UNIVERSIDADE FEDERAL DE MATO GROSSO
COORDENAÇÃO DE ENSINO DE GRADUAÇÃO EM
SISTEMAS DE INFORMAÇÃO

RELATÓRIO DE ESTÁGIO SUPERVISIONADO
IMPLANTAÇÃO DE CONTROLADOR DE DOMÍNIO ACTIVE DIRECTORY E GERENCIADOR DE ATUALIZAÇÕES WINDOWS SERVER UPDATE SERVICES

JAIRO MAGESTE PIMENTEL NETO

CUIABÁ – MT
2014

UNIVERSIDADE FEDERAL DE MATO GROSSO
COORDENAÇÃO DE ENSINO DE GRADUAÇÃO EM SISTEMAS DE INFORMAÇÃO

RELÁTORIO DE ESTÁGIO SUPERVISIONADO IMPLANTAÇÃO DE CONTROLADOR DE DOMÍNIO ACTIVE DIRECTORY E GERENCIADOR DE ATUALIZAÇÕES WINDOWS SERVER UPDATE SERVICES

JAIRO MAGESTE PIMENTEL NETO

Relatório apresentado ao Instituto de Computação da Universidade Federal de Mato Grosso, para obtenção do título de Bacharel em Sistemas de Informação.

CUIABÁ – MT
2014

UNIVERSIDADE FEDERAL DE MATO GROSSO
COORDENAÇÃO DE ENSINO DE GRADUAÇÃO EM SISTEMAS DE INFORMAÇÃO

JAIRO MAGESTE PIMENTEL NETO

Relatório de Estágio Supervisionado apresentado à Coordenação do Curso de Sistemas de Informação como uma das exigências para obtenção do título de Bacharel em Sistemas de Informação da Universidade Federal de Mato Grosso.

Aprovado por:

Prof. Dr. Roberto Benedito de Oliveira Pereira
Instituto de Computação
(ORIENTADOR)

Prof. Dr. Luis Cezar Darienzo Alves
Instituto de Computação
(PROFESSOR CONVIDADO)

Cap. QOECOM Josoé Moreira
Força Aérea Brasileira
(SUPERVISOR)

DEDICATÓRIA

A Deus graças pelas oportunidades que me concedeu em minha vida.

À minha família pelo apoio, mesmo distante, sempre acreditaram.

AGRADECIMENTOS

Agradeço primeiro ao Senhor, por ter me escolhido, me iluminado.

A minha família, em especial a minha mãe, Sonia Pimentel, que não há como mensurar seus sacrifícios para que eu possa escrever este relatório. Aos meus tios, que foram um norte, inspiração, em especial Rafael Mageste, e claro, meus irmãos, Junior Pimentel, Thais Oliveira, Vinicius Pimentel, Vivyan Pimentel e Samuel Pimentel.

Aos velhos amigos, em especial ao Allison Nunes Fernandes, que mesmo distante sempre foi uma referência, pessoal, profissional e acadêmica.

Aos novos amigos, Lucas Abido e Romildo Paiter, pela amizade saudável, com o objetivo comum sermos Bacharéis.

Aos meus professores, mestres, amigos.

Aos militares que sempre me ajudaram, André Eltz, Fagner Roque, entre outros grandes amigos que conquistei nestes dez anos de serviços na Força Aérea Brasileira.

A Força Aérea Brasileira.

SUMÁRIO

LISTA DE FIGURAS **7**

LISTA DE TABELAS **8**

LISTA DE SIGLAS E ABREVIATURAS **9**

RESUMO **11**

INTRODUÇÃO **12**

1. REVISÃO DE LITERATURA **13**

1.1. SISTEMA OPERACIONAL 13
1.1.1. Windows Server 2003 R2 ..... *14*
1.1.2. Active Directory *17*
1.1.3. GPOs *18*
1.1.4. Unidades Organizacionais *19*
1.1.5. Windows Server Update Services *19*

2. MATERIAIS, TÉCNICAS E MÉTODOS **21**

2.1. CENÁRIO ATUAL 21
2.2. HARDWARE 22
2.3. SOFTWARE 25
2.3.1. Windows Server 2003 R2 Standard Edition *25*
2.3.2. Active Directory *27*
2.3.3. Windows Server Update Services *28*
2.4. POLÍTICAS DE SEGURANÇA 29
2.5. CADASTRO DE USUÁRIOS 31
2.6. CENÁRIO PARA TESTE E VALIDAÇÃO: 32
2.7. MIGRAÇÃO 34

3. RESULTADOS **36**

3.1. LEVANTAMENTO DE REQUISITOS 36
3.2. CONFIGURAÇÃO DO ACTIVE DIRECTORY 36
3.2.1. Configurar GPOs *39*
3.2.2. Configurar GPOs WSUS *41*
3.2.3. Relacionar GPOs a Unidades Organizacionais *42*
3.2.4. Servidor de Dados *43*
3.3. TESTES DE GPOS E ATUALIZAÇÃO POR WSUS 45

4. DIFICULDADES ENCONTRADAS **50**

5. CONCLUSÕES **51**

6. REFERÊNCIAS BIBLIOGRÁFICAS **52**

ANEXOS **54**

ANEXO A – ANEXO E DA ICA 7-19/2012 54
ANEXO B – TUTORIAL DE CONFIGURAÇÃO DE DNS DO CCA-BR 64
ANEXO C - ANALISE DE REQUISITOS 68
ANEXO D – CONTEUDO DO ARQUIVO DE CONFIGURAÇÃO USB.ADM 75
ANEXO E - TERMO DE COMPROMISSO PARA CADASTRO NA REDE 76

LISTA DE FIGURAS

FIGURA 1 - WINDOWS SERVER 2003 CONFIGURAÇÕES DE SERVIÇOS 16
FIGURA 2 - ACTIVE DIRECTORY - EDITOR DE GPO 18
FIGURA 3 - WSUS TELA INICIAL COM STATUS DE ATUALIZAÇÕES E COMPUTADORES 20
FIGURA 4 - SERVIDOR DELL POWEREDGE 2950 FECHADO 22
FIGURA 5 - SERVIDOR DELL POWEREDGE 2950 ABERTO 22
FIGURA 6 - CONTROLADORA RAID PERC5/I 23
FIGURA 7 - CONTROLADORA RAID PERC5/I JANELA DE CONFIGURAÇÃO 24
FIGURA 8 - DIAGRAMA DO RAID 1 24
FIGURA 9 - DIAGRAMA DO RAID 0 25
FIGURA 10 - DIAGRAMA DO RAID 10 - CC BY-SA 3.0 25
FIGURA 11 - WINDOWS SERVER 2003 CONTRATO DE LICENÇA 26
FIGURA 12 - WINDOWS SERVER 2003 INFORMAÇÕES GERAIS DO SISTEMA 26
FIGURA 13 - WINDOWS SERVER 2003 GERENCIADOR DE ARQUIVOS 27
FIGURA 14 - WSUS DETALHE DE ATUALIZAÇÃO 29
FIGURA 15 - WSUS DEFINIÇÃO DE PRODUTOS E CLASSIFICAÇÕES A SINCRONIZAR 29
FIGURA 16 - ACTIVE DIRECTORY - CADASTRO DE USUÁRIO 31
FIGURA 17 - ACTIVE DIRECTORY - PROPRIEDADES DO USUÁRIO 32
FIGURA 18 – VIRTUALBOX TELA PRINCIPAL 33
FIGURA 19 – VIRTUALBOX CRIANDO SNAPSHOT 34
FIGURA 20 - ACTIVE DIRECTORY VISÃO GERAL 37
FIGURA 21 - ACTIVE DIRECTORY UNIDADE ORGANIZACIONAL DE GRUPOS 38
FIGURA 22 - GROUP POLIY MANAGEMENT MOSTRA AS UNIDADES ORGANIZACIONAIS E SUA GPOS 43
FIGURA 23 - WINDOWS EXPLORER GERENCIADOR DE DOCUMENTOS - PASTAS COMPARTILHADAS 43
FIGURA 24 - WINDOWS EXPLORER PROPRIEDADES DE PASTA - ABA DE COMPARTILHAMENTO 44
FIGURA 25 - WINDOWS EXPLORER PERMISSÕES DE COMPARTILHAMENTO 44
FIGURA 26 - TESTE DE GPOS - GPRESULT DE UM USUÁRIO 45
FIGURA 27 – TESTE DE GPOS - GPRESULT DE UM USUÁRIO DE TESTE 46
FIGURA 28 - TESTE DE GPO - BLOQUEIO DE CONFIGURAÇÕES E PAPEL DE PAREDE 47
FIGURA 29 - TESTE DE GPO - BLOQUEIO DA ESTAÇÃO 47
FIGURA 30 - WSUS - CONFIGURAÇÃO AUTOMÁTICA DO CLIENTE 48
FIGURA 31 - WSUS - RELATÓRIO DE COMPUTADOR ATUALIZADO 49
FIGURA 32 - WSUS - SOLICITAÇÃO DE INSTALAÇÃO COM DESLIGAMENTO DO WINDOWS XP 49

LISTA DE TABELAS

TABELA 1 - REQUISITOS DE SISTEMA DO WINDOWS SERVER 2003 R2 15
TABELA 2 - ESPECIFICAÇÕES DELL POWEREDGE 2950 23

LISTA DE SIGLAS E ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
AD	*Active Directory*
CCA-BR	Centro de Computação de Aeronáutica de Brasília
CINDACTA-I	Primeiro Centro Integrado de Defesa Aérea e Controle de Tráfego Aéreo
CPU	*Central Processing Unit*
DECEA	Departamento de Controle do Espaço Aéreo
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
DTCEA-GI	Destacamento de Controle do Espaço Aéreo de Chapada dos Guimarães
GPO	*Group Policy*
FAB	Força Aérea Brasileira
IDE	*Integrated Drive Electronics*
ICA	Instrução do Comando da Aeronáutica
IP	*Internet Protocol* ou Protocolo de internet
HD	*Hard Disk*
NTFS	*New Technology File System*
PCA	Plano do Comando da Aeronáutica
PCI-E	*Peripheral Component Interconnect Express*
RAID	*Redundant Array of Independent Drives*
RAM	Random Access Memory
RPM	Rotações por minuto
SCSI	*Small Computer System Interface*
SAS	*Serial Attached SCSI*

SATA	*Serial Advanced Technology Attachment*
UFMT	Universidade Federal de Mato Grosso
WSUS	*Windows Server Update Services*
USB	*Universal Serial Bus*

RESUMO

Implantação de Controlador de Domínio *Active Directory* e Gerenciador De Atualizações *Windows Server Update Services* é o tema do estágio realizado no Destacamento de Controle do Espaço Aéreo de Chapada dos Guimarães, DTCEA-GI, com o objetivo de substituir o *Desktop* com *Windows Server* 2000 para serviços de domínio e servidor de dados, por um servidor DELL PowerEdge 2950 com *Windows Server* 2003 R2, configurar os serviços de *Active Directory*, *Windows Server Update Services* e Servidor de Dados baseados em levantamentos de requisitos sobre políticas de segurança.

Os principais softwares utilizados foram: Sistema Operacional Microsoft *Windows Server* 2003 R2 como servidor de serviço; Microsoft *Active Directory* como controlador de domínio, gerenciando os objetos da rede; Microsoft Windows Server Update Services para gerenciar remotamente as atualizações de produtos Microsoft da rede; Sistema Operacional Microsoft *Windows* XP e virtualizador Oracle VirtualBox para realizar os testes das implementações do novo servidor, como políticas de grupo e as atualizações do produtos Microsoft.

Como resultado, o DTCEA-GI possui hoje uma rede mais segura e mais simples de se gerenciar, reduzindo a carga de trabalho dos militares da subseção de Tecnologia da Informação, e com melhores condições de uso e mais segurança para os usuários.

Palavras-Chave: Gerencia de Redes, Controlador de Domínio, Windows Server 2003, Microsoft *Active Directory*, *AD*, Atualização, *Windows Server Update Services*, *WSUS*, *Group Policy*, *GPO*, Políticas de Segurança, Levantamento de Requisitos, DTCEA-GI.

INTRODUÇÃO

O Destacamento de Controle do Espaço Aéreo de Chapada dos Guimarães, possuía quando do início do estagio, uma rede de computadores com dois problemas claros: o primeiro, a gestão da rede baseada em *Windows Server* 2000, sistema operacional que já não possui suporte da Microsoft, funcionando apenas para autenticar usuários e servidor de dados, sem diretivas de segurança claras; segundo, banda de acesso à internet muito restrita, somado ao pequeno número de militares subordinados a subseção de Tecnologia da Informação, tornava impraticáveis as constantes atualizações do *Windows Update*.

Porém, com a dependência cada vez maior dos meios computacionais, e uma tendência de reduzir o efetivo técnico dos destacamentos, tornou-se necessário uma atualização do servidor e seu sistema operacional, assim como a adoção de ferramentas administrativas mais eficientes.

Assim, o objetivo do estágio foi implementar um serviço de controle de domínio com políticas de segurança, servidor de dados e repositório para atualizações de pacotes das maquinas internas com produtos Microsoft.

Para isto foi necessário: verificar os requisitos básicos para implantação do controlador de domínio; realizar um levantamento de requisitos sobre as demandas e necessidades referentes a políticas de segurança; implementar o controlador de domínio com as políticas de segurança baseadas no levantamento de requisitos e o gerenciador de atualizações do *Windows* local; validar as políticas de segurança e os serviços implementados.

Para relatar o estágio supervisionado, tem-se primeiro a Revisão de Literatura, que tem por objetivo definir os objetos de estudo do estágio, como Sistemas Operacionais, as ferramentas da Microsoft *Active Directory* e WSUS.

Em Materiais, Técnicas e Métodos explana sobre a forma que se aplicou as ferramentas e métodos.

Resultados, descreve os passos para a migração entre os servidores, mostra as configurações e testes das implementações propostas para o novo servidor.

Por fim as dificuldades encontradas como Mão de Obra, Softwares Defasados, entre outros, e as Conclusões do relatório.

1. REVISÃO DE LITERATURA

A revisão de literatura tem por finalizar embasar teoricamente o trabalho, para tal, este trabalho abordou o conceito de sistemas operacionais, focando nos produtos da Microsoft, *Windows Server* 2003, devido ao Destacamento possuir a licença do mesmo, assim como os recursos e serviços de controle de domínio, pelo software *Active Directory* da Microsoft, GPOs e WSUS. Assunto esses tradados nas próximas seções.

1.1.Sistema operacional

Sistema Operacional é o *software* de sistema fundamental, que controla todos os recursos do computador e fornece a base sobre a qual os programas aplicativos podem ser escritos (Tanenbaum, 1999).

O computador é uma complexa combinação de componentes (processadores, memórias, discos, entre outros), programar sobre estes componentes é extremamente difícil. Logo surgiu a necessidade de isolar o programador da complexidade do *hardware*, isto se deu colocando uma camada de *software* por cima do *hardware* para gerenciar as partes do sistema, oferecendo ao usuário uma interface mais fácil de entender, esta camada é o sistema operacional (Tanenbaum, 1999).

Há algumas diferenças entre os diversos sistemas operacionais disponíveis, quanto ao funcionamento de seu kernel, responsável por gerenciar os recursos do computador, quanto ao número de processos, ao número de usuários, entre outros aspectos. O sistema operacional pode apresentar diferenças devido a sua utilização, duas utilizações importantes são a Desktop ou de usuário, e Servidores. As principais características são:

- Desktop: um sistema operacional "de mesa" é voltado ao atendimento do usuário doméstico e corporativo para a realização de atividades corriqueiras, como edição de textos e gráficos, navegação na Internet e reprodução de mídias simples. Suas principais características são a interface gráfica, o suporte à interatividade e a operação em rede. Exemplos de sistemas *desktop* são os vários sistemas *Windows* (XP, Vista, 7, etc.), o MacOS X e Linux (Maziero, 2013).

- Servidor: um sistema operacional servidor deve permitir a gestão eficiente de grandes quantidades de recursos (disco, memória, processadores), impondo prioridades e limites sobre o uso dos recursos pelos usuários e seus aplicativos. Normalmente um sistema operacional servidor também tem suporte a rede e multiusuários (Maziero, 2013). Exemplos de sistemas Servidor são os vários sistemas Windows Server (2003, 2008 e 2012), CentOS, Ubuntu Server, entre outros.

Conforme pode ser visto existe diferentes versões de sistemas operacionais, um melhor adequado a cada situação, dessa forma este trabalho foca no Windows 2003 server devido ao fato deste destacamento já possuir a licença e o mesmo ser um requisito interno.

1.1.1. Windows Server 2003 R2

O *Windows Server* 2003 é uma plataforma de infraestrutura para potencializar aplicações, redes e serviços da Web conectados a partir de um grupo de trabalho até uma central de dados. Fácil de implantar, gerenciar e usar, o Windows Server 2003 ajuda você a construir uma infraestrutura segura de TI que fornece uma plataforma de aplicação poderosa para construir rapidamente soluções conectadas e uma infraestrutura de informações para comunicação aprimorada e colaboração a qualquer dia e hora (Microsoft *Corporation*, 2014).

O *Windows Server* 2003 lançado em abril de 2003 substituiu o *Windows Server* 2000 como ferramenta para servidores da Microsoft, que por sua vez foi substituído pelo *Windows Server* 2008 em fevereiro de 2008.

A Tabela 1 mostra as principais diferenças entre as versões do *Windows Serve*r 2003 R2, sendo a versão instalada a *Standard Edition*.

Tabela 1 - Requisitos de Sistema do Windows Server 2003 R2

Requisitos de Sistema do Windows Server 2003 R2			
Requisito	Standard Edition	Enterprise Edition	Datacenter Edition
Velocidade Mínima de CPU	133 MHz	• 133 MHz para computadores baseados em x86 • 733 MHz para computadores baseados em x64	• 400 MHz para computadores baseados em x86 • 733 MHz para computadores baseados em x64
Velocidade de CPU Mínima Recomendada	550 MHz	733 MHz	733 MHz
RAM Mínima	128 MB	128 MB	512 MB
RAM Mínima Recomendada	256 MB	256 MB	1 GB
RAM Máxima	• 4 GB para computadores baseados em x86 • 32 GB para computadores baseados em x64	• 64 GB para computadores baseados em x86 • 1 TB para computadores baseados em x64	• 128 GB para computadores baseados em x86 • 1 TB para computadores baseados em x64
Suporte para Multiprocessadores	Até 4	Até 8	• Exigência de uma máquina com capacidade de 8 vias • Máximo de 64
Espaço em Disco para a Instalação	1,5 GB	• 1,5 GB para computadores baseados em x86 • 2 GB para computadores baseados em x64	• 1,5 GB para computadores baseados em x86 • 2 GB para computadores baseados em x64

O *Windows Server* 2003, por ser uma distribuição para servidores, diferente de uma versão para desktop como o *Windows* XP, possui diversas ferramentas de gerência de redes, como podemos observar na Figura 1.

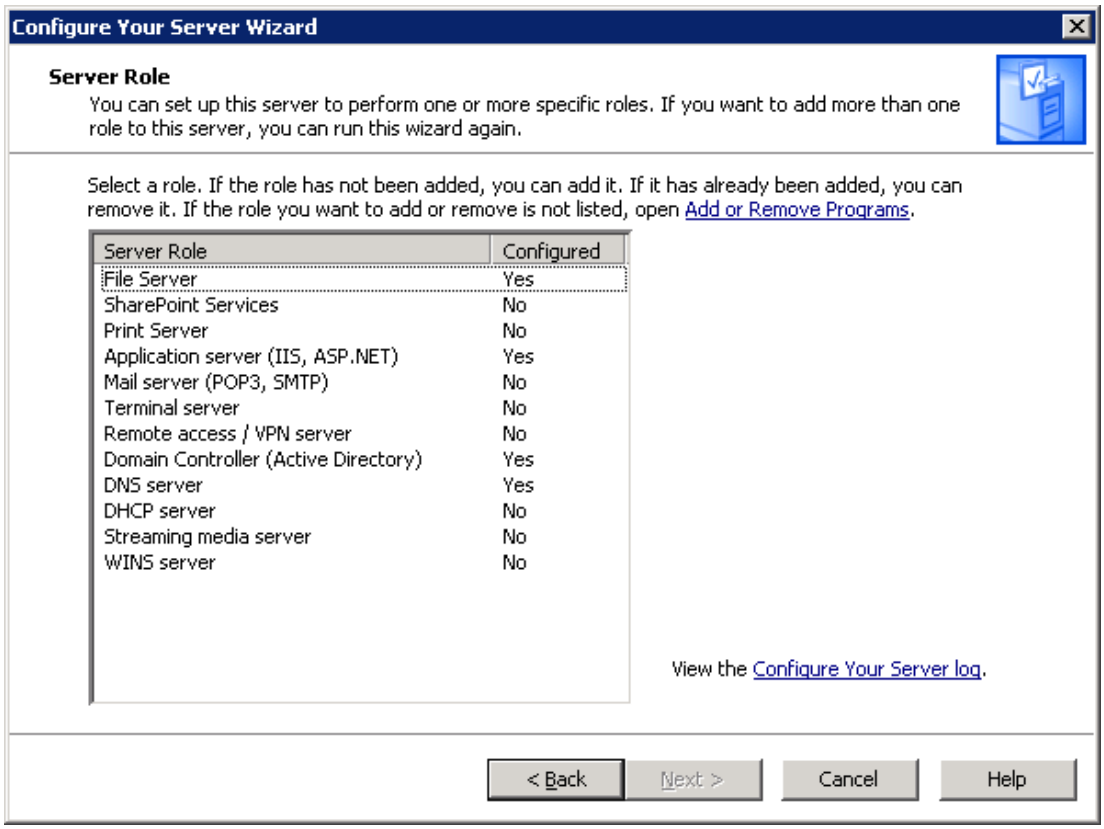


Figura 1 - Windows Server 2003 configurações de serviços

Os principais serviços utilizados no DTCEA-GI são:

- *Domain Controller* (*Active Directory*): Serviço de diretório é um conjunto de Atributos sobre recursos e serviços existentes na rede (Microsoft Corporation, 2014);
- *File Server*: O servidor de arquivos fornece um ponto centralizado na rede para armazenamento e compartilhamento de arquivos entre os usuários (Microsoft Corporation, 2014);
- DNS *Server*: Os servidores DNS (sistema de nomes de domínio) abrigam registros de um banco de dados DNS distribuído e usam os registros que abrigam para resolver consultas de nomes DNS enviadas por computadores clientes DNS, como consultas sobre nomes de sites da *Web* ou de computadores da rede ou da Internet (Microsoft Corporation, 2014);
- DHCP *Server*: Os servidores DHCP gerenciam centralmente endereços IP e informações afins, fornecendo-as automaticamente aos clientes. Isso permite que você defina configurações de rede

> cliente em um servidor, em vez de configurá-las em cada computador clientes (Microsoft Corporation, 2014).

Há outros serviços que não são nativos desta versão do *Windows Server*, porem essencial para a obtenção dos objetivos deste trabalho e que podem ser adicionados, como o WSUS (*Windows Server Update Services*) que gerencia as atualizações fornecidas pela Microsoft.

1.1.2. Active Directory

É um serviço de Diretório da Microsoft presente no *Windows Server* 2003, que centraliza informações dos objetos de uma rede de computadores vinculados a ele, de forma a facilitar o acesso a estas informações por usuários e administradores da rede.

Estes objetos do Diretório representam recursos compartilhados como servidores, arquivos, impressoras e contas de usuário e de computador da rede.

A ideia é que um usuário devidamente autenticado possa utilizar recursos (objetos) para o qual tenha permissão de uso, em qualquer ponto da rede. E que os administradores, tenham de forma centralizada a gerência de todos os objetos, definindo os relacionamentos entre os objetos, por exemplo, a quais computadores determinado usuário pode ter acesso.

Significa uma maneira de organizar e simplificar o acesso aos recursos de sua rede centralizando-os; bem como, reforçar a segurança e dar proteção aos objetos da *database* contra intrusos, ou controlar acessos dos usuários internos da rede. O *Active Directory* mantém dados como contas de usuários, impressoras, grupos, computadores, servidores, recursos de rede, etc. Ele pode ser totalmente escalonável, aumentando conforme a nossa necessidade. Esse serviço de diretório, é composto por objetos, ou seja, todo recurso da nossa rede é representado como um objeto no AD. Esses objetos possuem propriedades o que são chamados de atributos dos objetos. A base de dados do AD é um arquivo chamado NTDS.dit, onde todos os recursos são armazenados no mesmo.

A forma com que o AD relaciona seus recursos de rede, autorizando, definindo configurações, é através de políticas de Grupo, GPO.

1.1.3. GPOs

Group Policy são regras aplicadas a objetos do AD, definindo propriedades de seu funcionamento como permissões, configurações, e até instalação de aplicativos automaticamente.

As GPOs determinam os relacionamentos entre os objetos. Para isto o editor de GPO possui diversas diretrizes que podem ser configuradas. Estas diretrizes são separadas em dois grupos principais:

Computadores: Diretrizes relacionadas ao computador, independentemente de seu usuário, o computador recebe do AD estas diretrizes quando é iniciado. ;

Usuários: Diretrizes relacionadas ao usuário, independentemente do computador que está utilizando, são carregadas quando o usuário realiza o logon em um computador do domínio.

A Figura 2 mostra a janela do Editor de GPOs, a esquerda a arvores com as categorias das diretrizes, a esquerda as diretrizes da categoria selecionada, e ao centro, detalhes da diretriz selecionada.

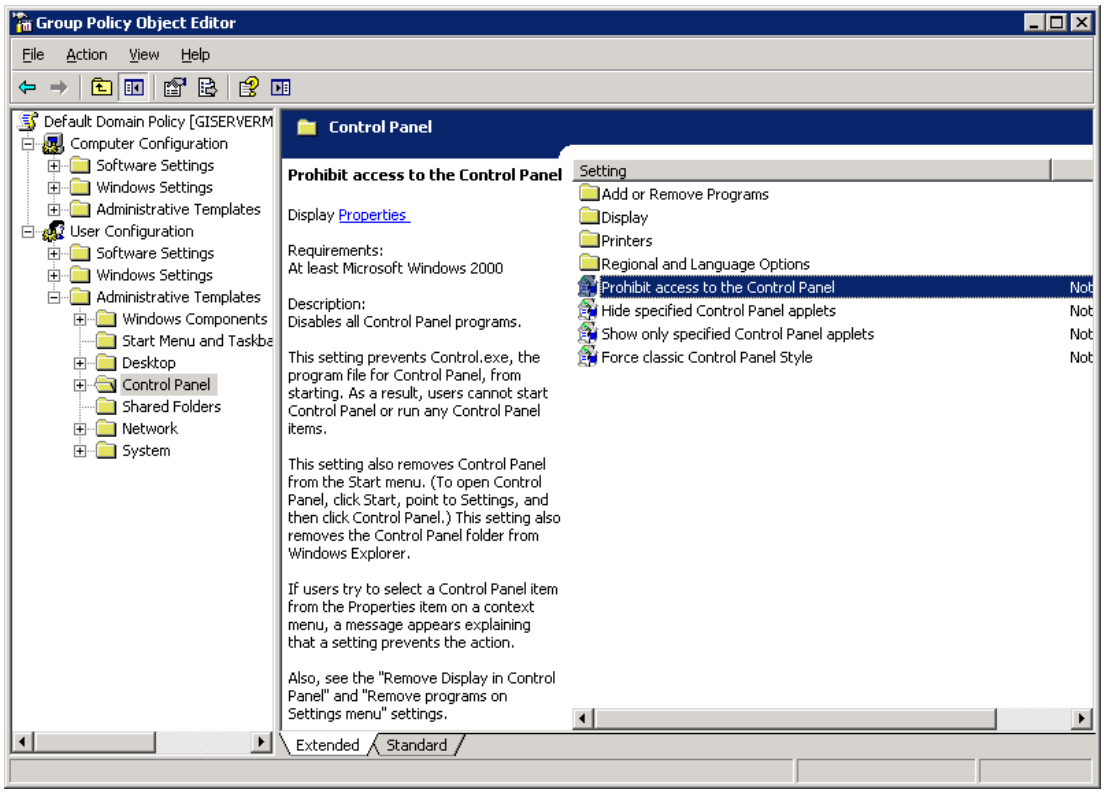


Figura 2 - Active Directory - Editor de GPO

1.1.4. Unidades Organizacionais

As unidades organizacionais são recipientes do *Active Directory* nos quais você pode inserir usuários, grupos, computadores e outras unidades organizacionais. É o menor escopo ou unidade à qual você pode atribuir configurações de Diretiva de Grupo ou delegar autoridade administrativa. Ao usar unidades organizacionais, você pode criar recipientes em um domínio que representam as estruturas hierárquicas e lógicas em sua organização. Dessa forma, você pode gerenciar a configuração e usar contas e recursos com base no seu modelo organizacional. (Microsoft Corporation, 2014).

1.1.5. *Windows Server Update Services*

O *Windows Server Update Services* (WSUS) é uma ferramenta da Microsoft com o objetivo de facilitar as atualizações dos produtos da Microsoft.

Permite que os administradores de rede implantem as atualizações mais recentes dos produtos nos computadores que estiverem executando o sistema operacional Windows. Com o WSUS, os administradores podem gerenciar integralmente e de forma centralizada a distribuição das atualizações lançadas no Microsoft Update.

O WSUS relaciona os produtos Microsoft dos computadores associados a ele com as atualizações disponíveis no Windows Update, e quando autorizado pelo administrador, faz o download das atualizações necessárias mantendo na rede local um repositório destas atualizações.

Manter um repositório local facilita o acesso dos clientes Microsoft às atualizações, reduzindo o tempo de download das atualizações.

Percebe-se que o WSUS é altamente escalonável, trabalhando com grupos, permitindo que a configuração rápida por produtos semelhantes, independentemente do número de computadores da rede.

O WSUS não é um serviço nativo do Windows Server 2003, sendo necessária a instalação separada do produto, porém estes são compatíveis, não sendo uma tarefa difícil sua instalação e configuração.

O WSUS permite ainda, distribuir os computadores em grupos e gerenciar individualmente as atualizações para cada grupo ou computador, facilitando a visualização das atualizações por categorias relacionadas aos computadores da rede.

A Figura 3 mostra a tela inicial do WSUS, com resumos e alertas. Nesta tela podemos iniciar a sincronização do WSUS com o *Windows Update*, onde ele verificara as alterações do repositório de atualizações do WSUS. Na lateral esquerda podemos ver uma arvore das visualizações disponíveis, tais como lista de sincronizações, grupos e computadores e principalmente, os updates.

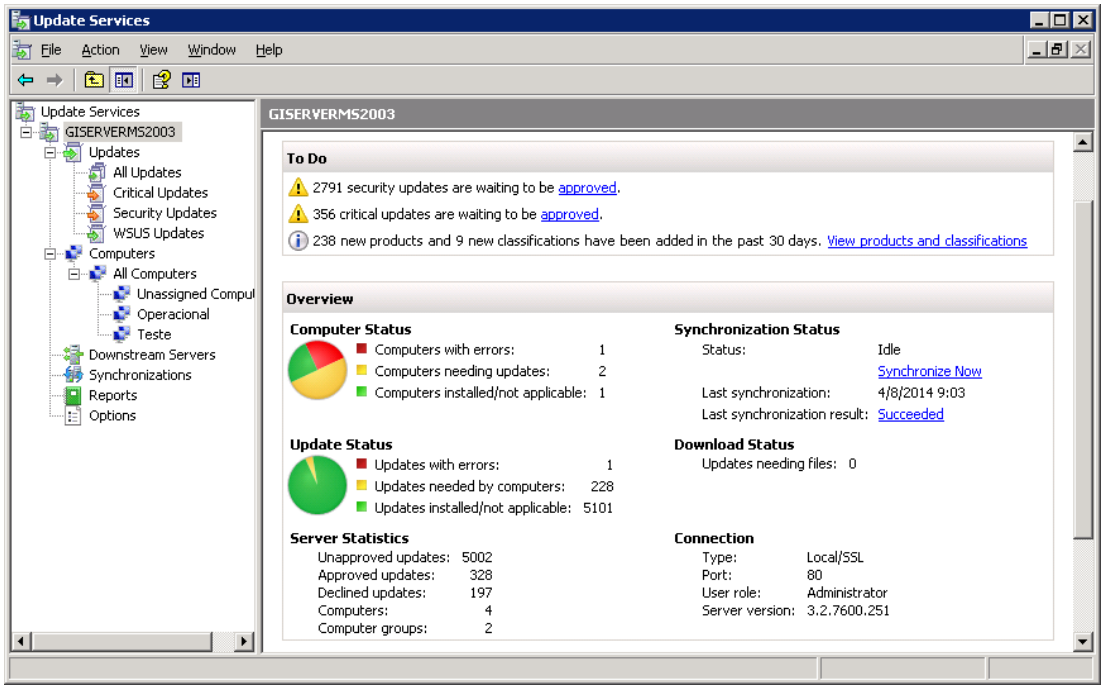


Figura 3 - WSUS Tela inicial com status de atualizações e computadores

O WSUS só fará o download das atualizações autorizadas pelo administrador, a sincronização simplesmente verifica as atualizações disponíveis de acordo com os produtos e classificações escolhidas.

Para a instalação do WSUS é necessário atender os seguintes requisitos mínimos:

- CPU: Mínimo 1 GHz, recomendado 1.5 GHz
- RAM: Mínimo 1 GB, recomendado 2
- Mínimo 1 GB de espaço livre na Partição do Sistema Operacional;
- Mínimo 2 GB de espaço livre na Partição do Database;
- Mínimo 20 GB de espaço livre na Partição do repositório das atualizações, recomendado 30 GB.

2. MATERIAIS, TÉCNICAS E MÉTODOS

2.1. Cenário Atual

O DTCEA-GI possui pequena rede de computadores para atender sua rotina. Esta rede é gerenciada por serviços da Microsoft utilizando o *Windows Server* 2000 *Service Pack* 4, instalado em um *Desktop*.

No *Windows Server* 2000 são utilizados os serviços de DHCP, *Active Directory* e servidor de Dados. DHCP fornece IPs para os clientes da rede, informando ainda Mascara, *Gateway* e DNS da rede (Como o DNS não foi devidamente configurado, o DHCP informa o DNS de uma Organização Militar Superior). O Serviço de Domínio é feito pelo *Active Directory* nativo do *Windows* 2000 Server. O AD gerencia os usuários e computadores do Domínio, porém é subutilizado, não havendo políticas de grupos ativas, servido apenas de controle de acesso dos usuários aos computadores e subsidia informações para o serviço de servidor de dados, para determinar permissões e restrições de acessos a determinados conteúdo. O Servidor de dados, simplesmente restringe acesso ou o permite, não possuindo cotas de capacidades por grupos ou usuários, ou ainda rotinas de *backup*.

O *Desktop* possui: processador Intel E2140 de dois núcleos, frequência de 1,6Ghz e 1Mb de *cache* L2, 1024Gb de Memória RAM (sendo 64Mb compartilhadas com o Vídeo *Onboard*) e dois discos rígidos IDEs, 75Gb e 120Gb, para instalação do sistema operacional e armazenamento de dados.

A Microsoft encerrou o suporte ao *Windows Server* 2000 em 13 de Julho de 2010, recomendando sua substituição (Microsoft Corporation, 2014).

Para a melhoria dos meios computacionais deste Destacamento, o CINDACTA I, através da Divisão de Informática, forneceu um Servidor DELL PowerEdge 2950 e uma licença para *Windows Server* 2003 R2 *Standard Edition* para substituir o *Desktop* com *Windows Server*.

2.2.Hardware

O *PowerEdge* 2950 da Dell utilizando processadores da família Intel oferece excelência, segurança, gerenciabilidade e baixo consumo de energia em um chassi de rack 2U para aqueles que buscam um equilíbrio entre a capacidade de expansão e a densidade de rack (Dell, 2014).

Figura 4 - Servidor Dell PowerEdge 2950 fechado

O *PowerEdge* como visto na Figura 4, possui construção robusta e de fácil manutenção, sendo fixado ao rack através de trilhos próprios, acompanhado com um organizador de cabos. Na Figura 5 observa-se o servidor aberto, na parte inferior (frente do servidor) estão os discos, a esquerda, a controladora Perc5/i, pouco acima, estão os *coolers* responsáveis por resfriar os dois processadores e os quatro pentes de memórias que estão abaixo da proteção de plástico preto, no canto superior esquerdo, estão as duas fontes de 750W redundantes, e ao seu lado está a parte da placa mãe e os slots PCI-E.

Figura 5 - Servidor Dell PowerEdge 2950 aberto

Pode-se ver na Tabela 2, as principais especificações do servidor recebido, destacando os oito núcleos de processamento, o que garante auto desempenho deste novo servidor, ainda mais comparado com processador Intel E2140 de dois núcleos de 1,6Ghz do servidor substituído.

Tabela 2 - Especificações Dell PowerEdge 2950

Especificações DELL PowerEdge 2950	
Processador	2 processadores Quad-Core Intel Xeon E5345 em até 2,33 GHz
Chipset	Intel 5000X, 1066 MHz e Front Side Bus (FSB) de 1333 MHz
Memória	8Gb (4 x 2Gb e 4 slots Livres) DIMM DDR2 667Mhz
Discos Rígidos	2 X SAS de 3,5" (15 K rpm) 146 GB RAID 1 (Disco Virtual de 146Gb) 4 X SATA de 3,5" (7200 rpm) 160 GB RAID 10 (Disco Virtual de 320Gb)
Baias de Unidade	6 HDs de 3,5"
Controladoras de Unidade	Perc5/i
Rede	NIC Broadcom® NetXtreme II 5708 Gigabit dupla 6 X Intel® PRO/1000 MT de porta única
Energia	Configuração CA com hot-plug redundante de 750 W

Observa-se ainda as duas configurações de Discos distintas, sendo a primeira original da Dell, o primeiro Disco Virtual com capacidade de 146Gb em 2 X HD 146Gb SAS 15K rpm em RAID 1, o segundo Disco Virtual com capacidade de 320Gb em 4 X HD 160Gb SATA 7200 rpm em RAID 10.

Figura 6 - Controladora Raid Perc5/i

O responsável por gerenciar os discos virtuais, é a Controladora RAID Perc5/i, mostrada na Figura 6. Ela é conectada as baias de discos do servidor por cabo próprio, controlando neste caso, os 6 discos, permitindo inclusive a utilização de tecnologias de discos diferentes, SAS e SATA, desde que em Discos Virtuais diferentes.

A configuração dos Discos Virtuais é feita pela janela de configuração da Perc5/i que pode ser iniciada quando ligado o servidor pressionando em momento oportuno Ctrl+R. A Figura 7 mostra a janela de configuração, com o primeiro Disco Virtual, e mostra os discos físicos associados a este.

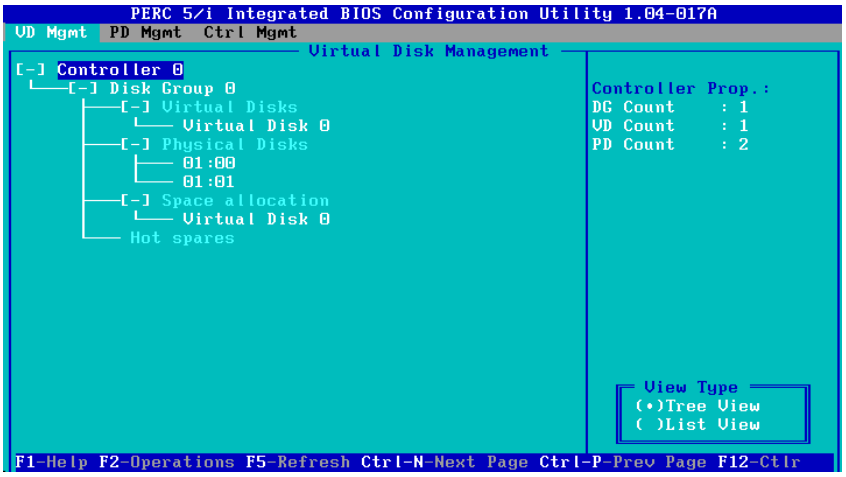


Figura 7 - Controladora Raid Perc5/i Janela de Configuração

A escolha de RAID 1 para o primeiro Disco Virtual foi definida buscando segurança, uma vez que ela permite a perda de um de seus dois discos físicos, sem perda de dados nem desempenho, pois o RAID 1, os discos recebem as mesmas informações simultaneamente como mostra a Figura 8.

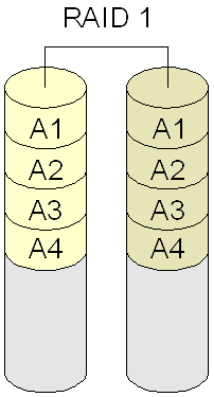


Figura 8 - Diagrama do RAID 1

Quanto ao segundo Disco Virtual foi escolhido o RAID 10, também pensando em disponibilidade, uma vez que o RAID 10 permite a perda de até dois discos físicos (dependendo da combinação) dos quatro discos utilizados. O RAID 10 ou RAID 1+0, primeiro divide a informação a ser gravada nos discos em duas partes distintas, visando aumentar a velocidade de gravação como no RAID 0 como na Figura 9. Em sequência ela grava parte da informação em dois discos simultaneamente, como no RAID 1.

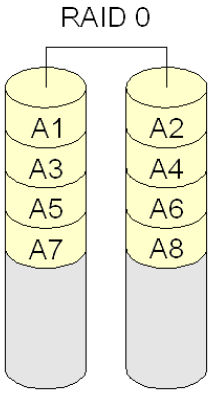


Figura 9 - Diagrama do RAID 0

Esta combinação entre as duas técnicas de RAID, permite o ganho de performance do RAID 0 com a segurança do RAID 1, porém com a perda da metade da capacidade da soma dos discos. O resultado podemos ver na Figura 10.

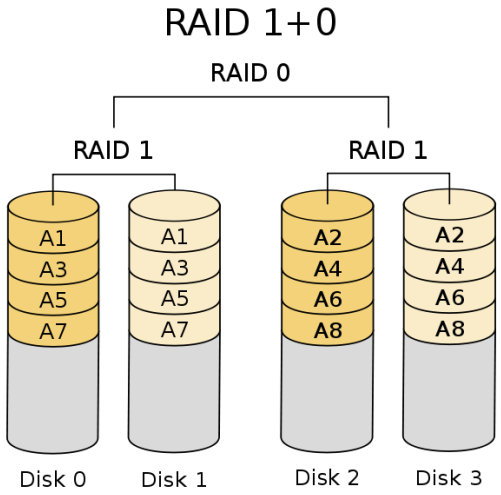


Figura 10 - Diagrama do RAID 10 - CC BY-SA 3.0

2.3.SOFTWARE

2.3.1. *Windows Server* 2003 R2 *Standard Edition*

Foi instalado no Servidor PowerEdge 2950, o sistema operacional da Microsoft, *Windows Server* 2003 R2 *Standard Edition* em inglês. O sistema operacional foi fornecido junto com o servidor, pelo CINDACTA-I. Sendo a base para os serviços de rede do DTCEA-GI, executando o Active Directoy, DNS, servidor de dados, WSUS, entre outros. A Figura 11 mostra um exemplo do Contrato de Licença do Windows, aceito durante a instalação.

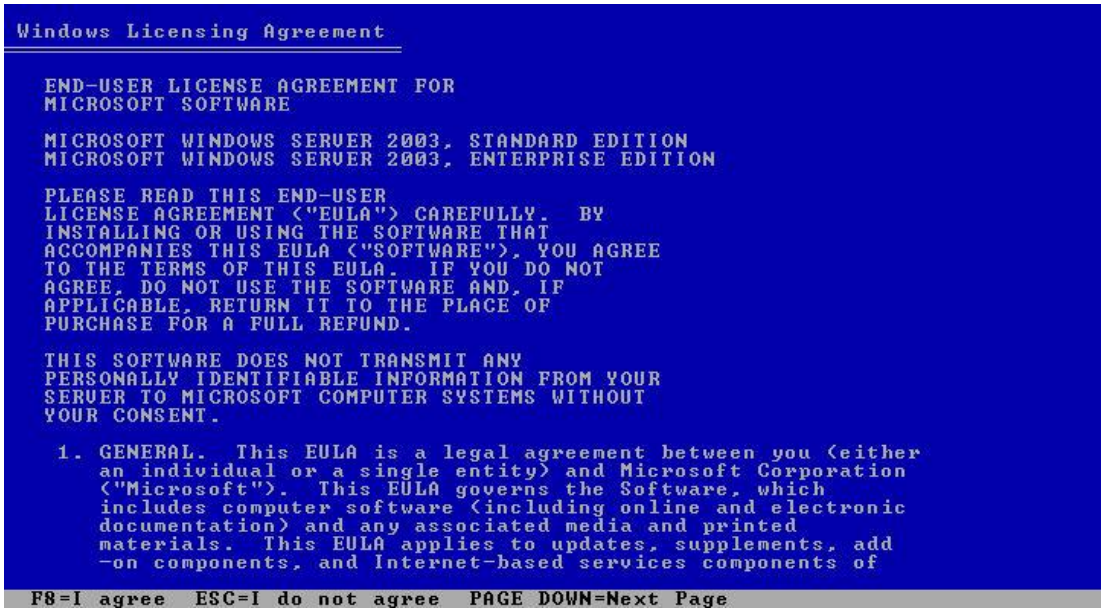


Figura 11 - Windows Server 2003 Contrato de Licença

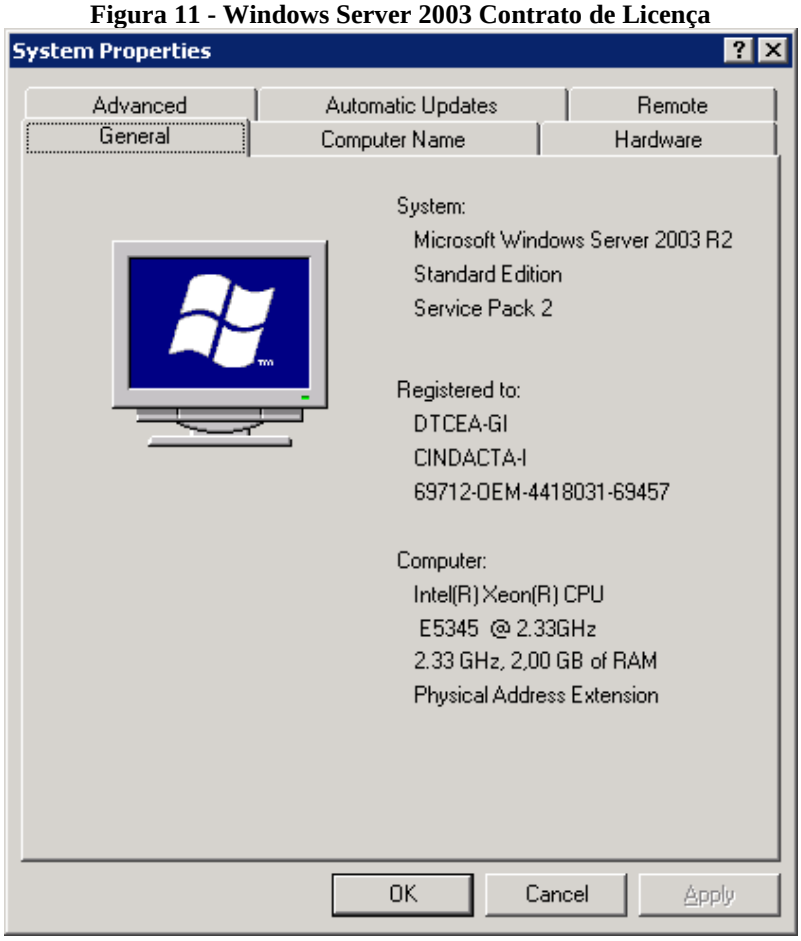


Figura 12 - Windows Server 2003 informações gerais do sistema

A Figura 12 mostra as propriedades do sistema do Windows Server 2003 instalada no DTCEA-GI. É possível ver os detalhes da versão instalada e principais informações de *hardware*, como processador e memória *RAM*.

A Figura 13 mostra como foi configurado os HDs, com três partições. A primeira (C:) para o sistema e aplicativos, a segunda (D:) para repositório do WSUS e a terceira (E:) para os dados dos usuários do Destacamento. Todas utilizando NTFS.

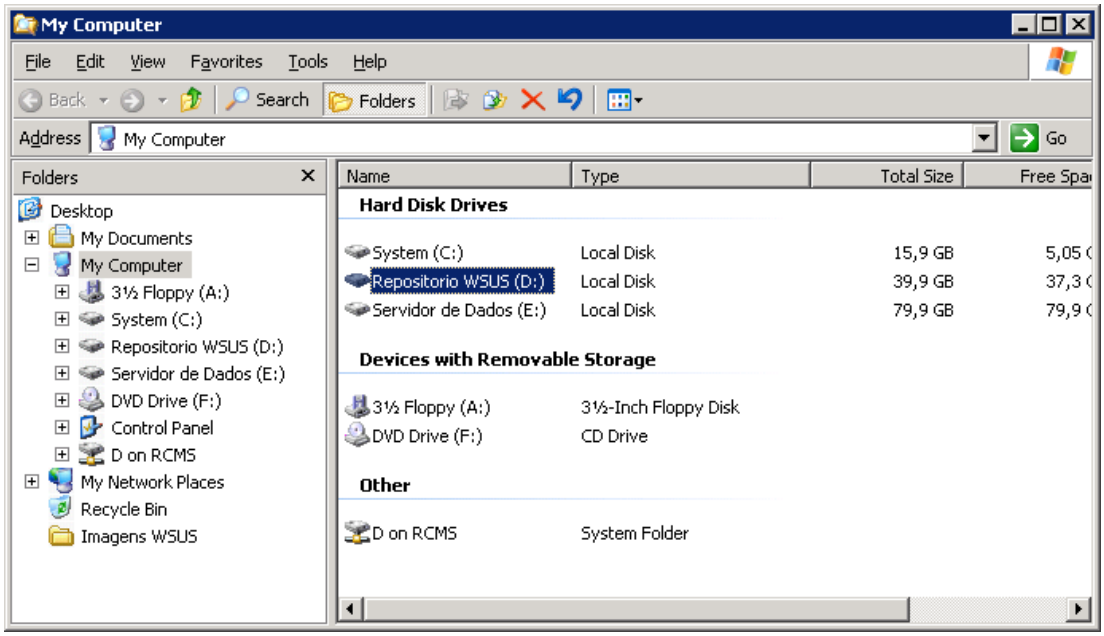


Figura 13 - Windows Server 2003 gerenciador de arquivos

2.3.2. Active Directory

Após instalar o *Windows Server* 2003, é ativado o serviço de *Active Diretory*, ele exige a ativação do serviço de DNS, com o principal motivo, resolver o nome do domínio na rede.

Durante a ativação, definiu-se um novo domínio, DTCEAGI-AD.intraer, para substituir o DTCEA-GI.cindacta1.intraer.

Para controlar o Domínio, as principais ferramentas do AD são:

- *Active Directory Users and Computers*: Gerencia os objetos do domínio, computadores, usuário, unidades organizacionais, entre outros objetos. Por esta ferramenta é possível criar unidades organizacionais e distribui os objetos do domínio de forma organizada, permitindo tanto aplicações de políticas restritas como abrangentes de forma da mesma forma. Pode-se criar e gerenciar usuários, por esta ferramenta, definindo sua unidade organizacional e a quais grupos pertence, definir horário de utilização dos ativos de rede, e quais computadores poderá utilizar.

- *Group Policy Management*: é a ferramenta do Active Directory utilizada para criar, editar e relacionar as GPOs com o domínio ou unidades organizacionais.

2.3.3. Windows Server Update Services

O WSUS deve ser instalado separadamente após a instalação do *Windows Server* 2003, sendo recomendado também a instalação do Microsoft *Report Viewer* 2008 para a exibição dos relatórios.

Durante a instalação é necessário informar o local que ficara o repositório do WSUS e o *Windows Internal Database*. Recomenda utilizar o IIS *Defaut Web site* do servidor, informando qual o endereço para os clientes acessarem os serviços de atualização.

Após a instalação, o WSUS executa um assistente de configuração, auxiliando o administrador com as configurações básicas.

Com o WSUS é possível visualizar detalhes das atualizações oferecidas pela Microsoft como mostra a Figura 14, mostrando o tipo de atualização (*Critical Updates*, *Definition Updates*, *Drives*, *Feature Packs*, *Security Updates*, Service Packs, *Tools*, *Update Rollups* e *Updates*), informa quantos computadores necessitam esta atualização, descrição e detalhes adicionais.

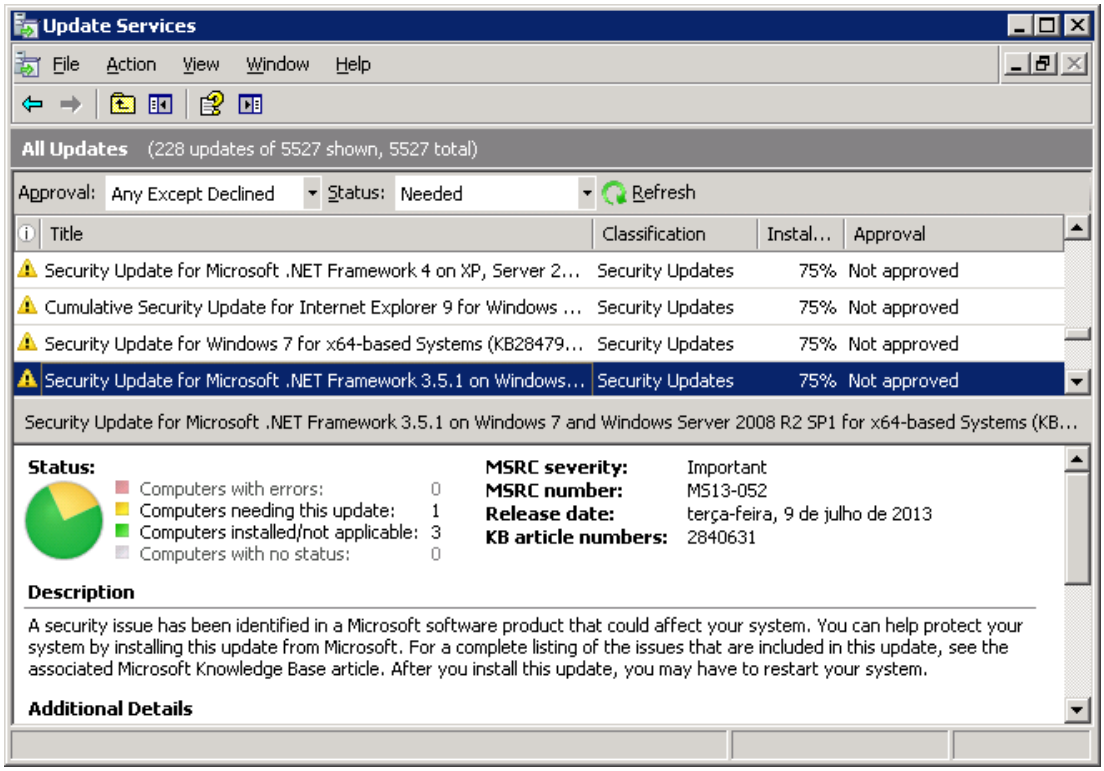


Figura 14 - WSUS detalhe de atualização

Em suas configurações, deve-se determinar quais produtos o seu WSUS dará suporte, ou seja, devemos configurar quais produtos Microsoft temos em nossa rede, pela janela mostrada na Figura 15. Pode-se ainda definir quais classificações o WSUS sincronizara com a Microsoft, caso a empresa, por exemplo, possua um software para gerenciar drives, ela não necessita sincronizar drives em seu WSUS.

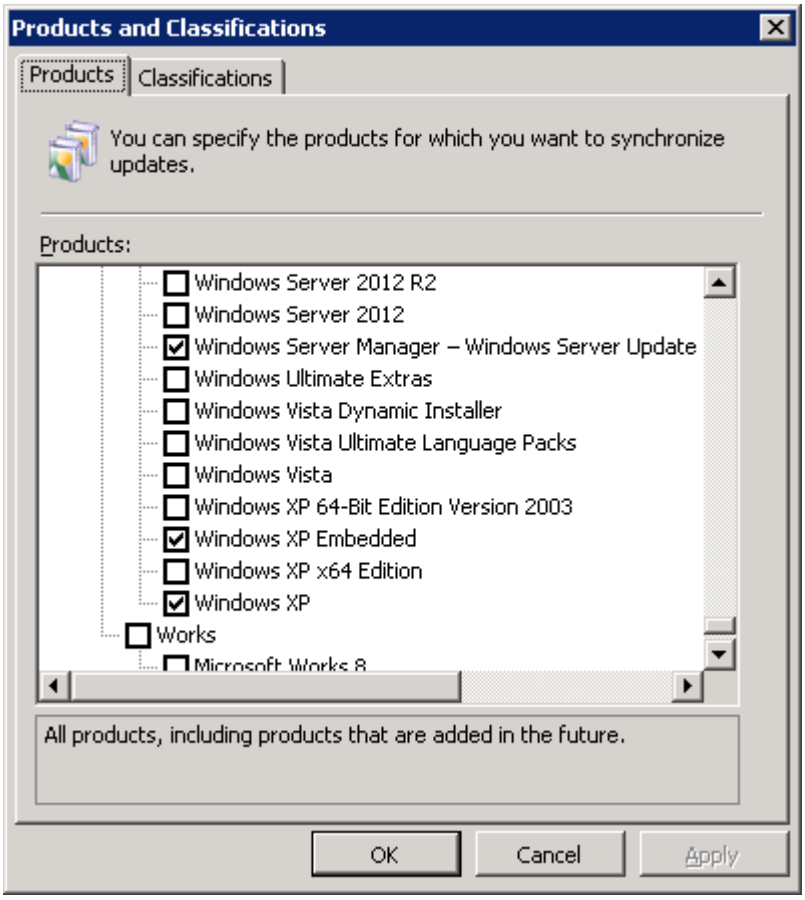


Figura 15 - WSUS definição de produtos e classificações a sincronizar

2.4. Políticas de Segurança

As políticas de segurança são regras, procedimentos, diretrizes a serem seguidas de forma a fortalecer a segurança da informação no DTCEA-GI.

Estas políticas de segurança são a base para a configuração das regras de utilização dos meios computacionais do Destacamento, logo, são a base para a configuração do gerenciador de domínio (*Active Directory* no *Microsoft Windows Server* 2003) definindo seus grupos de usuários, unidades organizacionais, diretrizes de uso de computadores, acesso a pastas compartilhadas e principalmente as políticas de grupo (GPOs).

A forma escolhida para documentar estas políticas e conhecer as necessidades do Destacamento, foi a realização de um Levantamento de Requisitos.

O Levantamento de Requisitos é o documento que mostra as necessidades a serem atendidas para a solução do problema. Neste caso, mostra quais os requisitos para se ter uma condição mínima de segurança de rede.

Para levantar estas necessidades, foram realizados discussões com os militares que trabalham, direta e indiretamente com a subseção de Tecnologia da Informação, a fim de consultar suas ideias para o novo servidor.

Foi realizada entrevista não estruturada com o Comandante do DTCEA-GI, afim de levantar seus anseios quanto ao novo servidor e elencar pontos que não o agradam do cenário anterior, de forma a corrigi-los no novo servidor, visto que o Comandante, tem uma grande vivência em diversas Organizações Militares, contribuindo com experiências externas ao Destacamento. Ele mostrou grande preocupação quanto ao servidor de dados e sua organização.

Porém, a principal base para o levantamento de requisitos foi a observação dos usuários do DTCEA-GI e seu relacionamento com os ativos de tecnologia da informação. Foram observadas discrepâncias como usuários sem senhas, diversos militares utilizando um único usuário da rede, documentos armazenados localmente, documentos armazenados em locais inadequados, mesmo dentro do servidor de arquivo, estações de trabalho logadas sem que estejam em uso.

A Força Aérea Brasileira, visando padronizar e melhorar a qualidade de seus serviços de tecnologia de informação possui uma serie de regulamentos que orientam os militares e civis relacionados a esta área a como atuar em seus ambientes de trabalho. De forma a atender estes regulamentos durante o estágio e adequar as configurações da rede a eles, foi realizado um estudo dentro dos principais regulamentos relacionados a tecnologia da informação.

O Anexo A mostra o regulamento que aborda o cenário deste estágio, o Anexo E da ICA 7-19/2012. Esta Instrução do Comando da Aeronáutica (Instrução de Preceitos de Segurança da Informação para o Departamento de Controle do Espaço Aéreo, DECEA) em seu Anexo E normatiza o Controle de Acesso Lógico das Redes de Telecomunicações, está alinhada com as conclusões dos demais métodos de levantamento de requisitos.

Outra fonte utilizada para o levantamento de requisitos foi a legislação da FAB, PCA 7-18/2012, Plano de Divulgação de Segurança da Informação do Departamento de Controle do Espaço Aéreo, que mostra o resultado de uma análise de risco referente, entre outro, ao usuário final, elencando o risco e necessidade de educação e conscientização do usuário. Porém este regulamento é voltado para a divulgação e conscientização, e não para a configuração de Domínio.

2.5. Cadastro de Usuários

O cadastro dos usuários é um passo importante para a segurança da rede, e atende a alguns dos requisitos definidos pela política de segurança.

O usuário a ser cadastrado dever preencher e assinar o Termo de Compromisso para utilização dos recursos de tecnologia da informação. O Anexo E apresenta este termo.

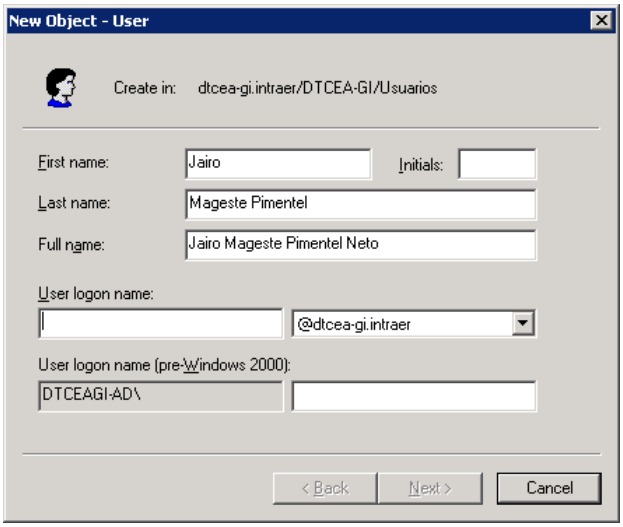


Figura 16 - Active Directory - Cadastro de Usuário

Com o Termo assinado pelo usuário e por seu chefe imediato, neste caso, o Comandante do DTCEA-GI, o administrador deverá realizar seu cadastro no AD. A Figura 16 mostra a janela para cadastro de usuário. Durante o cadastro do usuário, deve-se digitar a senha inicial padrão e marcar a opção que obrigue o usuário a trocar de senha no próximo *logon*.

Após o cadastro inicial o administrador deve completar o cadastro nas propriedades do usuário, Figura 17. Inserindo informações pessoais, grupos do AD a qual participa, de forma a atender as políticas do servidor de dados e de acesso à internet.

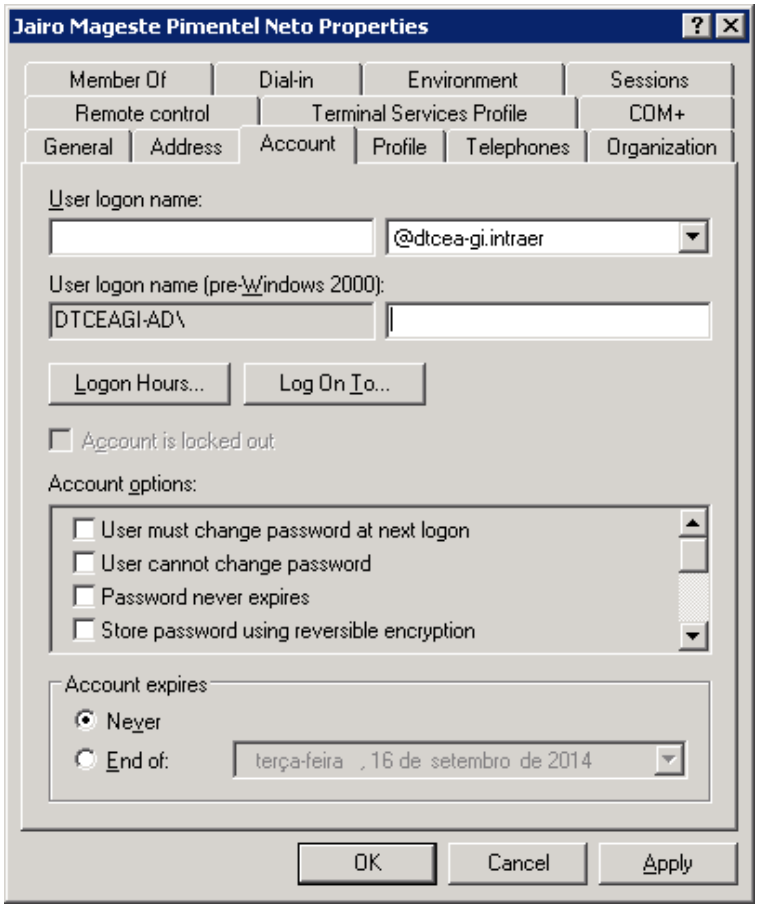


Figura 17 - Active Directory - Propriedades do Usuário

Na janela de propriedades do usuário, há a configuração de três requisitos da política de segurança: horário de utilização, definido em *Logon Hours...*, Computadores permitidos, definido em *Logon on to...* e Validade do Cadastro, definido em *Account expires*.

2.6. Cenário para teste e validação:

Durante a configuração do *Active Directory*, é necessário verificar se as regras que estão sendo implementadas no domínio estão sendo propagadas para seus objetos, principalmente computadores e usuários, e se a regra realmente possui o resultado desejado.

Para isto, faz-se necessário ter ativos a disposição da subseção de Tecnologia da Informação, como computadores, a fim de realizar os testes em sistemas operacionais Microsoft *Windows* XP. Porém não há disponibilidade de computadores no DTCEA-GI, muito pelo contrário, há demanda por computadores.

Visando minimizar os impactos durante os testes do AD, os testes em Windows XP foram realizados sobre maquinas virtuais no VirtualBox, uma vez que a licença do Windows XP permite a instalação em qualquer computador.

O VirtualBox é um Hypervisor, uma ferramenta da Oracle para gerenciamento de Maquinas Virtuais (Monitor de Máquina Virtual) sobre um sistema operacional hospedeiro. Na Figura 18 vemos sua janela principal.

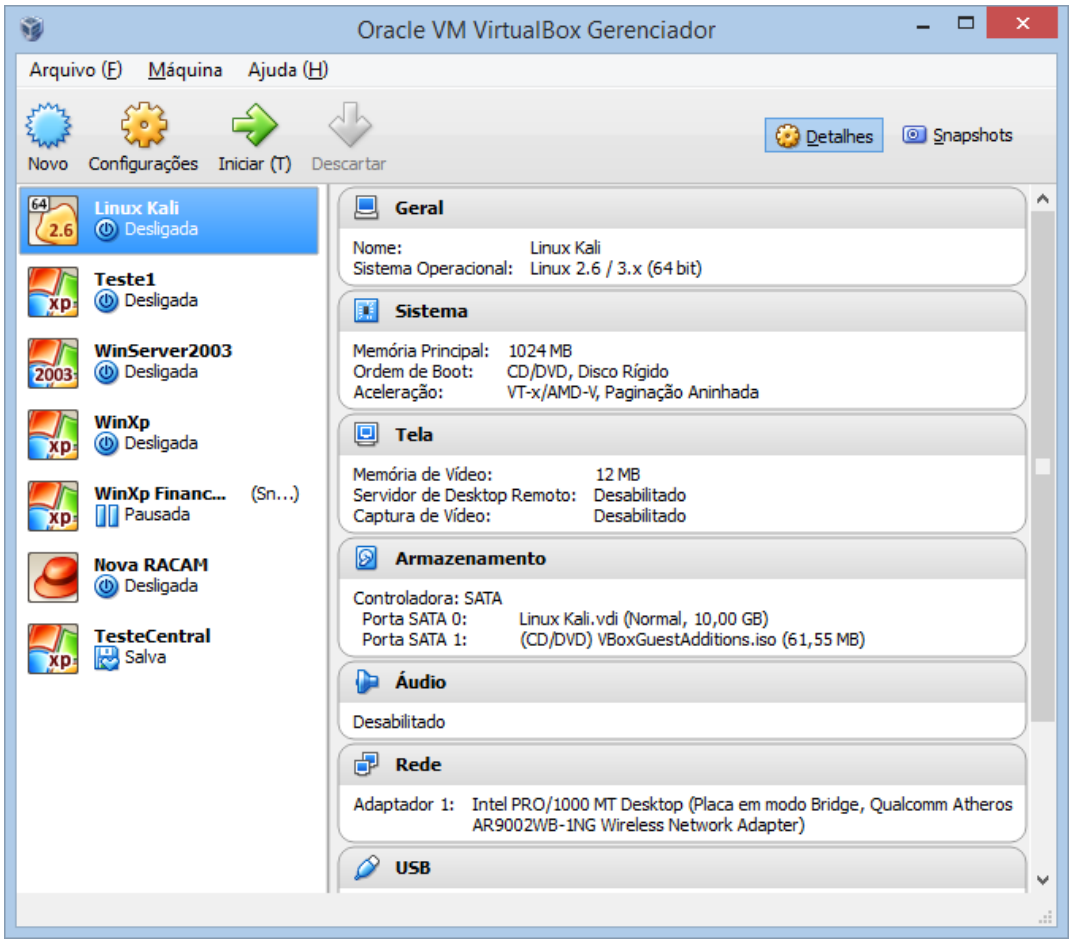


Figura 18 – VirtualBox Tela principal

Outra vantagem do VirtualBox, é a criação de *snapshot*, como na Figura 19, que cria um backup da instancia daquele momento da máquina virtual, que permite no futuro, caso seja necessário, retornar o sistema para sua exata configuração no momento do snapshot.

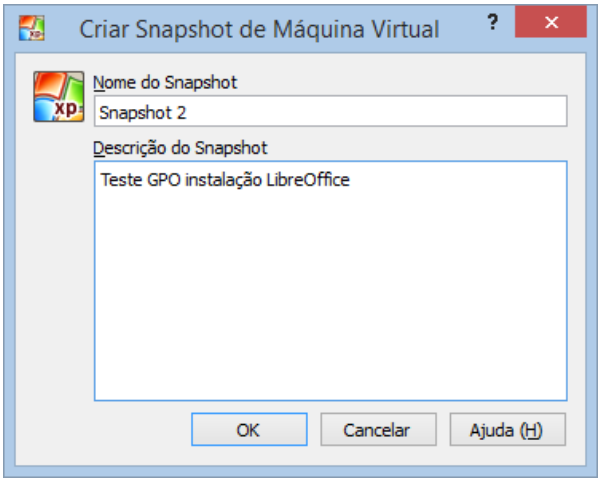


Figura 19 – VirtualBox Criando Snapshot

Esta funcionalidade é muito útil quando para fazer teste que implicam em grandes alterações do sistema operacional, como alterações em registros, instalações de atualizações críticas, instalações de aplicativos para testes, entre outras modificações.

2.7. Migração

Para a migração entre os dois servidores foi definido a criação de um novo domínio, permitindo sua configuração e teste sem comprometer o funcionamento do domínio antigo. A migração foi dividida em passos de forma a controlar melhor o processo e não comprometer o funcionamento da rede e computadores do DTCEA-GI

- Instalação do Windows Server 2003 R2;
- Configuração do DNS;
- Configuração do Active Directory;
- Criar Unidades Organizacionais
- Criar Grupos de Usuários;
- Cadastrar Usuários de Teste;
- Preparar cenário de Teste;
- Configurações de GPOs de Políticas de Segurança;
- Testes de GPOs;
- Instalação do WSUS no Windows Server 2003;
- Configuração de GPOs para atualização com o WSUS;
- Teste do WSUS;
- Criar Pastas Compartilhada e definir suas permissões;

- Cadastro de Usuários mediante a termos de responsabilidade;
- *BackUp* dos dados do servidor Windows Server 2000;
- Copiar dos Dados para o servidor Windows Server 2003;
- Formatar e ingressar Computadores no novo Domínio;
- Configuração do DHCP;
- Desligar servidor *Windows Server* 2000.

A configuração do DNS foi feita seguindo tutorial do CCA-BR, Anexo B, com apoio do CINDACTA-I.

3. RESULTADOS

3.1. Levantamento de Requisitos

O resultado da análise de políticas de segurança é o levantamento de requisitos de segurança para os meios computacionais do DTCEA-GI, Anexo C.

Este documento orientou de forma clara a criação as regras para a configuração do *Active Directory*, mostrando de forma objetiva quais as políticas implantar.

Com base nos Requisitos Funcionais e Requisitos Não Funcionais pode-se ser objetivo nas definições das diretrizes de cada GPO, critérios para cadastro de usuário, relacionamentos entre unidades organizacionais, grupos, usuários, computadores e GPOs.

Foram levantados quatorze requisitos, sendo doze funcionais e dois não funcionais. Eles buscam melhorar a segurança na utilização dos recursos de tecnologia da Informação e facilitar a administração de toda a rede.

3.2. Configuração do Active Directory

Para atender o Levantamento de Requisitos deve-se configurar o *Active Diretory*, sendo a ferramenta *Active Directory Users and Computers* responsável por grande parte destas configurações. A Figura 20 mostra a tela do *Active Directory Users and Computers*, À direita está a arvore do domínio com suas unidades organizacionais, e à esquerda seu Conteúdo, Unidade Organizacionais, Grupos, Computadores, Pastas Compartilhadas e Usuários.

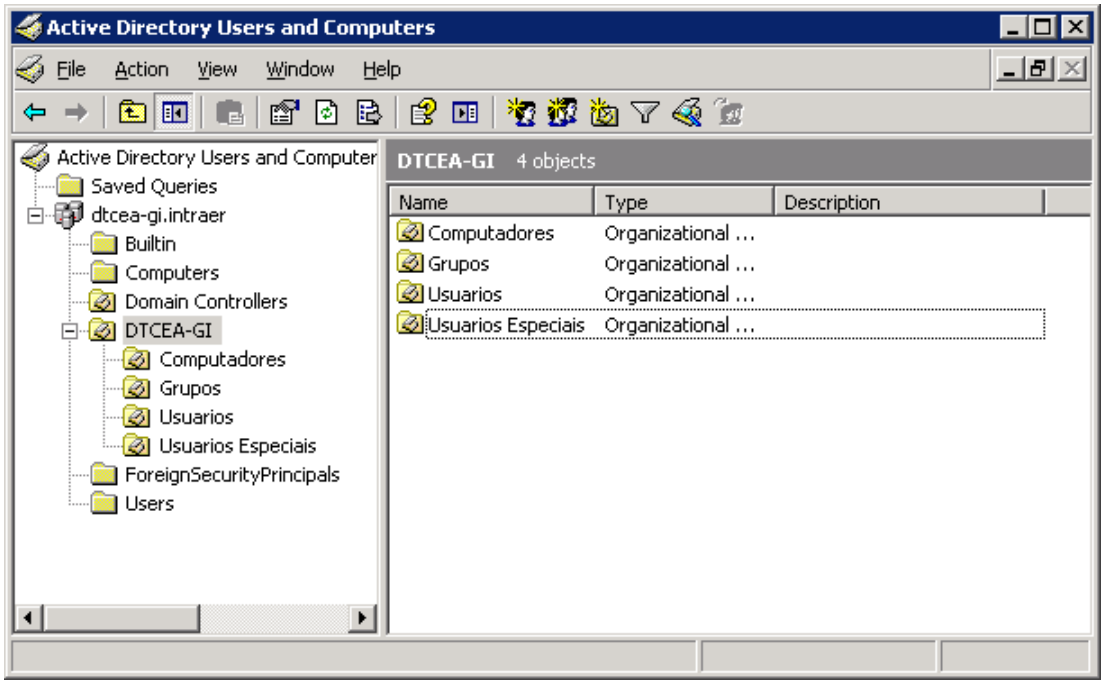


Figura 20 - Active Directory Visão geral

Primeiro passo após inicializar o AD é configurar as Unidades Organizacionais, pois, as GPOs são aplicadas a elas. Neste caso, a fim de fazer uma separação lógica por tipos de objetos, foi criado as seguintes unidades organizacionais: Computadores, Grupos, Usuários e Usuários Especiais, este último para receber Usuários com privilégios diferenciados, como administradores. Visto na Figura 20. A unidade organizacional Computadores, possui duas unidades, Teste e Operacional, para a separação de grupos no WSUS.

Em sequência, criar os Grupos. A Figura 21 mostra a configuração dos grupos no DTCEA-GI.

Os Grupos são divididos em três categorias, um grupo que separa os usuários por sua hierarquia no meio militar (H_Grupo), quanto ao local de trabalho, seção e/ou subseção (S_Grupo) e por fim quanto a alguma funcionalidade especifica (F_Grupo), como grupo que possui acesso à internet e administradores do DTCEA-GI.

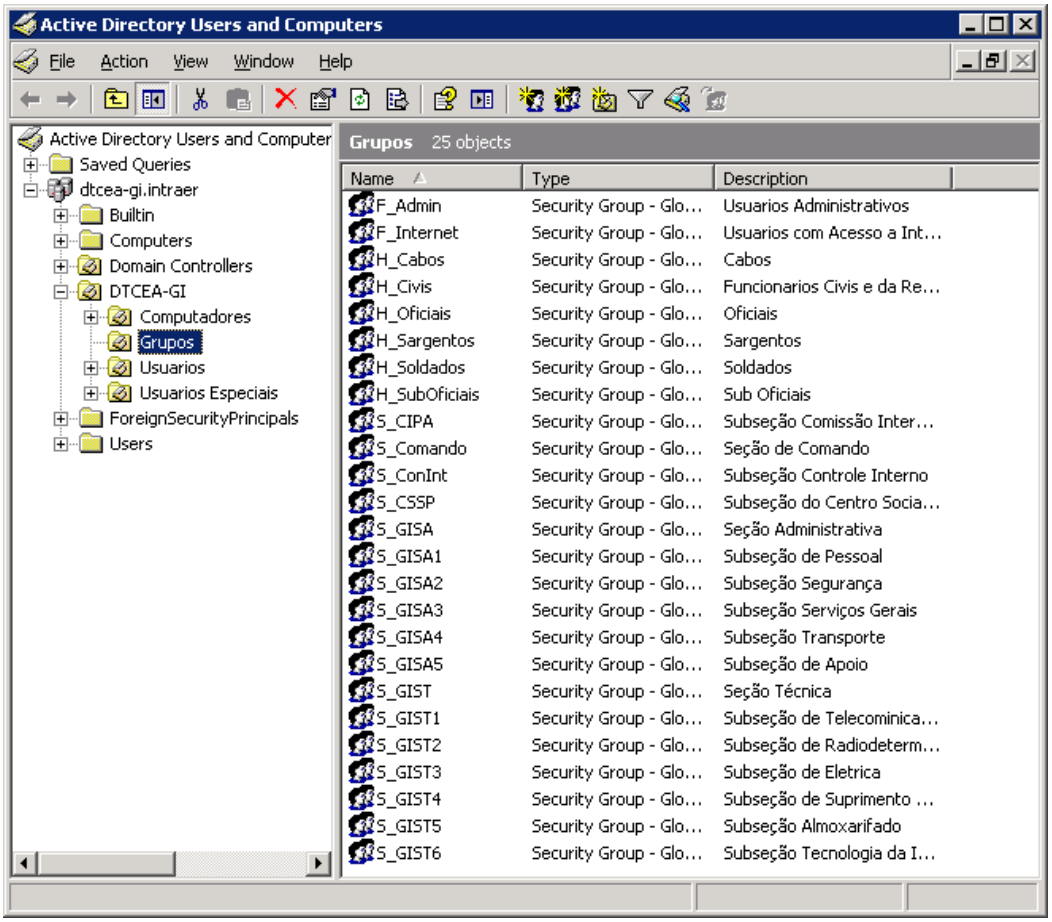


Figura 21 - Active Directory unidade organizacional de Grupos

A principal função dos grupos de setoriais e hierárquicos é definir as promissões de acesso no Servidor de Dados.

Após a criação dos grupos, criar os usuários para realizar os testes das GPOs. A exceção são os usuários administrativos, que foram criados imediatamente após a configuração do AD, atendendo as técnicas de boas práticas que não recomenda o uso da conta de administrador.

Basicamente há dois cenários de testes, o primeiro de regras que se aplicam a todos os usuários, como políticas de senhas, e o segundo, regra e acesso à internet. Para atender a estes dois cenários, foram criados dois usuários:

- Usuario1: Não possui grupo funcional;
- Usuario2: Possui acesso à internet.

Para os testes que se aplicam a todos os usuários comuns, utiliza-se alternadamente os dois usuários, e o de acesso à internet, compara-se os dois usuários.

Como mencionado no item 2.6, é criado o cenário de validação com o VirtualBox e Microsoft *Windows* XP.

3.2.1. Configurar GPOs

Com os computadores e usuários de testes, configurasse as GPOs e as testas. A configuração das GPOs, busca atender a análise de requisitos. Como boa pratica, buscasse não utilizar as GPOs *Defaut Domain Policy* e *Defaut Domain Controller Policy*, apenas atualizando itens definidos nestas políticas quando necessário. Nos demais casos, criasse uma GPO para cada requisito.

Dos Requisitos Funcionais atendidos por GPO temos:

- **Senha Forte** (GPO: *Defaut Domain Policy*)

  Este requisito já é configurado automaticamente no Domínio, com os seguintes valores:
  - *Computer Configuration*
    - *Windows Settings*
      - *Account Policies*
        - *Password Policy*
          - ***Minimum password length:*** *7 Character*
          - ***Password must meet complexity requirement:*** *Enabled*
- **Bloqueio da Estação** (GPO: UserBloqueioEstação)

  Esta GPO possui os seguintes valores:
  - *User Configuration:*
    - *Administrative Templates:*
      - *Control Panel:*
        - *Display:*
          - ***Password protect the screen saver:*** *Enabled*
          - ***Screen Saver:*** *Enabled*
          - ***Screen Saver executable name:*** *None*
          - ***Screen Saver timeout:*** 300(segundos)
- **Renovar Senha** (GPO: CompSenhaAtualizar)

  Esta GPO possui os seguintes valores:
  - *Computer Configuration*
    - *Windows Settings*
      - *Security Settings*
        - *Account Policies*
          - *Password Policy*
            - ***Maximum Password Age*****:** 90 *days*
            - ***Minimum Password Age*****:**

1 *day*

- **Bloqueio de Senha** (GPO: CompSenhaAtualizar)

  Esta GPO possui os seguintes valores:
  - *Computer Configuration*
    - *Windows Settings*
      - *Security Settings*
        - *Account Policies*
          - *Account Lockout Policy*
            - ***Account lockout duration:*** 30 *minutes*
            - ***Account lockout threshold:*** 5 *invalid logon attempts*
            - ***Reset lockout counter after:*** 30 *minutes*
- **Restrição de Mídias** (GPO: CompMidias)

  Este requisito não possui uma política nativa do AD, sendo configurada alterando uma chave do registro, para alterar esta chave por GPO é necessário adicionar um arquivo ".adm" que informa os parâmetros desta chave a ser alterada. Este arquivo está no Anexo D. A chave modificada é
  [*HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\usbstore*]
  "Start"=dword:00000004
  O arquivo usb.adm deve ser adicionado ao *Administrative Templates*, adicionando a nova política.
  - *Computer Configuration*
    - *Administrative Templates*
      - USB *Management*
        - **USB *Storage Service***: *StartUp Type: Disabled*
- **Configuração de Uso da Internet** (GPO: UserProxy)

  Esta GPO possui os seguintes valores:
  - User configuration
    - Windows Settings
      - Internet Explorer Maintenance
        - Connection
          - **Proxy Settings**: Valores Reservados
- **Restrição de Uso da Internet** (GPO: UserProxyBloqueio)

  Esta GPO possui os seguintes valores:
  - *User Configuration*
    - *Administrative Templates*
      - *Windows Components*
        - *Internet Explorer*
          - *Internet Control Panel*
            - ***Disable the Connections page:*** *Enabled*
- **Restrição de Configurações** (GPO: UserControlPanelBloqueio)

Esta GPO possui os seguintes valores:

- *User Configuration*
  - *Administrative Templates*
    - *Control Panel*
      - ***Prohibit access to the Control Panel***
        Enabled

Dos Requisitos Não Funcionais atendidos por GPO temos:

- **Papel de Parede** (GPO: UserPapeldeParede)

  Esta GPO possui os seguintes valores:

  - *User Configuration*
    - *Administrative Templates*
      - *Desktop*
        - *Active Desktop*
          - *Active Desktop Wallpaper*
            Enabled
            //servidor/compartilhada/papel.jpg
            Center

3.2.2. Configurar GPOs WSUS

Para os computadores utilizarem o WSUS, também são necessárias GPOs com as políticas informando como irão realizar as atualizações e que grupo do WSUS pertencem.

- **Configurações Gerais WSUS** (GPO: CompWSUS)

  Esta GPO possui os seguintes valores:

  - *Computer Configuration*
    - *Administrative Templates*
      - *Windows Components*
        - *Windows Update*
          - ***Configure Automatic Update:***
            Enabled
            4 (*Auto download and schedule...*)
            0 (*Every day*)
            11:00
          - ***Specify intranet* Microsoft *update server location:***
            Enabled
            http://servidor
            http://servidor
          - ***Enable cliente-side targeting:***
            disabled
          - ***Reshedule Automatic Updates scheduled installations:***
            Enabled
            1 (minuto)

- ***No auto-restart with logged on users for scheduled automatic update installations:***
  Enabled
- ***Automatic Updates detection frequency Properties:***
  Enabled
  15 (horas)
- ***Allow Automatic Updates immediate installation Properties:***
  Enabled
- ***Delay Restart for scheduled installations Properties:***
  Disabled
- ***Re-prompt for restart with scheduled installations Properties:***
  Enabled
  30 (minutos)
- ***Enable recommended updates via Automatic Updates Properties:***
  Enabled

- **Grupo Operacional** (GPO: CompWSUSGrupoOperacional)

  Esta GPO possui os seguintes valores:
  - *Computer Configuration*
    - *Administrative Templates*
      - *Windows Components*
        - *Windows Update*
          - ***Enable cliente-side targeting:***

            Enabled
            Operacional
- **Grupo Teste** (GPO: CompWSUSGrupoOperacional)

  Esta GPO possui os seguintes valores:
  - *Computer Configuration*
    - *Administrative Templates*
      - *Windows Components*
        - *Windows Update*
          - ***Enable cliente-side targeting:***

            Enabled
            Teste

3.2.3. Relacionar GPOs a Unidades Organizacionais

Após configurar cada GPO, deve-se atribuí-las as unidades organizacionais que possuem os objetos controlados por esta política. A Figura 22 mostra a configuração das unidades organizacionais e suas GPOs.

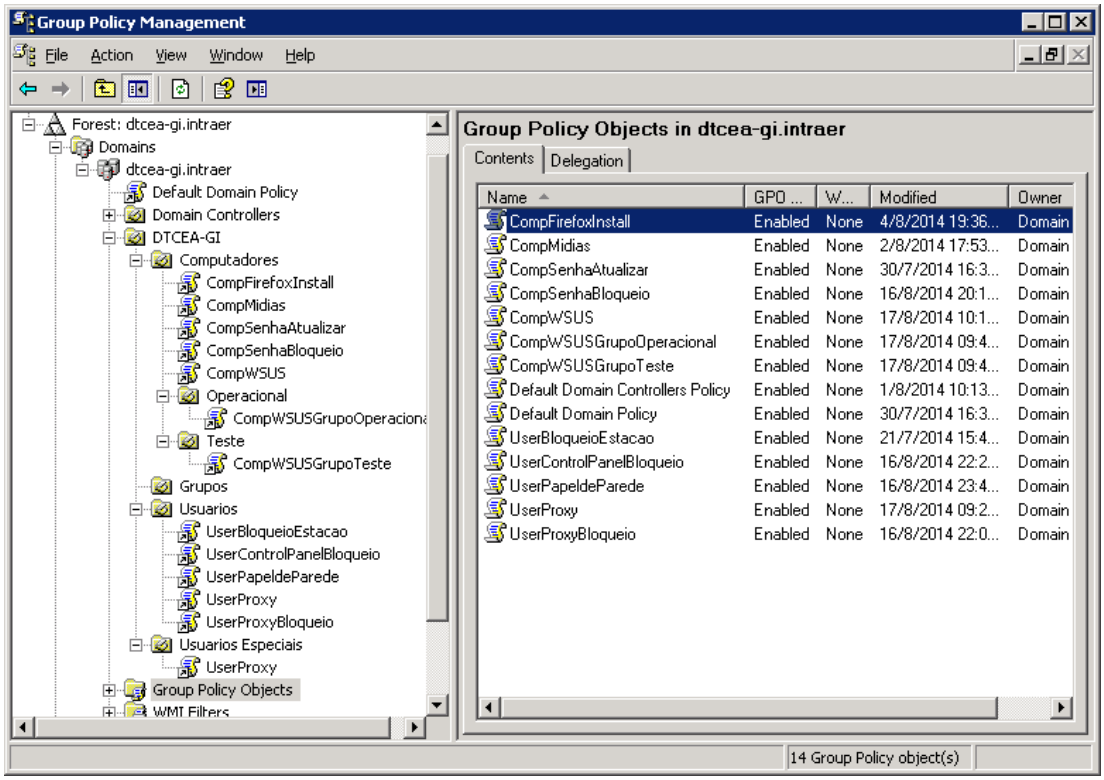


Figura 22 - Group Poliy Management mostra as Unidades Organizacionais e sua GPOs

3.2.4. Servidor de Dados

Dentre os requisitos definidos, está a Integridade e Confidencialidade dos Dados, para isto, deve-se utilizar um servidor de dados. Para a configuração básica de um servidor de dados, devemos criar no Gerenciador de Documentos *Windows Explorer* as pastas, a Figura 23 mostra o Gerenciador de Documentos e suas pastas.

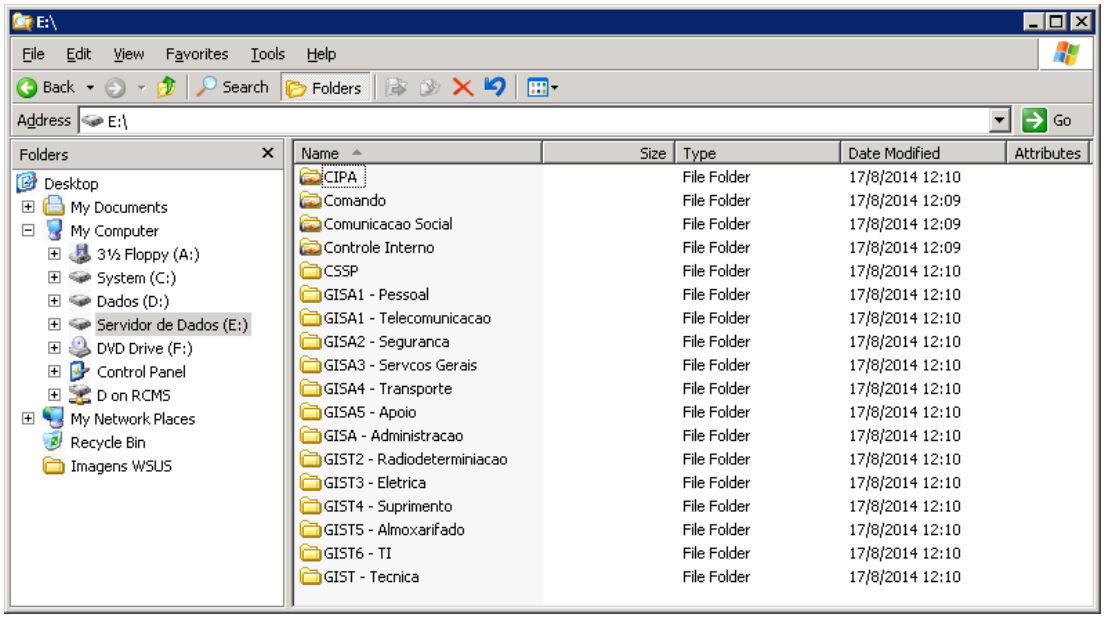


Figura 23 - Windows Explorer Gerenciador de Documentos - Pastas compartilhadas

Em seguida, configurar seu compartilhamento, nas propriedades da pasta, conforme mostra a Figura 24.

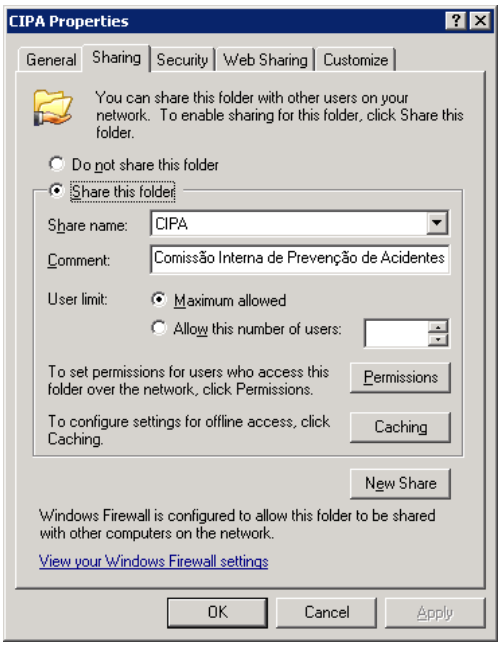


Figura 24 - Windows Explorer Propriedades de pasta - Aba de compartilhamento

Por último, deve-se definir os grupos ou usuários que possuem acesso à pasta, e qual o tipo de acesso. A Figura 25 mostra os grupos ou usuários relacionados à pasta, e as permissões do objeto selecionado.

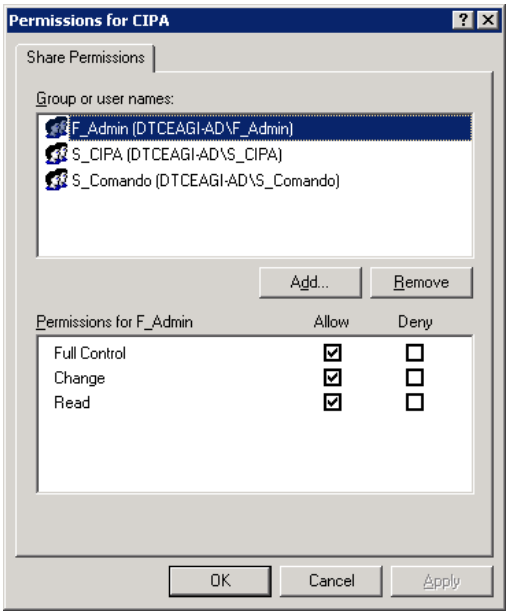


Figura 25 - Windows Explorer Permissões de Compartilhamento

Assim, somente terão acesso à determinada pasta o usuário que estiver em um dos grupos com permissão, como o nível de permissão estabelecido. Garantindo que somente tenha acesso aos dados o usuário devidamente autorizado.

3.3. *Testes de GPOs e Atualização por WSUS*

Os resultados dos testes de GPOs realizados no Microsoft *Windows* XP como sistema operacional convidado no VirtualBox, apresentou bons resultados, verificando que as GPOs foram replicadas com sucesso, e funcionaram corretamente.

Foram verificadas de duas formas, através do terminal de comando do *Windows*, através do comando GPRESULT, que lista as informações de GPOs do computador e usuário logado, a segunda, através de testes práticos com o sistema operacional.

A Figura 26 e a Figura 27 mostram o resultado do comando GPRESULT para dois usuários distintos em um mesmo computador.

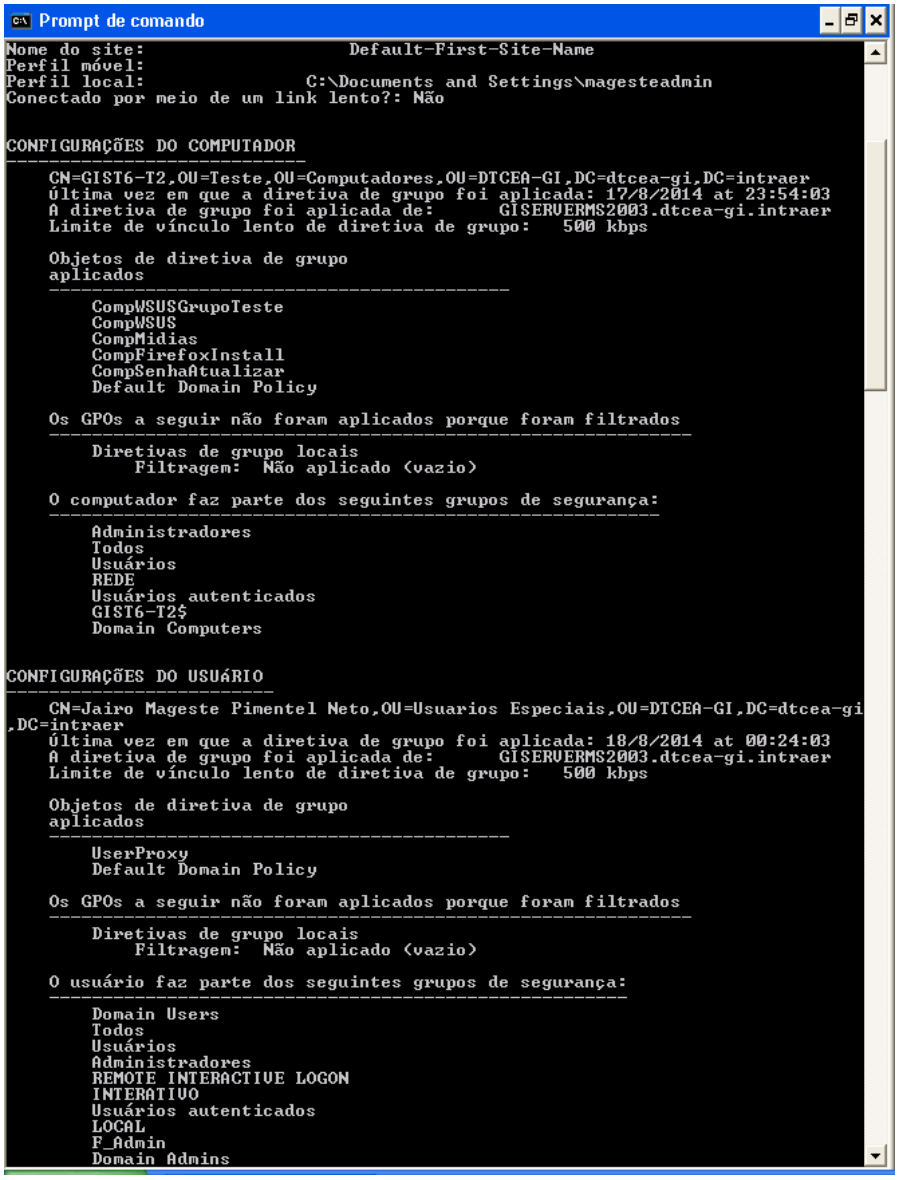


Figura 26 - Teste de GPOs - gpresult de um usuário

Com este comando é possível analisar as GPOs aplicadas, tanto das configurações do computador, como as configurações de usuário. Informa ainda GPOs atribuídas e não aplicadas, especificando o motivo, por exemplo, GPO vazia no escopo de computador ou usuário.

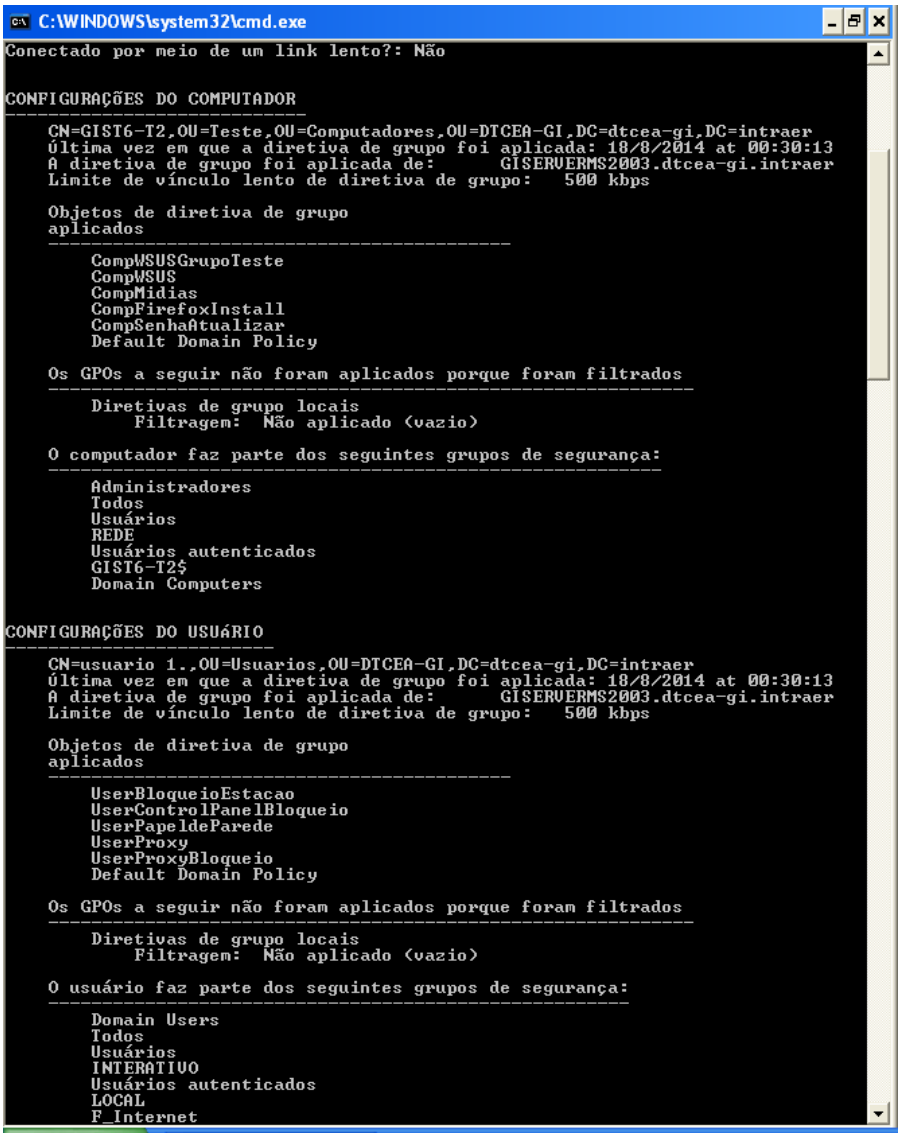


Figura 27 – Teste de GPOs - gpresult de um usuário de Teste

Facilita a análise das GPOs no cliente antes de verificar por testes práticos, pois, as GPOs só terão resultado caso estejam relacionadas no GPRESULT.

O GPRESULT ainda informa os grupos de segurança a qual o computador e usuário participam.

Após confirmada a replicação da GPO pelo terminal de comandos, verifica-se o funcionamento real da GPO. Utilizando o cenário de teste, logando com o usuário de teste no Windows XP no VirtualBox.

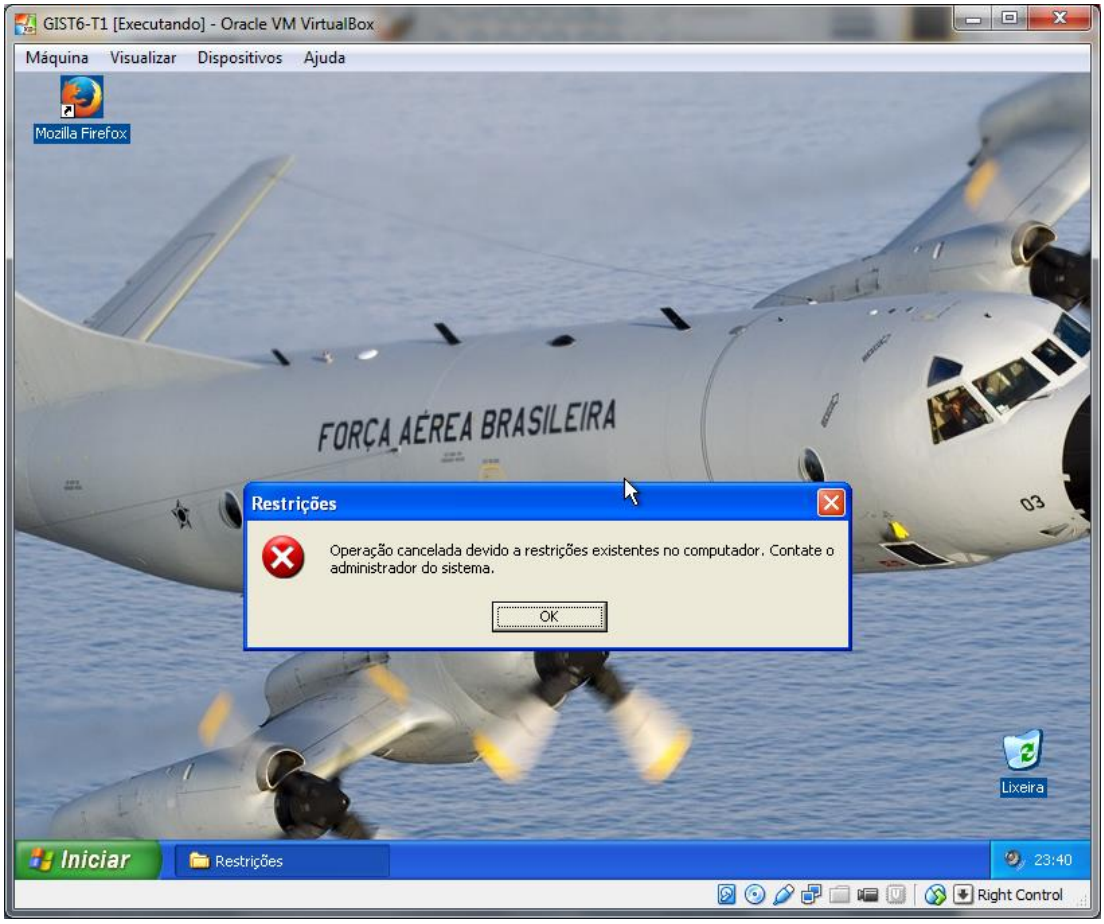


Figura 28 - Teste de GPO - Bloqueio de configurações e Papel de Parede

Na Figura 28 mostra a aplicação de duas GPOs, a UserControlPanelBloqueio que bloqueia o acesso do usuário a itens de configuração do sistema, confirmado a aplicação da GPO pela caixa de diálogo de restrição exibida. A segunda é a UserPapeldeParede, que define o Papel de Parede da Área de Trabalho do usuário.

Outra GPO importante para a segurança, é a UserBloqueioEstacao, Figura 29, exigindo que o usuário digite novamente sua senha, após cinco minutos de inatividade do computador.

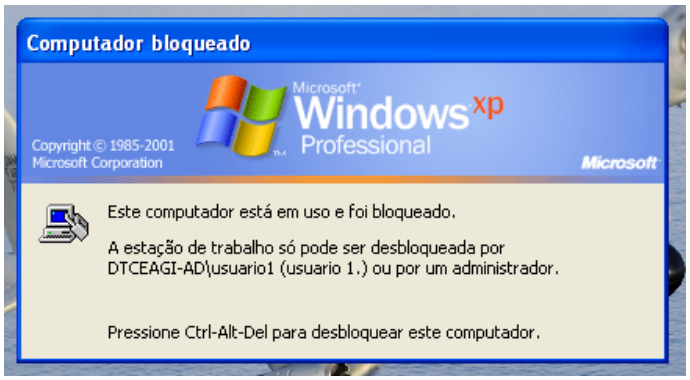


Figura 29 - Teste de GPO - Bloqueio da estação

Observa-se que a GPO de configuração do WSUS consta no gpresult, Figura 26, em seguida verifica-se as configurações de atualização do *Windows* correspondem as configuradas na GPO CompWSUS. A Figura 30 mostra a janela de Atualizações Automáticas do cliente, que foi configurada de acordo com a GPO, e não é possível editar.

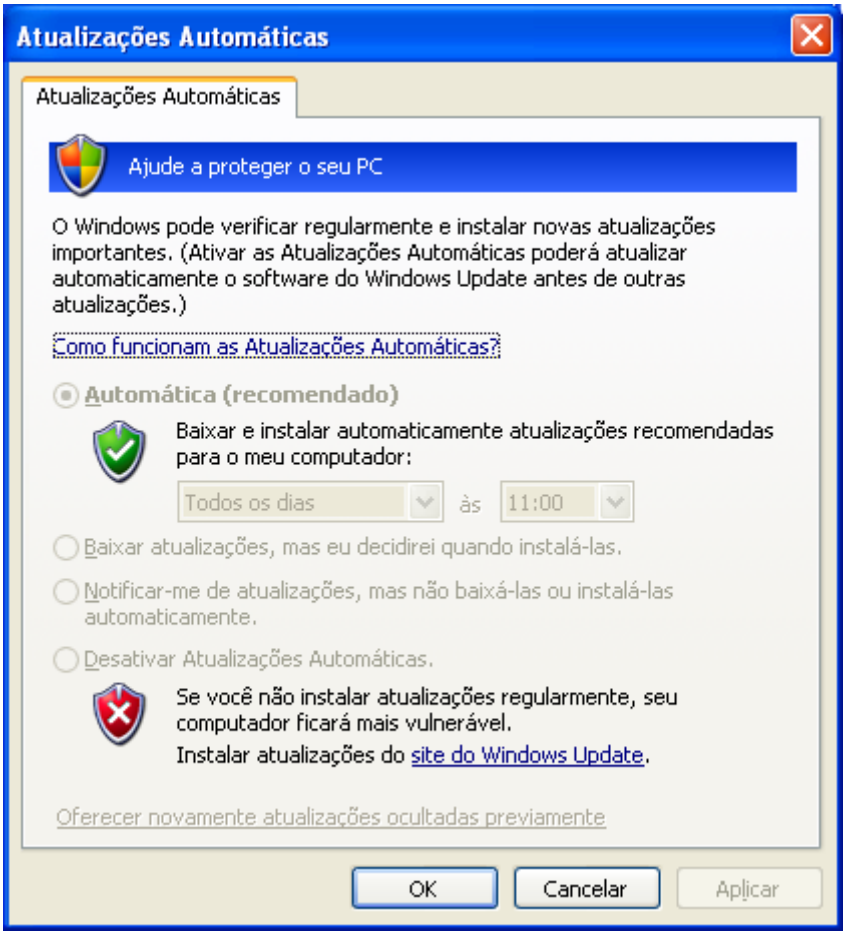


Figura 30 - WSUS - Configuração automática do Cliente

Para verificar o funcionamento do WSUS, autorizado apenas uma atualização para o computador de teste, após aprovada, o download para repositório do WSUS acontece quando é feita sua sincronização com o Windows Update. Em seguida, em momento propicio, o Computador realizara o download, e apenas realizara a instalação no horário agendado pela GPO. Estes passos foram verificados com sucesso.

Em seguida realiza-se a autorização de todas as atualizações necessárias do computador. A Figura 31 mostra o relatório gerado pelo WSUS referente a um dos sistemas operacionais de teste, informando não haver atualizações pendentes, e das

atualizações sincronizadas, 5330 atualizações estão instaladas ou não se aplicam a este computador.

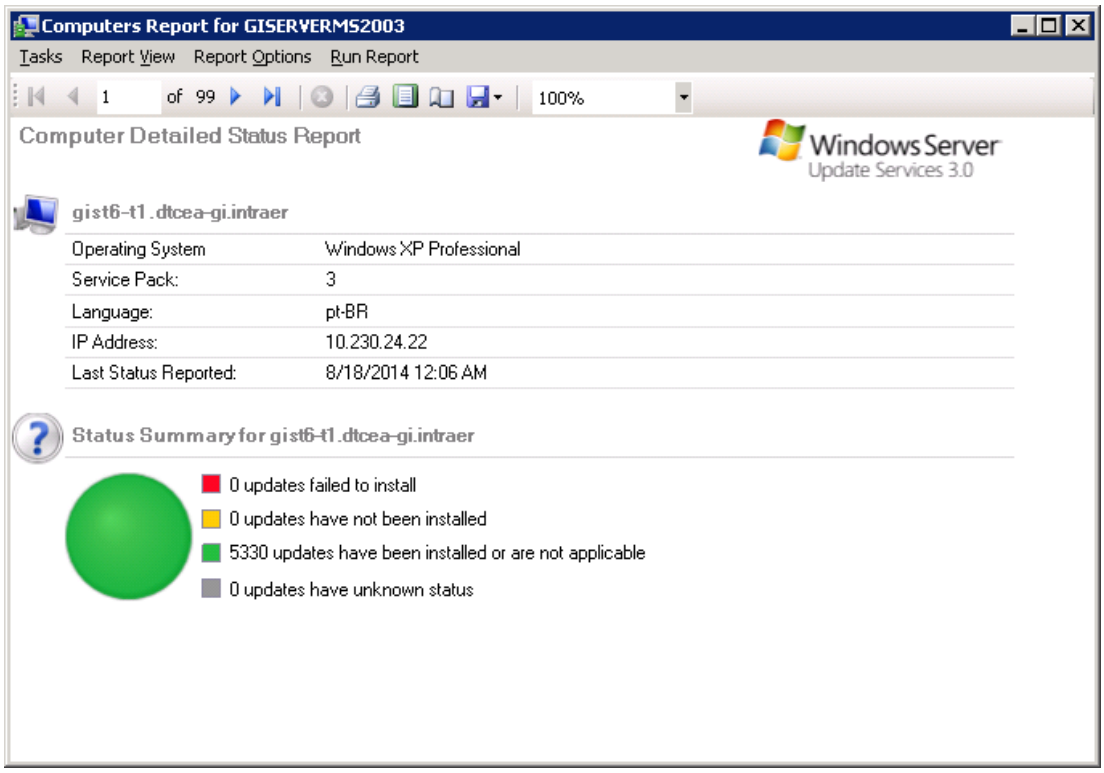


Figura 31 - WSUS - Relatório de Computador Atualizado

Em alguns casos, pode ser necessário reiniciar o computador para que determinada atualização seja instalada. Neste caso é necessária a intervenção do usuário. A Figura 32 mostra esta solicitação. No caso do DTCEA-GI, optou-se por não reiniciar o computador automaticamente.

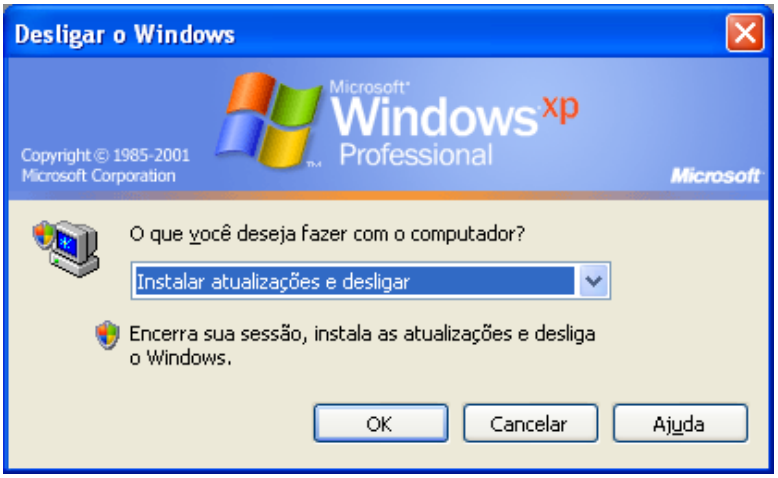


Figura 32 - WSUS - Solicitação de instalação com desligamento do Windows XP

Os resultados de todos os testes foram satisfatórios. Mostraram que as GPOs funcionaram, assim como o WSUS com seu repositório.

4. DIFICULDADES ENCONTRADAS

SUPORTE TÉCNICO: Devido à falta de mão de obra qualificada, uma vez que esta é selecionada por recrutamento de jovens de 18 anos residentes na cidade de Chapada dos Guimarães-MT, a subseção de Tecnologia da Informação possui um contingente muito limitado para realizar as melhorias da rede e manter seu funcionamento durante o processo, recaindo a tarefa de suporte técnico ao Soldado subordinado a esta subseção. Como agravante este soldado concorre à escala de serviço de guarda de 24h, ficando indisponível cerca de 40% de seu tempo de trabalho.

Há uma perspectiva de melhora da qualidade técnica dos soldados recrutados, uma vez que a Escola Estadual Coronel Rafael de Siqueira, Unidade de Ensino da cidade de Chapada dos Guimarães, passou a oferecer o curso de Técnico em Informática para seus alunos. O oferecimento deste curso possibilita que a Força Aérea Brasileira, no momento de seleção de recrutas, tenha a opção de selecionar jovens formados ou em formação no referido curso.

USO DE SOFTWARES DEFASADOS: o sistema operacional da maioria dos computadores deste Destacamento é o *Windows* Xp *Professional*, que teve o fim do suporte em 08 de abril de 2014 (Microsoft *Corporation*, 2014)

O *Windows Server* 2003 ainda possui suporte da Microsoft, suporte estendido, mas este tem data prevista para acabar em 14 de julho de 2015 (Microsoft *Corporation*, 2014).

FALTA DE CULTURA DE SEGURANÇA DIGITAL: é comum observar usuários compartilhando senhas, até mesmo contas de usuários que não trabalham no DTCEA-GI. Utilização de senhas curtas, senhas repetidas e de baixa complexidade.

5. CONCLUSÕES

Verificou-se que o Servidor Dell PowerEdge 2950 atende aos requisitos do *Windows Server* 2003, por consequência ao *Active Directory* e ao WSUS instalado separadamente. Ainda possui recurso para outros serviços.

Realizado o Levantamento de requisitos referente às políticas de segurança, baseado em entrevistas não estruturadas, observações de usuários e regulamentos do Comando da Aeronáutica.

Implementado o controlador de Domínio, sendo suas GPOs dirigidas pela análise de requisitos. Tornando mais objetiva as configurações, agilizando o processo e o documentando. Assim como o WSUS, para gerenciar as atualizações automáticas da Microsoft.

Validou-se todas as configurações propostas, mostrando um ganho de tempo e de recursos, principalmente segurança da rede. Observou-se ainda que o WSUS é uma ferramenta de grande importância, pois reduz de forma considerável a utilização da internet, uma vez que baixa somente uma vez o pacote de atualização para o repositório WSUS. Representa também um ganho de tempo para os administradores na hora de formatar computadores da rede, pois fará o download direto do servidor.

Ampliar o escopo da política de segurança que foi voltada para imposições ao usuário final e para medidas de orientação e educação.

Políticas para melhorar a qualificação e controle dos profissionais que atuam na área de Tecnologia da informação, principalmente por eles não serem originalmente desta área.

6. REFERÊNCIAS BIBLIOGRÁFICAS

Comando da Aeronáutica. (20 de Junho de 2014). *Centro de Documentação da Aeronáutica*. Fonte: Cendoc: https://www.cendoc.aer.mil.br/

Copyright 'winDeploy. (07 de Agosto de 2014). *Disabling USB storage devices using Group Policy*. Fonte: winDeploy: http://www.windeploy.co.uk/blog/index.php/2009/09/disabling-usb-storage-devices-using-group-policy/

Dell. (10 de Agosto de 2014). *Dell PowerEdge 2950 III*. Fonte: Dell: http://www1.la.dell.com/br/pt/gen/Empresa/pedge_2950_3/pd.aspx?refid=pedge_2950_3&s=gen

Maziero, C. A. (2013). *Sistemas Operacionais: Conceitos e Mecanismos.* Curitiba. Fonte: http://dainf.ct.utfpr.edu.br/~maziero/lib/exe/fetch.php/so:so-livro.pdf

Microsoft Corporation. (10 de Agosto de 2014). *Ciclo de Vida de Suporte da Microsoft ao Windows XP Professional*. Fonte: Ciclo de Vida de Suporte da Microsoft: http://support.microsoft.com/lifecycle/?p1=3223

Microsoft Corporation. (18 de 08 de 2014). *Ciclo de Vida Windows Server 2003 R2*. Fonte: Microsoft Life Cycle: http://support.microsoft.com/lifecycle/?p1=10394

Microsoft Corporation. (27 de Agosto de 2014). *Fim de Suporte para WIndows Server 2000*. Fonte: Microsoft Connections: http://www.microsoft.com/brasil/connections/pecas/comunicado_fim_suporte/2/index2.html

Microsoft Corporation. (12 de Agosto de 2014). *Função do servidor de arquivos*. Fonte: TechNet Microsoft: http://technet.microsoft.com/pt-br/library/cc780253(v=ws.10).aspx#BKMK_Config

Microsoft Corporation. (12 de Agosto de 2014). *Função do servidor DHCP*. Fonte: TechNet Microsoft: http://technet.microsoft.com/pt-br/library/cc756865(v=ws.10).aspx

Microsoft Corporation. (12 de Agosto de 2014). *Função do servidor DNS*. Fonte: TechNet Microsoft: http://technet.microsoft.com/pt-br/library/cc738344(v=ws.10).aspx

Microsoft Corporation. (05 de Agosto de 2014). *GPResult*. Fonte: TechNet Microsoft: http://technet.microsoft.com/pt-br/library/cc733160(v=ws.10).aspx

Microsoft Corporation. (12 de Agosto de 2014). *Introdução ao Active Directory - Parte 1*. Fonte: Technet Microsoft: http://technet.microsoft.com/pt-br/library/cc668412.aspx

Microsoft Corporation. (25 de Julho de 2014). *Pagina Inicial WSUS*. Fonte: TechNet Microsoft: http://technet.microsoft.com/pt-br/windowsserver/bb332157.aspx

Microsoft Corporation. (20 de Agosto de 2014). *Unidades organizacionais*. Fonte: Microsoft TechNet: http://technet.microsoft.com/pt-br/library/cc758565(v=ws.10).aspx

Microsoft Corporation. (10 de Agosto de 2014). *Windows Server 2003 Informações do Produto*. Fonte: Microsoft Windows Server 2003:

https://www.microsoft.com/brasil/servidores/windowsserver2003/evaluation/default.mspx

Oracle. (10 de Agosto de 2014). *VirtualBox Documentation*. Fonte: VirtualBox: https://www.virtualbox.org/wiki/Documentation

Tanenbaum, A. S. (1999). *Sistemas Operacionais.* Porto Alegre: Bookman.

Taylor, A. (2009). *Windows Server Update Services 3.0 SP2 Deployment Guide.* Microsoft Corporation.

Taylor, A. (2009). *Windows Server Update Services 3.0 SP2 Operations Guide.* Microsoft Corporation.

Wikipédia. (14 de Agosto de 2014). *Raid*. Fonte: Wikipédia: http://pt.wikipedia.org/wiki/RAID

ANEXOS

Anexo A – Anexo E da ICA 7-19/2012

Anexo E - Norma de Controle de Acesso Lógico das Redes de Telecomunicações

SUMÁRIO

1 OBJETIVO
2 APLICAÇÃO
3 DEFINIÇÕES
4 RESPONSABILIDADES
5 CONSIDERAÇÕES DE SEGURANÇA DA INFORMAÇÃO EM REDES DE TELECOMUNICAÇÕES
6 DIRETRIZES PARA IMPLANTAÇÃO DAS REDES DE TELECOMUNICAÇÕES
7 DESCRIÇÃO DA NORMA DE SEGURANÇA DA INFORMAÇÃO
8 REGISTROS GERADOS
9 PONTOS DE VERIFICAÇÃO
10 FLUXOGRAMA
11 DOCUMENTOS DE REFERÊNCIA
12 ANEXOS

1 OBJETIVO

Estabelecer diretrizes para implementação de controles de acesso lógico para as redes de telecomunicações gerenciadas pelo DECEA em conformidade com a ROCA 20-7 "Regulamento do Departamento de Controle do Espaço Aéreo".

2 APLICAÇÃO

Esta Norma de Segurança da Informação é de aplicação no Departamento de Controle do Espaço Aéreo e suas Organizações Militares subordinadas.

3 DEFINIÇÕES

Os conceitos e definições estão listados na MCA 7-1 "Glossário de Segurança da Informação do DECEA".

Para efeito desta Norma de Segurança da Informação, entende-se por:

3.1 CONTROLE DE ACESSO LÓGICO

Conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso às informações.

3.2 REDE DE TELECOMUNICAÇÕES

Uma rede de telecomunicações pode ser composta de várias sub-redes, dependendo do tipo de serviço que é provido ao usuário final. As redes de telecomunicações estão sendo aperfeiçoadas para suportar a transmissão de informações com a introdução de novas tecnologias, tanto do lado dos equipamentos da rede (elementos de rede) quanto dos meios de transmissão (redes de transporte) e dos sistemas de operação para gerenciamento de Redes de Telecomunicações.

3.3 USUÁRIO

Servidor militar ou civil, prestador de serviço ou fornecedor do DECEA e das suas Organizações Militares subordinadas que obteve autorização do responsável pela área interessada para acesso aos ativos de Informação, formalizada por meio da assinatura do Termo de Responsabilidade.

3.4 QUEBRA DE SEGURANÇA DA INFORMAÇÃO

Ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação.

3.5 TERMO DE RESPONSABILIDADE

Termo assinado pelo usuário concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e autenticidade e a legalidade das informações que tiver acesso, bem como assumir responsabilidades decorrentes de tal acesso.

4 RESPONSABILIDADES

4.1 ASSICEA – ASSESSORIA DE SEGURANÇA DE SISTEMAS DA INFORMAÇÃO DO CONTROLE DO ESPAÇO AÉREO

Estabelecer as diretrizes de controle de acesso lógico para as redes de telecomunicações e fiscalizar o cumprimento dessas diretrizes.

4.2 SSSI – SECÃO DE SEGURANCA DE SISTEMAS DA INFORMACÃO.

Implementar as diretrizes estabelecidas e comunicar à ASSICEA os incidentes de segurança da informação quando da ocorrência mediante ao não cumprimento das diretrizes de controle de acesso lógico.

5 DIRETRIZES PARA IMPLANTAÇÃO DAS REDES DE TELECOMUNICAÇÕES

5.1 GESTÃO DE ATIVOS

5.1.1 O DECEA e suas Organizações Militares subordinadas devem identificar e classificar os respectivos requisitos de segurança da informação dos ativos de informação.

5.1.2 Os requisitos de segurança da informação dos ativos de informação devem ser definidos por meio de critérios que atendam à disponibilidade, à integridade, à confidencialidade e à autenticidade da informação.

5.1.3 O inventário dos ativos de informação que compõem as redes de telecomunicações deve incluir todas as informações necessárias que permitam a recuperação de um ativo de informação após um incidente de segurança da informação grave ou um desastre, incluindo: identificar o valor de cada ativo de informação, tipo de ativo, formato, determinar com clareza e objetividade o conteúdo do ativo de informação, localização, informações sobre cópias de segurança da informação, informações sobre licenças, a classificação da informação deste ativo e a importância do ativo de informação para o negócio do DECEA.

5.1.4 Na elaboração e administração do inventário de ativos de informação deve-se identificar o(s) responsável(is) – proprietário(s) e custodiante(s) – de cada ativo de informação.

5.1.5 O inventário de ativos de informação deve ser completo, cobrindo todos os ativos de telecomunicações de valor, incluindo informações de recursos de rede, serviços e rede de aplicações.

5.1.6 Os requisitos de segurança da informação dos ativos de informação devem ser categorizados, no mínimo, em cinco categorias de controle de segurança da informação: a) tratamento da informação; b) controles de acesso físico e lógico; c) gestão de risco de segurança da informação; d) tratamento e resposta a incidentes de segurança da informação; e f) gestão de continuidade dos negócios nos aspectos relacionados à segurança da informação.

5.2 SEGURANÇA EM RECURSOS HUMANOS

5.2.1 Todo servidor militar ou civil, prestador de serviço ou fornecedor do DECEA e de suas organizações militares subordinadas, deve assinar o Termo de Responsabilidade para ser liberado o acesso aos recursos da rede de telecomunicações. Este Termo deve ser elaborado pela própria Organização Militar e armazenado de modo seguro.

5.2.2 Os direitos de acesso de todo servidor militar ou civil, prestador de serviço ou fornecedor do DECEA às informações e aos recursos de processamento da informação devem ser retirados após o encerramento de suas atividades, contratos ou acordos, ou devem ser ajustados após a mudança destas atividades.

5.3 GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES

5.3.1 As Organizações Militares subordinadas ao DECEA devem elaborar um procedimento de segurança da informação para as atividades de sistemas associados a recursos de processamento e comunicação das informações, tais como procedimentos de inicialização e desligamento de computadores, geração de cópias de segurança da informação, manutenção de equipamentos, tratamento de mídias, segurança e gestão do tratamento das correspondências e das salas de computadores.

5.3.2 Deve-se adotar a Norma de Segurança da Informação de Gestão de Mudanças para avaliação do impacto das alterações no ambiente e para controlar os recursos de processamento da informação e sistemas.

5.3.3 Deve ser estabelecido um procedimento de segurança da informação referente à administração e execução de funções ou áreas de responsabilidade críticas para o negócio do DECEA e suas organizações militares subordinadas mantendo a segregação de funções.

5.3.4 Os recursos de desenvolvimento, teste e produção devem ser separados para reduzir o risco de acessos ou modificações não autorizadas aos sistemas operacionais.

5.3.5 Devem ser implantados nas redes de telecomunicações controles de segurança da informação para prevenir, detectar e remover código malicioso e controlar códigos móveis.

5.3.6 Um sistema centralizado para gerência de *software* de antivírus das redes de telecomunicações deve ser implantado.

5.3.7 Deve-se adotar a Norma de Segurança da Informação de Cópias de Segurança para todos os sistemas críticos das redes de telecomunicações.

5.3.8 Os ativos de informação presentes nas redes de telecomunicações devem ser monitorados e os eventos de segurança da informação devem ser registrados conforme orientação da ASSICEA.

5.3.9 O monitoramento das redes de telecomunicações deve ser utilizado para checar a eficácia dos controles de segurança da informação adotados e para verificar a conformidade com esta Norma de segurança da informação de controle de acesso lógico das redes de telecomunicações. Além disso, um sistema de controle, monitoração e restrição de acesso ao conteúdo da internet deve ser implementado nas redes de telecomunicações.

5.3.10 As conexões da rede com outras redes externas, principalmente a Internet, devem ser protegidas por controles de segurança da informação especificados pela ASSICEA.

5.3.11 Um sistema de prevenção de intrusos (IPS) e um sistema de detecção de intrusos (IDS) deve ser implementado nas redes de telecomunicações.

5.3.12 Uma solução de correlação de eventos de segurança da informação e um servidor de logs dedicado (Log Server) devem ser implementados nas redes de telecomunicações.

5.4 GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

5.4.1 Deve ser elaborado um procedimento de segurança da informação para notificação e resposta dos diferentes tipos de incidentes de segurança da informação e fragilidades que possam ter impacto na segurança dos ativos de informação do DECEA e de suas Organizações Militares subordinadas.

5.4.2 Todos os servidores militares ou civis, prestadores de serviço ou fornecedores que desempenham atividades no âmbito do DECEA e das suas Organizações Militares subordinadas devem ser alertados sobre sua responsabilidade de notificar, o mais rapidamente possível, qualquer incidente de segurança da informação.

5.4.3 Deve ser criada uma equipe de resposta a incidente para avaliar, responder, tratar e aprender com incidentes de segurança da informação. Essa equipe deve ser autorizada a tomar decisões imediatas sobre como lidar com os incidentes de segurança da informação.

5.4.4 Todas as responsabilidades e procedimentos devem estar definidos para o manuseio efetivo de incidentes de segurança da informação e fragilidades, uma vez que estes tenham sido notificados.

5.4.5 Um processo de melhoria contínua deve ser aplicado a respostas, monitoramento, avaliação e gestão total de incidentes de segurança da informação.

5.5 GESTÃO DE CONTINUIDADE DO NEGÓCIO

5.5.1 Deve-se adotar o processo de gestão de continuidade do negócio para minimizar o impacto sobre o DECEA e de suas Organizações Militares subordinadas em recuperar perdas de ativos de informação a um nível aceitável, por meio da combinação de ações de prevenção e recuperação.

5.5.2 Os planos de continuidade de negócio devem tratar as vulnerabilidades das Organizações Militares subordinadas ao DECEA, que podem conter informações sensíveis e que necessitar de proteção adequada.

5.5.3 As Organizações Militares subordinadas ao DECEA devem considerar durante o desenvolvimento e implementação do plano de continuidade de negócio a inclusão de um plano de reabilitação de emergência dos serviços de telecomunicações que garantam as comunicações dos serviços de telecomunicações essenciais para as atividades operacionais do DECEA.

5.5.4 Os Planos de continuidade de negócio devem ser testados, reavaliados e melhorados, de forma a manter todas as informações atualizadas.

5.6 CONFORMIDADE

Na ocorrência de desastres naturais, acidentes e outras emergências ou riscos, as Organizações Militares subordinadas ao DECEA devem dar prioridade às comunicações essenciais para manter as atividades críticas do DECEA em operação.

5.7 DOCUMENTAÇÃO

Toda a infraestrutura das redes de telecomunicações deve ser documentada e mantida atualizada.

5.8 MEDIDAS DE SEGURANCA DA INFORMAÇÃO DE REDES DE TELECOMUNICAÇÕES CONTRA ATAQUES CIBERNÉTICOS

5.8.1 PROTEÇÃO DOS RECURSOS DE REDE

5.8.1.1 Os recursos de telecomunicações devem estar protegidos apropriadamente. Assim, pode-se evitar interferências significantes à entrega dos serviços das redes de telecomunicações, causados por comportamento inesperado. Este pode ser provocado, intencionalmente ou não, por programas maliciosos distribuídos por usuários de serviços das redes de telecomunicações gerenciadas pelo DECEA.

5.8.1.2 Para proteger recursos de rede IP (como servidores e roteadores) de ataques cibernéticos (por exemplo, ataques de negação de serviços), as Organizações Militares subordinadas ao DECEA devem ter mecanismos para filtrar as comunicações ou limitar a banda de comunicação IP, portas de comunicação e protocolos de aplicação. Dependendo do serviço de telecomunicações, tais mecanismos de filtragem de comunicações devem ser implementados em associação ao controle de processamento de sinais, autenticação de usuários e controle de acesso.

5.8.2 MEDIDAS CONTRA PERSONIFICAÇÃO DE ORIGEM

5.8.2.1 As Organizações Militares subordinadas ao DECEA devem implementar controles de segurança da informação para proteção contra personificação de endereços IP (IP Spoofing).

5.8.2.2 Para prevenir personificação de uma origem por meios privilegiados, convém que controles de segurança da informação apropriados contra acesso não autorizado sejam implementados nos sistemas de informação provendo autenticação de usuários e introduzindo controles de senha e/ou funções de autenticação forte, por exemplo: uso obrigatório de senhas

imprevisíveis sob certo tamanho e a introdução de senha única e autenticação forte por dispositivos de senha única.

5.9 MEDIDAS DE SEGURANCA PARA CONGESTIONAMENTO DE REDE

5.9.1 MECANISMO DE DETECÇÃO E LIMITAÇÃO DE CONGESTIONAMENTO DE REDE

5.9.1.1 Os equipamentos críticos de telecomunicações devem possuir mecanismos para detectar congestionamento de rede e evitar a concentração das comunicações no caso de um congestionamento de rede.

5.9.1.2 Deve-se prever a gestão de capacidade dos equipamentos das redes de telecomunicações ajustando os limites de desempenho dos equipamentos de comunicação e implementando mecanismos para controlar o número de comunicações antes de atingir este limite. Além disso, todo o tráfego da rede deve ser processado por equipamentos distribuídos, quando possível.

5.9.2 COLETA PRÉVIA DE INFORMAÇÕES QUE PODEM CAUSAR CONGESTIONAMENTO:

As Organizações Militares subordinadas ao DECEA devem elaborar um procedimento de segurança da informação para reportar a coleta prévia de informações e manter as pessoas necessárias informadas.

5.9.3 MEDIDAS PARA MELHORA TEMPORÁRIA DA CAPACIDADE

Deve-se considerar a escala de uma potencial paralisação ou desastre para a utilização de um centro de processamento distribuído de rede, com a instalação de equipamentos complementares e as mudanças necessárias na configuração dos ativos de informação para se adaptar, caso ocorra um incidente grave ou até mesmo um desastre interrompendo as operações críticas das Organizações Militares subordinadas ao DECEA. Esta ação poderá ser incorporada em uma estratégia de Gestão de Continuidade das Operações, a fim de manter a operacionalidade dos sistemas críticos em face de eventuais óbices na operação desses sistemas.

5.9.4 COLETA PRÉVIA DE INFORMAÇÕES QUE ALERTEM O MAU FUNCIONAMENTO

Uma vez que desastres, acidentes e fenômenos sociais tendem a ser as causas de falhas em equipamentos de telecomunicações e congestionamento de redes, as Organizações Militares subordinadas ao DECEA devem considerar a adoção de medidas de antecipação, previstas em Planos de continuidade de negócios, recolhendo informações relevantes e acumulando o conhecimento de forma regular.

6 DESCRIÇÃO DA NORMA DE SEGURANÇA DA INFORMAÇÃO

6.1 CONTROLE DE ACESSO LÓGICO

6.1.1 Um procedimento de segurança da informação de concessão e revogação de direitos de acesso a sistemas e serviços deve ser definido e implantado pelas Organizações Militares subordinadas ao DECEA.

6.1.2 Os usuários devem estar cientes de suas responsabilidades em relação à guarda das senhas de acesso, pois o compartilhamento de senhas compromete a rastreabilidade das ações realizadas nos sistemas e expõe o usuário autorizado às responsabilidades por atos prejudiciais executados por outra pessoa. Deve ser solicitado aos usuários um termo de sigilo das senhas.

6.1.3 A autorização de cada privilégio concedido deve ser registrada de forma a gerar evidências de sua execução por parte dos responsáveis, mantendo a rastreabilidade para o caso de incidentes de segurança ou de auditorias e para que os privilégios possam ser reavaliados posteriormente.

6.1.4 As modificações nos privilégios de acesso dos usuários de sistemas do DECEA e das Organizações Militares subordinadas devem ser registradas de forma a gerar evidências do controle sobre a concessão adequada desses privilégios, mantendo a rastreabilidade para o caso de incidentes de segurança da informação ou de auditorias.

6.1.5 Os registros de modificações de privilégios de acesso devem ser verificados periodicamente de modo a garantir que os privilégios não foram concedidos de maneira equivocada ou não autorizada, além de manter o controle de expiração dos privilégios concedidos.

6.1.6 Um procedimento de segurança da informação para formação e uso de senhas de acesso, deve ser elaborado pelo DECEA e suas Organizações Militares subordinadas. Este procedimento deve ser revisado e aprovado pela ASSICEA.

6.1.7 Um procedimento de segurança da informação para os serviços de rede de telecomunicações deve ser elaborado pelo DECEA e suas Organizações Militares subordinadas. Este procedimento deve prevenir acesso não autorizado aos serviços de rede e especificar que os usuários somente recebam acesso para os serviços que tenham sido especificamente autorizados a usar.

6.1.8 Os acessos de usuários remotos às redes de telecomunicações devem ser autenticados por uma solução de VPN – Virtual Private Network implementada pelas Seções de Segurança de Sistemas de Informação presentes nas Organizações Militares subordinadas ao DECEA. A solução empregada deve estar em conformidade com a ICA 200-8 "Medidas de Segurança para Equipamentos Cripotécnicos e de Comunicações".

6.1.9 Devem ser implantados mecanismos de identificação automática de equipamentos para autenticar conexões (Identificação de equipamento em redes).

6.1.10 As portas de diagnóstico e configuração devem ser protegidas contra acessos não autorizados (Proteção e configuração de portas de diagnóstico remotas).

6.1.11 As redes de telecomunicações devem ser segregadas em domínios lógicos e os seus serviços devem ser segregados em redes virtuais (Segregação de redes).

6.1.12 As restrições de conexões dos usuários às redes de telecomunicações devem ser implementadas (Controle de conexão de rede).

6.1.13 Um procedimento de segurança da informação de mecanismos seguros de *logon* deve ser implementado no acesso às redes de computadores (Procedimentos seguros de entrada no sistema – *logon*).

6.1.14 Os usuários devem ter um identificador único na rede de computadores (Identificação e autenticação de usuário).

6.1.15 Devem ser implementadas, nas redes de telecomunicações, técnicas de autenticação que permitam validar a identidade de um usuário (Identificação e autenticação de usuário).

6.1.16 Um sistema de gerenciamento e manutenção de senhas deve ser implementado nas redes de telecomunicações.

6.1.17 Os mecanismos de restrição para o uso de programas utilitários de sistemas devem ser implementados nas redes de telecomunicações (Uso de utilitários de sistema).

6.1.18 Mecanismos de desconexão e desligamento automáticos de estações de trabalho em locais de alto risco devem ser implementados nas redes de telecomunicações (Desconexão de terminal por inatividade).

6.1.19 O DECEA e suas Organizações Militares subordinadas devem implementar restrições de horário para conexão às redes de telecomunicações (Limitação de horário de conexão).

6.1.20 Um procedimento de segurança da informação de acesso às informações e funções dos sistemas de aplicação deve ser implementado nas redes de telecomunicações (Restrição de acesso à informação).

6.1.21 O DECEA e suas Organizações Militares subordinadas devem abrigar isoladamente os sistemas de aplicações sensíveis e relevantes para atingir a missão da organização militar (Isolamento de sistemas sensíveis).

6.2 ELABORAÇÃO E ADMINISTRAÇÃO DE CONTAS DE ACESSO

6.2.1 A criação de contas de acesso aos ativos de informação requer procedimentos prévios de credenciamento para qualquer usuário.

6.2.2 Disponibilizar ao usuário, que não exerce funções de administração da rede local, somente uma única conta institucional de acesso, pessoal e intransferível.

6.2.3 Utilizar conta de acesso, no perfil de administrador, somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação.

6.2.4 O DECEA e suas Organizações Militares subordinadas devem responsabilizar o usuário pela quebra de segurança da informação ocorrida com a utilização de sua respectiva conta de acesso, mediante assinatura de um Termo de Responsabilidade.

6.2.5 A criação de contas de serviço exige regras específicas vinculadas a um processo automatizado.

6.2.6 As Seções de Segurança de Sistemas de Informação devem estabelecer regras para credenciamento, bloqueio e exclusão de contas de acesso de seus usuários, bem como para o ambiente de desenvolvimento.

6.3 ATIVOS DE INFORMAÇÃO

6.3.1 O DECEA e suas Organizações Militares subordinadas devem utilizar ferramentas de proteção contra acesso não autorizado aos ativos de informação que favoreçam, preferencialmente, a administração de forma centralizada.

6.3.2 O DECEA e suas Organizações Militares subordinadas devem respeitar o princípio do menor privilégio, para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação conforme o RCA 205-1 "Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica".

6.3.3 Utilizar ativo de informação homologado pela ASSICEA nas aplicações de controle de acesso e de tratamento das informações sigilosas.

6.3.4 Registrar eventos relevantes, previamente definidos, para a segurança da informação e rastreamento de acesso às informações sigilosas.

6.3.5 Criar mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

6.3.6 O uso dos ativos de informação que não guarde relação com o exercício do cargo, função, emprego ou atividade será considerado indevido e passível de imediato bloqueio de acesso, sem prejuízo da apuração das responsabilidades administrativa, penal e civil.

6.3.7 As Seções de Segurança de Sistemas de Informação presentes nas Organizações militares subordinadas ao DECEA devem estabelecer regras para o uso da internet, do correio eletrônico e de mensagens instantâneas.

6.4 REDES DE TELECOMUNICAÇÕES

6.4.1 O DECEA e suas Organizações Militares subordinadas devem conceder credenciais de acesso à rede de telecomunicações após a data de contratação ou de entrada em exercício do usuário.

6.4.2 Excluir credenciais de acesso à rede de telecomunicações quando houver desligamento do usuário.

6.4.3 Registrar os acessos à rede de telecomunicações de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo a ser definido pela Assessoria de Segurança de Sistemas de Informação do Controle do Espaço Aéreo.

6.4.4 Utilizar mecanismos automáticos para inibir que equipamentos externos se conectem à rede de telecomunicações.

6.4.5 Manter, na rede de telecomunicações, mecanismos que permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados.

6.4.6 Utilizar a legislação específica presente no RCA 205-1 "Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica" para a concessão de acesso às informações sigilosas, no âmbito da rede de telecomunicações, por meio de canal seguro.

6.4.7 Gravar o acesso remoto à rede de telecomunicações em *logs* para posterior auditoria, contendo informações específicas que facilitem o rastreamento da ação tomada.

7 REGISTROS GERADOS

Não aplicável.

8 PONTOS DE VERIFICAÇÃO

A correta aplicação desta Norma de Segurança da Informação pode ser verificada constatando a implantação dos requisitos de segurança da informação nas redes de telecomunicações.

9 FLUXOGRAMA

Não aplicável.

10 DOCUMENTOS DE REFERÊNCIA

10.1 DCA 7-2 Política de Segurança da Informação do DECEA, 2010.

10.2 PCA 7-11 Plano Diretor de Segurança da Informação do DECEA, 2010.

10.3 DCA 102-1 Requisitos Básicos das Redes de Comunicações do COMAER, 2008.

10.4 DCA 21-2 Diretriz para Implantação do Centro de Gerenciamento Técnico do SISCEAB, 2009.

10.5 RCA 205-1 Regulamento para Salvaguarda de Assuntos Sigilosos da Aeronáutica, 2006.

10.6 ROCA 20-7 Regulamento do Departamento de Controle do Espaço Aéreo, 2010.

10.7 ABNT NBR ISO/IEC 27002 Código de Práticas para a Gestão da Segurança da Informação, 2005.

11 ANEXOS

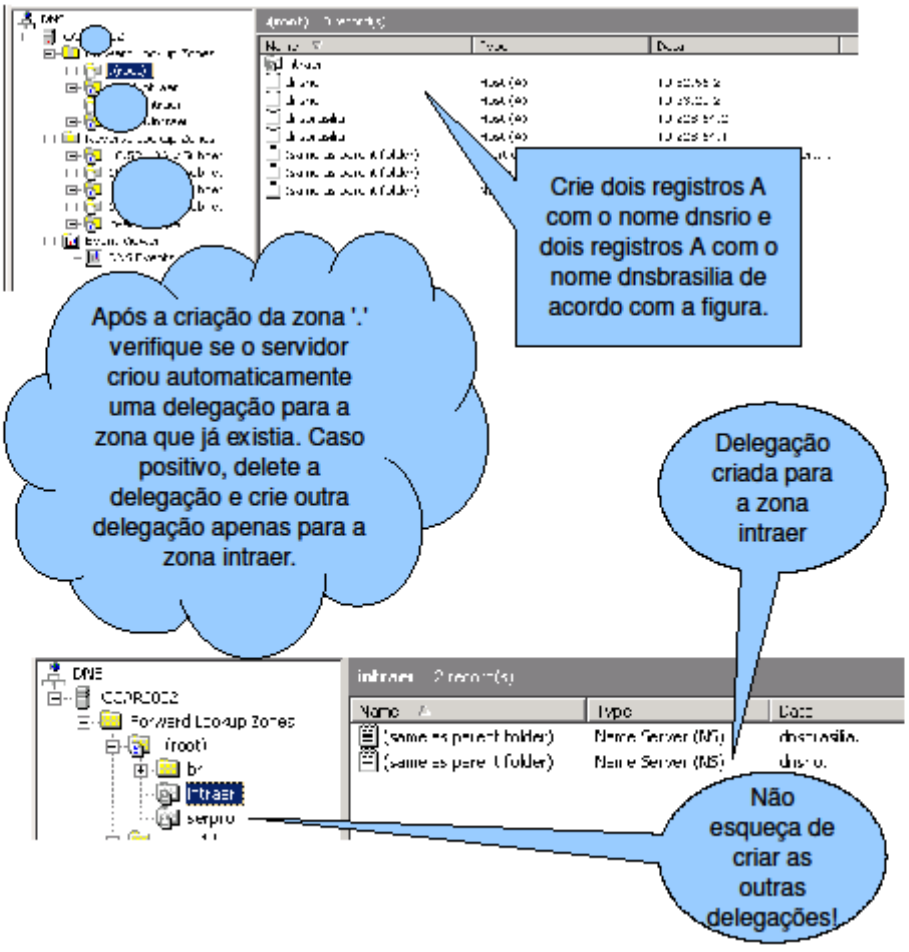
Não aplicável

Anexo B – Tutorial de configuração de DNS do CCA-BR

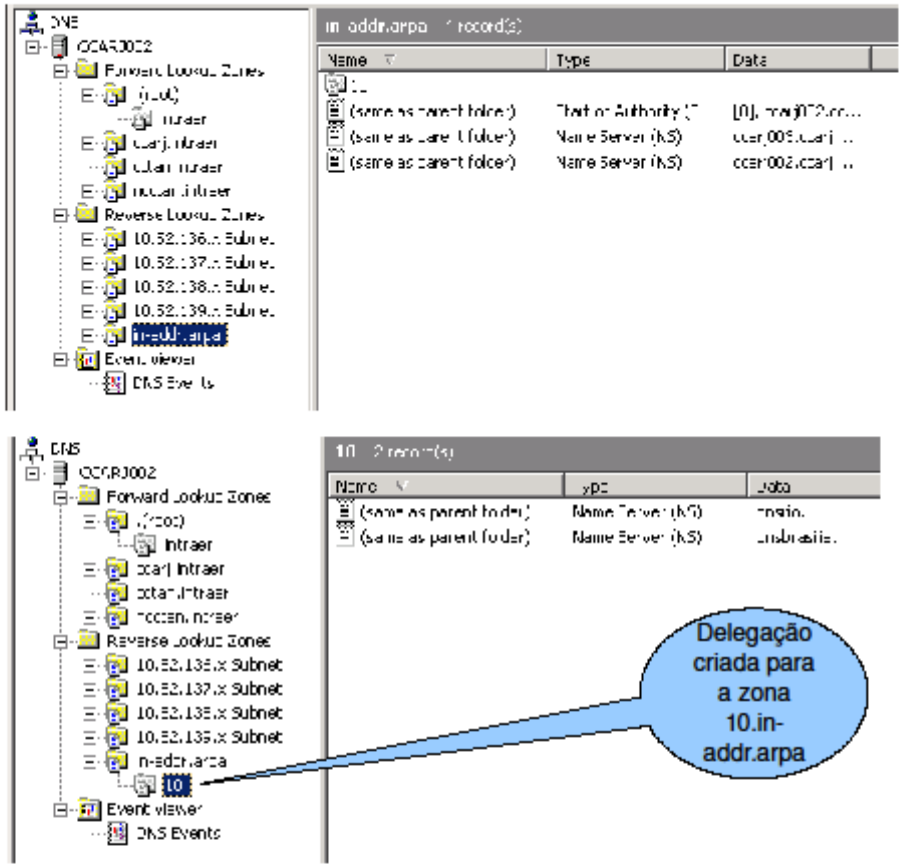
COMANDO DA AERONÁUTICA
DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO
CENTRO DE COMPUTAÇÃO DA AERONÁUTICA DO RIO DE JANEIRO

Finalidade: Informar a correta configuração do servidor DNS Windows nas unidades do COMAER.

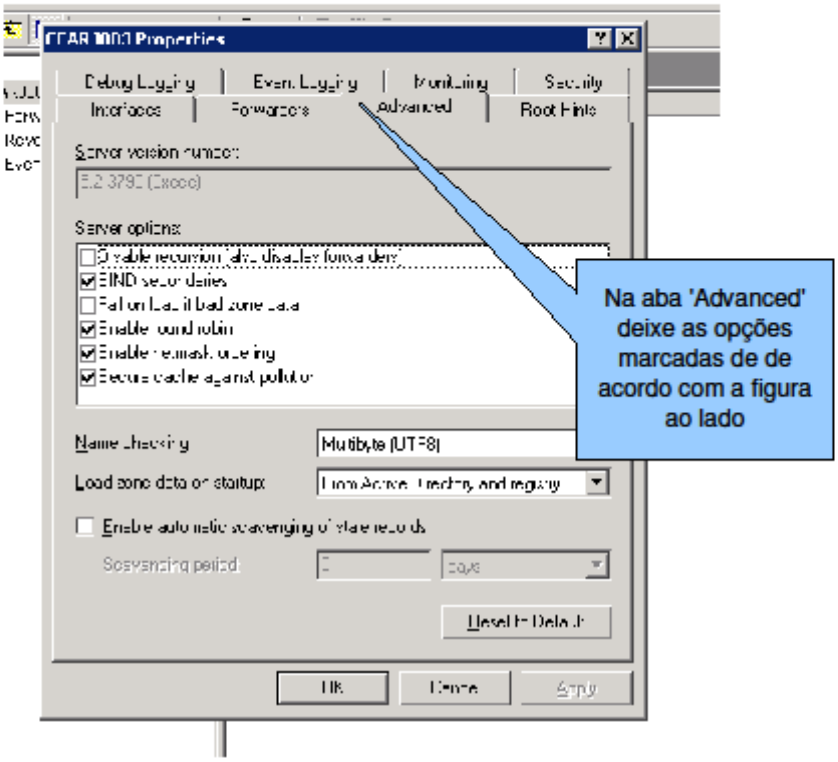
Estando na tela inicial do Windows vá em **Iniciar->Ferramentas Administrativas->DNS.**
Crie uma zona primária '.' de acordo com a figura.
Crie quatro registros A para os dns corporativos da **intraer.**
Crie uma delegação para a zona **intraer** contendo os quatro DNS corporativos da INTRAER.
NOVO: Crie também delegações para a zona **gov.br, serpro e bace.org.uk**
Um passo a passo detalhado com um exemplo de configuração no Windows 2000 pode ser obtido no endereço ftp://ftp.ccarj.intraer/dns/dnswindows2000.pdf



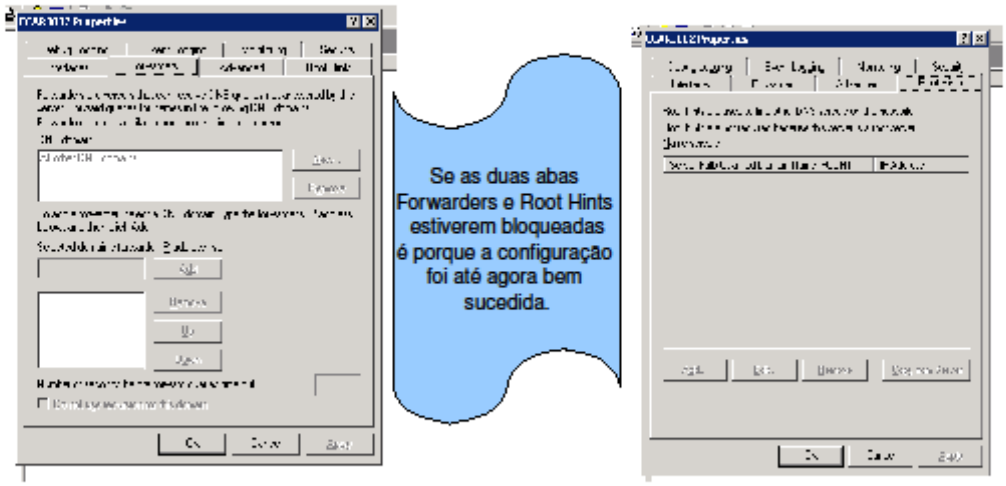
Faça a mesma coisa para zona reversa **in-addr.arpa**, lembrando que não é necessário criar os registros A apenas a delegação para a zona 10.in-addr.arpa

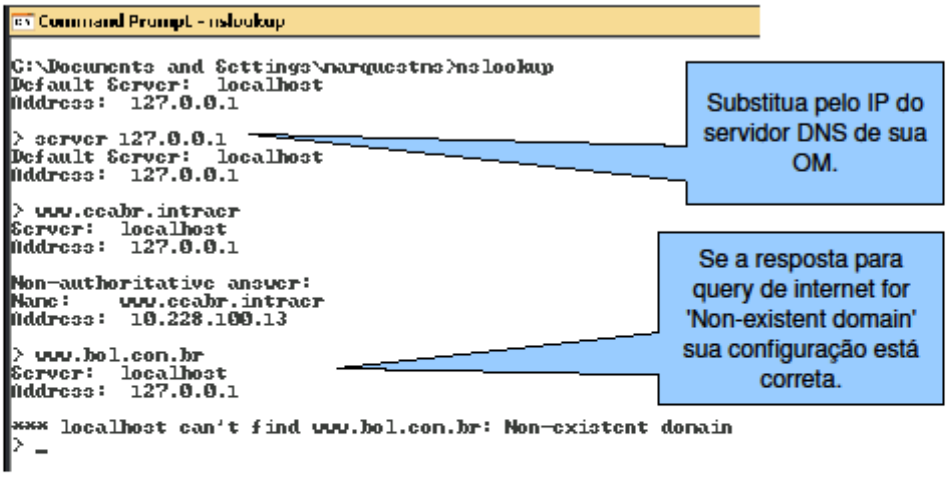


Click com o botão direito do mouse em cima do ícone que representa o servidor e vá em propriedades e configure a aba Advanced de acordo com a figura.



Verificando a configuração:





Todas as máquinas clientes
da organização devem estar configuradas
para utilizarem o DNS interno da OM.
Em caso de dúvida mande
um email para sgr@ccarj.intraer
ou entre em contato com
o SAUTI pelo site www.sauti.intraer
ou pelo telefone 0800-722-0108

Anexo C - Analise de Requisitos

COMANDO DA AERONÁUTICA

DESTACAMENTO DE CONTROLE DO ESPAÇO AÉREO DE CHAPADA DOS GUIMARÃES

SEGURANÇA E USO DE MEIOS COMPUTACIONAIS

2° SGT BET JAIRO MAGESTE PIMENTEL NETO

CHAPADA DOS GUIMARÃES - MT 2014

COMANDO DA AERONÁUTICA

DESTACAMENTO DE CONTROLE DO ESPAÇO AÉREO DE CHAPADA DOS GUIMARÃES

SUBSEÇÃO DE MEIOS COMPUTACIONAIS

SEGURANÇA E USO DE MEIOS COMPUTACIONAIS

2° SGT BET JAIRO MAGESTE PIMENTEL NETO

Levantamento de requisitos realizado pela subseção de Meios Computacionais do DTCEA-GI, visando a implantação do novo servidor Dell PowerEdge 2950 e Sistema Operacional Windows 2003 Server

CHAPADA DOS GUIMARÃES - MT 2014

SUMÁRIO

Introdução....4
1. - Levantamento de Requisitos....4
1.1 - Visão Geral....4
1.2 - Objetivo....4
1.3 - Requisitos funcionais....5
1.4 - Requisitos não funcionais....7
1.5 - Histórico....7

4

Introdução

Este documento especifica os requisitos de Políticas de Segurança e de Uso Ativos de Tecnologia da Informação do Destacamento de Controle do Espaço Aéreo de Chapada dos Guimarães (DTCEA-GI), fornecendo ao gerente de rede, informações necessárias para configurações de serviços aos usuários dos Meios Computacionais desta.

1. - Levantamento de Requisitos

A elaboração do levantamento de requisitos foi realizada por meio de entrevistas e reuniões não estruturadas com Chefe do DTCEA-GI, observação do comportamento do usuário e Brainstorming com os sargentos especialistas em eletrônica, feito ainda levantamento nos regulamentos da Comando da Aeronáutica.

Com base nesses levantamentos se obteve as informações necessárias para determinar as características de segurança e uso da rede de computadores, visando melhorar o uso dos computadores e garantir a segurança da rede.

1.1 - Visão Geral

Os Meios Computacionais do DTCEA-GI, é a base para o funcionamento administrativo e técnico desta Organização Militar, provento meios para os usuários acessarem os diversos Sistemas Web de uso da Força Aérea Brasileira, e-mails (ExpressoMail), gerenciador de documentos (Sigadaer), sistemas de gerenciamento técnico de material e pessoal (Siloms), controle de pessoal (Sigpes), entre outros.

1.2 - Objetivo

O objetivo deste documento é definir diretrizes para a elaboração de políticas de configuração do Active Directory (AD) e do servidor de Dados do DTCEA-GI.

5

1.3 - Requisitos funcionais

[RF_001] - **Cadastrar Usuário**: O administrador do Domínio, deve cadastrar o usuário, fornecendo a ele uma senha inicial a ser alterada no próximo login, deve preencher todos os dados do novo usuário. Conforme determina a ICA 7-19/2012, anexo E item 6.1 (Controle de Acesso Logico) e 6.2 (Elaboração e Administração de Contas de Acesso);

[RF_002] - **Senha Forte**: Este caso de uso define que a senha deve ter requisitos mínimos de complexidade e tamanho a ser definida pelo usuário. Conforme determina a ICA 7-19/2012, anexo E item 5.8.2.2 (Para prevenir personificação de uma origem por meios privilegiados, convém que controles de segurança da informação apropriados contra acesso não autorizado sejam implementados nos sistemas de informação provendo autenticação de usuários e introduzindo controles de senha e/ou funções de autenticação forte, por exemplo: uso obrigatório de senhas ICA 7-19/2012 37/58 imprevisíveis sob certo tamanho e a introdução de senha única e autenticação forte por dispositivos de senha única);

[RF_003] - **Bloqueio da estação**: Este caso de uso define que a estação de trabalho do usuário deve ser bloqueada automaticamente ou realizado o Logoff automático em caso de ociosidade, evitando a utilização desta estação por terceiros caso o usuário deixe a estação ativa. Conforme determina a ICA 7-19/2012, anexo E item 6.1.18 (Mecanismos de desconexão e desligamento automáticos de estações de trabalho em locais de alto risco devem ser implementados nas redes de telecomunicações (Desconexão de terminal por inatividade)) e recomenda o PCA 7-18/2012, item 4.2.7.2 (...Esse controle determina que se a máquina ficar mais de 5 minutos sem interação com o usuário, deve-se bloquear automaticamente a estação de trabalho...);

[RF_004] - **Renovar senha**: Este caso de uso define o Usuário deve alterar periodicamente sua senha de acesso, cabendo ao autenticador, não permitir uso de senhas anteriormente utilizadas por este usuário;

[RF_005] - **Bloqueio de senha**: Realizar o bloqueio automático da senha (conta do usuário) em caso de múltiplas tentativas de acesso com senha incorreta;

6

[RF_006] - **Horário de Utilização**: Define horário, para que determinado usuário, possa utilizar os meios computacionais, não permitindo a utilização fora do expediente por exemplo. Conforme determina a ICA 7-19/2012, anexo E item 6.1.19 (O DECEA e suas Organizações Militares subordinadas devem implementar restrições de horário para conexão às redes de telecomunicações (Limitação de horário de conexão));

[RF_007] - **Computadores Permitidos**: Impede que usuários utilizem computadores que não estão alocados em seus locais de trabalho;

[RF_008] - **Limitar acesso remoto**: Os computadores só devem permitir acesso remoto de estações de trabalho da subseção de Meios Computacionais, com usuários administradores do Domínio. Conforme determina a ICA 7-19/2012, anexo E item 6.1.10 (As portas de diagnóstico e configuração devem ser protegidas contra acessos não autorizados (Proteção e configuração de portas de diagnóstico remotas));

[RF_009] - **Restrição de Mídias**: Visando reduzir a proliferação de malweres e proteger os dados deste destacamento, implementa controle sobre unidades de disco e de armazenamento removível, impedindo que o sistema leia e grave CDs/DVDs e monte unidades de Armazenamento a partir das portas USB;

[RF_010] – **Configuração e Restrição de Uso da Internet**: Configurar automaticamente o proxy apenas para usuários com permissão de uso da internet, impedindo que esta configuração seja alterada por todos os usuários. Conforme determina a ICA 7-19/2012, anexo E item 5.3.9 (...Além disso, um sistema de controle, monitoração e restrição de acesso ao conteúdo da internet deve ser implementado nas redes de telecomunicações);

[RF_011] - **Restrição de Configurações**: Impede que o usuário tenha acesso a configurações do sistema, ou configurações de interesse da administração dos Meios Computacionais, ou caso tenha acesso, não possa alterá-los. Conforme determina a ICA 7-19/2012, anexo E item 6.1.17 (Os mecanismos de restrição para o uso de programas utilitários de sistemas devem ser implementados nas redes de telecomunicações (Uso de utilitários de sistema));

7

[RF_012] – **Integridade e Confidencialidade de Dados**: Garantir que os dados não sejam perdidos ou alterados por usuários que não tenha permissão; e que somente acessem os dados, usuários que tenho direito a acessa-los. Conforme determina a ICA 7-19/2012, anexo E item 6.1.20 (Um procedimento de segurança da informação de acesso às informações e funções dos sistemas de aplicação deve ser implementado nas redes de telecomunicações (Restrição de acesso à informação)).

1.4 - Requisitos não funcionais

[RNF_001] – **Papel de Parede**: Permite que a administração dos Meios Computacionais gerencie o papel de parede de todas as estações de trabalho de forma centralizada.

[RNF_002] – **Validade de Cadastro**: Os cadastros de usuários, devem ter validade máxima igual a data engajamento do militar, sendo atualizada após a apresentação da nova data de engajamento. Conforme determina a ICA 7-19/2012, anexo E item 5.2.2 (Os direitos de acesso de todo servidor militar ou civil, prestador de serviço ou fornecedor do DECEA às informações e aos recursos de processamento da informação devem ser retirados após o encerramento de suas atividades, contratos ou acordos, ou devem ser ajustados após a mudança destas atividades).

1.5 - Histórico

Versão	Data	Descrição	Autor	Assinatura
0.01	10/07/2014	Delineamento inicial dos documentos de requisito	2S Mageste	

Anexo D – Conteudo do arquivo de configuração USB.adm

```
CLASS MACHINE
 CATEGORY  !!CATUSBManagement
  POLICY !!POLUSBManagement
   EXPLAIN !!POLUSBManagement_Help
   KEYNAME "System\CurrentControlSet\Services\usbstor"
   PART !!Part00 DROPDOWNLIST
   VALUENAME "Start"
    ITEMLIST
     NAME !!Name00 VALUE NUMERIC 0
     NAME !!Name01 VALUE NUMERIC 1
     NAME !!Name02 VALUE NUMERIC 2
     NAME !!Name03 VALUE NUMERIC 3
     NAME !!Name04 VALUE NUMERIC 4 DEFAULT
    END ITEMLIST
   END PART
  END POLICY
 END CATEGORY

[strings]
CATUSBManagement="USB Management"
POLUSBManagement="USB Storage Service"
POLUSBManagement_Help="Enables the changing of the
startup type for the USB Storage Service.\nDisabled
should be selected from startup type.\n\nYou should also
set permissons on following
files:\n\n%SystemRoot%\Inf\Usbstor.pnf\n%SystemRoot%\Inf
\Usbstor.pnf"
Part00="Startup type"
Name00="Boot"
Name01="System"
Name02="Auto Load"
Name03="Load On Demand"
Name04="Disabled"
```

Anexo E - Termo de Compromisso para Cadastro na Rede

CADASTRO NA REDE INTERNA DO DTCEA-GI

NOME COMPLETO: *Jairo Mageste Pimentel Neto* POSTO/GRAD.:*2S*

NOME DE GUERRA: *Mageste* SARAM: *414708-1*

Diretivas de utilização da rede interna

1. Todos os recursos computacionais (login, e-mail, internet, impressão, dados, etc), quando cedidos, destinam-se ao uso em serviço, sendo seus conteúdos propriedades deste centro.

2. Somente a Seção de Informática está autorizada a realizar a instalação de sistemas operacionais, programas, aplicativos ou quaisquer equipamentos periféricos e/ou acessórios nos computadores da rede administrativa.

3. O uso de aplicativos não instalados no computador (Portable) é proibido.

4. Somente a Seção de Informática está autorizada a realizar testes de rede (de qualquer natureza).

5. O usuário **não** deve retirar do sistema que utiliza a permissão de acesso aos usuários ***system*** e ***administradores*** em pastas do sistema sob pena de inutilizar o sistema operacional.

6. As senhas fornecidas pela Seção de Informática são responsabilidade do usuário, que responderá disciplinar e/ou criminalmente pela má utilização, não devendo, portanto, serem repassadas a terceiros.

7. As realizações de cópias de segurança (backup) competem ao usuário, que poderá solicitar apoio à Seção de Informática.

8. É de responsabilidade do usuário solicitar as atualizações cadastrais que julgar relevantes para o bom andamento do serviço.

9. As cessões podem ser interrompidas quando o Setor de Informática considerar necessário ao serviço ou quando houver risco potencial.

10. As orientações fornecidas pelo Comandante também serão consideradas como diretrizes.

11. As diretivas de informática que forem veiculadas pela página web do CINDACTA1 (www.cindacta1.intraer) serão consideradas de conhecimento do público interno, sendo este responsável por seguir as normas estabelecidas pela Seção de Informática.

12. Toda solicitação de apoio e/ou material deverá ser destinada ao serviço de atendimento aos usuários da tecnologia da informação (SAUTI) que designará um responsável pelo atendimento, devendo o usuário anotar o número da solicitação. (SAUTI: http://www.sauti.intraer ou 0800-722-0108).

Concordo com as regras descritas acima para utilização dos recursos de tecnologia da informação.

_____
Assinatura do solicitante

Chapada dos Guimarães, ____de_____de_____

Aprovo: _____
Assinatura do chefe imediato

AÇÕES DA SUBSEÇÃO DE TECNOLOGIA DA INFORMAÇÃO
LOGIN DA REDE: _____
CRIAÇÃO DE : ( ) Cadastro na Rede Interna _____ **Executor**

SEÇÕES:

( )Comando	( )Cipa	( )Centro Social	( )Controle Interno	( )Aloj. De Apoio
( )GISA	( )GISA-1	( )GISA-2	( )GISA-3	( )GISA-4
( )GISA-5	( )GIST	( )GIST-1	( )GIST-2	( )GIST-3
( )GIST-4	( )GIST-5	( )GIST-6		