UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

DEPARTAMENTO ACADÊMICO DE INFORMÁTICA

ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

GUILHERME LUIZ KRYNCZAK

MARCIO LUIZ BARBATO JUNIOR

INTEGRAÇÃO DO PROTOCOLO LDAP NA IMPLEMENTAÇÃO DE POLÍTICAS DE SEGURANÇA EM UMA REDE DE COMPUTADORES

TRABALHO DE CONCLUSAO DE CURSO

PONTA GROSSA

2015

GUILHERME LUIZ KRYNCZAK

MARCIO LUIZ BARBATO JUNIOR

INTEGRAÇÃO DO PROTOCOLO LDAP NA IMPLEMENTAÇÃO DE POLÍTICAS DE SEGURANÇA EM UMA REDE DE COMPUTADORES

Trabalho de Conclusão de Curso apresentada como requisito parcial à obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas, do Departamento Acadêmico de Informática, da Universidade Tecnológica Federal do Paraná.

Orientador: Prof. Msc. Rogério Ranthum

PONTA GROSSA

2015

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Campus Ponta Grossa

Diretoria de Pesquisa e Pós-Graduação
Tecnologia em Análise e Desenvolvimento de Sistemas

TERMO DE APROVAÇÃO

INTEGRAÇÃO DO PROTOCOLO LDAP NA IMPLEMENTAÇÃO DE POLÍTICAS DE SEGURANÇA EM UMA REDE DE COMPUTADORES

por

GUILHERME LUIZ KRYNCZAK

MARCIO LUIZ BARBATO JUNIOR

Este Trabalho de Conclusão de Curso foi apresentado em 05 de novembro de 2015 como requisito parcial para a obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____

Rogério Ranthum
Prof. Orientador

_____

Richard Duarte Ribeiro
Membro titular

_____

Geraldo Ranthum
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso –

Dedicamos este trabalho as nossas famílias pelo apoio incondicional e compreensão em todos os momentos.

AGRADECIMENTOS

Marcio Luiz Barbato Junior:

Primeiramente agradeço a Deus por ter me dado força e saúde para conseguir completar esta etapa.

Ao Professor Rogério Ranthum pela orientação e empenho dedicado a elaboração deste trabalho.

Agradeço a Minha Família pela compreensão da minha ausência e incentivo nos momentos difíceis.

Agradeço a Minha Namorada Daiane de Oliveira pelo incentivo, pelo companheirismo e por nunca me deixar desistir.

Agraço ao meu amigo e colega Guilherme pelos conhecimentos trocados não somente na elaboração deste trabalho como na vida profissional.

A todos que em algum momento fizeram parte da minha caminhada nesta universidade meus mais sinceros agradecimentos.

Guilherme Luiz Krynczak:

Primeiramente gostaria de agradecer ao meu Pai Jorge e à minha mãe Lidia por terem tido total compreensão e por terem acreditado em mim nos momentos difíceis.

Agradeço ao Professor Rogério Ranthum por ter nos orientado e a nos ter dado a confiança necessária para conseguir elaborar, desenvolver e finalizar este trabalho.

Agradeço ao meu amigo Marcio que me ajudou a concluir o objetivo deste trabalho e por toda a companhia dedicada a vencermos esta fase, além da grande amizade existente entre nós.

E finalmente agradeço a minha Namorada Kamila dos Santos Simão por ter ficado ao meu lado em todos os momentos que precisei, por ter me falado palavras de incentivo, por não me deixar desistir dos meus sonhos e por me fazer o homem mais feliz possível ao seu lado.

RESUMO

BARBATO, Marcio. KRYNCZAK, Guilherme. **INTEGRAÇÃO DO PROTOCOLO LDAP NA IMPLEMENTAÇÃO DE POLÍTICAS DE SEGURANÇA EM UMA REDE DE COMPUTADORES**. 2015. 60 páginas. Trabalho de Conclusão de Curso de Tecnologia em Análise e Desenvolvimento de Sistemas - Universidade Tecnológica Federal do Paraná. Ponta Grossa, 2015.

Com a demanda das empresas buscando formas rápidas e eficientes de melhor se adaptar às tecnologias atuais e buscando maneiras de reduzir custos através da centralização de serviços, este trabalho tem por objetivo integrar o serviço *Microsoft Active Directory* com o serviço *OpenLDAP* em ambiente virtualizado. Foi realizada uma revisão na literatura onde foram levantadas as principais tecnologias para a integração dos serviços, passando por redes de computadores, suas topologias e melhores práticas de segurança, serviços de diretório, controladores de domínio, *Microsoft Active Directory*, *OpenLDAP*, DNS e políticas de grupo. Para implementar o serviço *Microsoft Active Directory* foi utilizado um servidor virtual *Microsoft Windows Server* 2012 R2 o qual serve de base para os serviços *Active Directory Domain Services* (AD DS) e *Active Directory Certificate Services* (AD CS). O serviço *OpenLDAP* foi instalado em um servidor virtual CentOS 6 e também o *software* LDAP *Synchronization Connector*. Para realizar a sincronia entre as bases de dados foi utilizado o *software* LDAP *Synchronization Connector*, o qual tem como função realizar o serviço de integração a fim de facilitar um serviço considerado complicado, que é a implementação tradicional da sincronização. São demonstradas as etapas básicas iniciando por instalação e configuração de um domínio *Microsoft Active Directory* e instalação e inicialização de uma base de dados *OpenLDAP* até a implementação de políticas de segurança as quais foram usadas para restrições de acesso no sistema operacional *Microsoft Windows*, visando o fortalecimento da rede computacional. No fim deste trabalho é demonstrada a sincronia de contas de usuário do *Microsoft Active Directory* com a base de dados *OpenLDAP* de forma simplificada devido a utilização do LDAP *Synchronization Connector*, como também são demonstradas por meio de políticas de segurança, restrições que impedem o acesso à informações indevidas. Com estas restrições atingimos o objetivo de melhorar a segurança em uma rede corporativa.

Palavras-chave: *Active Directory*. *OpenLDAP*. Integração. Políticas de Segurança. LDAP *Synchronization Connector*.

ABSTRACT

BARBATO, Marcio. KRYNCZAK, Guilherme. **LDAP integration in *the* implementation of security policies in a computer network.** 2015. 60 pages. Trabalho de Conclusão de Curso de Tecnologia em Análise e Desenvolvimento de Sistemas - Federal Technology University - Parana. Ponta Grossa, 2015.

With the demand from companies seeking fast and efficient ways to better adapt to current technologies and seeking ways to reduce costs by centralizing services, this work has as objective the integration of the Microsoft Active Directory service and OpenLDAP service in a virtualized environment. It was made a revision on literature where the key technologies have been raised to the integration of the Services, going through computer networks, its topologies and security best practices, Directory Services, Domain controllers, Microsoft Active Directory, OpenLDAP, DNS and group policies. To implement the Microsoft Active Directory service, it was used a virtual Microsoft Windows Server 2012 R2, which provides the basis for the Active Directory Domain Services (AD DS) and Active Directory Certificate Services (AD CS) database. The OpenLDAP service was installed on a virtual CentOS 6 Server besides LDAP Synchronization Connector software. To achieve synchronization between the databases it was used the LDAP Synchronization Connector software, which has the function of performing the integration service in order to make easier a service that is considered complicated. The basic steps starting with installation and configuration of a Microsoft Active Directory Domain and installation and initialization of an OpenLDAP database is demonstrated by implementing security policies, which will be used to apply access restrictions on a Microsoft Windows operating system, aimed at strengthening the network computer. At the end of this paper it is demonstrated the synchronization between Microsoft Active Directory user accounts and an OpenLDAP database in a simplified way due to the use of LDAP Synchronization Connector, as also demonstrated by means of security policies, restrictions that prevent access to unauthorized information. With such restrictions we achieved the goal of improving security in a corporate network.

Keywords: *Active Directory. OpenLDAP. Integration. Security Policies. LDAP Synchronization Connector.*

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

AD	*Active Directory* - Diretório Ativo
AD CS	*Active Directory* Certificate *Services* - Serviços de Certificados do *Active Directory*
AD DC	*Active Directory Domain Services* - Serviços de Domínio do *Active Directory*
API	*Application Programming Interface* - Interface de Programação de Aplicativos
CA	*Certificate Authority* - Autoridade de Certificação
CentOS	*Community Enterprise Operational System*
CMD	*Command Prompt* - *Prompt* de Comando
CSV	*Comma Separated Value* - Valores Separados por Virgula
DHCP	*Dynamic Host Configuration Protocol* - Protocolo de Configuração Dinâmica de *Host*
DNS	*Domain Name System* - Sistema de Nome de Domínio
DSRM	*Directory Services Restore Mode* - Restauração dos Serviços de Diretório
DVD	*Digital Versatile Disk* - Disco Digital Versátil
FQDN	*Fully Quallified Domain Name* - Domínio Completamente Expressado
GPO	*Group Policy Object* - Objeto de Política de Grupo
HD	*Hard Disk* - Disco Rígido
IP	*Internet Protocol* - Protocolo de Internet
JDBC	*Java Database Connectivity* - Conectividade de Banco de Dados Java
LDAP	*Lightweight Directory Access Protocol*
LSC	LDAP *Synchronization Connector* - Conector de sincronização LDAP
MMC	*Microsoft Management Console* - Console de Administração *Microsoft*
MX	*Mail Exchanger* - Intercâmbio de Correio
Netbios	*Network Basic Input/Output System* - Sistema Básico de Rede de Entrada/Saída
OpenLDAP	*Open Lightweight Directory Access Protocol*
OU	*Organization Unit* - Unidade Organizacional
PDC	*Primary Domain Controller* - Controlador de Domínio Primário
RFC	*Request for Comments*
RSA	Ronald Rivest, Adi Shamir e Leonard Adleman
SHA	*Secure Hash Algorithm* - Algoritmo - Algoritmo de *Hash* Seguro

TCP/IP	*Transmission Control Protocol* / *Internet Protocol* - Protocolo de Controle de Transmissão / Protocolo de Internet
TI	Tecnologia de Informação
USB	*Universal Serial Bus*
WPD	*Windows Portable Devices* - Dispositivos portáteis do *Windows*

SUMÁRIO

1 INTRODUÇÃO

Como forma de crescimento, uma empresa concentra seus dados em meios digitais para melhor se adaptar às tecnologias atuais, e devido ao rápido crescimento da tecnologia da informação nos últimos anos, gerou-se muitos serviços que, para controle de acesso a informação, demandam autenticação. Porém isto gerou um novo problema: os usuários possuíam vários usuários e senhas diferentes para acesso, o que gerava esquecimento de qual usuário e senha utilizar e em qual momento.

Para resolver este problema foi necessário desenvolver um serviço de diretório rápido e eficiente para buscar e organizar as informações desses usuários de forma centralizada. Será demonstrado neste trabalho a instalação do serviço de Domínio do *Active Directory* (*MICROSOFT*, 2000) e a instalação do *OpenLDAP* (*THE OPENLDAP FOUNDATION*, 2003). Estes serviços de diretório funcionam de maneira hierárquica visando melhorar a busca e inserção de informações, tornando-a mais ágil e simples (SANTOS, 2013).

Nos dias de hoje todas as informações são usadas para que uma organização tome decisões que contribua com o objetivo de estar à frente do mercado, uma vez que na era da tecnologia, a informação é o maior diferencial, tanto para o pontapé inicial quanto para o sucesso da organização. A cada momento mais organizações buscam formas de controlar estas informações, as quais são acessadas e disponibilizadas em estações de trabalho para seus funcionários.

Uma maneira de garantir a segurança da informação em uma organização onde há um grande número de computadores é através de políticas de segurança, com integração ao protocolo LDAP.

1.1 OBJETIVOS GERAL

Promover a integração entre base *Microsoft Active Directory* e base *OpenLDAP* e utilizar políticas de segurança para gerenciamento de uma rede de computadores.

1.2 OBJETIVOS ESPECÍFICOS

- Implantar o Serviço *Microsoft Active Directory* e *OpenLDAP* em ambiente um virtualizado com *Windows Server* 2012 R2 (*MICROSOFT*, 2013) e CentOS 6 (*COMMUNITY ENTERPRISE OPERATING SYSTEM*, 2011) respectivamente;
- Configuração de um domínio *Microsoft Active Directory*;
- Configuração de uma Base de Dados LDAP;
- Replicação da Base de Dados *Microsoft Active Directory* para a base *OpenLDAP*;
- Aplicar políticas de segurança para restringir acessos indevidos.

1.3 JUSTIFICATIVA

Este trabalho lida com uma demanda que existe pela segurança da informação. Atualmente, as empresas têm toda a sua regra de negócio baseada em informações sigilosas e fundamentais para a continuidade do seu negócio, além disso seus usuários e também pessoas não autorizadas tentam burlar o sistema diariamente (RADECK, 2012).

O assunto abordado neste trabalho tem grande importância para empresas que buscam melhorar e facilitar a administração dos seus servidores de autenticação de usuários. A integração proposta neste trabalho proporciona a centralização da administração, a segurança com disponibilidade e replicação de dados, bem como a integração entre dois protocolos distintos de serviço de diretório.

2 REFERENCIAL TEÓRICO

2.1 REDES DE COMPUTADORES

Uma rede de computadores é um conjunto de dispositivos (normalmente conhecidos como nós) conectados por *links* de comunicação. Um nó pode ser um computador, uma impressora ou outro dispositivo de envio/recepção de dados, que estejam conectados a outros nós de rede (FOROUZAN, 2006).

Todo ambiente de rede precisa armazenar informações para possibilitar o seu gerenciamento (autenticação, grupos de usuários, permissões, cotas de armazenamento e impressão, compartilhamentos e etc.). Atualmente, a maioria das grandes organizações possui ambientes de rede heterogêneos, com várias plataformas presentes (Linux, *Windows*, Solaris…) e com redes virtuais fisicamente conectadas, muitas vezes distribuídas geograficamente.

Um exemplo de organização desse tipo é a UTFPR, que possui uma grande rede de dados interconectando todos os seus *campus*, espalhados pelo estado (ERICH, 2006).

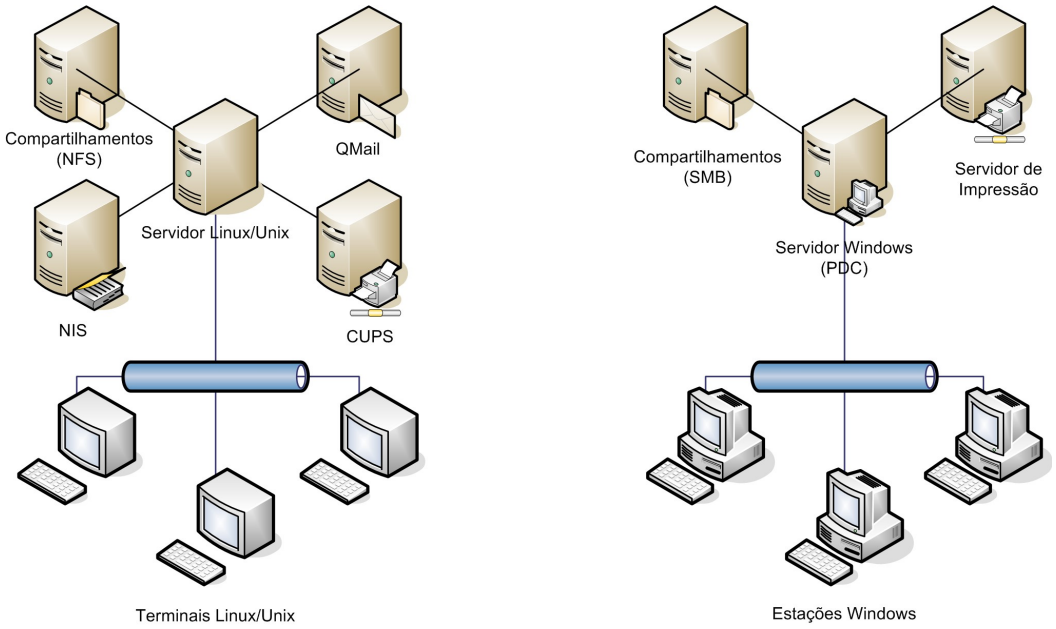

Figura 1 – Exemplo de redes heterogêneas.
Fonte: (ERICH, 2006)

Esse exemplo ilustra uma rede heterogênea composta de um ambiente *Windows* e um ambiente Linux. Apesar de ambos os ambientes estarem fisicamente

conectados (utilizando a mesma infraestrutura), não existe comunicação entre os serviços.

Segundo ERICH (2006), um problema decorrente desse tipo de implantação é que para cada plataforma ou para cada rede local virtual existente no ambiente de rede (rede física), é necessário suprir essas mesmas informações de gerenciamento. Se não for adotada uma boa solução de gerenciamento, podem surgir problemas decorrentes da replicação desses dados. Os principais são: redundância, falta de sincronia nas informações, dificuldade de organização, maior custo no suporte e falta de segurança.

2.1.1 Topologia de Rede

Segundo Forouzan (2006), o termo topologia se refere a maneira em que a rede é organizada fisicamente. A topologia da rede é a representação geométrica da relação entre todos os *links* e os dispositivos de uma conexão, denominados nós, entre si. Existem quatro tipos básicos de topologia de rede, são eles: malha, estrela, barramento e anel.

- Malha: Em uma topologia de malha, cada dispositivo possui um *link* ponto a ponto dedicado a cada um dos demais nós presentes na rede, onde dedicado significa transporte de tráfego apenas entre os dois nós (Forouzan, 2006).
- Estrela: Segundo Martinez (2015), topologia estrela é a que utiliza um nó central para chavear e gerenciar a comunicação entre as estações. É esta unidade central que vai determinar a velocidade de transmissão, como também converter sinais transmitidos por protocolos diferentes. Neste tipo de topologia é comum acontecer o *overhead*[1] localizado, já que uma máquina é acionada por vez, simulando um ponto-a-ponto
- Barramento: Topologia em barramento é multiponto, um longo cabo atua como um *backbone* o qual tem função de interligar todos os dispositivos ligados na rede, os nós são conectados ao barramento

[1] Qualquer processamento ou armazenamento em excesso, seja de tempo de computação, de memória, de largura de banda ou qualquer outro recurso que seja requerido para ser utilizado ou gasto para executar uma determinada tarefa.

através de cabos transceptores o qual é uma conexão que vai do dispositivo ao cabo principal (Forouzan, 2006).

- Anel: A topologia em anel utiliza em geral ligações ponto-a-ponto que operam em um único sentido de transmissão. O sinal circula no anel até chegar ao destino. Esta topologia é pouco tolerável à falha e possui uma grande limitação quanto a sua expansão pelo aumento de retardo de transmissão (MARTINEZ, 2015).

2.1.2 Redes Ponto-a-Ponto

Em uma rede ponto a ponto, também chamada de modelo de Grupo de Trabalho ou *Workgroup* em ambientes *Windows*, computadores são conectados em grupos para que outros usuários possam compartilhar recursos e informações. Não há um local central para autenticação de usuários, armazenamento de arquivos ou acesso a recursos.

Isso significa que os usuários devem lembrar em qual computador do grupo de trabalho está o recurso ou a informação compartilhada que desejam acessar, e também qual o *login* utilizado neste computador, para conseguir acesso ao recurso desejado. Neste modelo de redes são dificultadas as ações administrativas como alteração de dados de usuários ou *backup* de dados pois cada recurso pode estar em um computador diferente ou em mais de um computador (*Microsoft*, 2008).

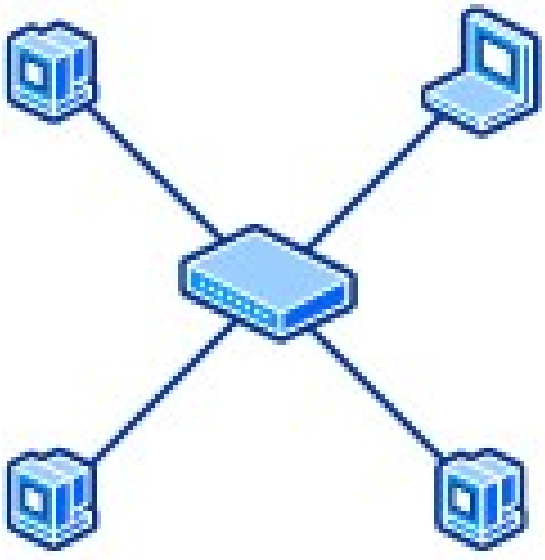

Figura 2 – Exemplo de redes ponto-a-ponto.
Fonte: (*MICROSOFT*, 2008)

Segundo BATTISTI e POPOVICI (2015), o modelo de redes *Workgroup* é um modelo em que cada servidor é independente do outro. Cada servidor tem sua própria lista de usuários, grupos, políticas de segurança e de administração. Este modelo é recomendado apenas para redes muito pequenas, nas quais o trabalho de criação de uma rede baseada em cliente-servidor não seria mais recompensador.

2.1.3 Redes Cliente-Servidor

São também chamadas de redes baseadas em servidor. Consiste de um servidor centralizado onde os usuários compartilham e acessam recursos da rede. Este servidor dedicado controla níveis de acesso de usuário aos recursos compartilhados. Os dados compartilhados ficam armazenados em local único facilitando tarefas administrativas como *backups* (*Microsoft*, 2008).

Cada computador conectado à rede é chamado de computador cliente. Em uma rede baseada em servidor, os usuários têm uma conta de usuário e senha para efetuar *login* no servidor e acessar os recursos compartilhados. Os sistemas operacionais de servidor são desenvolvidos para suportar a carga quando vários computadores clientes acessarem os recursos dos servidores. Na figura abaixo está demonstrado um exemplo de rede baseadas em servidor (*Microsoft*, 2008).

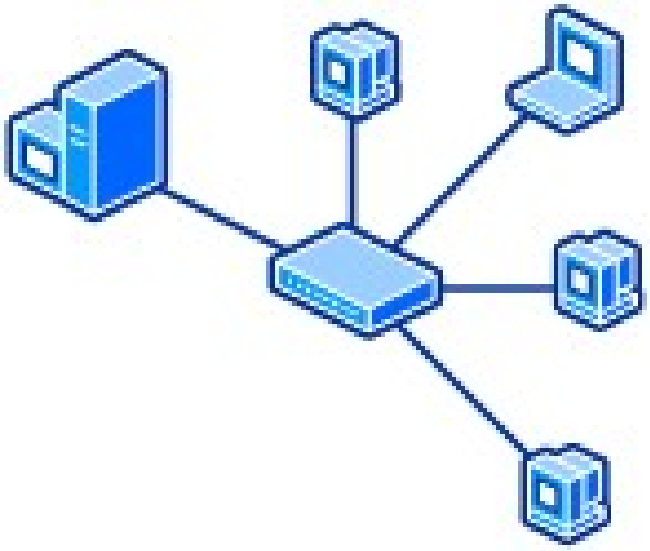

Figura 3 – Exemplo de redes cliente-servidor.
Fonte: (*MICROSOFT*, 2008)

2.1.4 Segurança em Redes de Computadores

A segurança de qualquer sistema computacional é um aspecto fundamental de sua arquitetura, principalmente quando estes são acessíveis por redes públicas, como a Internet. A segurança de sistemas distribuídos envolve os seguintes aspectos:

- Autenticação (identificação) de usuários e serviços
- Autorização (acesso) seletiva aos recursos
- Privacidade (confidencialidade)
- Disponibilidade

A autenticação é o processo de identificar o usuário (ou serviço) e validar se essa identificação é autêntica. Sem essa funcionalidade corretamente garantida, um usuário mal-intencionado pode se passar por um usuário legitimo. Da mesma forma para os servidores, sem essa garantia, um serviço malicioso pode ser passar pelo serviço autêntico e interceptar dados indevidamente (WINCKLER, 2014).

2.2 SERVIÇOS DE DIRETÓRIO

Serviços de diretório em computação são usados para organizar o processo de pesquisa de informações. Sendo essas de qualquer tipo, tais como: dados de usuários, setores de empresas e recursos da rede. Serviços de diretório funcionam de maneira hierárquica visando melhorar a busca e inserção de informações tornando-as mais ágil e simples. Exemplos do dia a dia podem ser encontrados em agendas telefônicas que organizam os dados de forma alfabética para que a busca e inserção seja mais rápida (SANTOS, 2013).

De maneira simplificada podemos afirmar que diretórios são bancos de dados. Entretanto as operações destes são mais simples do que em bancos de dados relacionais, já que estes utilizam tabelas, *trigger*, semáforos entre outros para a organização da informação, e em diretórios a estrutura segue a forma de árvore (TRIGO, 2007) apud (SANTOS, 2013).

Segundo BATTISTI e POPOVICI (2015), diretório nada mais é que um banco de dados com informações sobre usuários, senhas e outras necessárias ao

funcionamento de um sistema, quer seja um conjunto de aplicações *Mainframe*, um grupo de servidores de rede local, ou outro sistema qualquer.

Um serviço de diretório deve permitir extensão, podendo servir a diversos propósitos. Além de permitir inserções de registros, deve-se permitir também inserções de outros diretórios organizacionais sucessivamente, como subdiretórios. Esta organização cria uma estrutura de hierarquia de diretórios ou árvore de diretórios.

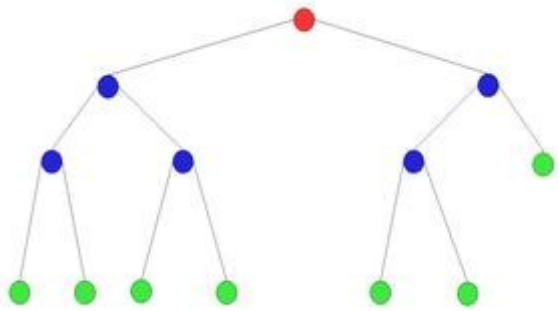

Figura 4 – Representação de uma hierarquia de diretórios.
Fonte: (SCRIMGER et al, 2002, p.642) apud (SANTOS, 2013).

2.3 CONTROLADORES DE DOMÍNIO PRIMÁRIO

Controladores de domínio primário são máquinas servidoras dentro de um domínio, o qual é composto por computadores organizados abaixo deste, com o propósito de gerencia de rede computacional, controlando permissões e recursos dos computadores membro. Um domínio pode ser denominado por árvore, e um conjunto de domínios são chamados de floresta. Essa floresta é controlada por um controlador de domínio primário (PDC) (MINASI et al, 2000).

Uma rede computacional pode ter somente um controlador de domínio primário, porém esta tarefa poderá ser dividida entre várias máquinas servidoras, as quais podem exercer tarefas como gerencia de usuários e permissões. Entretanto somente o controlador de domínio primário poderá realizar atualizações para que este posteriormente replique as atualizações na rede. Em redes de porte maior, ambos podem dividir a tarefa para que o PDC não seja sobrecarregado. Outra vantagem desta arquitetura é que se eventualmente o PDC sofrer indisponibilidade um servidor de *backup* poderá assumir o papel de PDC (SANTOS, 2013).

2.4 *MICROSOFT ACTIVE DIRECTORY*

Surgindo junto com o *Windows Server* 2000, o *Microsoft Active Directory* trouxe várias vantagens para os administradores de rede. Antes de a solução ser apresentada, os usuários nas empresas tinham um sério problema relacionado a sistemas: o esquecimento de suas inúmeras senhas para diversas aplicações diferentes.

A ideia de centralização de recursos funciona no AD com um banco de dados que possui as principais informações, como usuários, grupos, membro dos grupos, senhas, etc. Assim, o acesso à informação fica viável e de simples conferência,

Com a implementação do AD, os usuários passaram a ter apenas uma senha sincronizada com as mais diversas aplicações utilizadas na empresa (RADECK, 2012). Os principais elementos de um domínio gerenciado por *Active Directory*, são: Contas de usuários, Contas de Computador e Grupo de Usuário (BATTISTI, POPOVICI, 2015) os quais serão descritos abaixo.

Uma Conta de Usuário é um objeto do *Active Directory* que possui informações variadas sobre este. Cada usuário do domínio deve possuir a sua conta de usuário visto que essa proverá acesso aos recursos dos computadores e outros dispositivos presentes no domínio.

Conta de Computador é um objeto do *Active Directory* que possui função similar ao de contas de usuário, porém este é exclusivo para computadores, sejam eles estações de trabalho, servidores membros do domínio ou equipamentos de rede, os quais podem ser gerenciados pelo *Active Directory*. Contas de computador podem ser criadas antes da inserção da máquina no domínio, ou no momento da inserção.

Grupos de Usuário no *Active Directory* podem ser divididos em: grupos de segurança e grupos de distribuição. O grupo de segurança é normalmente utilizado para atribuição de permissões de acesso aos recursos da rede, já os grupos de distribuição são normalmente utilizados para organização, como por exemplo mandar um e-mail para os funcionários de um determinado setor da empresa (BATTISTI, POPOVICI, 2015).

Já segundo VIDAL (2007), Contas de usuários é um objeto do AD, em que as principais informações que encontramos nesse objeto são o primeiro nome, último nome, descrição, usuário, senha entre outros.

O Objeto Contas de Computador é um objeto pertencente ao computador que é adicionado ao domínio. No momento que este adentra o domínio automaticamente é criado a sua conta no AD, não importando se é um computador de um colaborador ou um servidor da empresa. Grupos de usuários é um objeto cuja principal função é facilitar o gerenciamento e as atribuições de permissões de acesso a recursos.

O *Active Directory* é organizado através de elementos chamados de Unidades Organizacionais. Estes foram introduzidos a partir do *Windows* 2000 *Server*, com a implementação do *Active Directory* e tem como por objetivo solucionar problemas de administração (BATTISTI, POPOVICI, 2015). Este elemento permite criar dentro de um domínio várias unidades organizacionais capazes de separarem objetos utilizando critérios definidos pelo administrador do domínio.

As ferramentas administrativas do *Active Directory*, ou *snap-ins* como são chamadas, fornecem as funcionalidades necessárias para o suporte do serviço de diretório. Estas ferramentas utilizam uma estrutura comum chamada *Microsoft Management Console* (MMC), que são janelas personalizáveis semelhantes ao *Windows* Explorer (BERGAMASCHI, 2011).

Os *snap-ins* são encontrados em Iniciar -> Painel de Controle -> Ferramentas Administrativas, e são os seguintes:

• Usuários e Computadores do *Active Directory* - gerencia os objetos usuários, computadores, grupos, entre outros;

• Serviços e Sites do *Active Directory* - gerencia replicação, topologia de rede e serviços relacionados;

• Domínios e Relações de Confiança do *Active Directory* - configura e mantém relações de confiança e os níveis funcionais do domínio e da floresta;

• *Schema* do *Active Directory* - examina e modifica a configuração dos atributos e das classes de objeto do *Active Directory*. Como não é comum alterar o *Schema*, não é instalado por padrão (BERGAMASCHI, 2011).

A versão do *Windows Server* 2008 R2 possui todos os *snap-ins* mencionados, e uma ferramenta exclusiva, a Central Administrativa do *Active Directory*. Localizada em “Ferramentas Administrativas” no Painel de Controle. Com

uma única interface gráfica aprimorada é possível: gerenciar os objetos, conectar e gerenciar a um ou vários domínios ou controladores de domínio na mesma instância da Central Administrativa e realizar pesquisas de dados do *Active Directory* (BERGAMASCHI, 2011).

2.5 *LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL - LDAP*

Segundo a *OpenLDAP Foundation* (2003), LDAP é uma implementação de um protocolo leve para acesso a diretórios, LDAP funciona sobre uma conexão TCP/IP ou sobre qualquer outra conexão orientada a serviços (*THE OPENLDAP FOUNDATION*, 2003).

LDAP utiliza um modelo de conexão cliente-servidor, contendo as informações organizadas em formato de árvore. O cliente se comunica e faz uma requisição, o servidor responde ou redireciona à um outro servidor onde poderá ser adquirido maiores informações. Não importa qual servidor LDAP o usuário se comunique, sempre será apresentada a mesma estrutura de árvore (*THE OPENLDAP FOUNDATION*, 2003).

Segundo ERICH, as informações da fonte de dados são armazenadas no banco de dados do LDAP e são organizadas de forma similar ao DNS, isto é, são feitas de forma hierárquica partindo da raiz e chegando, por exemplo, até a um dispositivo de rede (ERICH, 2005).

A fundação *OpenLDAP*, diz que as informações no servidor LDAP são armazenadas de forma hierárquica, seguindo uma estrutura parecida com árvores e esta geralmente é organizada seguindo limites geográficos ou internos da organização que usa o serviço (*The OPENLDAP FOUNDATION*, 2003).

Um servidor LDAP é responsável pela autenticação do usuário na rede e as informações deste usuário ficam armazenadas na sua base de dados do servidor. O mesmo permite ou não que o cliente realize consultas e modificações, podendo também ser utilizado como agenda de contatos (ERICH, 2005).

A informação presente no servidor LDAP é protegida de acesso desautorizado usando um mecanismo de autenticação para verificar a identidade do solicitante ao servidor. O LDAP também verifica a integridade e confiabilidade das informações (*THE OPENLDAP FOUNDATION*, 2003).

2.6 *ACTIVE DIRECTORY* X *OPENLDAP*

	Active Directory	Open LDAP
Replicação do banco de dados	x	X
Autenticação dos usuários	x	X
Administração centralizada da segurança com policy	X	
Única senha para todos os serviços	X	
Integração com DNS	X	X
Gerenciamento Centralizado	X	
Tem custo a licença de uso	X	
Acesso por linha de comando	X	X
Serviços de redes como e-mail, web, domínio de rede e Proxy autenticam na base de dados	X	X
Suporte a IPv4 e IPv6;	X	X
Transporte seguro - SSL e TLS;	X	X
Capacidade de atender a múltiplos bancos de dados simultaneamente;	X	X
Interface amigável de administração	X	

Figura 5 – Tabela comparativa entre *Active Directory* e *OpenLDAP*
Fonte: (VIACONNECT, 2012).

As vantagens da utilização do *OpenLDAP*:

- A centralização dos dados, que evita a duplicação e facilita a manutenção;
- A distribuição entre diversos servidores, pelo fato de ser hierárquico, tornando-se um sistema distribuído;
- A replicação de dados por meio de um servidor escravo (apud TRIGO, 2007).

Segundo apud TRIGO (2007), são inúmeras as aplicações e os serviços que permitem a integração com o LDAP.

As vantagens da utilização do *Microsoft Active Directory*:

- Administração com utilização de *Policy*;
- Suporte a Conexões SSL;
- Integração com as ferramentas *Microsoft*;
- Autenticação Centralizada;
- Replicação de Banco de Dados (VIACONNECT, 2012).

2.7 *DOMAIN NAME SYSTEM* – DNS

Domain Name System, ou sistema de nomes de domínio, é um protocolo utilizado para transformar nomes de domínios em endereços IPs. Esse protocolo foi criado para que não fosse necessário realizar acessos diversos na Internet utilizando endereços IPs, pois são difíceis de memorizar e podem ser alterados a qualquer momento pelo administrador do sistema (ALMEIDA, 2010).

O DNS em um serviço de e-mail é bastante importante pois ao invés de realizar um envio utilizando por exemplousuario@200.33.44.55, o envio é realizado utilizando usuario@dominio.do.usuario. A primeira forma citada é de difícil memorização como foi dito anteriormente, já a segunda proporciona uma melhor associação do endereço com sua função.

O servidor DNS é composto por diversos tipos de registros, como por exemplo o MX (*Mail Exchanger*). Este registro é o responsável por indicar quem é o servidor de e-mail de um determinado domínio (ALMEIDA, 2010). Exemplo de consulta de MX abaixo:

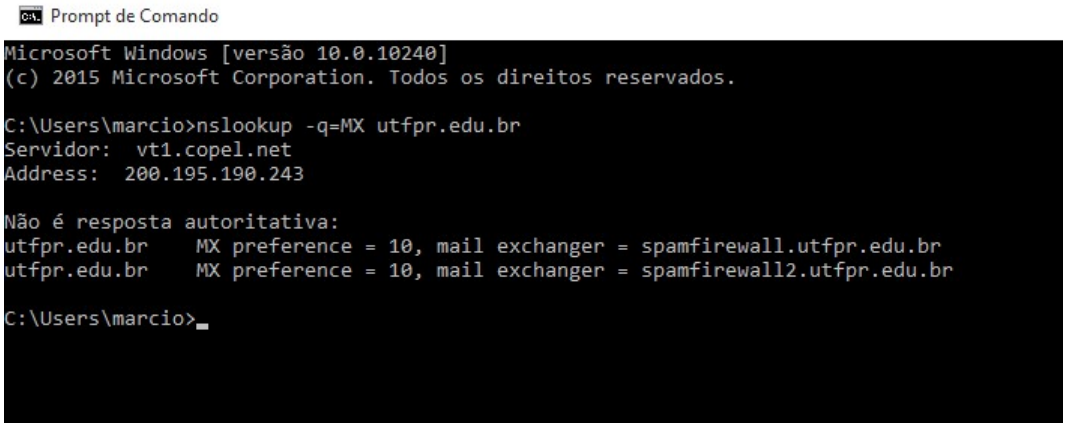

Figura 6 – Exemplo de consulta de MX.
Fonte: Autoria Própria (2015)

Um servidor DNS é composto por três elementos (SANTOS, 2013):

- Espaço de nome: Ambiente de nome da Internet ou uma área de nome interno definido conforme a necessidade.
- Resolvedores: Clientes ou locais de onde surgem as solicitações para a resolução de nomes. Estes enviam ao servidor DNS as solicitações para conversão e podem ser de estações de trabalho até outros servidores.

- Servidor de nomes: Computador que possui uma aplicação do servidor DNS e responde às solicitações dos clientes.

Na Internet, o DNS tenta resolver o endereço www.empresa.com.br digitado em um navegador, caso não tenho sucesso outro servidor DNS será chamado de tempo em tempo para efetuar a resolução do nome em endereço IP e assim sucessivamente. Entretanto na rede interna o servidor DNS é utilizado para localizar recursos dentro da mesma, como por exemplo a consulta a um compartilhamento de rede \\tcc.interno\Impressora, e para tal será consultado o DNS Servidor (SANTOS, 2013).

2.8 POLÍTICAS DE GRUPO

As políticas de grupo são infraestruturas programáveis que permitem aos administradores de redes especificar configurações específicas e gerenciadas para diversos usuários e computadores através de rotinas padrões chamadas *Templates* e de preferências especificas. É possível criar configurações de políticas de grupo que afetam um grupo de computadores e usuários do domínio, como também que afetam apenas um computador ou usuário (BATTISTI, POPOVICI, 2015).

Segundo RADECK (2012), as principais funções das GPOs são facilitar o trabalho do administrador da rede, oferecendo recursos que podem ser implementados tanto em sites, domínios ou até mesmo em unidades organizacionais específicas, oferecendo uma segurança e tranquilidade no gerenciamento da rede. Seus principais recursos podem ser designados somente para os usuários que fazem parte do domínio na estação de trabalho quanto para qualquer usuário, que esteja no domínio, localmente na estação de trabalho.

Para BATTISTI e POPOVICI (2015), podemos resumir aplicações de politicas de grupo em automação de tarefas, as quais facilitam a vida dos administradores de TI da rede.

As GPOs podem ser feitas em dois níveis: nível de usuário e nível de computador. As GPOs em nível de usuário são aplicadas em qualquer estação que o usuário fizer *login*, já as GPOs de nível de computador serão aplicadas a qualquer usuário que fizer *login* nas estações afetadas (BATTISTI e POPOVICI, 2015).

Segundo BATTISTI e POPOVICI (2015) as GPOs podem ser usadas para as seguintes tarefas: centralizar o gerenciamento das configurações definidas no registro do *Windows*, atribuições de *script*, redirecionamento de pastas, gerenciamento de *software* e definições de configurações de segurança.

- Definições de registro: As GPOs criam arquivos de definições do registro os quais são carregados e aplicados nas estações de trabalho do usuário, nas partes referentes à configuração de computadores e configuração de usuários.
- Atribuição de *Scripts*: Conceito de execução de *scripts* por GPOs. Este, segundo BATTISTI e POPOVICI (2015), está caindo em desuso. Com ele é possível executar *scripts* na hora do *login* e do encerramento da estação de trabalho.
- Redirecionamento de Pastas: Pode-se redirecionar pastas da máquina local a um compartilhamento no servidor. Com isto os dados do usuário passam a estar disponíveis na rede e poderão ser acessados de qualquer estação de trabalho.
- Gerenciamento de *Software*: Com este tipo de GPO pode-se fazer instalação, desinstalação e atualização de *software* diretamente do servidor do *Active Directory*.
- Definição de configurações de Segurança: Este tipo de GPO pode ser usado para editar configurações relativas à segurança como por exemplo bloqueio de acesso ao painel de controle do *Windows*, configurações de rede e de acesso a internet.

3 DESENVOLVIMENTO

Para alcançar a segurança desejada na implementação deste trabalho, foram utilizados dois tipos de servidores para controle de usuários e dispositivos conectados na rede. São estes, *Microsoft Active Directory* e *OpenLDAP*. Também é utilizado o *software* LSC, que tem a função de realizar a interconexão e integração das bases LDAP e *Active Directory*.

3.1 MATERIAIS

Para a realização deste trabalho, utilizou-se de uma máquina servidora com o sistema operacional *Windows* 10, utilizando o serviço de virtualização gratuito Hyper-V, escolhido por ser gratuito e nativo junto ao sistema operacional.

Nele foram criadas 3 máquinas virtuais: uma utilizando o sistema operacional *Microsoft Windows Server* 2012 R2, para ser a máquina servidora que fornecerá o recurso do *Microsoft Active Directory*; a segunda máquina virtual com o sistema CentOS versão 6 para ser a máquina servidora do recurso LDAP; e a terceira máquina virtual rodando o sistema *Microsoft Windows* 7, para ser a máquina cliente da rede.

3.2 *WINDOWS SERVER* 2012 R2

Este servidor teve como nome “W2K12R2” e teve como função ser o controlador de domínio principal, e também como autoridade de certificação para o objetivo deste trabalho.

3.2.1 Serviços de Domínio *Active Directory* (AD DS)

A instalação do *Microsoft Active Directory Domain Services* foi o primeiro passo para que pudessemos começar a integração proposta pelo trabalho. Como citado acima, o *Active Directory Domain Services* necessitou ser instalado no Sistema Operacional *Microsoft Windows Server* 2012 R2.

Para realizar esta instalação abriu-se o painel de gerenciamento de servidores disponível no Sistema Operacional e adicionou-se a função Serviços de Domínio *Active Directory* (AD DS).

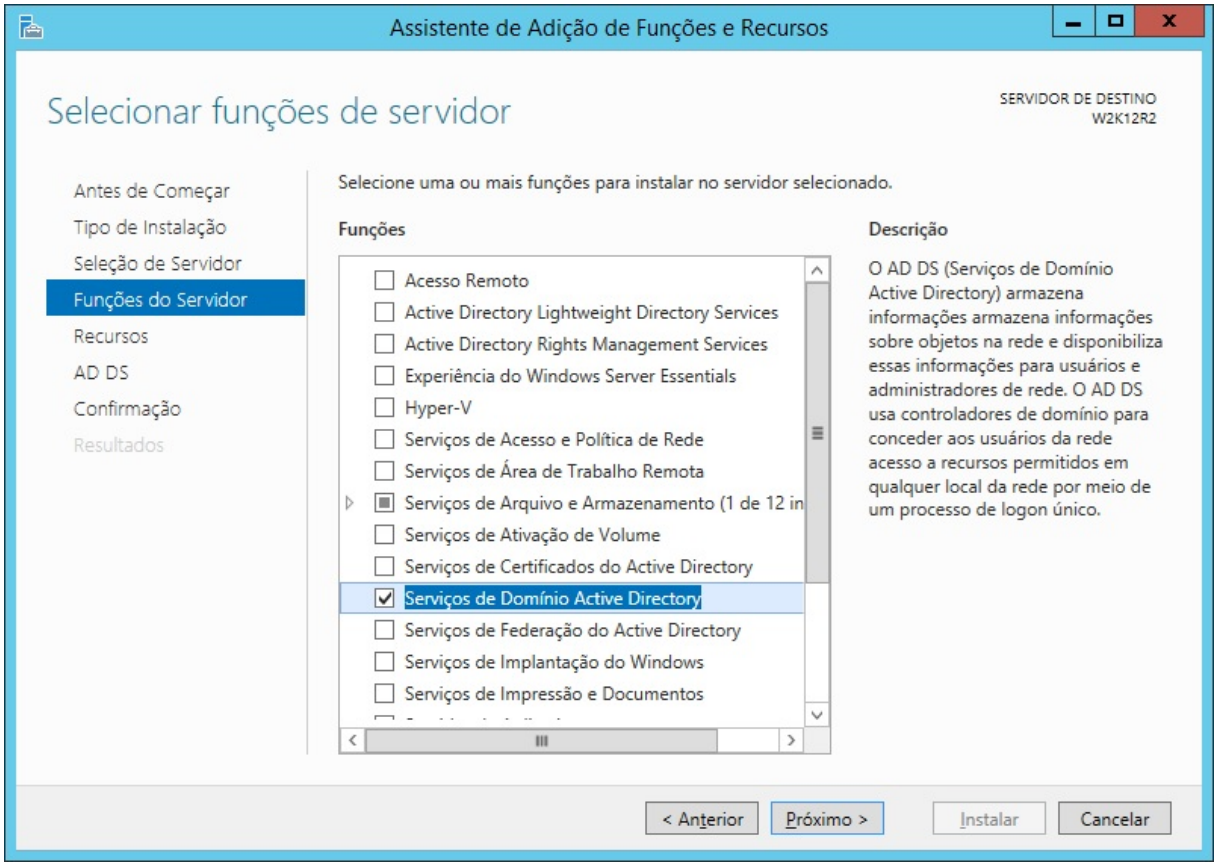

Figura 7 – Seleção da função de Serviços de Domínio *Active Directory* para instalação.
Fonte: Autoria Própria (2015)

Após a instalação estar concluída promoveu-se este servidor a um controlador de domínio primário para que pudesse ser criado o domínio que foi utilizado na integração deste trabalho.

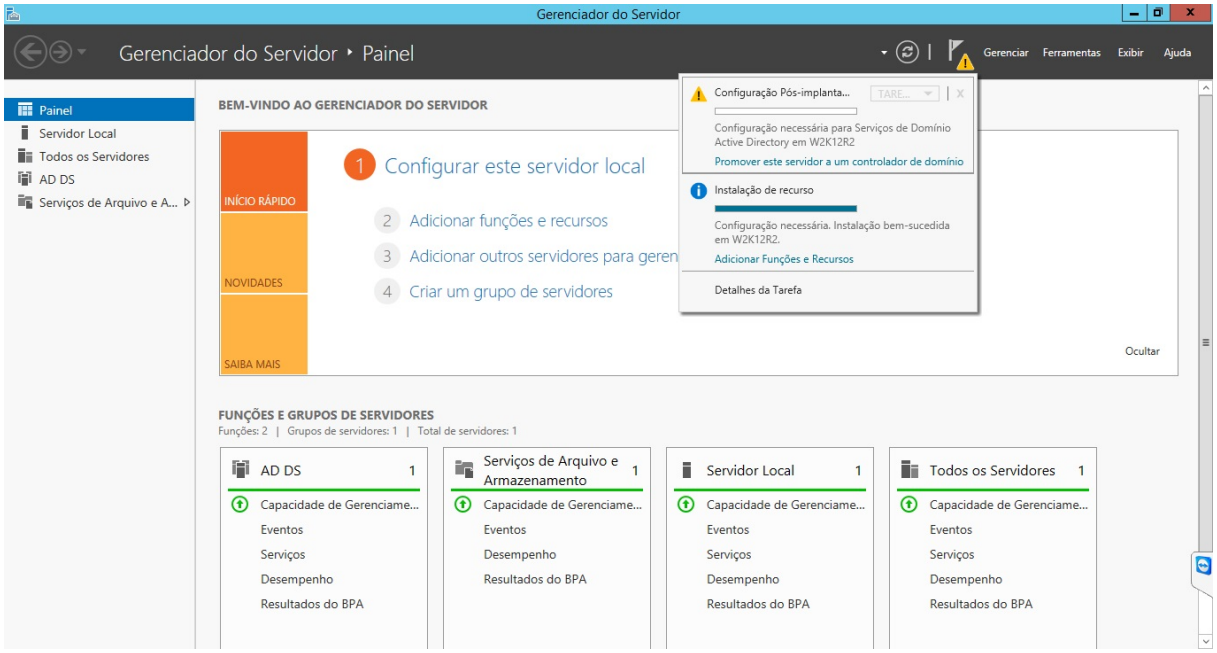

Figura 8 – Promovendo o servidor a um controlador de domínio.
Fonte: Autoria Própria (2015)

Pode-se observar que na primeira configuração de implantação de um AD DS obteve-se três operações possíveis, e para o trabalho desenvolvido foi usada a opção de adicionar uma nova floresta com um domínio raiz para a mesma. O domínio raiz é o domínio principal desta floresta e que a rede enxerga como identificação domínio completamente expressado (do inglês, FQDN).

O domínio raiz criado para este trabalho foi o “tcc.interno” e pode ser utilizado para encontrar o endereço deste servidor na rede. Para existir um exemplo, este servidor na rede foi denominado “W2K12R2.tcc.interno”.

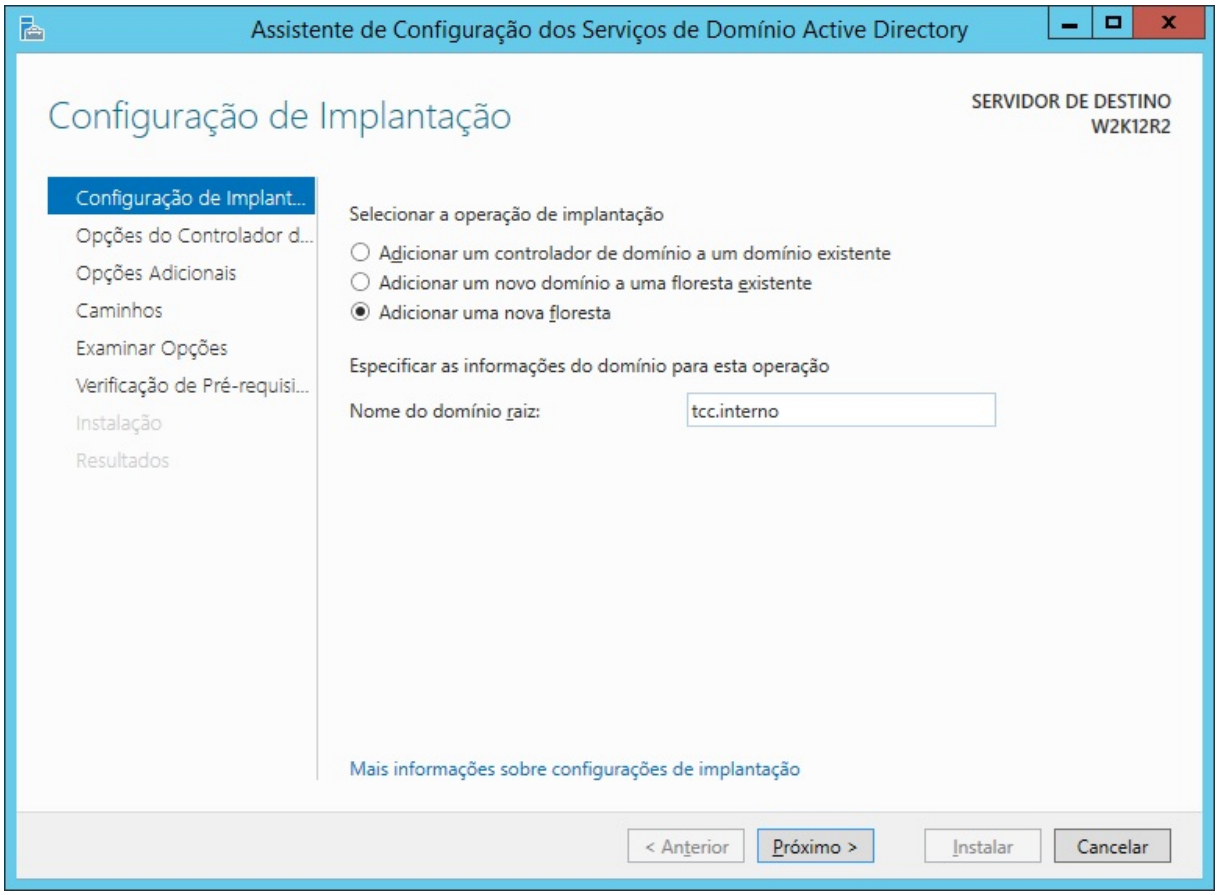

Figura 9 – Adicionando uma nova floresta como domínio raiz “tcc.interno”.
Fonte: Autoria Própria (2015)

Nesta etapa definiu-se a senha do modo de restauração dos serviços de diretório, a qual pode-se utilizar para recuperar a base de dados do *Active Directory,* caso o mesmo viesse a encontrar erros graves.

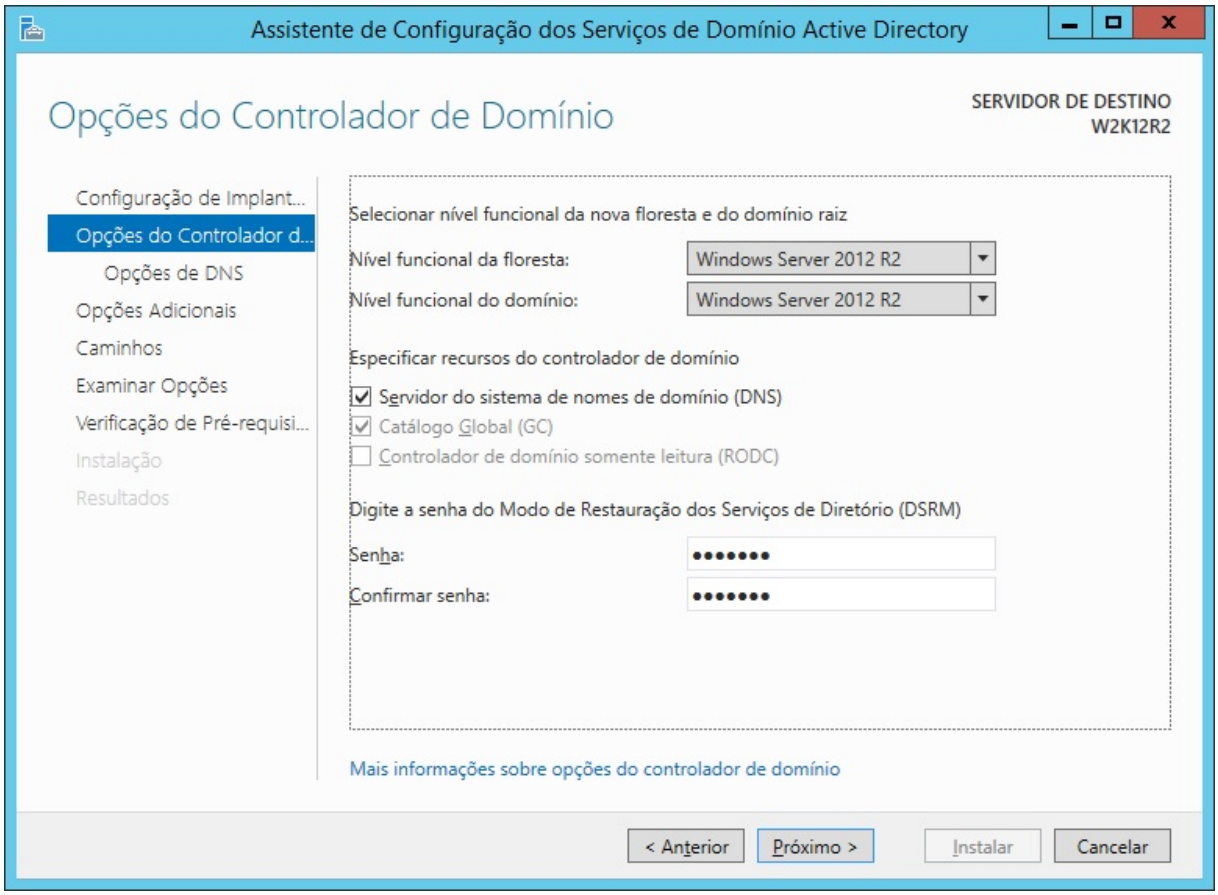

Figura 10 – Definindo uma senha para o modo de Restauração dos Serviços de Diretório (DSRM).
Fonte: Autoria Própria (2015)

O nome de domínio Netbios “TCC” que foi utilizado serviu para a resolução do nome do domínio para uma conta de usuário.

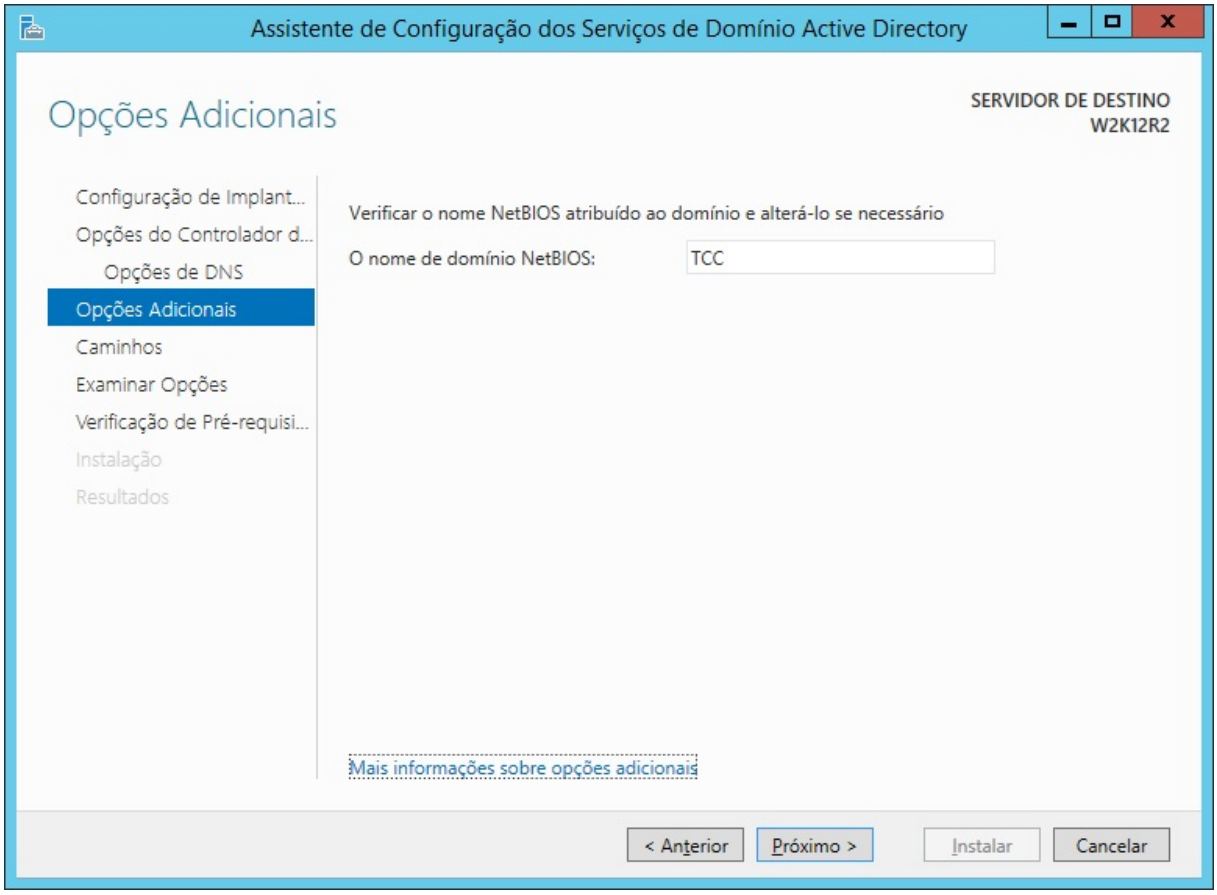

Figura 11 – Definindo o nome de domínio *Netbios* para o domínio raiz “tcc.interno”.
Fonte: Autoria Própria (2015)

O *Netbios* em uma rede sem domínio é composto pelo nome do computador. Para identificar a autenticação do usuário, pode-se notar a forma de como é preenchido o campo de *login*. É utilizado “nome_do_domínio\nome_do_usuário” para uma autenticação de um usuário em um domínio, e como exemplo neste trabalho usou-se “TCC\usuário”.

Ao tentar autenticar um usuário em uma rede sem domínio, utilizou-se “nome_do_computador\nome_do_usuário” para a autenticação. Um exemplo disto é a autenticação do usuário administrador neste servidor antes do mesmo ter sido promovido a controlador de domínio primário, que era no formato “W2K12R2\administrador”.

Após todos os passos especificados nesta seção, pode-se concluir a instalação do AD DS e a criação do domínio que foi utilizado na integração LDAP.

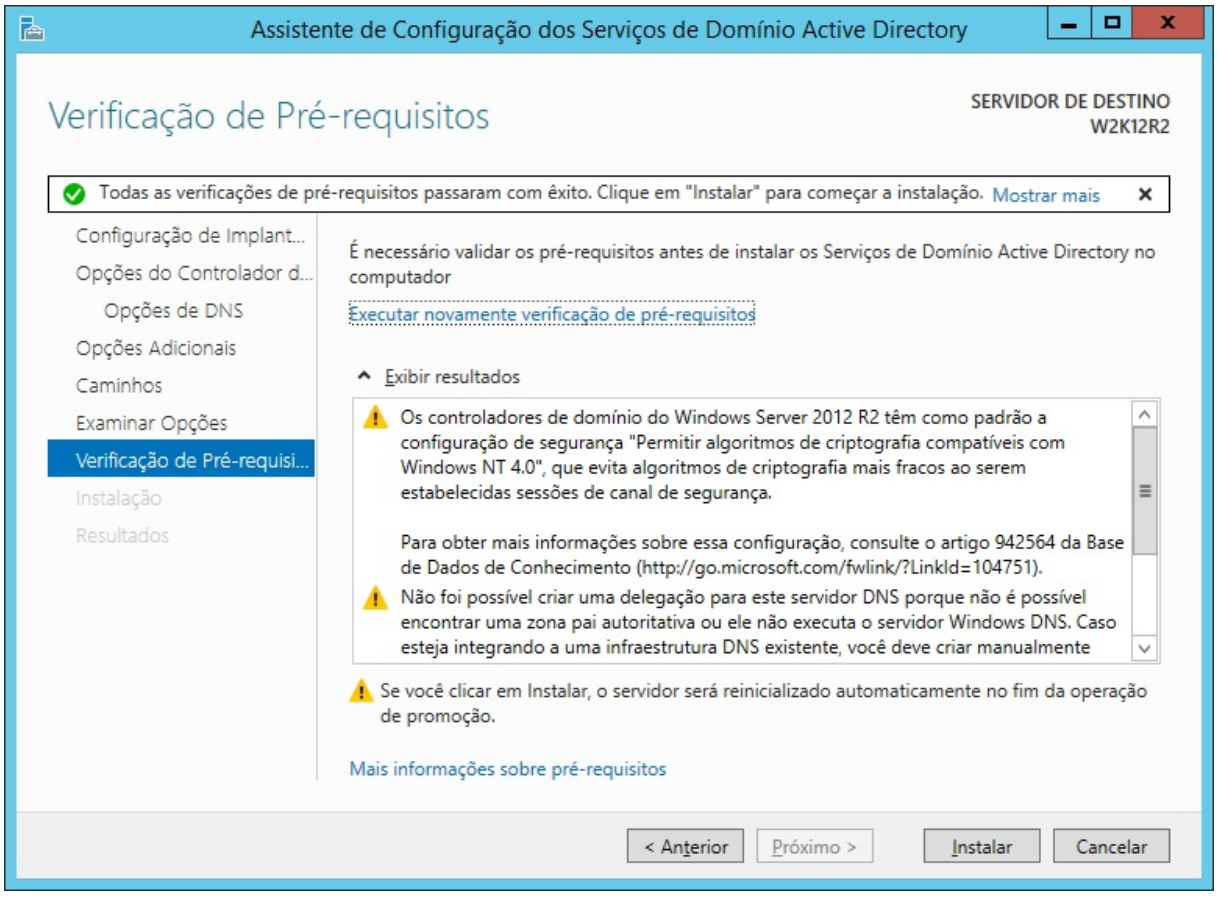

Figura 12 – Validação de Pré-requisitos para se implantar o AD DS.
Fonte: Autoria Própria (2015)

3.2.2 Serviços de Certificados do *Active Directory* (AD CS)

O serviço de certificados do *Active Directory* (AD CS) é responsável por emitir o certificado de autenticidade do servidor, o qual foi utilizado pelo *software* LSC para realizar a interconexão e integração das bases LDAP e *Active Directory*.

Para adicionar esta função ao servidor, abriu-se novamente o painel de gerenciamento de servidores e adicionou-se a função Serviços de Certificados do *Active Directory* (AD CS).

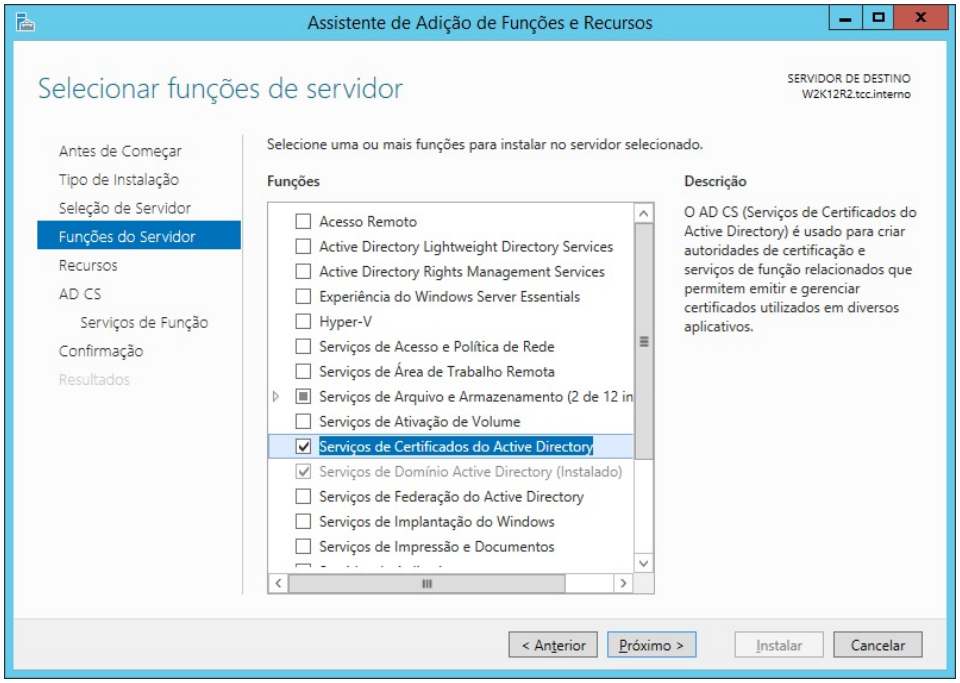

Figura 13 – Seleção da função de Serviços de Certificados do *Active Directory* para instalação.
Fonte: Autoria Própria (2015)

Após ter sido instalado a função, realizou-se a configuração da função do AD CS para se emitir um certificado que serviu de auxílio para a relação de confiança entre as bases LDAP e *Active Directory*.

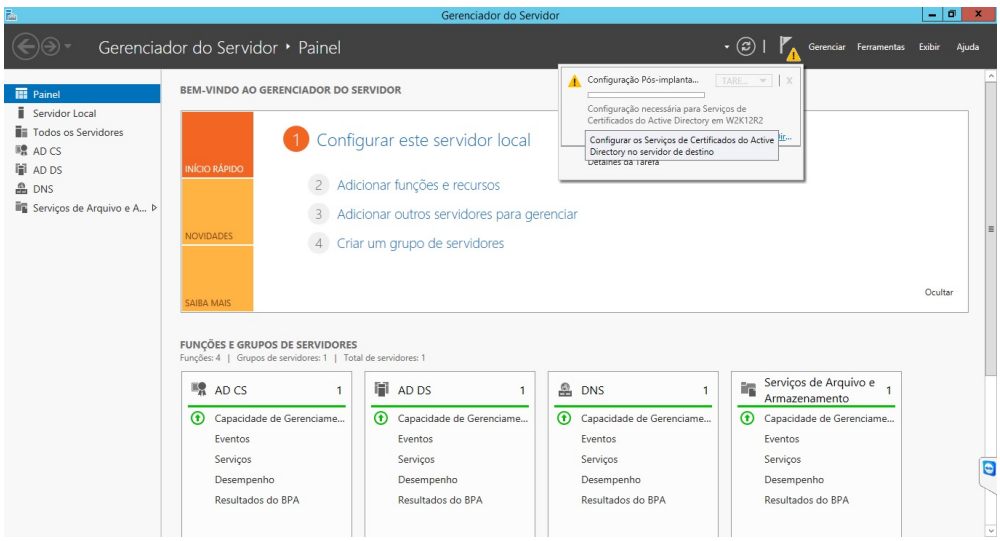

Figura 14 – Configurando os Serviços de Certificado do *Active Directory*.
Fonte: Autoria Própria (2015)

Nesta etapa da configuração, necessitou-se apenas do serviço de função de autoridade de certificação, devido ao fato que não se necessitou de nenhum serviço *WEB* extra oferecido pelo mesmo para nosso trabalho.

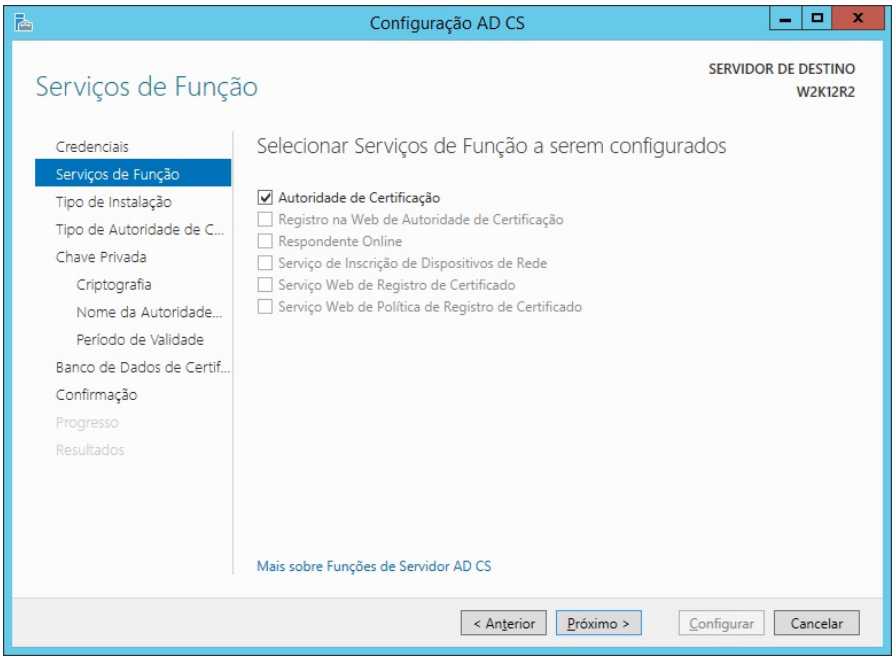

Figura 15 – Selecionando o serviço de função necessário.
Fonte: Autoria Própria (2015)

Especificou-se que a instalação deste AD DS seria de uma autoridade de certificação do tipo Corporativa para que fosse possível emitir um certificado.

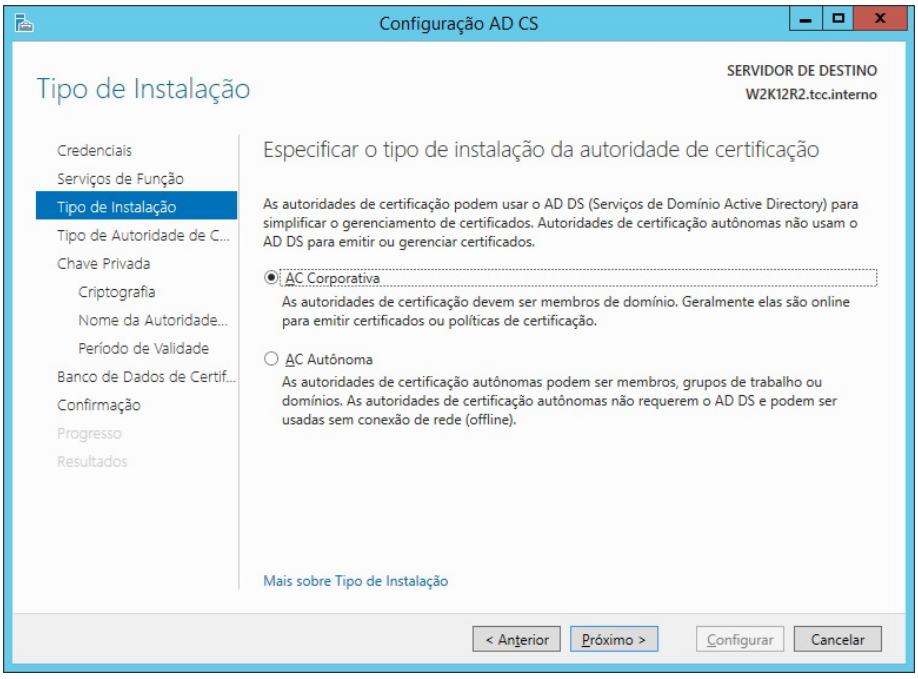

Figura 16 – Especificando qual é o tipo da instalação da autoridade de certificação.
Fonte: Autoria Própria (2015)

Nesta etapa da configuração foi decidido que o tipo de autoridade de certificação fosse uma autoridade de certificação raiz, pois não há nenhuma outra autoridade presente em nosso escopo, impossibilitando atuação deste AD CS como uma autoridade subordinada.

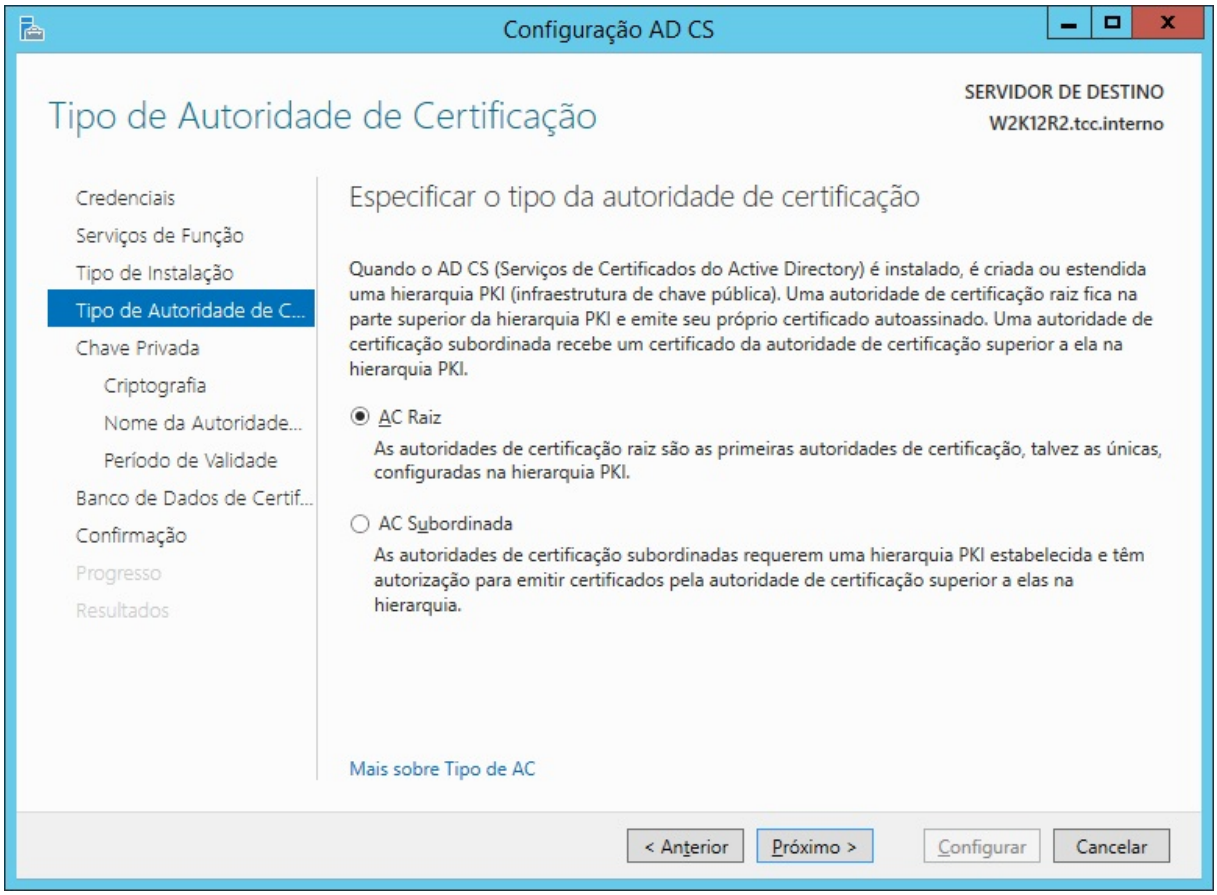

Figura 17 – Especificando qual é o tipo da autoridade de certificação.
Fonte: Autoria Própria (2015)

Na etapa seguinte foi criada uma nova chave privada que foi utilizada para que fosse possível a emissão do certificado.

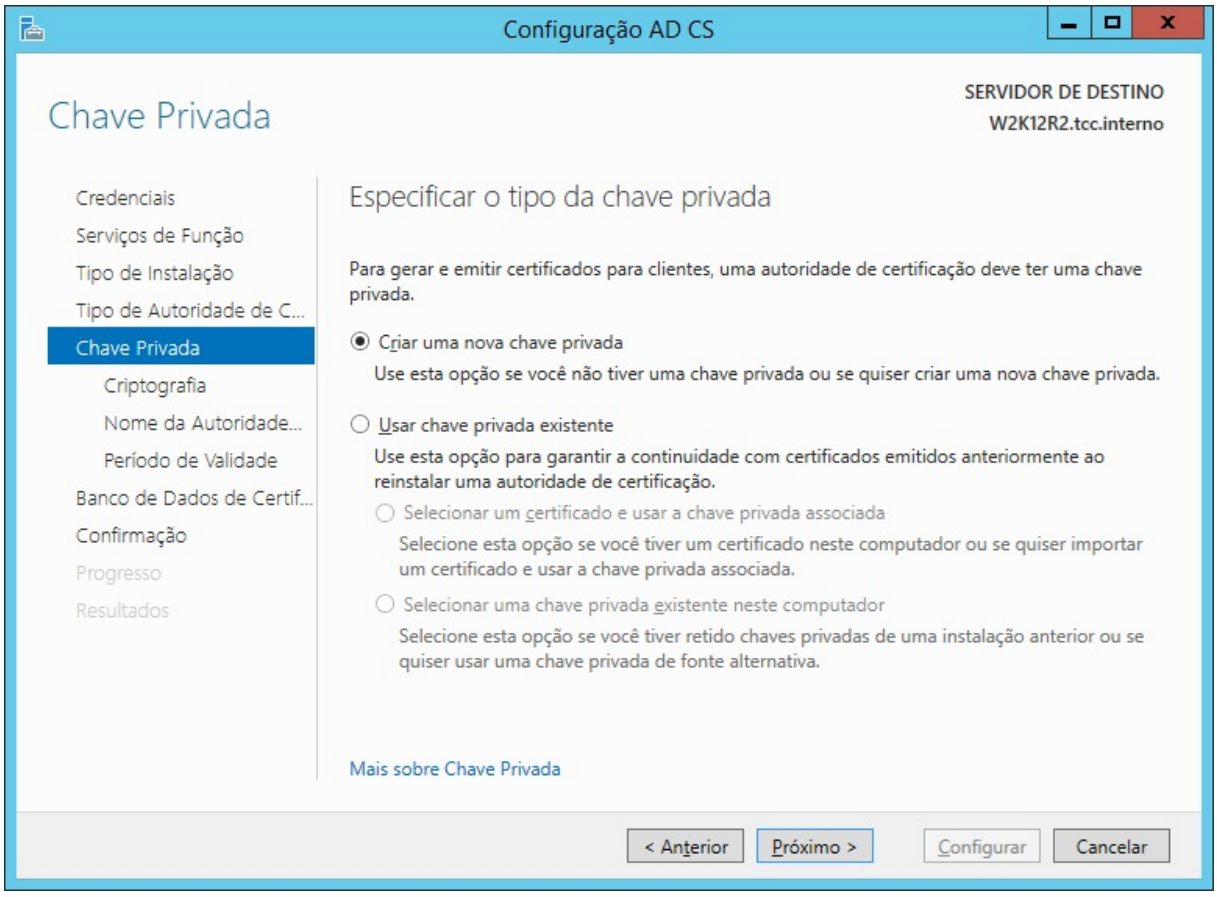

Figura 18 – Especificando o tipo da chave privada.
Fonte: Autoria Própria (2015)

Por não se ter nenhum certificado emitido para o servidor, realizou-se a criação de uma nova chave privada para emitirmos nosso certificado.

A criptografia de nosso certificado foi mantida no padrão sugerido pela *Microsoft*, que é a do provedor criptográfico RSA[2] com 2048 bits no comprimento da chave, utilizando o algoritmo de *Hash* SHA1.

[2] RSA é um algoritmo de criptografia de dados, que deve o seu nome a três professores do Instituto de Tecnologia de Massachusetts (MIT): Ronald Rivest, Adi Shamir e Leonard Adleman.

No primeiro campo, adicionou-se um nome comum para a autoridade de certificação. Este nome foi definido aleatoriamente e teve como um sufixo os caracteres “-CA”. Neste trabalho o nome comum da autoridade de certificação ficou como “tcc-W2K12R2-CA”.

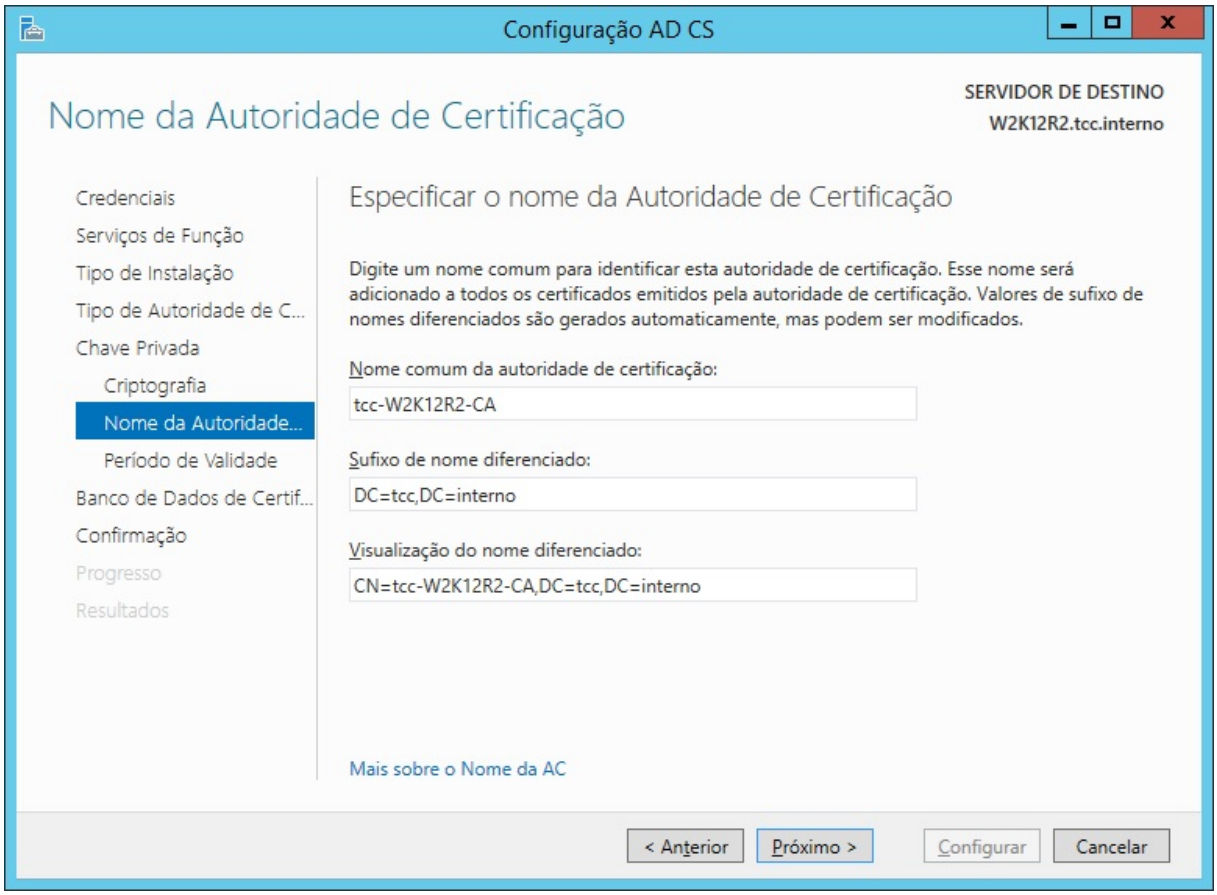

Figura 19 – Especificando o nome da Autoridade de Certificação.
Fonte: Autoria Própria (2015)

É importante ter-se o cuidado de preencher corretamente o primeiro campo citado acima, para que a autoridade de certificação estivesse correta para emitir o certificado. O período de validade deste certificado tem como padrão 5 anos.

Após todos os passos especificados nesta seção, pode-se concluir a configuração do AD CS.

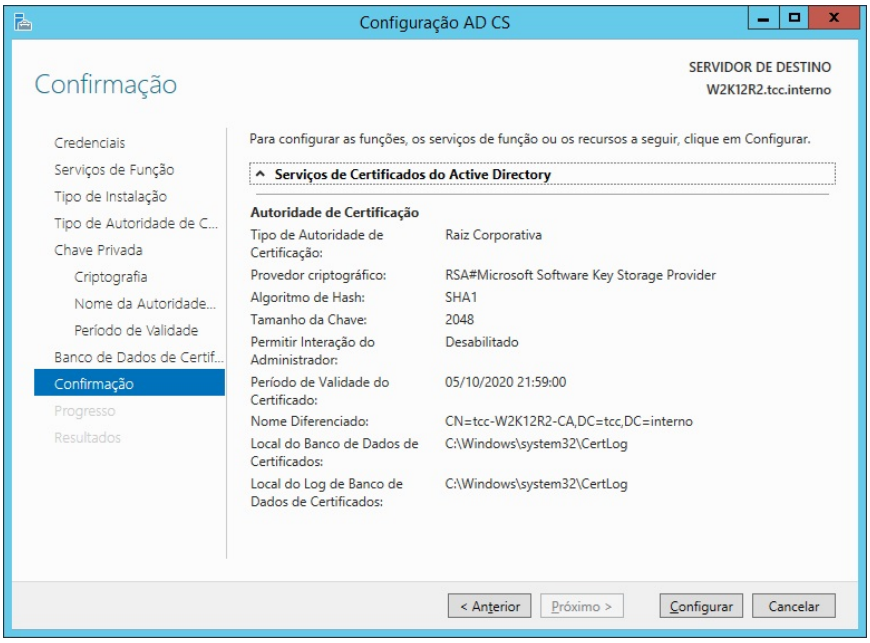

Figura 20 – Confirmando o que foi definido, implantou-se o AD CS.
Fonte: Autoria Própria (2015)

Para emitir-se o certificado, utilizou-se o CMD com permissão elevada de administrador e executou-se o comando “certutil –ca.cert nome_do_certificado.crt”.

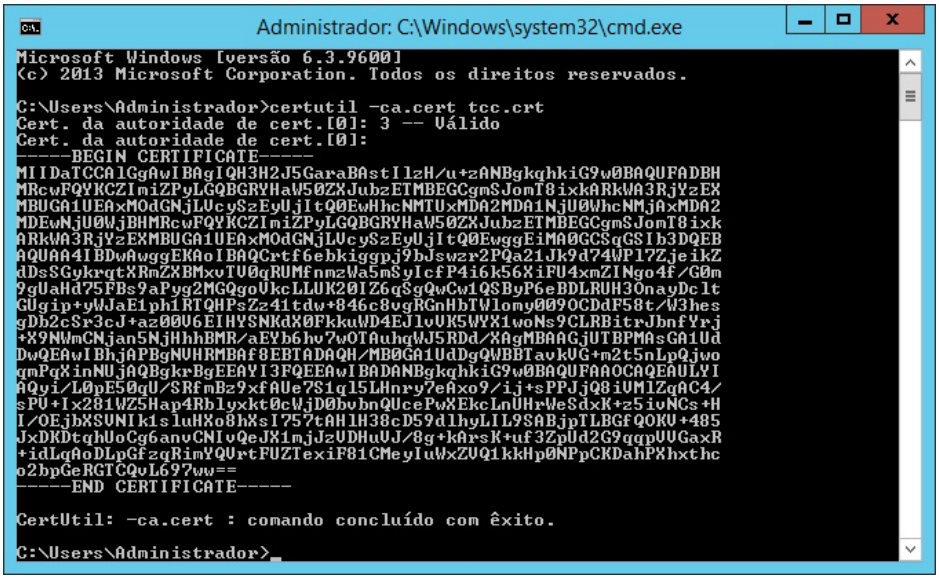

Figura 21 – O resultado da emissão do certificado.
Fonte: Autoria Própria (2015)

O certificado foi emitido com sucesso e estava pronto para ser exportado para ser utilizado no LSC.

3.3 CENTOS 6

Este servidor teve como nome “CENTOS”, e foi usado como o *host* para o serviço do *OpenLDAP,* além de ser também o servidor da aplicação LSC usada para fazer a integração entre as bases. Neste trabalho o “CENTOS” esteve respondendo pelo IP 192.168.1.25 com máscara de rede 255.255.255.0 entregues por DHCP.

A instalação do Centos 6 não foi descrita neste trabalho, visto que foi utilizado a instalação padrão mínima disponibilizada sem a adição de nenhum pacote extra. Os pacotes necessários foram instalados via repositórios abertos após o sistema operacional já estar funcional.

3.3.1 OpenLDAP

A instalação do serviço *OpenLDAP* foi um passo necessário para a integração proposta neste trabalho. Ela foi facilmente instalada pois os pacotes são disponibilizados em repositórios públicos do CentOS. Para tal foi utilizado o comando:

```
#yum install OpenLDAP OpenLDAP-clients OpenLDAP-Servers -y
```

O gerenciador de pacotes yum se encarregou de preencher todas as dependências necessárias, efetuar o *download* e instalação delas.

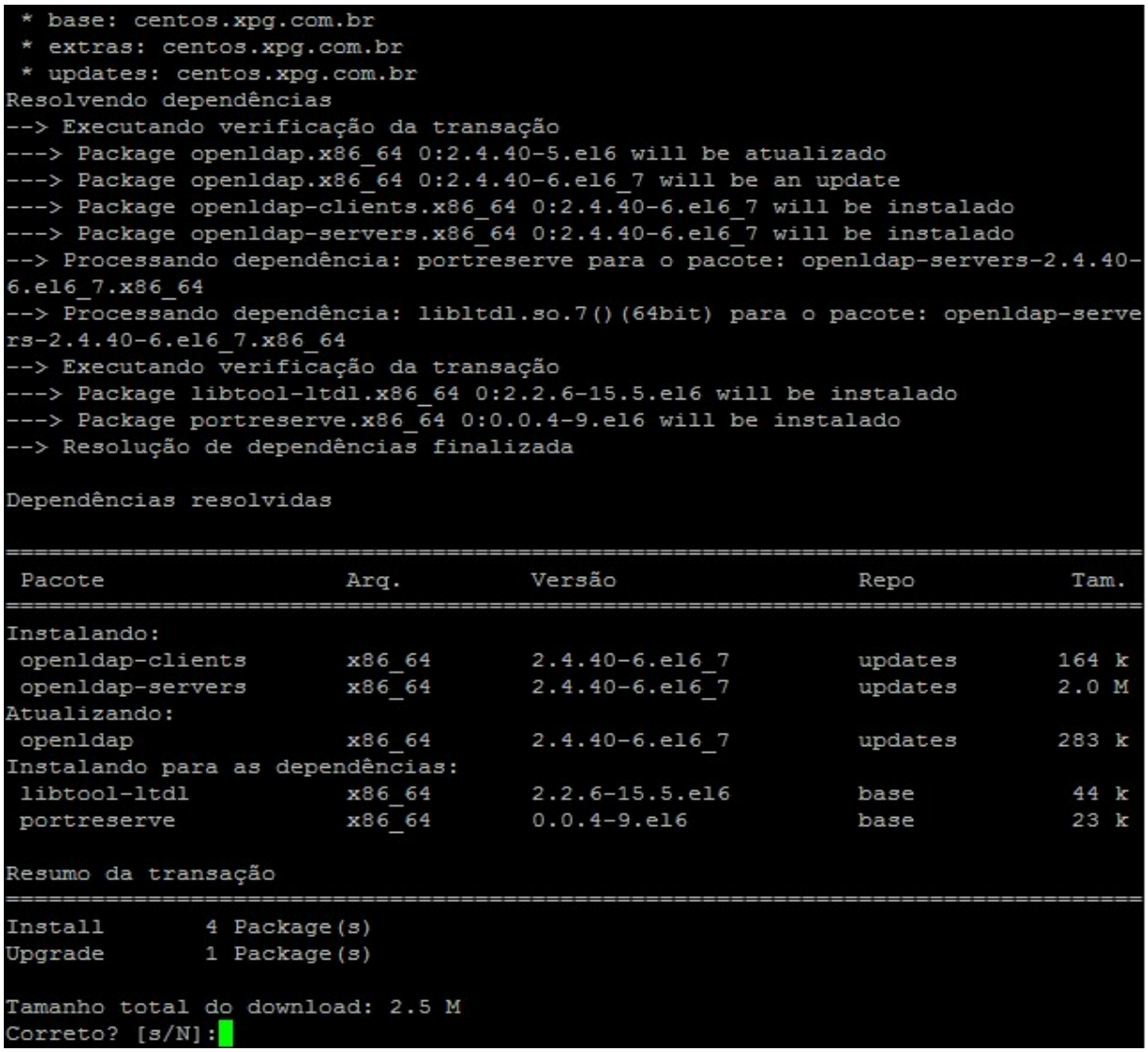

Figura 22 – Instalação *OpenLDAP*.
Fonte: Autoria Própria (2015)

Após a instalação dos pacotes necessários para o funcionamento do serviço do *OpenLDAP*, foi necessário criar a base de dados. Como foi integrada esta com o domínio *Microsoft Active Directory* descrito anteriormente, foi necessário inicializar a base com o mesmo nome do domínio “tcc.interno”, o qual foi gerado invocando o comando ldapadd como abaixo:

ldapadd -h local*host* -a -W -x -D "dc=tcc,dc=interno" -f /etc/*OpenLDAP*/inicializar.ldif

O arquivo de configurações passado possui o seguinte conteúdo:

Figura 23 – Arquivo de configuração *OpenLDAP*.
Fonte: Autoria Própria (2015)

Após essa inicialização e com o serviço do slapd inicializado, foi possível acessar a base *OpenLDAP* através de um navegador de LDAP qualquer. Neste trabalho foi usado o *software* LDAP Admin.

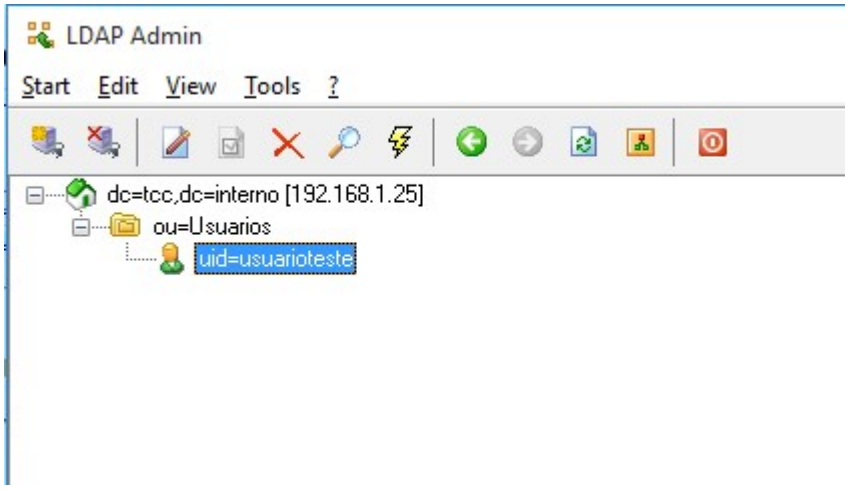

Figura 24 – Navegador LDAP Admin conectado a base *OpenLDAP*.
Fonte: Autoria Própria (2015)

3.3.2 LSC – *LDAP Synchronization Connector*

O *software* LSC foi escolhido para a integração proposta neste trabalho devido a sua proposta de diminuir a complexidade em se realizar a integração de bases *OpenLDAP* com *Active Directory* e por ser um *software* de código aberto (LDAP Synchronization Connector, 2015).

O *software* é capaz não apenas de integração de bases *OpenLDAP* com *Active Directory*, mas também com qualquer outra fonte de dados como bases com

conector JDBC, arquivos em formato CSV e API Rest (BAHLOUL, 2008), porém neste trabalho a única integração abordada foi com bases *Active Directory*.

A instalação do *software* LSC pode ser dada de duas maneiras: fazendo-se o *download* dos arquivos compactados em tar.gz do site do fabricante ou utilizando repositórios fornecidos para sistemas que utilizam pacotes .RPM e .DEB. Neste trabalho fez-se a instalação pelo primeiro método, efetuando-se o *download* dos arquivos .tar.gz e descompactando-os manualmente. Neste trabalho foi utilizada a versão 1.2 do *software* LSC.

O único requerimento para a instalação e execução do *software* LSC é que o servidor possua instalado uma versão da Java *Virtual Machine* acima da versão 6. Neste trabalho usou-se a versão 7u80. Antes de executar o *software*, é necessário configurar a variável de ambiente JAVA_HOME para o sistema. Neste trabalho a configuração foi feita no arquivo de *profile* do usuário da seguinte forma:

```
# JAVA_HOME=/usr/java/jre1.7.0_80
```

Para conexões seguras também é necessário importar o certificado gerado no AD CS para a cadeia de certificados do Java. Este pode ser feito utilizando o seguinte comando, onde o tcc.crt foi o arquivo gerado anteriormente:

```
# /usr/java/jre1.7.0_80/bin/keytool -import –keystore
/usr/java/jre1.7.0_80/lib/security/cacerts -file tcc.crt
```

O arquivo principal de configurações do *software* LSC é o lsc.properties. Este se encarrega de receber as informações como *strings* de conexão das bases a serem integradas, regras de quais tipos de objetos devem ser integrados (como contas de usuários, grupos de usuários e contas de computadores) e também quais ações devem ser executadas pelo *software*, criação, edição e deleção de objetos.

O arquivo de configuração que foi responsável pela integração proposta neste trabalho tem suas principais configurações de conexão na figura abaixo:

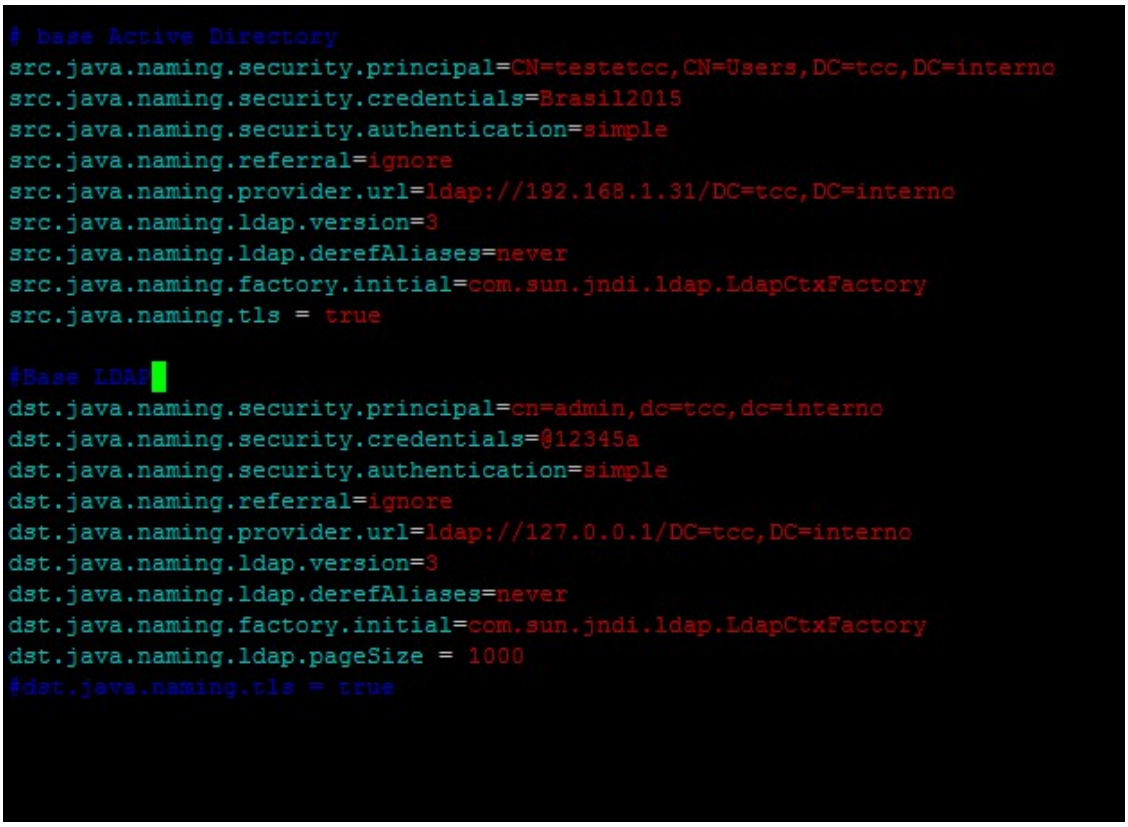

Figura 25 – Parâmetros de conexão do arquivo lsc.properties.
Fonte: Autoria Própria (2015)

O arquivo de certificado que foi gerado utilizando o servidor do AD CS foi necessário para confirmar a identidade do servidor *Active Directory*, sua importação é feita pela cadeia de certificados do Java.

O LSC não possui a função de *daemon*, ou seja, é necessária a execução em tempos pré-programados, a qual pode ser realizada pelo executor de tarefas padrão do Linux: o utilitário cron.

A execução do *software* LSC é feito chamando-se diretamente seu arquivo binário. No caso deste trabalho foi utilizado o seguinte comando.

/usr/local/lsc/bin –f /usr/local/lsc/etc/ -s all –c all

3.4 *WINDOWS* 7

Esta estação teve como nome “TESTE-PC” e foi utilizada para demonstrar o impacto da utilização das políticas de grupo no desenvolvimento deste trabalho de conclusão de curso.

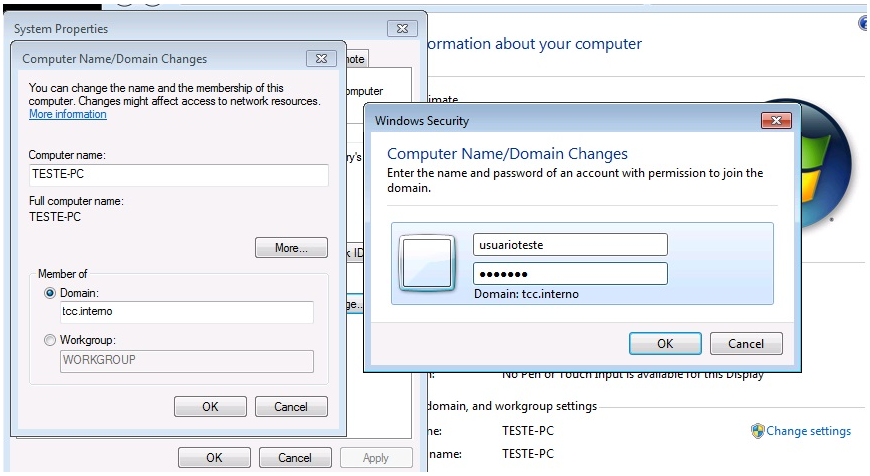

Figura 26 – A tela de autenticação para inserção do computador no domínio TCC.INTERNO.
Fonte: Autoria Própria (2015)

A inserção deste computador no domínio criado para este trabalho foi o passo inicial para que se pudesse demonstrar os efeitos das políticas de grupo aplicadas no computador.

A autenticação foi realizada com o usuário “usuarioteste” que estava criado no *Active Directory* e sincronizado com a base LDAP.

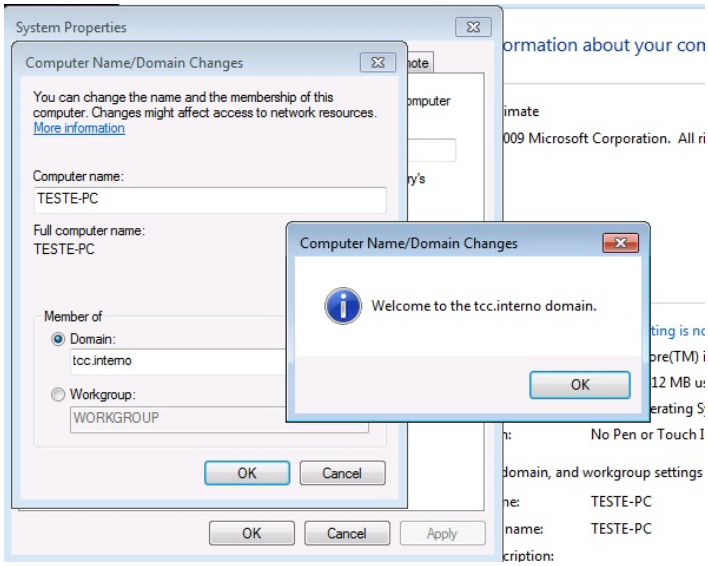

Figura 27 – Após a autenticação for validada pelo controlador de domínio, o computador é inserido no domínio com sucesso.
Fonte: Autoria Própria (2015)

O computador após ser inserido no domínio estava pronto para receber as alterações de política de grupo.

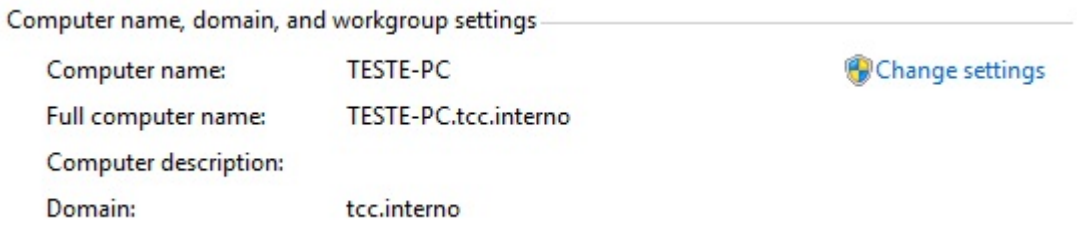

Figura 28 – Informações sobre o computador.
Fonte: Autoria Própria (2015)

3.5 GERENCIAMENTO DE POLÍTICA DE GRUPO

Como dito por BATTISTI e POPOVICI (2015), existem dois níveis de objetos de políticas de grupo (GPOs) que podem ser feitas: GPOs de usuário e GPOs de computador, e neste trabalho existe um demonstrativo para ambos os níveis.

Os objetos de políticas de grupos são criados no Gerenciamento de Política de Grupo do servidor controlador de domínio *Active Directory* e gerenciados em uma árvore de unidades organizacionais idêntica às existentes no domínio.

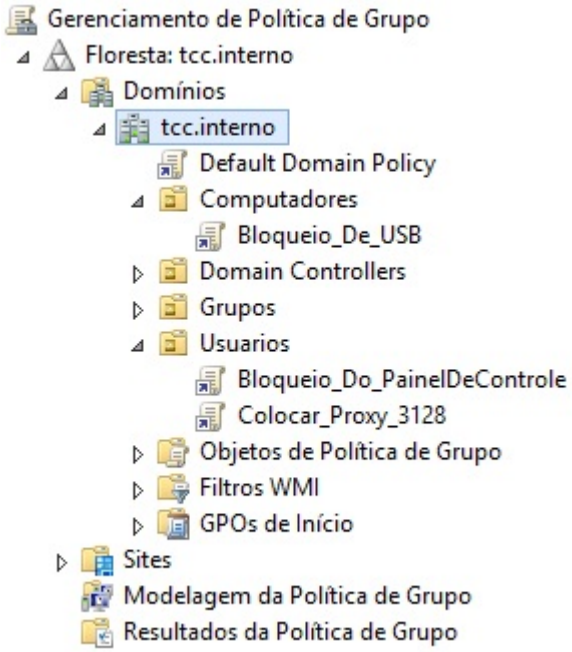

Figura 29 – Floresta tcc.interno desenvolvida no trabalho.
Fonte: Autoria Própria (2015)

Os objetos de políticas de grupo criados são armazenados na unidade organizacional “Objetos de Política de Grupo” do Gerenciamento de Política de Grupo aonde são livres para serem vinculadas à outra unidade organizacional.

Foram criados três objetos de políticas de grupo diferentes para serem demonstrados no escopo deste trabalho:

- GPO para Bloqueio de USB;
- GPO para Bloqueio de Painel de Controle;
- GPO para inserir um endereço *proxy* para os navegadores.

Destes três objetos de políticas de grupo criados, o responsável pelo bloqueio de USB é do nível de Computador, enquanto que os responsáveis por bloqueio do Painel de Controle e de inserção de endereço *Proxy* para os navegadores são de nível de Usuário.

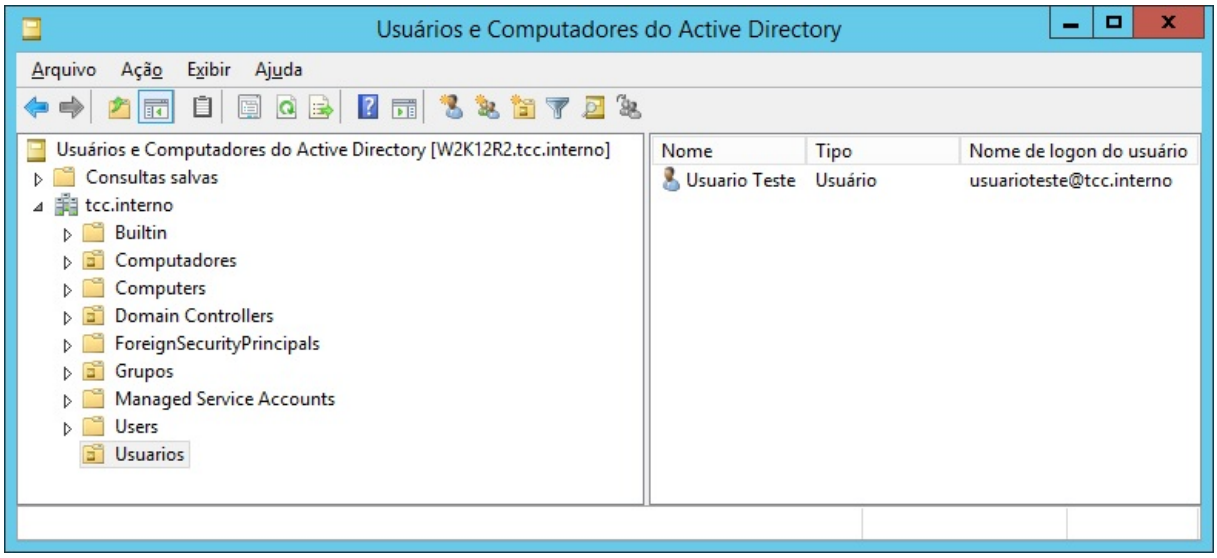

Figura 30 – Conteúdo da unidade organizacional “Usuarios” no *Active Directory*.
Fonte: Autoria Própria (2015)

As GPOs de nível de usuário foram aplicadas aos integrantes da unidade organizacional “Usuarios”, que em nosso exemplo contém o usuário “usuarioteste”.

As GPOs de nível de computador foram aplicadas aos integrantes da unidade organizacional “Computadores”, que em nosso exemplo contém o computador “TESTE-PC”.

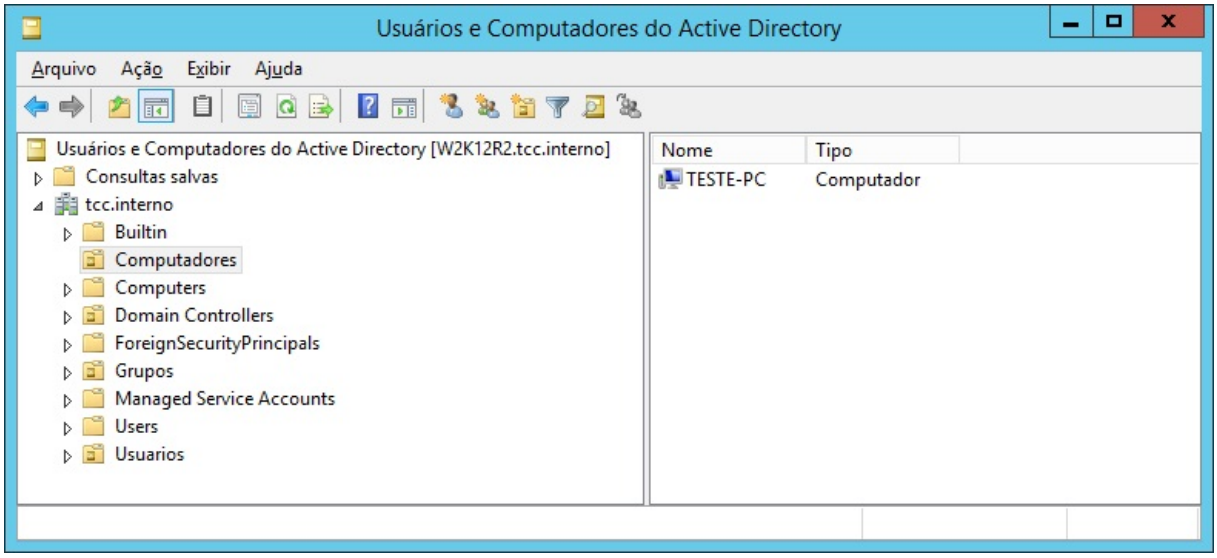

Figura 31 – Conteúdo da unidade organizacional “Computadores” no *Active Directory*.
Fonte: Autoria Própria (2015)

A GPO abaixo é responsável por bloquear o acesso à dois tipos de dispositivos USB, sendo o primeiro tipo os dispositivos WPD (*Windows Portable Devices* - Dispositivos portáteis do *Windows*), como por exemplo, celulares e câmeras digitais, e o segundo tipo os dispositivos de armazenamento removível, como por exemplo, HDs externos e pendrives.

Figura 32 – GPO de Bloqueio de USB.
Fonte: Autoria Própria (2015)

A GPO abaixo foi responsável por bloquear o acesso ao Painel de Controle e outras configurações do computador contidas dentro do Painel de controle, como por exemplo as ferramentas administrativas.

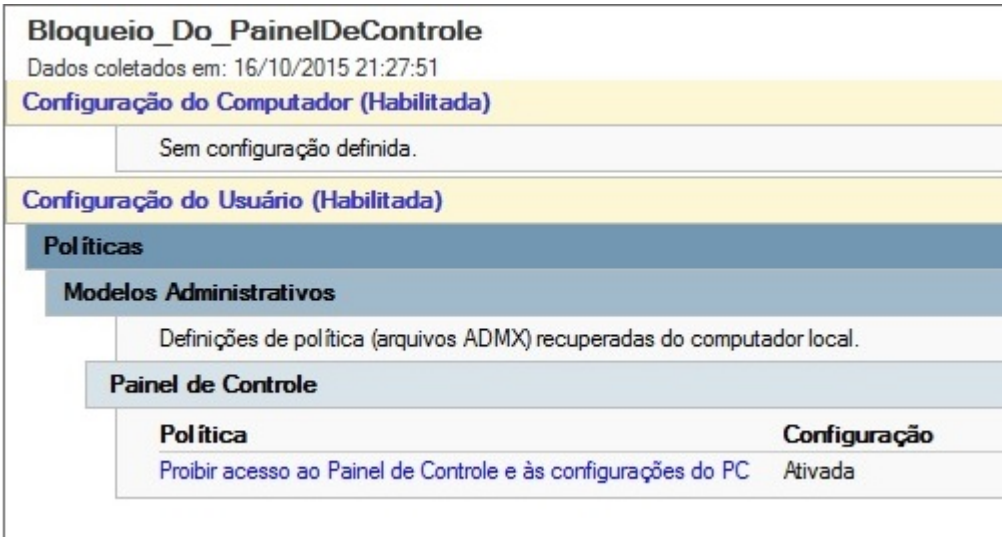

Figura 33 – GPO de Bloqueio ao Painel de Controle.
Fonte: Autoria Própria (2015)

A GPO abaixo foi responsável por configurar um endereço *Proxy* para o perfil do usuário que está utilizando o computador e por impedir que o mesmo conseguisse alterar esta configuração por conta própria.

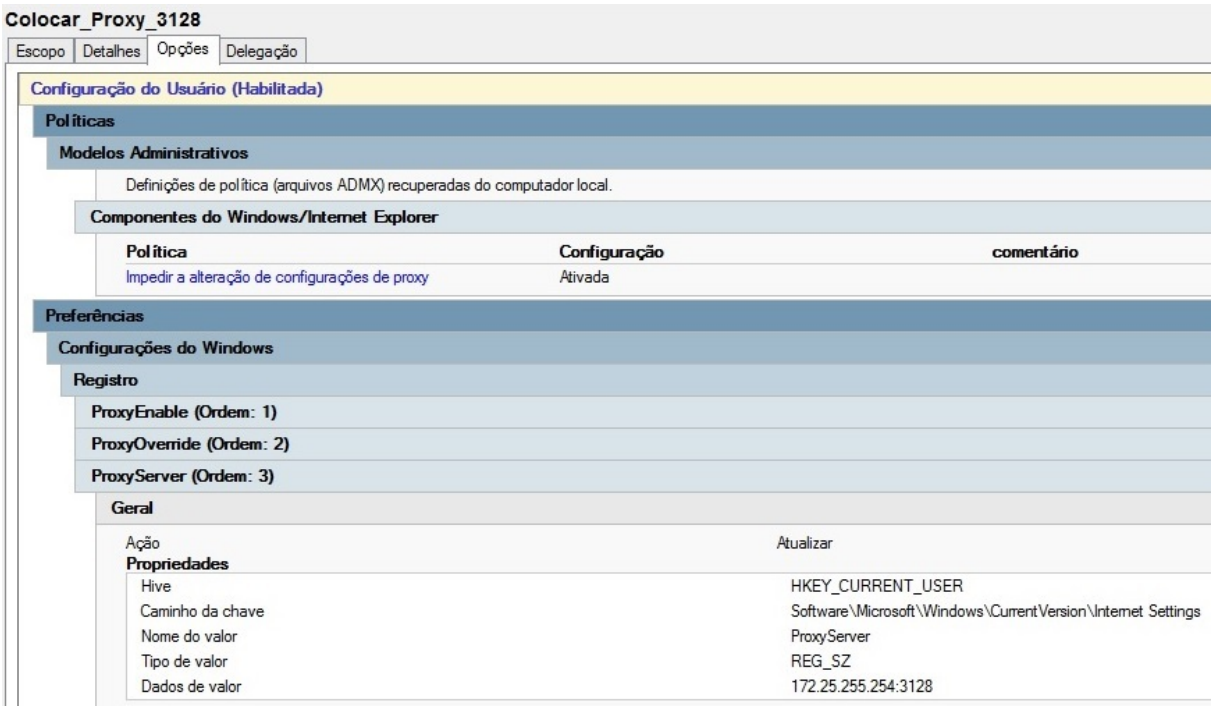

Figura 34 – GPO de configuração de endereço *Proxy*.
Fonte: Autoria Própria (2015)

Aqui tem-se o conjunto de diretivas resultantes de modo de usuário ao utilizar o comando “GPRESULT /R” no *prompt* de comando, aonde pode-se notar que estavam sendo aplicadas as GPOs de usuário “Bloqueio_Do_PainelDeControle” e “Colocar_*Proxy*_3128”.

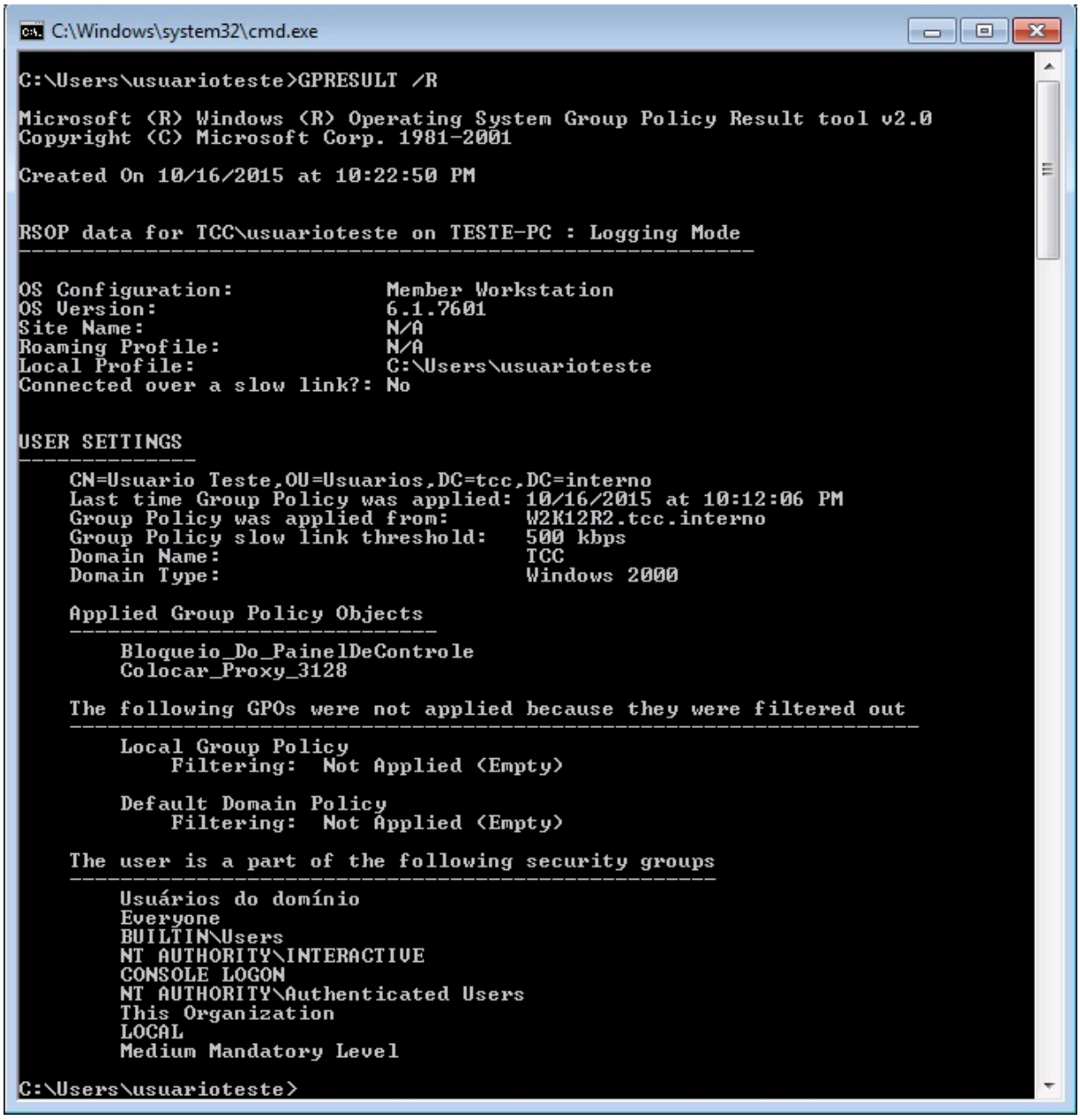

Figura 35 – RSOP de modo Usuário.
Fonte: Autoria Própria (2015)

Aqui tem-se o conjunto de diretivas resultantes de modo de computador ao utilizar o comando “GPRESULT /R /SCOPE COMPUTER” no *prompt* de comando, aonde pode-se notar que está sendo aplicada a GPO de computador “Bloqueio_De_USB”.

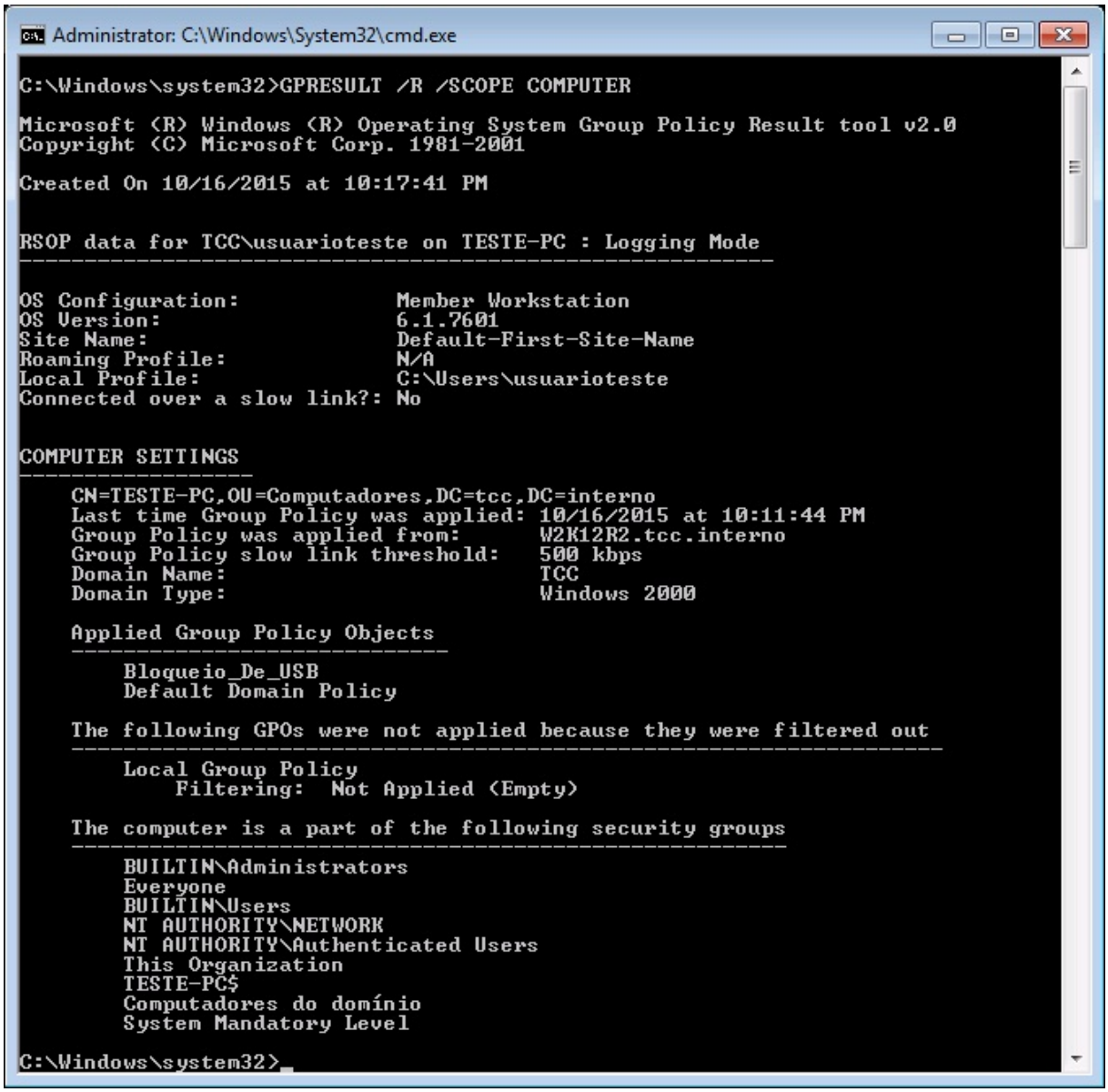

Figura 36 – RSOP de modo Computador.
Fonte: Autoria Própria (2015).

Ao tentar-se abrir o painel de controle via o menu iniciar, obteve-se a mensagem de erro demonstrando que a operação foi cancelada devido às restrições existentes no sistema. O mesmo erro é apresentado caso se tentasse iniciar o painel de controle através de outra forma, tal como através do menu executar.

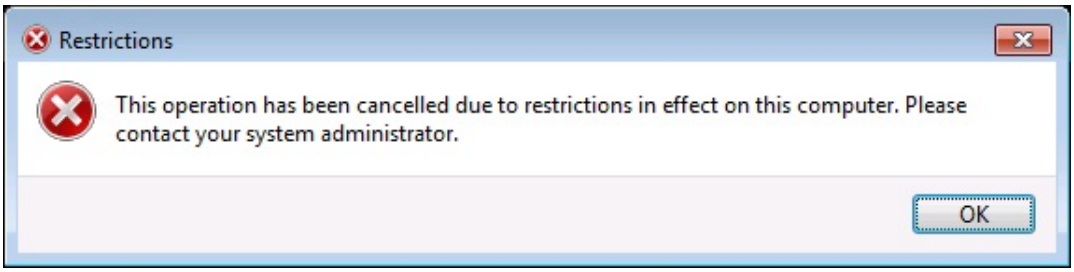

Figura 37 – Exemplo do erro ao tentar acessar o painel de Controle.
Fonte: Autoria Própria (2015).

Ao verificarmos a opção de configuração do servidor *proxy* para as opções de internet, pode-se notar que as informações de endereço e porta estão configuradas automaticamente sem possibilidade de alteração.

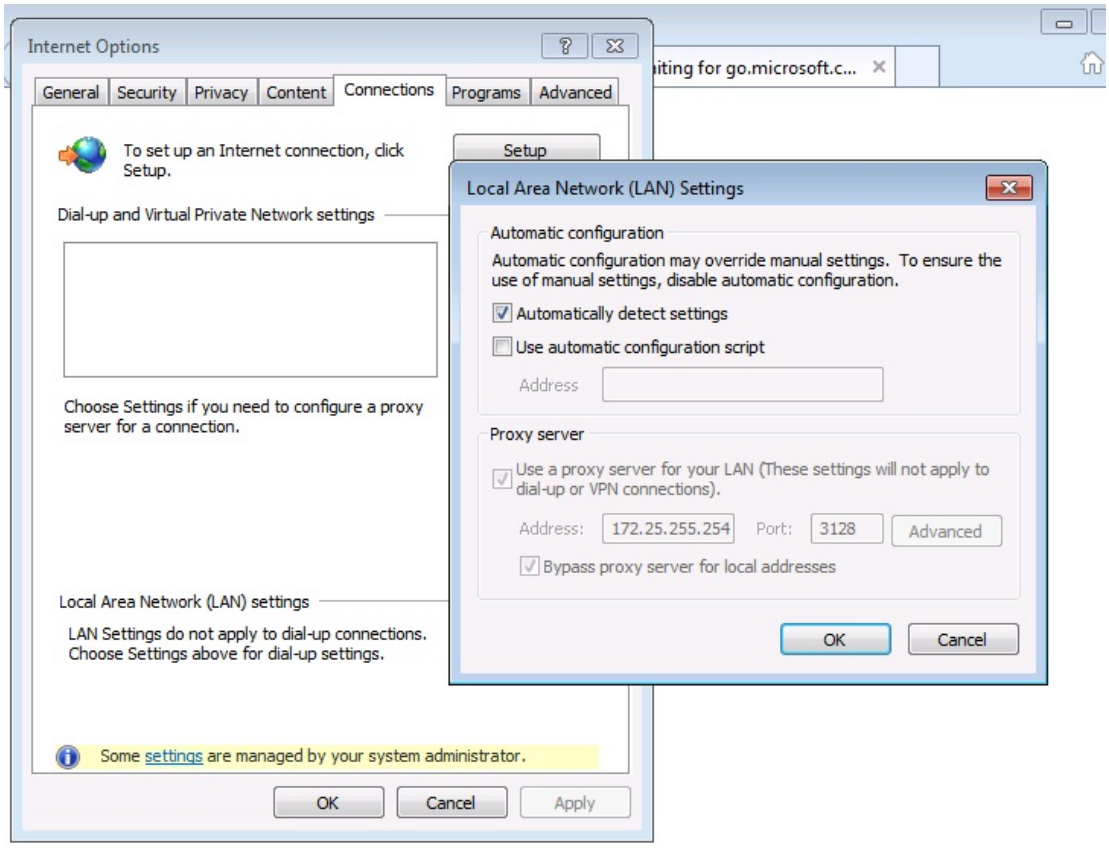

Figura 38 – Exemplo da configuração *Proxy* aplicada pela GPO de configuração de *Proxy*.
Fonte: Autoria Própria (2015).

Ao tentar-se acesso a unidade de DVD em D:\ recebeu-se um erro notificando o acesso negado à unidade de armazenamento de mídia.

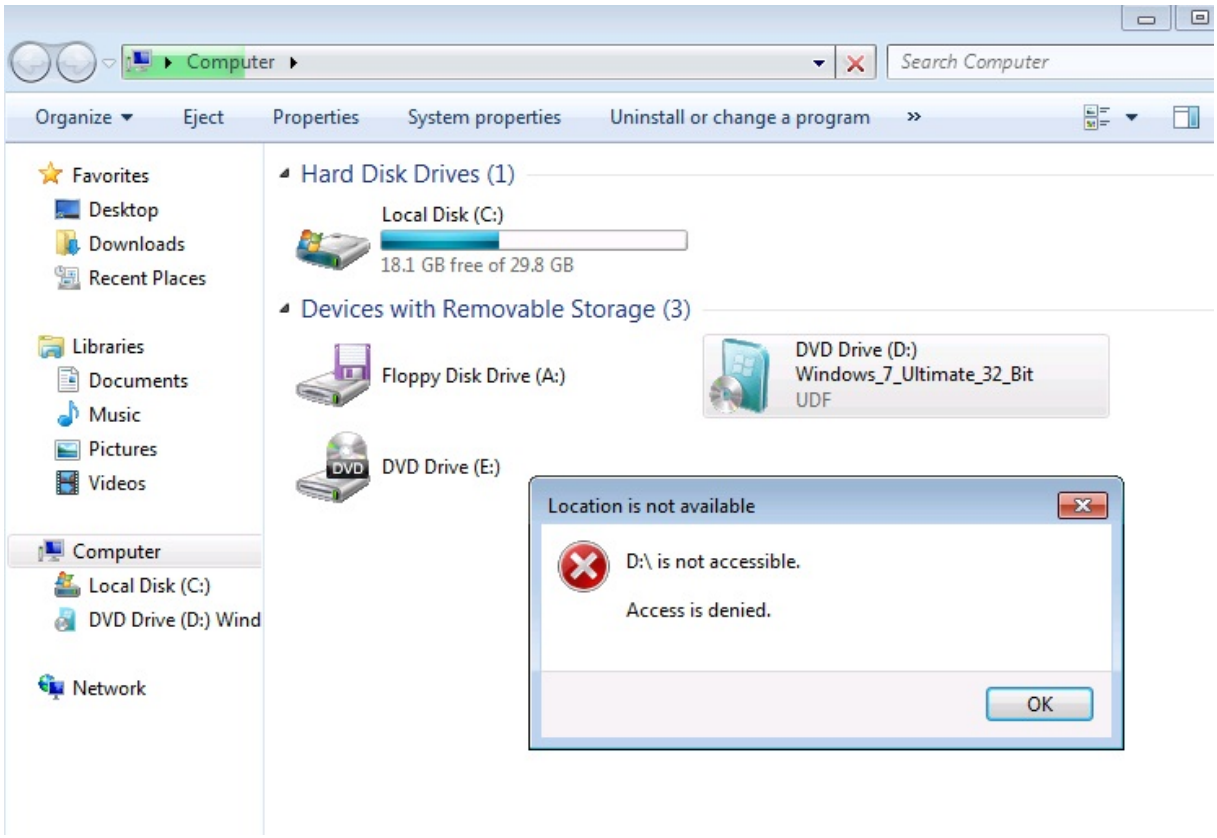

Figura 39 – Exemplo de erro ao tentar acessar uma unidade de armazenamento removível.
Fonte: Autoria Própria (2015).

4 RESULTADOS

Com a integração dos bancos de dados *Microsoft Active Directory* conseguiu-se elevar o nível de segurança da rede de computadores, devido ao fato de se possibilitar uma redundância do serviço de diretório e não apenas de dados, os quais levariam mais tempo para retornar a disponibilidade do serviço.

Nesta integração do serviço de diretório, conseguiu-se espelhar os dados de contas de usuário, porém há a possibilidade de sincronizar também outros objetos do *Active Directory* tais como: contas de computador, grupos de segurança, grupos de distribuição, entre outros, melhorando a disponibilidade dos dados e segurança da informação.

Com a sincronização utilizando o *software* LSC não foi possível o espelhamento total do objeto de contas de usuário. Não foi possível se fazer a sincronização de senha, devido a utilização de *Hash*s diferentes para senha do *OpenLDAP* e do *Microsoft Active Directory*.

O campo responsável pela senha do objeto conta de usuário, no *OpenLDAP* é o userPassword, já no *Microsoft Active Directory* o campo responsável pela senha do objeto de conta de usuário é o unicodePWD. É possível, porém alterar esta senha de outra forma, como por exemplo, construindo um serviço *WEB* que possibilite ao usuário alterar a sua senha, que por sua vez é gravada nas duas bases através deste serviço *WEB* e assim possibilitando a homogeneidade das senhas.

Deve-se realizar esta integração quando se tem a necessidade de ter uma maior segurança de nossas informações, visto que com a integração das bases *Microsoft Active Directory* e *OpenLDAP* conseguiu-se ter a redundância da estrutura do diretório.

Outro motivo para realizar esta integração é quando quer-se aumentar a quantia de *software*s que poderão autenticar usando este serviço de diretório. Existem *software*s que somente sincronizam suas senhas em bases *Microsoft Active Directory* e outros que somente sincronizam em bases *OpenLDAP*. Para tal, podemos utilizar a sincronia demostrada neste trabalho.

Não se deve realizar esta sincronia, quando possuímos um ambiente *Microsoft Windows* Homogêneo, visto que se aumenta a demanda de recursos de *hardware* para um serviço que será melhor aplicado em ambientes heterogêneos,

também quando não houver tempo ou recursos disponíveis para o desenvolvimento da aplicação WEB responsável pela alteração de senhas dos usuários.

5 CONSIDERAÇÕES FINAIS

5.1 CONCLUSÃO

Para atender ao objetivo geral deste trabalho, o qual era realizar a integração de uma base *Microsoft Active Directory* com uma base *OpenLDAP* foi utilizado o *software* LSC. A integração sem este *software* como apresentada por SANTOS (2013) é complexa e trabalhosa, e existem muitas pequenas configurações que podem não ser observadas, inviabilizando toda a sincronia.

A utilização do *software* LSC facilita a integração das bases *Active Directory* e *OpenLDAP*. Entre os benefícios da utilização, podemos citar: único arquivo de configuração, instalação por pacotes .RPM ou .DEB (como visto no item 3.3.2.) e ser o único serviço necessário a ser instalado. Porém este *software* não consegue resolver todos os problemas que surgem desta integração.

A configuração do *software* LSC não é intuitiva. Sua documentação não é numerosa, e faltam exemplos de como realizar as tarefas dentro do programa nomeadas de *tasks*. Estas *tasks* são encarregadas do que sincronizar, e sem elas há apenas a conexão nas duas bases.

O principal problema encontrado na sincronização foi a padronização de campos entre as bases. As senhas utilizam campos e criptografia diferentes, e por esta razão não foi possível realizar a sincronia de senhas dos usuários diretamente. Para tal são necessárias intervenções externas, como criação de um serviço *WEB* para a alteração de senha pelo usuário.

Também foi o objetivo deste trabalho demonstrar as configurações necessárias para inicializar as bases *Microsoft Active Directory* e *OpenLDAP*. Estas estão descritas no capitulo 3.

Com a integração de bases *Active Directory* e *OpenLDAP*, elevou-se o grau de confiabilidade da rede devido a redundância dos dados replicados em ambas as bases o que em caso de desastre pode ajudar a recuperar mais facilmente as informações.

Com a utilização dos dois serviços distintos, aumentou-se a quantidade de possíveis serviços de autenticação em um único serviço de diretório. Caso algum

serviço não seja compatível com uma das bases, pode-se utilizar a outra como serviço de diretório de autenticação.

Com a utilização de políticas de segurança do *Microsoft Active Directory* atingiu-se outro objetivo do trabalho. Segundo BATTISTI e POPOVICI (2015) estas contribuem para a elevação da segurança na rede de computadores, com o papel de regulamentação e configuração em massa de objetos do domínio. As políticas permitiram a rápida e eficiente configuração de restrições para a melhor administração de uma rede computacional.

Foi demonstrado neste trabalho a utilização de restrições que dificultam o roubo de dados por meio de bloqueio de algum dispositivo removível de armazenamento de dados, como também foram implementadas restrições de navegação à internet através da obrigatoriedade de navegação por um servidor *proxy* fictício, além de realização de bloqueio de acesso as ferramentas administrativas presentes no sistema operacional *Windows* 7.

5.2 TRABALHOS FUTUROS

Para complementar este trabalho, pode-se implementar mais *tasks* do *software* LSC para sincronia de Grupos de Usuário e Contas de Computador do *Active Directory* para o *OpenLDAP*. Também pode-se implementar a sincronia inversa utilizando como fonte o *OpenLDAP* e o *Microsoft Active Directory* como destino.

REFERÊNCIAS

DE ALMEIDA, T. T.; **Estudo de Caso: Implementação de um Serviço de e-mail para o Departamento de Computação**. Ouro Preto, 2010.

BATTISTI, Julio; POPOVICI, Eduardo; ***Windows Server* 2012 R2 e *Active Directory*: Curso Completo**. Juatuba: Instituto Alpha, 2015.

BAHLOUL, Sébastien; OUAZANA, Raphaël; Et al. **LDAP *Synchronization Connector*.** 2008. Disponível em: <http://lsc-project.org/wiki/> Acesso em: 30 de setembro de 2015.

BERGAMASCHI, R. J. P.; **Interoperabilidade com Kerberos+ Samba+ LDAP+ *Active Directory***." Lavras (2011).

ERICH. S. M. **Autenticação Integrada Baseada em Serviço de Diretório LDAP**. Disponível em: <https://linux.ime.usp.br/~cef/mac499-06/monografias/erich/monografia.pdf>. Acesso em: 30 de setembro de 2015.

FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores**. Mcgraw Hill Brasil, 2006.

LDAP *Synchronization Connector*. **LDAP *Synchronization Connector***. Disponível em: <http://lsc-project.org/wiki/>. Acesso em: 29 de setembro de 2015.

MARTINEZ, Marina. **Topologias de Rede.** Disponível em: <http://www.infoescola.com/informatica/topologias-de-redes/> Acesso em: 12 de outubro de 2015.

Microsoft. **Visão Geral dos Serviços de Domínio *Active Directory*.** 2007. Disponível em: < https://technet.*Microsoft*.com/pt-br/library/cc731053.aspx> Acesso em: 08 de outubro de 2015.

Microsoft. **Redes ponto a ponto e Redes baseadas em servidor.** 2008. Disponível em: <https://msdn.*Microsoft*.com/pt-br/library/cc527483%28v=ws.10%29.aspx?f=255&MSPPError=-2147217396> Acesso em: 12 outubro de 2015.

MINASI. Mark. Et al. **Dominando o *Windows* 2000 *Server***. São Paulo: Pearson Education do Brasil, 2001.

Netbios Working Group. ***Protocol standard for a Netbios service on a TCP/UDP transport: Concepts and methods*.** 1987. Disponível em: <http://www.rfc-editor.org/info/rfc1001> Acesso em: 08 de outubro de 2015.

SANTOS, Maximiller dos. **Uso de LDAP implementado em *software* livre para integrar a autenticação dos controladores de domínio MS-*Active Directory* e Samba/Linux.** Trabalho de Conclusão de Curso Tecnologia em Análise e Desenvolvimento de Sistemas – Universidade Tecnológica Federal do Paraná. Medianeira, 2013.

RADECK, Fernando. **Configuração de políticas de segurança no *Windows Server* 2008: *Active Directory***. Curitiba, 2012.

THE OPENLDAP FOUNDATION. ***OpenLDAP 2.4 Administrator's Guide***. Disponível em: <http://www.*OpenLDAP*.org/doc/admin24/*OpenLDAP*-Admin-Guide.pdf>. Acesso em: 03 de outubro de 2015.

TRIGO, H. Clodonil. ***OpenLDAP* – Uma Abordagem Integrada**. São Paulo: Novatec, 2007.

VIACONNECT, **Autenticação *OpenLDAP* vs *Microsoft Active Directory***. 2012. Disponível em: <http://www.viaconnect.com.br/catalogo/catalogo_*Active*_*OpenLDAP*.PDF> Acesso em: 15 de outubro de 2015.

VIDAL, Josue**. Redes e Servidores: Entendendo *Active Directory*.** 2006. Disponível em: <http://imasters.com.br/artigo/4735/servidores_*Windows*/entendendo_*Active_Directory*> Acesso em: 08 de outubro de 2015.

VON WINCKLER, Gabriel Araujo. **Proposta de arquitetura para federações de nuvens computacionais acadêmicas**. 2014. Tese de Doutorado. Universidade de São Paulo.