é

[12] Active Directory Migration Tools

que agora é possível renomear um domínio DNS e NETBIOS. Com isto se o projeto de implantação do Active Directory na rede for alterado, é possível alterar o domínio sem ter que “matar” o domínio já existente. Outra ferramenta que é novidade no Windows Server 2003 é a GPMC já mencionada anteriormente. Esta ferramenta é uma console de gerenciamento de políticas já existentes para extensões do Active Directory. Quando se executa a aplicação, ele traz toda a estrutura do Active Directory para aplicação sendo possível visualizar quais OUs do Active Directory já possui alguma política. Através dele também se pode:

- Criar novas políticas vinculadas a alguma OU desejada;
- Criar/Remover um “link” de uma política já existente para uma OU;
- Visualizar/Editar/Excluir todas as políticas já existentes no domínio;

Esta ferramenta não se aplica a apenas OUs do Active Directory, ele também pode ser aplicado para Sites criados em seu domínio. Esta ferramenta não vem instalada por padrão no Windows Server 2003, mas pode ser baixada no site da Microsoft gratuitamente. No caso dela não estar instalada, o modo de configuração das Group Policy é modo normal via Active Directory.

Em questões de desempenho, a Microsoft melhorou a questão de replicação e sincronização das informações do Active Directory. Agora o administrador da rede pode escolher o que vai ser replicado e ao contrário de antes eram replicadas todas as informações, agora são replicadas apenas as alterações. Outro recurso criado é no caso da instalação de um novo Domain Controller na rede, caso ele pertença a um domínio já existente, a replicação pode ser feita utilizando uma mídia como, por exemplo, uma fita DAT. Com isto o administrador aumenta o desempenho da rede. Em questão de confiabilidade, os novos recursos que vieram no Active Directory do

Windows 2003 é a monitoração da integridade da replicação entre os Domains Controllers.

2.6 - Segurança Corporativa

Segurança corporativa é a segurança que se deve ter dentro de uma empresa ou corporação. Esta segurança está ligada a várias áreas e uma delas é a área de informática que pode ser dividida em 2 partes:

- Segurança Física
- Segurança Lógica

O que é segurança física? É quando se tem de fazer a segurança física do computador, segurança do hardware. E deve ter esta segurança sempre que se possuem dados importantes que tem muito valor para a corporação.

Um bom exemplo onde deve ter uma segurança física eficiente são no CPD[13] de bancos, universidades, empresas de planos de saúde e etc. Estas corporações trabalham com dados muito importantes para ela. Não que as outras pequenas corporações não trabalhem com dados importantes, mas estas citadas acima devem ter um cuidado maior ainda.

Como deve ser esta segurança? Deve-se tomar cuidado com quem acessa fisicamente os servidores. O acesso aos servidores deve ser feito mediante informado uma senha de acesso onde poucos poderão ter acesso. Citando um exemplo, o DATAPUC é o departamento responsável pelo processamento de dados da PUC Minas. Para entrar no departamento é necessário toda uma identificação do funcionário. A cada área que for acessar lá dentro, é necessário informar uma senha

[13] Centro de Processamento de Dados

de acesso. Os servidores estão numa sala onde quase ninguém entra, pois ela fica trancada e só liberada mediante digitação de senha. O backup dos dados destes servidores é feito através de um Robô programado para fazer os backups automaticamente. Não existe contato humano com as fitas DATs de backup. Isto também é uma forma de segurança física, ou seja, ela é a segurança dos equipamentos onde armazena-se informações importantes. No caso de um servidor de banco, imagine o que aconteceria se fosse roubado ou furtado um servidor contendo os dados dos clientes daquela agência com saldos, senhas e tudo mais. Seria um caos para o banco e o prejuízo seria muito grande.

E a segurança lógica, o que ela é? A segurança lógica é dividida em 2 outras partes que seria: a segurança relativa à proteção da rede de computadores e a segurança na implementação de linhas de código. A segurança numa rede de computadores seria a implementação de um bom firewall no servidor de internet, um bom antivírus em todas as estações da rede, configurar apenas os serviços necessários e sempre manter o sistema operacional atualizado, pois a cada dia que passa uma nova "brecha" é descoberta. Se não ficar atento, o administrador pode ser surpreendido a qualquer momento. A implementação de um firewall, em principio, é o primeiro passo a tomar na configuração de segurança da rede. Ele deve apenas liberar o acesso externo $\rightarrow$ interno necessário. No caso de universidades e bancos, geralmente o que deve ser acessado externamente é o site da corporação. Raramente é necessário liberação de outro serviço no firewall. Quanto mais portas forem liberadas no firewall, as chances de invasão na sua rede aumentam.

Após a configuração do firewall, é importante implementar um bom antivírus que sempre esteja atualizado e que todas as máquinas tenham instalado. Hoje em

dia existem na internet os programas que ficam rodando escondidos na máquina e que, na maioria das vezes, não se percebe a existência deles. Eles são os Spywares[14]. Estes programas são instalados sem que o usuário perceba e quando se percebe já é tarde. Já existem ferramentas que instala no computador para retirar estes Spywares e alguns são eficientes o suficiente para deixar a máquina sem estes programas.

Segundo a Symantec [Symantec, 2002], hoje para as corporações existem duas alternativas para o gerenciamento de segurança. Eles são:

- Gerenciamento interno de segurança
- Gerenciamento terceirizado de segurança

As corporações sempre se questionam quando ela decide terceirizar, se é possível ter este gerenciamento terceirizado sem ter altos custos. É uma difícil tarefa avaliar isto. Deve ser analisado os riscos que se corre e os benefícios que se ganha terceirizando um serviço de segurança.

Segundo a Symantec [Symantec, 2002], são item que devem ser considerados com muita cautela na contratação de um serviço de segurança terceirizado.

- Manutenção do controle da empresa
- Experiência dos profissionais de segurança
- Variedade e flexibilidade dos serviços
- Custo dos benefícios
- Filosofia e cultura do programa de segurança
- Compromisso com o contrato de serviços

[14] Software de dupla personalidade sendo sua segunda, utilizada para recolher informações habituais de um usuário e enviadas ao fabricante do spyware.

- Tecnologia suportada
- Disponibilidade de instalações para operações de segurança

Dos fatores citados acima, para a Symantec [Symantec, 2002], o mais difícil pode ser a avaliação do custo de terceirização, isto porque a maioria das empresas tem dificuldades para estimar o impacto financeiro de tal decisão. Em um estudo da InfoWorld [Dinley, 2001], de 100 profissionais que tem os serviços de segurança terceirizados, 61% não sabe o quanto eles economizariam nos 12 meses após a terceirização das funções de Tecnologia da Informação (TI). Os profissionais parecem não estar preparados para esta terceirização, pois a pesquisa mostra que apenas 39% estão por dentro dos custos da terceirização de funções de TI. Para se ter um gerenciamento de segurança é necessário ter recurso humano, hardware de suporte, equipamentos e softwares para gerenciar toda a segurança. Para a Symantec [Symantec, 2002], quando uma empresa considera a terceirização dos serviços de segurança gerenciados, deve estimar também algumas variáveis durante o período do contrato:

- Capital e custos operacionais relevantes
- Custo de supervisão do provedor de serviços de gerenciamento de segurança
- Custo da transição, alteração na direção e nível de recursos e modificações no contrato.

Os custos de hardware e software são determinados pela empresa para que ela tenha um bom programa de gerenciamento de segurança. Estes custos englobam servidores, estações de trabalho, softwares de segurança como antivírus e firewall. Todos os softwares, na maioria das vezes terão um custo de licenciamento, e este licenciamento deve ser calculado incluindo os patches de atualizações que no ciclo de vida do software acaba se tornando necessário. Manutenção também deve ter

seu custo embutido no custo total de propriedade. Segundo a Symantec [Symantec, 2002], a manutenção do software representa normalmente entre 15 e 25 porcento do custo anual do software. No contrato de manutenção, deve-se ficar atento à cobertura e suporte da manutenção. Algumas empresas cobrem 24 horas do dia e outras somente no horário comercial. Dependendo do foco da empresa, no caso de ser uma empresa que não pode parar, é interessante que o contrato de manutenção seja de disponibilidade 24 horas. Em questão de pessoal, a equipe de segurança deve ser formada por profissionais experientes e, hoje em dia, é difícil ter esta base e conseguir mantê-la, além do alto custo. Estes custos com pessoal não engloba somente o salário, mas os adicionais como bônus, horas extras e treinamentos. Esse treinamento deve ser constante para estes profissionais de segurança, pois a cada dia que passa, existem novas formas de ataques e também novas formas de defesas. Segundo a Symantec [Symantec, 2002], estes custos devem incluir:

- Treinamento no produto ou tecnologia
- Treinamento na conscientização geral de segurança
- Classes para preparação da certificação
- Custos de certificação
- Participação nas principais conferencias e encontros de segurança
- Assinaturas de livros e revistas para manter profissionais de segurança atualizados com as novas tecnologias, dicas, técnicas, ameaças e proteção.

Esse treinamento é importante para que as empresas sempre estejam com profissionais qualificados a atender a segurança necessária uma vez que aparece mais e mais vulnerabilidades. Os custos de instalações devem contabilizar equipamentos, redundância, eletricidade, refrigeração e sistemas contra incêndios. Às vezes a construção de um centro de operações de segurança é inviável para

muitas empresas, pois o curso pode passar de U$ 100.000.000 segundo a Symantec [Symantec, 2002]. Pode-se achar que seria melhor existir um gerenciamento interno de segurança ao ter um gerenciamento terceirizado, mas talvez, pode-se estar enganados em certo ponto. O serviço terceirizado já possui toda experiência de segurança, assim o risco de ameaças diminui consideravelmente.

O tempo de implantação de um gerenciamento terceirizado também é um fator importante. No caso de um gerenciamento de segurança interno este tempo pode ser muito alto. No caso de um gerenciamento terceirizado, a empresa contratada para prover os serviços estará disponibilizando uma equipe de profissionais experientes, fornecerá todos os recursos para proteger a empresa 24 horas por dia. Se fosse criar um sistema de gerenciamento interno, é necessário contratação de profissionais, treinamento para eles, contratação de recursos e os riscos seriam todos assumidos pela empresa.

Contudo, calculando no decorrer de 2 anos aproximadamente, pode ser mais lucrativo e mais seguro para a empresa a contratação de serviços de gerenciamento de segurança, pois para uma empresa começar isto internamente ela pode pagar caro pela falta de experiência.

2.7 - Auditoria

Em uma rede corporativa sempre é necessário à utilização de um sistema de auditoria e o Windows Server 2003 trabalha muito bem com isto. Segundo Battisti [Battisti, 2003], auditoria é um processo de acompanhamento das ações que são executadas nos servidores de domínio através da rede, tanto ações do próprio

sistema operacional, como por exemplo, inicialização, mas principalmente ações de usuário, como um logon ou um acesso a arquivos de uma pasta compartilhada.

Todos os serviços que o Windows inicializa, quando um usuário efetua o logon na rede, automaticamente gera um registro desta ação do usuário ou serviço. O processo de auditoria consiste em analisar estes registros de sistema e identificar possíveis problemas. Porém pode-se configurar os servidores e ou estações de trabalho para gerar registro de outras ações. Uma destas ações, por exemplo, é acesso a objetos de um computador, auditoria local de logon em cada estação, uso de privilégios, controle de processos e etc. Todas estas ações podem ser configuradas para ser auditadas. Porém quanto mais ações forem configuradas para serem auditadas, as estações ou servidores terão que gastar mais processador e memória para as auditorias. Com isto também, as máquinas deverão ter mais espaço em disco, pois estes registros gerados ocuparão espaço no disco da máquina.

A visualização destes registros é feito através da ferramenta Event Viewer (Visualizar Eventos) que no, Windows Server 2003, são classificados em registros de aplicação, segurança, sistema, Active Directory, Servidor DNS e serviço de replicação. No Windows 2000, o Event Viewer gerencia apenas registros de aplicativo, segurança e sistema como mostra a Figura 1.

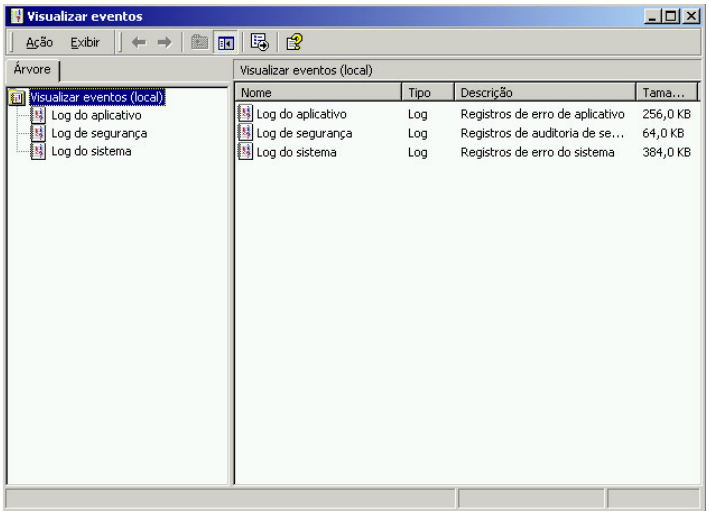


Figura 1: Tela da ferramenta de Visualizar Eventos

Para configurar estas auditorias utiliza-se a ferramenta de Diretiva de Grupo que encontra-se no Painel de Controle. A Figura 2 abaixo mostra esta ferramenta.

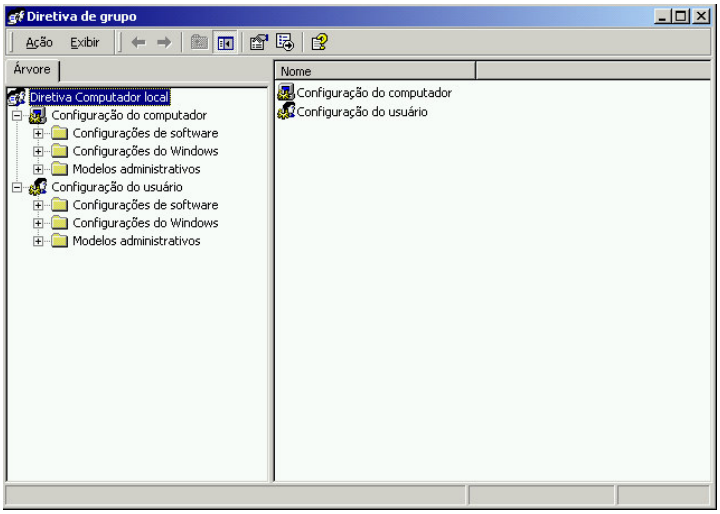


Figura 2: Tela de configurações de Diretiva de Grupo

No ambiente da rede acadêmica da PUC Minas, será utilizado muito estas ferramentas, principalmente os registros de segurança a partir dos quais serão gerados relatórios de utilização dos laboratórios. Este registro de segurança, além de ser útil para emissão de relatórios, poderá ser utilizado também para identificar usuários que estejam violando as regras dos laboratórios como acesso a sites

impróprios, execução e instalação de jogos dentre outros que será relatado nos próximos capítulos.

2.8 - Login Individual

O Login individual é um sistema que foi desenvolvido no intuito de gerar um usuário para cada aluno da PUC Minas, na rede acadêmica. A criação deste login individual veio devido a vários problemas que eram enfrentados pelos técnicos acadêmicos, um deles a questão de segurança. Antes da implantação do Login, não era possível identificar os alunos que violavam as regras dos laboratórios porque era um utilizado um único usuário para os alunos. Cada aluno tendo seu usuário e adotando auditoria de políticas de segurança, é possível identificar os alunos infratores. Outro motivo que levou à criação do login foi o fato de que os laboratórios estavam sendo usados por pessoas que não são do meio acadêmico da PUC Minas. Desta forma os laboratórios ficavam lotados e os alunos que possuem o benefício, não podiam utilizar. Com a implantação do login, os laboratórios foi racionalizado privilegiando os alunos.

O sistema foi modelado utilizando a metodologia UML[15] e desenvolvido na linguagem Delphi com banco de dados MySQL. A função do sistema será de gerar os usuários dos alunos da PUC Minas nos controladores de domínio da rede acadêmica. Através de configurações criadas no sistema, os usuários, que são mais 30 mil ao todo, serão criados dentro de seus respectivos cursos e unidades. A estrutura de Unidades e Cursos será criada no Active Directory automaticamente na execução do sistema pela primeira vez. O banco de dados do sistema já traz as

[15] Unified Modeling Language, traduzindo Linguagem de Modelagem Unificada

unidades e cursos atuais da PUC Minas, o que permite a criação da estrutura no Active Directory.

Os alunos são cadastrados no sistema através de arquivo de texto fornecido pelo DATAPUC ou individualmente mediante apresentação de comprovante de matrícula na PUC Minas. Este arquivo que tem um formato específico é gerado com todos os alunos de cada unidade e enviado para as mesmas. Cada unidade é responsável pelo processamento deste arquivo no sistema de login individual. Este arquivo deve ser processado todo início de semestre após o término das matrículas. Cada aluno é uma linha do arquivo que traz informações como matrícula, nome, curso, período, turno e situação. Esta situação é que determina a situação do usuário na rede e será detalhado estas situações no próximo capítulo.

O sistema de login individual foi desenvolvido para funcionar integrado com o Windows Server 2003 e Active Directory. Está sendo utilizado o Windows Server 2003 porque além de ser uma nova tecnologia, a nova versão do Active Directory trouxe novas ferramentas que facilitam a vida do administrador de rede. Estas novas ferramentas são novos comandos que são utilizados via Prompt que facilmente podem ser usados. O sistema de login utiliza destes comandos para criar, remover e alterar objetos no Active Directory. É utilizado apenas 3 comandos para trabalhar com estes objetos, eles são: DSADD, DSMOD E DSRM Com o comando DSADD pode-se adicionar qualquer tipo de objeto no Active Directory, estes objetos são usuários, computadores e OUs. Com o comando DSMOD pode-se fazer quaisquer modificações no Active Directory, nos usuários é possível mudar qualquer informação que esteja cadastrado pra ele. O DSRM é utilizado apenas para remover o usuário, computador ou OU do Active Directory.

3 – Rede Acadêmica da PUC Minas

3.1 - Rede acadêmica

A PUC Minas possui duas redes de computadores. Sendo que uma é a rede administrativa onde ficam ligados os computadores dos setores como Secretaria, Biblioteca, Apoio Comunitário e etc. Nesta rede os alunos não possuem acesso, pois os servidores de banco de dados que possuem todos os dados da PUC estão ligados a ela. Se os alunos tivessem acesso a esta rede, o risco de tentativa de invasão dos servidores seria muito maior. Para resolver este problema, foi criado a rede acadêmica, que estão ligados os laboratórios de informática.

A rede acadêmica possui um “link” WAN de internet que chega na PUC Coração Eucarístico e de lá é repassado para as Unidades através de links WAN entre elas. Ligado a este link, um servidor Firewall faz a proteção de ataques externos e que filtra acessos internos. Ligado a este Firewall, cada unidade possui um Firewall e um Proxy para compartilhamento de internet. Cada unidade possui um domínio que atualmente se chama pucmg.net, utilizando o Windows Server 2003, e neste domínio estão os laboratórios de informática que são acessados pelos alunos da PUC para aulas e desenvolvimentos de trabalhos acadêmicos.

Os domínios não se enxergam atualmente mas é plano para o futuro criar relação de confiança entre estes domínios para que um aluno de uma unidade consiga utilizar sua senha em qualquer outra unidade que estiver acessando.

3.2 - Login Individual aplicado à rede acadêmica.

O sistema de login individual deve ser instalado em todos os servidores de domínio da PUC Minas para que os usuários sejam criados corretamente. Se o sistema for instalado em um sistema operacional que não seja Windows Server 2003, é liberado somente a funcionalidade de consulta e impressão de carta de instruções.

O ideal é utilizar o sistema de login no servidor apenas para criação de cursos, unidades, usuários. As demais funcionalidades podem ser utilizadas em outra estação com qualquer sistema operacional. Com um servidor de domínio, deve-se ter o maior cuidado pois, se um dia ele parar, sua rede toda estará fora do ar e, uma rede fora do ar, é muito trabalho para os administradores. Os usuários são criados sempre no início do semestre, e no seu decorrer, os alunos solicitam sua senha na sala dos técnicos. As senhas são emitidas de acordo com a demanda dos alunos e é impressa mediante apresentação da carteira de aluno da PUC, ou documento de identidade ou comprovante de matrícula. Caso um aluno de uma unidade A queria utilizar os computadores de uma unidade B, o mesmo deve solicitar aos técnicos a criação de um usuário para o acesso. Esta criação é feita mediante a apresentação do comprovante de matrícula. No caso de unidades que tem acesso ao sistema SGA Administrativo, com a apresentação da carteira de aluno da PUC ou identidade, o técnico de laboratório pode averiguar a situação daquele aluno no sistema e criar seu usuário caso o aluno esteja matriculado. Estes casos de alunos de outras unidades acontecem sempre, uma vez que, estes alunos costumam fazer matérias fora de sua unidade de origem para ficar regular ou adiantar o curso. A cada novo semestre, estes usuários de outras unidades são

bloqueados, pois eles não estarão no arquivo de dados fornecido pelo DATAPUC. Caso eles voltem a utilizar os computadores no semestre seguinte, ele apenas solicita o desbloqueio do usuário apresentando o comprovante de matrícula.

Na rede acadêmica, os usuários possuem um perfil único que chama Perfil Ambulante. O conceito de perfil, são as configurações do computador que são carregadas quando ele vai utilizá-lo. Às vezes é necessário à existência de um perfil na rede e com o login individual, esta questão de perfil é tratada por cursos. Cada curso pode ter um perfil separado. Também existem os scripts de logon que ficam nos servidores e estes também são tratados como os perfis, por curso. É possível também informar no sistema que usuários de um determinado curso irá pertencer a um grupo criado no Active Directory. Estes cadastros de configurações por curso serão abordados no próximo capítulo.

3.3 - Segurança na rede acadêmica

A questão de segurança deve ser olhada com atenção pois a rede acadêmica é acessada por diversos alunos. Hoje é implementado na rede acadêmica um firewall no servidor gateway[16] e software antivírus em todas as estações. Utiliza-se também um software da Microsoft chamado SUS que já foi citado anteriormente, em síntese, sua função é baixar as atualizações de segurança do Windows e repassa elas para as máquinas sem que elas acessem internet, tudo pela rede local. O software antivírus é instalado a versão Server no controlador de domínio e a versão Client nas estações, o Server busca automaticamente atualizações de definições de vírus no site do produto e, automaticamente.

[16] Saída da sua rede para a internet

Estas definições são repassadas para cada estação da rede no momento que ela é ligada.

Com é utilizado o Windows Server 2003, é possível bloquear vários recursos das estações utilizando a ferramenta de Group Policy. Através dela é possível configurar várias políticas de segurança nas estações, como bloquear acesso a ferramentas restritas do administrador, ativar auditoria de logon, e etc. Com o Windows 2000 Server também existe este recurso mas, no Windows Server 2003 existem mais políticas implementadas nesta ferramenta. Outro recurso, que o Windows Server 2003 trouxe para questão de segurança, é a nova versão para o protocolo de autenticação chamado Kérberos. Com esta versão, tornar-se mais difícil quebrar uma senha que esteja armazenada no Active Directory. É importante frisar que é necessário utilizar uma política de senha complexa fazendo com que os usuários não utilizem senhas fáceis de quebrar.

Através de uso do Firewall e servidor de Proxy conseguimos bloquear acesso a vários sites que não são do meio acadêmico, como, por exemplo, sites de hackers, pornográficos e conteúdo impróprio. Utilizando o firewall, são liberadas apenas as portas necessárias. Para outras portas, que não devem ser acessadas do laboratório mas que são necessárias para acessar de outros computadores, é feito um filtro por IP para que este acesso seja liberado corretamente. Para este serviço de firewall é utilizado o software iptables[17] em ambiente Linux. Utilizando o serviço de proxy SQUID em ambiente Linux, é bloqueado o acesso aos sites indevidos. Existe uma largura de banda para uma determinada faixa de IP e regras para liberação de sites sem passagem pelo proxy como por exemplo sites internos da PUC Minas.

[17] Software de firewall para Linux

4 – Apresentação do Sistema

4.1 - Instalador

Como já mencionado anteriormente, o sistema de Login Individual foi desenvolvido para rodar nas plataformas Windows 9x/ME/NT/2000/XP/2003. No entanto, a utilização completa do sistema está disponível apenas no Windows Server 2003, devido à existência do Active Directory. Para que o sistema de login funcione corretamente, foi desenvolvido um instalador, personalizado que solicita ao administrador, parâmetros de conexão com o banco de dados. Além de copiar para o computador arquivos específicos para o funcionamento do sistema, o instalador cria na máquina, o Driver ODBC do MySQL configurado com o banco de dados do sistema de Login Individual. A Figura 3 mostra a solicitação de parâmetros para a criação do Driver ODBC no sistema operacional.

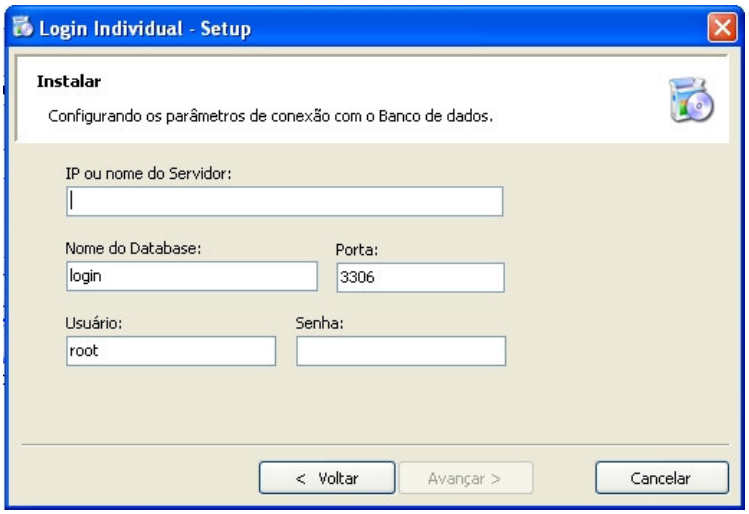


Figura 3: Parâmetros de banco de dados

Na próxima tela é configurado o diretório onde serão armazenado os arquivos gerados pelo sistema, Script de Logon padrão, Profile padrão, e Domínio. Estes arquivos contêm os scripts do Windows Server 2003 para a criação, modificação e remoção de usuários do Active Directory. A Figura 4 mostra esta solicitação de parâmetros gerais.

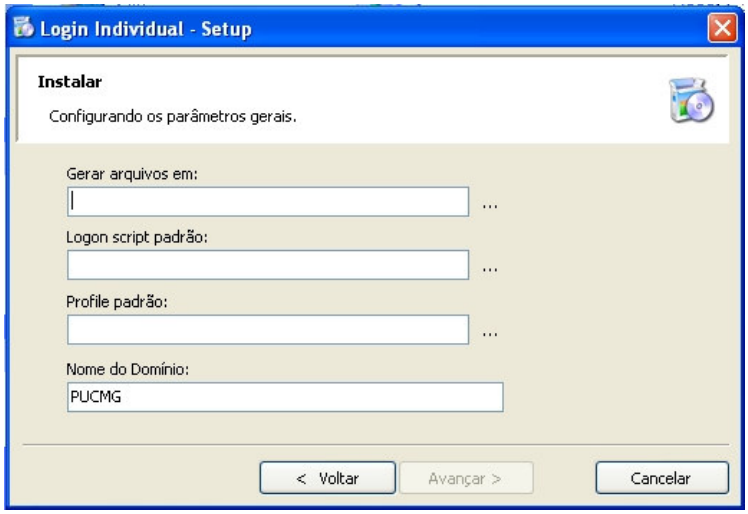


Figura 4: Parâmetros Gerais do Instalador

Após a passagem dos parâmetros para o Instalador, este irá copiar os arquivos necessários para o computador deixando assim o sistema instalado e Driver ODBC configurado. O banco de dados MySQL, necessário ao sistema, deve ser instalado separadamente. Depois de instalado o banco de dados, é necessário à execução de um Script SQL utilizando uma ferramenta de conexão, para a criação do banco de dados do sistema. Após a instalação do MySQL e do sistema de login, o sistema de login individual, o sistema já está pronto para funcionamento.

4.2 - Características

O sistema é todo baseado nos comandos do Windows Server 2003, dsadd, dsmod e dsrm. Estes comandos possuem muitos parâmetros que são criados, modificados ou removidos da estrutura do Active Directory. O sistema, a partir das informações contidas no banco de dados, gera arquivos de script que serão executados após execução de comandos do sistema.

Ao executar o sistema de Login no Windows Server 2003 pela primeira vez, o sistema pergunta para o administrador se ele deseja que seja criado dentro da estrutura do Active Directory as OUs das Unidades e Cursos da PUC já cadastrados em banco de dados. O administrador não criando esta estrutura, a criação de usuários pode não funcionar corretamente. No caso do administrador instalar o sistema em um controlador de domínio que já possua esta estrutura, ele vai clicar em “Não” e prosseguir na utilização do sistema. Executando em outra plataforma Windows isto não é feito.

O sistema possui as seguintes funcionalidades:

- Cadastro de usuário individual e por processamento de arquivo de texto
- Pesquisa de usuário para impressão da carta de instruções e alteração de senha
- Cadastro de configurações por curso
- Cadastro de Unidades e Cursos
- Alteração de senha do sistema

4.3 - Cadastro de Usuários

O cadastro de usuários no sistema pode ser feito de duas formas:

- Através de arquivo de Texto (todos os alunos de uma vez),
- Individualmente.

O arquivo de texto deve ser fornecido pelo DATAPUC. Este arquivo possui em cada linha as informações do aluno como: matrícula, nome, curso, período, turno, código da carteira de aluno e situação. Esta situação é que defini se o aluno terá seu usuário criado ou não no servidor Active Directory. As possíveis situações são:

- 0 – Não matriculado,
- 1 – Matriculado,
- 2 – Trancado,
- 3 – Cancelado,
- 4 – Transferido,
- 5 – Formado,
- 6 – Calouro Desistente,
- 7 – Desligado.

Das situações anteriores, apenas três situações permitem que o usuário permaneça no Active Directory, e apenas a situação 1, permite que o usuário faça o logon nos laboratórios. As situações 0 e 2 deixam o usuário bloqueado para o Logon podendo ser reativado mediante comprovante de matrícula. Nas demais situações, o usuário é excluído do Active Directory. O processamento do arquivo é feito linha a linha e assim que um aluno é processado, é gravado no arquivo de script do Windows Server 2003, qual operação a ser feita com o usuário. Neste script teremos

várias linhas ou uma linha no caso de cadastro individual, contendo comandos como dsadd, dsmod e dsrm. Estes comandos com os parâmetros passados, irão fazer operações no Active Directory de criação, alteração e remoção de usuários. Uma vez gravando no arquivo, caso a situação seja diferente de 0, 1 e 2, o registro é excluído do banco de dados. Na Figura 5, a tela de cadastro de usuário e processamento de arquivos.

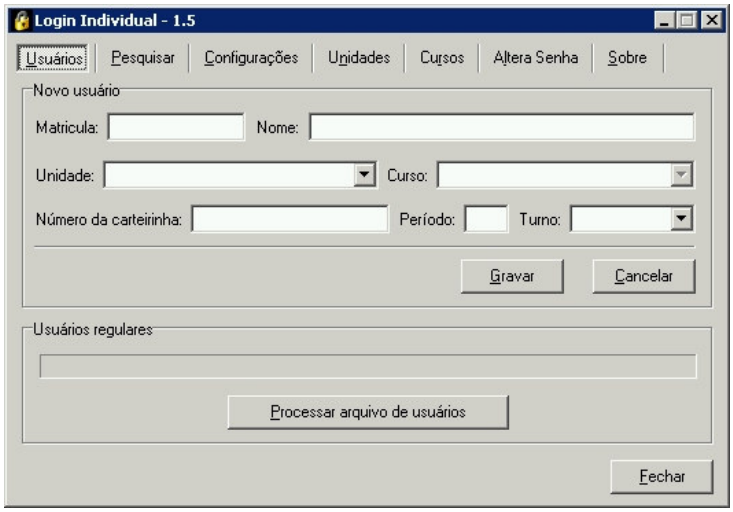


Figura 5: Cadastro de usuário e processamento de arquivo

4.4 - Impressão de Instruções e Alteração de Senha

A funcionalidade de pesquisa de usuário tem como objetivo, localizar o usuário para a impressão de instruções e alteração de senha. Pode-se fazer esta pesquisa através do número de matrícula, ou nome do aluno ou utilizando um leitor de código de barra passando a carteira do aluno com o sistema focando para o campo Numero da Carteirinha. A pesquisa retorna para o administrador os alunos cadastrados de acordo com o que foi informado nos campos. Pode-se visualizar na pesquisa a matricula, nome, situação e se já foi impresso a carta de instruções. Uma vez encontrado o aluno desejado, clica-se nele e habilita os botões de alteração de senha e emissão de instruções. Na figura 6 pode-se visualizar como é esta tela do sistema.

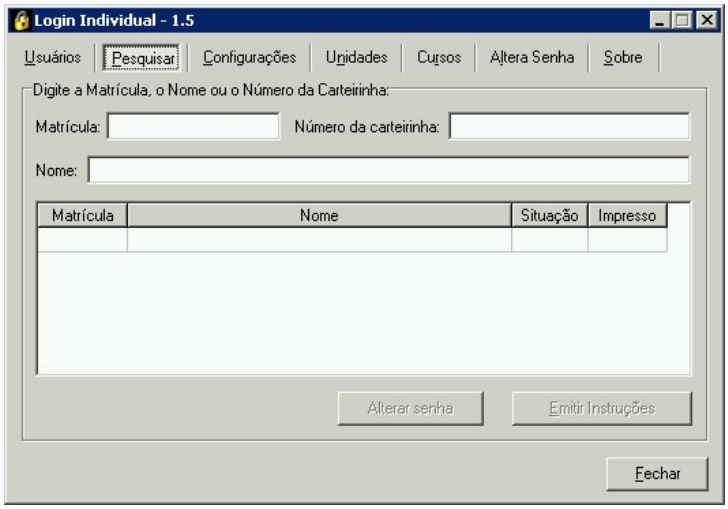


Figura 6: Tela de pesquisa de alunos para impressão de carta de instruções ou alteração de senha.

4.5 - Cadastro de Configurações

Esta funcionalidade do sistema é feita individualmente por curso. Tem como objetivo diferenciar configurações de Logon Script[18], Profile[19] e Grupo[20] para os usuários. Se for necessário ter alguma configuração específica por curso, este cadastro deve ser feito antes do processamento ou cadastro individual de usuários. Só após poderá efetuar o processamento do arquivo. Uma vez cadastrado estas configurações, no momento do processamento do arquivo ou criação individual de usuário, é verificado, para o aluno, se existe uma configuração específica para o curso que ele está matriculado e, caso não exista, são utilizadas as configurações padrões definidas na instalação do sistema. Na Figura 7 uma amostra da tela de cadastro de configurações.

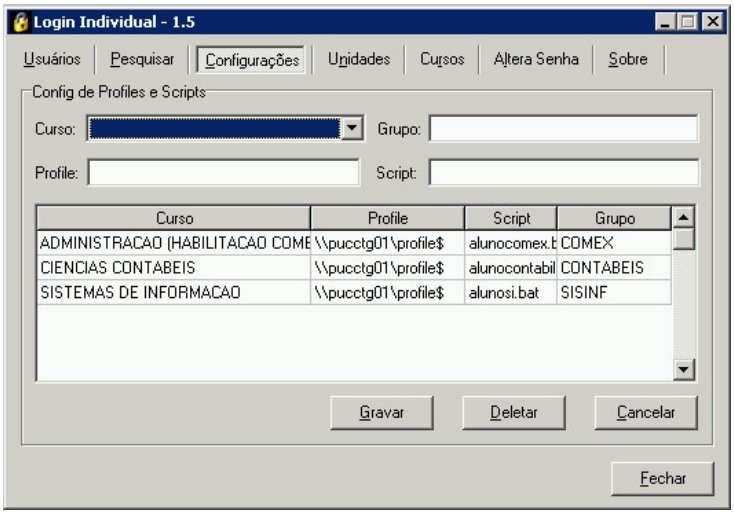


Figura 7: Tela de cadastro de configurações de Profile, Script de Logon e Grupo

[18] Script de usuário que é executado no momento do logon
[19] Perfil utilizado pelo usuário no computador
[20] Grupo de usuários definido no Active Directory

4.6 - Cadastro de Unidades e Cursos

A funcionalidade de cadastro de Unidades e Cursos será utilizada quando a PUC criar uma nova unidade ou abrir um curso novo na Instituição. O objetivo desta funcionalidade é manter a organização do Active Directory na criação de usuários. Cadastrando um curso novo ou uma unidade nova no sistema, automaticamente será criado no Active Directory as respectivas OUs para organização dos usuários utilizando os comandos do Windows Server 2003, dsadd ou dsmod. Nas figuras 8 e 9, as telas de cadastro de Unidades e Cursos.

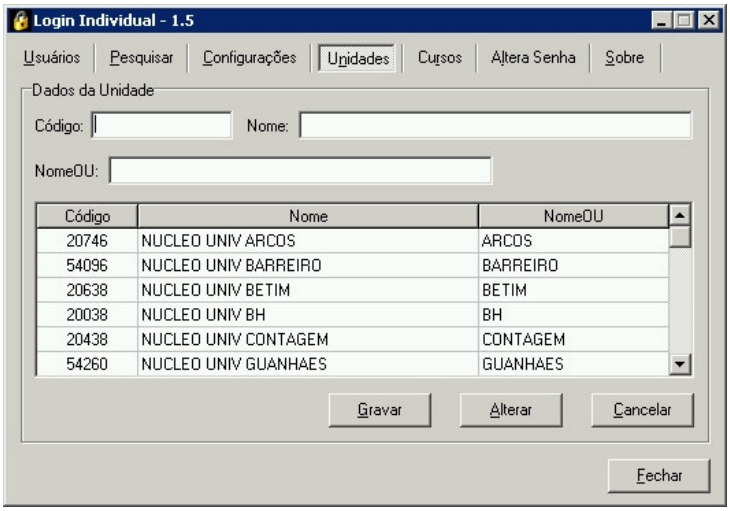


Figura 8: Tela de cadastro de Unidades

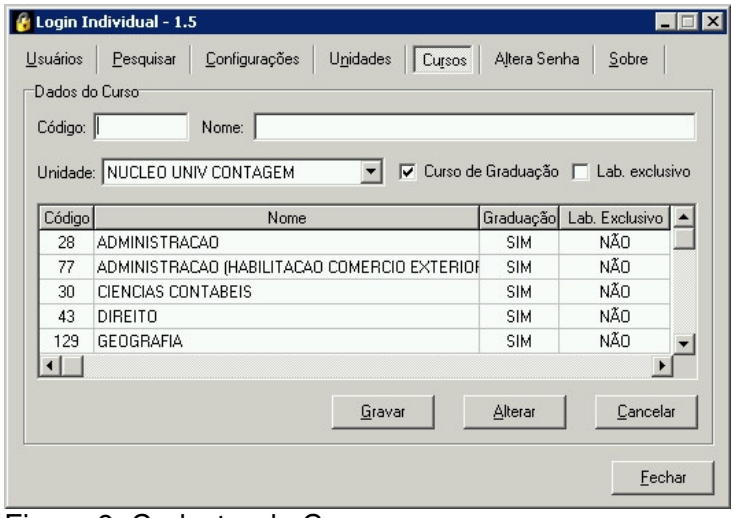


Figura 9: Cadastro de Cursos

4.7 - Alteração de Senha

A funcionalidade de alteração de senha permite alterar a senha de usuário e o login do sistema. Foi criada esta funcionalidade para aumentar mais a segurança do sistema, pois, o mesmo vem com o usuário e senha padrão. Para que esta alteração seja feita é necessário entrar com a senha atual. Na figura 10 a tela de alteração de senha.

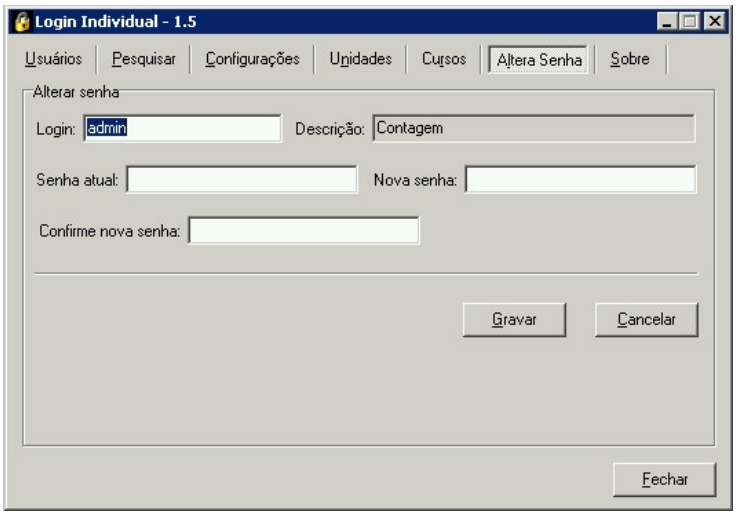


Figura 10: Tela de alteração de senha de acesso ao sistema

5 – Conclusão

Com a implantação do sistema de login individual, verificamos que os laboratórios da PUC, como um todo, ficaram mais disponíveis para os alunos, uma vez que muitas vezes existiam pessoas que não são do meio acadêmico utilizando os laboratórios. Além disto, obteve-se melhoras com relação à segurança pois, com a utilização de auditoria na rede e nas máquinas locais, é possível identificar alunos que estão infringindo as normas do laboratórios, como acesso a sites impróprios, instalação de jogos nos computadores ou mesmo se efetuar um ataque maia agressivo à rede. O sistema de login também proporcionou a liberação de laboratórios exclusivos e um espaço em disco de 15 MegaBytes para alunos do curso de Sistemas de Informação na unidade da PUC Contagem.

Existem 2 projetos para o sistema de login. O primeiro é o desenvolvimento de uma interface Web do sistema, para que não seja necessário ir ao servidor para criação de usuários, alteração de senhas, status do usuário, liberar acesso aos laboratórios de Sistemas de Informação e etc. O projeto do sistema com o funcionamento pela Web já está em desenvolvimento utilizando a linguagem o PHP sobre e o servidor de Apache[21]. O segundo projeto seria o estudo da plataforma .NET[22] da Microsoft para o desenvolvimento do sistema de login individual com acesso direto ao Active Directory, sem utilização de linhas de comando. No desenvolvimento deste projeto, é necessário verificar o desempenho de acesso ao Active Directory para saber se é mais viável utilizar o sistema compilado na plataforma .NET.

[21] Servidor de páginas Web para plataforma Linux e Windows

[22] Maquina virtual desenvolvida pela microsoft que agiliza o desenvolvimento e tornaos sistemas mais portaveis para diversas plataformas

Referências

BATTISTI, Júlio. Windows Server 2003 Curso Completo
Editora Axcel Books,
Rio de Janeiro, 2003.

MICROSOFT. Active Directory. Disponível em:
http://www.microsoft.com/brasil/windowsserver2003/tec_active.mspx
Acesso em: 8 de outubro de 2004

HARA, Fábio. Novas Ferramentas do Windows Server 2003. Disponível em :
http://superdownloads.ubbi.com.br/materias/20040204,227,1.html
Acesso em 9 de outubro de 2004

HARA, Fábio. Windows 2003 Server. Disponível em:
http://superdownloads.ubbi.com.br/materias/20030213,177,1.html
Acesso em 9 de outubro de 2004

CAMPOS, Eduardo. Uma arma chamada Windows 2003.
Revista Network, São Paulo.
Ano 4, N° 51, maio 2003.

SYMANTEC, Gerenciando a Segurança Corporativa. Disponível em:
http://66.90.88.250/downloads/414_seg_corporativa.zip
Acesso em 5 de novembro de 2004

ALLEN, Robbie. Active Directory Cookbook for Windows Server 2003 and Windows 2000.
Editora O'Reilly

DINLEY, D. "Should outsourcing be part of your IT act?"
InfoWorld Outsourcing Study, InfoWorld,
12 de fevereiro de 2001.

Anexos

Anexo A – Banco de Dados

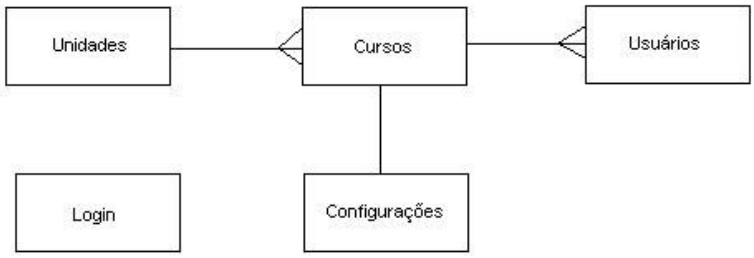
Anexo B – Modelo ER

Anexo C – Partes do código fonte da aplicação gerada

Anexo A

```
#
# Table structure for table configuracoes
#

CREATE TABLE `configuracoes` (
  `COD_CURSO` int(10) NOT NULL default '0',
  `PROFILE` varchar(100) default NULL,
  `SCRIPT` varchar(100) default NULL,
  `GRUPO` varchar(20) NOT NULL default '',
  PRIMARY KEY  (`COD_CURSO`),
  KEY `COD_CURSO` (`COD_CURSO`)
) TYPE=InnoDB;

#
# Table structure for table cursos
#

CREATE TABLE `cursos` (
  `COD_CURSO` int(10) NOT NULL default '0',
  `DESCRICAO` varchar(80) NOT NULL default '',
  `COD_UNIDADE` varchar(10) NOT NULL default '0',
  `OU` varchar(250) default NULL,
  `GRADUACAO` char(1) NOT NULL default '',
  `LAB_EXCLUSIVO` char(1) default NULL,
  PRIMARY KEY  (`COD_CURSO`),
  KEY `COD_UNIDADE` (`COD_UNIDADE`)
) TYPE=InnoDB;

#
# Table structure for table login
#

CREATE TABLE `login` (
  `LOGIN` varchar(20) NOT NULL default '',
  `COD_UNIDADE` varchar(10) default NULL,
  `DESCRICAO` varchar(50) default NULL,
  `SENHA` varchar(16) default NULL,
  PRIMARY KEY  (`LOGIN`)
) TYPE=InnoDB;

#
# Table structure for table unidades
#

CREATE TABLE `unidades` (
  `COD_UNIDADE` varchar(10) NOT NULL default '0',
  `DESCRICAO` varchar(50) default NULL,
  `NOMEOU` varchar(100) default NULL,
  PRIMARY KEY  (`COD_UNIDADE`)
) TYPE=InnoDB;

#
# Table structure for table usuarios
#

CREATE TABLE `usuarios` (
  `MATRICULA` varchar(15) NOT NULL default '0',
  `COD_CURSO` int(5) unsigned NOT NULL default '0',
  `TURNO` char(1) NOT NULL default '',
  `COD_SITUACAO` int(5) unsigned default NULL,
  `NOME` varchar(50) NOT NULL default '',
  `PERIODO` char(2) NOT NULL default '0',
  `SENHA` varchar(20) NOT NULL default '',
  `LAB_EXCLUSIVO` char(1) NOT NULL default '',
  `IMPRESSO` char(1) NOT NULL default '0',
  `N_CARTEIRA` varchar(25) default NULL,
  PRIMARY KEY  (`MATRICULA`),
  KEY `NOME` (`NOME`),
  KEY `MATRICULA` (`MATRICULA`),
  KEY `LAB_EXCLUSIVO` (`LAB_EXCLUSIVO`)
) TYPE=InnoDB;
```

Anexo B



Anexo C

Código fonte do processamento de arquivos

```
if OpenArquivoDialog.Execute then
begin
     Linhas := TStringList.Create;
     Linhas.LoadFromFile(OpenArquivoDialog.FileName);

     TotalLinhas := Linhas.Count-1;

     LinhaDupla := Linhas.Strings[TotalLinhas];
     Linhas.Insert(Linhas.Count, LinhaDupla);

     SubstituiCaracteres(Linhas);
end
else
begin
     MessageDlg('Erro ao abrir o arquivo!', mtError, [mbOK], 0);
     Exit;
end;

Caminho := NomeArquivo('C_Usuarios');

AssignFile(Usuarios, Caminho);
Rewrite(Usuarios);

ProgressBar.Position := ProgressBar.Position + 2;

for NLinha := 0 to TotalLinhas do
begin
     Linha := Linhas.Strings[NLinha];

     Tam := Length(Linha);

     Indice := 1;
     Cont := 0;

     i := 1;

     for NChar := 0 to Tam do
     begin
          Caracter := Copy(Linha, i, 1);

          if Caracter = ';' then
          begin
               case Cont of
                    0 : Dados[1] := Copy(Linha, Indice, i-Indice);
                    1 : Dados[2] := Copy(Linha, Indice, i-Indice);
```

```
                        2 : Dados[3] := Copy(Linha, Indice, i-Indice);
                        3 : Dados[4] := Copy(Linha, Indice, i-Indice);
                        4 : Dados[5] := Copy(Linha, Indice, i-Indice);
                        5 : Dados[6] := Copy(Linha, Indice, i-Indice);
                        6 : begin
                                  Dados[7] := Copy(Linha, Indice, i-
Indice);
                                  Dados[8] := Copy(Linha, i+1, Tam-1);   //
+ Copy(Linha, i+5, Tam-i);

                                  Break;
                              end;
                    end;

                    Inc(Cont);
                    Indice := i + 1;

                    i := i + Length(Copy(Linha, Indice, i-Indice));
               end;
               Inc(i);
          end;

          Senha := GeraSenha;

          Configuracao := Configuracoes(Dados[3], Dados[6]);

          OpenSQL('select LAB_EXCLUSIVO from cursos where COD_CURSO =
"'+Dados[3]+'"');
          LabExclusivo :=
dtm_Tabelas.qrySelect.FieldByName('LAB_EXCLUSIVO').AsString;

          {
          Configuracao[1] -> Script
          Configuracao[2] -> Profile
          Configuracao[3] -> NomeCurso
          Configuracao[4] -> NomeUnidade
          Configuracao[5] -> OUCurso
          Configuracao[6] -> NomeOU
          Configuracao[7] -> Grupo
          }

          //Grava No MySQL e grava ou apaga no 2003

          if not ChavePrimaria('MATRICULA', 'usuarios', Dados[1], False)
then // nao existe no Banco
          begin
               if (Dados[7] = '1') then    //insere
               begin
                    ExecSQL('insert into usuarios (MATRICULA, COD_CURSO,
TURNO, COD_SITUACAO, NOME, PERIODO, SENHA, LAB_EXCLUSIVO, IMPRESSO,
N_CARTEIRA)
values("'+Dados[1]+'","'+Dados[3]+'","'+Dados[5]+'","'+Dados[7]+'","'+Dados
[2]+'","'+Dados[4]+'","'+Senha+'","'+LabExclusivo+'","0","'+Dados[8]+'")');

                    LinhaCmd := 'dsadd user
"CN='+Dados[1]+','+Configuracao[5]+',OU=Unidades,DC=pucmg,DC=net" -samid
'+Dados[1]+' -upn '+Dados[1]+'@pucmg.net -display "'+Dados[2]+'" -pwd
'+Senha+' -fn "'+Dados[2]+'" -desc "Curso: '+Configuracao[3]+' Periodo:
'+Dados[4]+' Turno: '+Dados[5]+'" -office "'+Configuracao[4]+'" -profile
'+Configuracao[2]+' -loscr '+Configuracao[1]+' -mustchpwd yes';

                    if Trim(Configuracao[7]) <> '' then
                    begin
                         LinhaCmd := LinhaCmd + ' -memberof CN='+
Configuracao[7]+',CN=Users,DC=pucmg,DC=net';
                    end;

                    Writeln(Usuarios, LinhaCmd);
               end
               else
```

```
               if (Dados[7] = '2') then    //insere desabilitado
               begin
                    ExecSQL('insert into usuarios (MATRICULA, COD_CURSO,
TURNO, COD_SITUACAO, NOME, PERIODO, SENHA, LAB_EXCLUSIVO, IMPRESSO,
N_CARTEIRA)
values("'+Dados[1]+'","'+Dados[3]+'","'+Dados[5]+'","'+Dados[7]+'","'+Dados
[2]+'","'+Dados[4]+'","'+Senha+'","'+LabExclusivo+'","0","'+Dados[8]+'")');

                    LinhaCmd := 'dsadd user
"CN='+Dados[1]+','+Configuracao[5]+',OU=Unidades,DC=pucmg,DC=net" -samid
'+Dados[1]+' -upn '+Dados[1]+'@pucmg.net -display "'+Dados[2]+'" -pwd
'+Senha+' -fn "'+Dados[2]+'" -desc "Curso: '+Configuracao[3]+' Periodo:
'+Dados[4]+' Turno: '+Dados[5]+'" -office "'+Configuracao[4]+'" -profile
'+Configuracao[2]+' -loscr '+Configuracao[1]+' -mustchpwd yes -disabled
yes';

                    if Trim(Configuracao[7]) <> '' then
                    begin
                         LinhaCmd := LinhaCmd + ' -memberof CN=' +
Configuracao[7]+',CN=Users,DC=pucmg,DC=net';
                    end;

                    Writeln(Usuarios, LinhaCmd);
               end;
          end
          else    //ja existe no banco
          begin
               if (Dados[7] = '1') then     //atualiza
               begin
                    ExecSQL('update usuarios set COD_CURSO="'+Dados[3]+'",
TURNO="'+Dados[5]+'", COD_SITUACAO="'+Dados[7]+'", NOME="'+Dados[2]+'",
PERIODO="'+Dados[4]+'", N_CARTEIRA="'+Dados[8]+'" where
MATRICULA="'+Dados[1]+'"');

                    //Esta linha deve atualizar com dsmod SEM mexer com
disable
                    LinhaCmd := 'dsmod user
"CN='+Dados[1]+','+Configuracao[5]+',OU=Unidades,DC=pucmg,DC=net" -upn
'+Dados[1]+'@pucmg.net -display "'+Dados[2]+'" -fn "'+Dados[2]+'" -desc
"Curso: '+Configuracao[3]+' Periodo: '+Dados[4]+' Turno: '+Dados[5]+'" -
office "'+Configuracao[4]+'" -profile '+Configuracao[2]+' -loscr
'+Configuracao[1] + ' -disabled no';

                    if Trim(Configuracao[7]) <> '' then
                    begin
                         LinhaCmd := LinhaCmd + ' -memberof CN=' +
Configuracao[7]+',CN=Users,DC=pucmg,DC=net';
                    end;

                    Writeln(Usuarios, LinhaCmd);
               end
               else
               if (Dados[7] = '0') or (Dados[7] = '2') then    //atualiza
desabilitado
               begin
                    ExecSQL('update usuarios set COD_CURSO="'+Dados[3]+'",
TURNO="'+Dados[5]+'", COD_SITUACAO="'+Dados[7]+'", NOME="'+Dados[2]+'",
PERIODO="'+Dados[4]+'", N_CARTEIRA="'+Dados[8]+'" where
MATRICULA="'+Dados[1]+'"');

                    LinhaCmd := 'dsmod user
"CN='+Dados[1]+','+Configuracao[5]+',OU=Unidades,DC=pucmg,DC=net" -disabled
yes';

                    if Trim(Configuracao[7]) <> '' then
                    begin
                         LinhaCmd := LinhaCmd + ' -memberof CN=' +
Configuracao[7]+',CN=Users,DC=pucmg,DC=net';
                    end;
```

```
                    Writeln(Usuarios, LinhaCmd);
               end
               else
               begin         //remove
                    ExecSQL('delete from usuarios where
MATRICULA="'+Dados[1]+'"');

                    LinhaCmd := 'dsrm
"CN='+Dados[1]+','+Configuracao[5]+',OU=Unidades,DC=pucmg,DC=net" -
noprompt';

                    Writeln(Usuarios, LinhaCmd);
               end;
          end;

          ProgressBar.Position := ProgressBar.Position + 1;
     end;

     CloseFile(Usuarios);

     try
        WinExec(PChar(Caminho), SW_MINIMIZE);
     except
           MessageDlg('Erro ao atualizar cadastro de usuários no Active
Directory!'#13'Você deverá executar "'+Caminho+'" manualmente.',
mtInformation, [mbOK], 0);

           Exit;
     end;

     Linhas.Free;

     MessageDlg('Arquivo processado com sucesso! Aguarde a criação dos
usuários...', mtInformation, [mbOK], 0);
```

Código fonte da função de alteração de senha de usuário

```
     btnInstrucoes.Enabled := False;
     btnAltSenha.Enabled := False;

     if Trim(dtm_Tabelas.qryUsuarios.SQL.Text) = '' then
        Exit;

     Matricula :=
dtm_Tabelas.qryUsuarios.FieldByName('MATRICULA').AsString;
     OUCurso := dtm_Tabelas.qryUsuarios.FieldByName('OU').AsString;

     if not (dtm_Tabelas.qryUsuarios.RecordCount = 0) then
     begin
          if dtm_Tabelas.qryUsuarios.FieldByName('COD_SITUACAO').AsString =
'Trancado' then
          begin
               Exit;
          end
          else
          if dtm_Tabelas.qryUsuarios.FieldByName('IMPRESSO').AsString =
'SIM' then
          begin
               ExecSQL('update usuarios set SENHA = "1234" where MATRICULA
= "'+Matricula+'"');

               if not ExecComando('A_' + Matricula, 'dsmod user
"CN='+Matricula+','+OUCurso+',OU=Unidades,DC=pucmg,DC=net" -pwd 1234 -
mustchpwd yes') then
               begin
                    MessageDlg('Erro ao alterar a senha do usuário!',
mtInformation, [mbOK], 0);

                    Exit;
```

```
          end;
     end
     else
         Exit;
end;

btnInstrucoes.Enabled := False;
btnAltSenha.Enabled := False;
```

Código da geração de OU do Active Directory

```
procedure TfrmLogin.VerificaOU;
          var JaCriouOU, CodCurso : ShortString;
              NomeCurso, OU, NomeOU, Caminho : String;
              Parametros : TRegistry;
              CriaOU : TextFile;
              i : Integer;
begin
     try
        with Parametros do
        begin
             Parametros := TRegistry.Create(KEY_ALL_ACCESS);
             Parametros.RootKey := HKEY_LOCAL_MACHINE;

             CloseKey;

             OpenKey('Software\LoginIndividual', False);

             JaCriouOU := ReadString('OU');
        end;
     except
           MessageDlg('Erro ao ler dados do Registro! A reinstalação do
sistema pode resolver o problema', mtError, [mbOK], 0);
           Application.Terminate;
           Exit;
     end;

     if JaCriouOU = '0' then
     begin
          if MessageDlg('Existem OU''s que ainda não foram criadas no
Active Directory do Windows 2003. Deseja criá-las? Obs.: Não será possível
criar usuários sem que essas OU''s sejam criadas.', mtConfirmation,
[mbYes,mbNo], 0) <> mrYes then
             Exit;

          Caminho := NomeArquivo('CriaOU');

          AssignFile(CriaOU, Caminho);
          Rewrite(CriaOU);

          OpenSQL('select COD_UNIDADE, NOMEOU from unidades');

          for i:=0 to dtm_Tabelas.qrySelect.RecordCount-1 do
          begin
               NomeOU :=
dtm_Tabelas.qrySelect.FieldByName('NOMEOU').AsString;

               OU := 'dsadd ou "OU='+NomeOU+',OU=Unidades,DC=pucmg,DC=net"
-desc "'+NomeOU+'"';

               Writeln(CriaOu, OU);

               OU := 'dsadd ou
"OU=Usuarios,OU='+NomeOU+',OU=Unidades,DC=pucmg,DC=net" -desc
"'+NomeOU+'"';

               Writeln(CriaOu, OU);

               dtm_Tabelas.qrySelect.Next;
          end;

          OpenSQL('select COD_CURSO, cursos.DESCRICAO as DESCRICAO, NOMEOU
from cursos, unidades where unidades.COD_UNIDADE = cursos.COD_UNIDADE');

          for i:=0 to dtm_Tabelas.qrySelect.RecordCount-1 do
          begin
               NomeCurso :=
dtm_Tabelas.qrySelect.FieldByName('DESCRICAO').AsString;
```

```
               CodCurso :=
dtm_Tabelas.qrySelect.FieldByName('COD_CURSO').AsString;
               NomeOU :=
dtm_Tabelas.qrySelect.FieldByName('NOMEOU').AsString;

               OU := 'dsadd ou
"OU='+NomeCurso+',OU=Usuarios,OU='+NomeOU+',OU=Unidades,DC=pucmg,DC=net" -
desc "'+NomeCurso+'"';

               Writeln(CriaOu, OU);

               ExecSQL('update cursos set OU =
"OU='+NomeCurso+',OU=Usuarios,OU='+NomeOU+'" where COD_CURSO = '+CodCurso);

               dtm_Tabelas.qrySelect.Next;
          end;

          Parametros.WriteString('OU', '1');

          CloseFile(CriaOU);

          try
             WinExec(PChar(Caminho), SW_MINIMIZE);
          except
               MessageDlg('Erro ao criar OU!! O cadastro de usuários no
Windows 2003 não será executado automaticamente.', mtInformation, [mbOK],
0);
          end;
     end;
end;
```